AI VOID FIELD GUIDE

Mastering Zero Trust Security: A Comprehensive Guide

Embark on a comprehensive journey to master Zero Trust Security, understanding its core principles and learning a structured approach to implement it effectively in modern organizations.

AI VOID

2026-05-28 15:47 IST

Contents

CHAPTER 01

01 Zero Trust Imperative

```
+++
title = "The Zero Trust Imperative: Why Traditional Security Isn't Enough
Anymore"
date = 2026-05-28
draft = false
type = "page"
contentType = "tutorial"
categories = ["Cybersecurity", "Networking", "Cloud Security"]
tags = ["Zero Trust", "Security Architecture", "Identity and Access
Management", "Network Security", "Cloud Computing", "DevOps Security"]
difficulty = "beginner"
description = "Understand the fundamental shift from traditional perimeter
security to Zero Trust, why it's essential in modern cybersecurity, and its
core principles."
slug = "zero-trust-imperative"
platform = ["Cloud", "Enterprise"]
readingTime = 15
status = "new"
author = "AI Expert"
showReadingTime = true
showTableOfContents = true
toc = true
weight = 1
+++

Welcome to the cutting edge of cybersecurity! In this chapter, we're going to
embark on a journey to understand one of the most transformative concepts in
modern security: Zero Trust. If you've ever wondered why traditional firewalls
and network perimeters aren't enough to protect against today's sophisticated
threats, you're in the right place.

We'll explore what Zero Trust truly means, why it has become an "imperative"
rather than just a buzzword, and how it fundamentally shifts our approach to
security. We'll lay the groundwork for understanding the principles that will
guide every subsequent step of our learning.

## The Cracks in the Castle Wall: Why Traditional Security Fails

For decades, cybersecurity operated on a simple, intuitive model: the "castle-
and-moat" defense. Imagine your organization as a castle. You build strong
walls (firewalls, intrusion detection systems) and deep moats (DMZs, network
segmentation) around your most valuable assets. Once an identity or device was
inside the network perimeter, it was generally considered trustworthy.

This model, while effective in simpler times, struggles profoundly in today's
complex digital landscape.

### The Modern Threat Landscape

The world has changed dramatically. Our "castle" no longer has clear walls.
-   **Cloud Adoption:** Resources are scattered across multiple cloud
providers and SaaS applications, outside any traditional network perimeter.
-   **Remote Work:** Users access corporate data from home networks, coffee
shops, and personal devices, blurring the lines of "inside" and "outside."
-   **Sophisticated Attacks:** Threat actors are more advanced. They don't
```

```
just try to breach the front gate; they look for weak points, exploit stolen
credentials, and move laterally *within* a seemingly secure network.
-   **Insider Threats:** Malicious or negligent insiders, who are already
"inside the castle," pose a significant risk that perimeter defenses can't
address.

**📌 Key Idea:** The traditional perimeter-based security model assumes trust
once inside the network, a dangerous assumption in the face of modern threats.

### The Consequences of Assumed Trust

When you assume trust, a single compromised credential or device can be
catastrophic. An attacker who gains access to one part of your internal
network can often move freely to other, more sensitive areas. This "lateral
movement" is how many major data breaches unfold, often remaining undetected
for months.

**⚠️ What can go wrong:** Assuming trust after initial authentication allows
attackers to move laterally through your systems unchecked once they've gained
a foothold, turning a small breach into a major incident.

## Embracing the Zero Trust Imperative

Enter Zero Trust. It's not a product you buy, but a strategic approach to
security that challenges the fundamental assumption of trust. Instead, it
operates on a simple, radical principle: **Never trust, always verify.**

### What is Zero Trust?

Zero Trust is a security model that requires strict identity verification for
every person and device trying to access resources on a private network,
regardless of whether they are inside or outside the network perimeter. It
means no implicit trust is granted to assets or user accounts based solely on
their physical or network location.

**🧠 Important:** Zero Trust is a philosophy and an architectural approach,
not a specific technology or vendor solution. It demands a holistic shift in
how an organization approaches security.

### Why Does Zero Trust Exist?

Zero Trust emerged because the traditional perimeter model failed to cope with
the evolving threat landscape and the dissolution of the traditional network
boundary. It addresses the critical need to protect resources in a world
where:
-   The network is everywhere.
-   Users are everywhere.
-   Threats can come from anywhere, including from "inside."

### What Problem Does Zero Trust Solve?

Zero Trust solves the problem of *implicit trust*. By removing this
assumption, it forces organizations to:
1.  **Verify everything:** Every access request, every user, every device is
rigorously authenticated and authorized.
2.  **Limit blast radius:** Even if a breach occurs, the attacker's ability to
move laterally and access other resources is severely restricted.
3.  **Enhance visibility:** Constant verification and monitoring provide a
much clearer picture of who is accessing what, from where, and with what
device.

## The Core Principles: A New Mental Model
```

```
The Zero Trust model is built upon three foundational principles. These are
the pillars that support the entire security strategy. Think of these as your
guiding stars.

1.  **Verify Explicitly:**
    -   **What it means:** Always authenticate and authorize based on all
available data points, including user identity, location, device health,
service, and data classification. No user or device is inherently trusted.
    -   **Why it matters:** Every request for access is treated as if it
originated from an untrusted network. This removes the dangerous assumption
that internal traffic is safe.
    -   **How it works:** This involves strong authentication (like Multi-
Factor Authentication - MFA), device compliance checks, and understanding the
context of the access request.

2.  **Use Least Privileged Access:**
    -   **What it means:** Grant users and devices only the minimum access
necessary to perform their specific task, for the shortest possible duration.
    -   **Why it matters:** Reduces the "blast radius" if an account or device
is compromised. An attacker gains access only to a very limited set of
resources, preventing wide-scale damage.
    -   **How it works:** Just-in-Time (JIT) access, Just-Enough Access (JEA),
and granular permissions are key components.

3.  **Assume Breach:**
    -   **What it means:** Design your security architecture with the
expectation that breaches *will* occur. Plan for containment, detection, and
response, rather than solely prevention.
    -   **Why it matters:** Even with the best defenses, no system is
impenetrable. This principle shifts focus to resilience and rapid recovery,
minimizing impact when an incident inevitably happens.
    -   **How it works:** Micro-segmentation, continuous monitoring, and
robust incident response plans are essential.

Let's visualize this shift in mindset:


<div class="diagram-wrap"><img src="
JREFUeJzsfXeYVEX29nvqdk8Pw8QekpIkKUEQEFAwoyA5LEEkSoY1sSK4CCYQUVBRQaKohAWERRFwC
BIMICA5gzhDkkx3TwKmp/
vW+f64t8eZe6tZxt3vt8j2+zzz7FrVdW91c6uvuqXPe8x4ggggiiCCCCCKIIIIIIogggggiiCCCCCKI
IIIIIoggggiiCCCCCKIIIIIIoggggiiCCCCCKIIIIIIogggggiiCCCCCKIIIL/Mfh8vsT/
9hwi+N+C+G9PoLD4Ty0Sn89X3uPxlFX1paenJ3m93J3m93jeZOfp6r5eent7U6/W2Luw8vF7vS16v950wc/
xD3zU9PT3pj4yzwuPxlE1PT6/0n7jWv4twv4XP53tQ0fasa+Mra/3Hswc82/M76E/
OjaEzMzM5H/3GhFE8EeQnp7+aGHHMPPPXXq93hXVter3eBLO/wHr6o/uZ1+t90uPxNPwjY/
+TuNENNI/H0+i/PYf/36D/
9gRUmD59ektmfhbAldFWlldDWZuWJSUtI7RJRlcJBoPbiSieJiSieiF5NSkoE/
ouWVlZxQOBEm3273f+j09Hk8zIloJAMy9VgjgcDAZ7JCcn
v2a9JjPH+mOkuq4PSKuq4HkpOTTPvNo
9gRUmD59ektmfhbAldAfEV1NTk4uX7JkycccvXLju1m5qtEdJWZc+66640qamp865evZqt63
pQCBHUT14//33P+bfvT6nX56gqNY43MnN+1b
600B0JyZjwghnkxKStoFABkZGfWllDDW
IlW3sIZCU2Ih/J1Ajwh+sn5mGqiE3iNmV4xbz
ouWVlZxQOBQEm3273f+j09Hk8zIloJAMy9VgjgcDAZ7JCcnIlJAMy8VgjgRKSkpKd3sewLAJ0KIHklJSUvzj8vIyGiuisjJm+/UT5ZpV
v2a9JjPH+ny+75l5V3Jycr9Qu8/nK8+/NjK8/M84QQQxITE3fkH+P1ev/OzDHJycmvWtq/B/AggEFut3t6YUnX8iTbxbDmbfz7U
r709PSKuq4HkpOTT1nnkJGRUF3dB8c8Lj8fzutvtnkBEly33e1IIcTQxMXG7pX0cM7ejo5
uUrRo0TPvv/
9+kWLFionGjRv3cDqdU5l5U1pa2l2lP79u1Lf+CBB+5JSEhYYf4W0HV91+7du/vX/v6xs+0hDa
Z2ZmHjh480OAvzCzy/
z3yyCMTAJQ4ePePDg8AsXLmQws3A4AAHKZRVRUlkt06dLVxNTD1tDxORxswAFrvQlb67oOt9v9v9v9VE5OzqE
jR45My8nJy1ply5cg/
HxMTUOHbs2MLc3NwAAA2AIz4+vmJGRsacmJmZ+zZcVA==/
RLpfrlkAgoDNzLIDXBw4c+IbqN47g5sa0adPaEtF8ABnMnAkgg4guOxwOUbRo0eLp6ekHiSiXmXPN/
/

```
W73e7b4uLiyp84cWIJft9XL5cpU+a2ChUqvC6lPHz8+PGxp0+fPs7MeqNGjYYEAoGzUVFRro0bN85w
OBx6MBiURCQffvjhF4oUKdKXiADg1Llz5wZs27btQN26dcuVK1duOYBUAPovv/
zS5fjx4+lSSr1169YpAC47HI4n3G53Rv7v4/
P5RgE4uHTp0hSfz0fFihUTgUBANG7cuG5MTMx3zIycnJxh69evn63rupBSittuuy25SpUqT3377bcf
SSmFw+EgKaVgZnHrrbcm3nnnnfOuXr265ocffpguhKDQOhdC0IMPPjjB4/
EsP3To0BZd14mZRbFixeIrVKjQedu2bbOJyElEUUQUJaWMKl68eKWyZcu+kp6evjwtLW0TEUUBiCpb
tmwTTdNKnj17dp3f778MY31rzKw5nc7oQCCgA9CISDP7ROgziYmJNTMyMo5KKZH/
M8ysaZrmlFIyM7uIyAnACSCKiFzm2o+DsTfkITY2lu+8886DFStWbBxu7/2z44Y0WKZNm1YPwBsAyg
GIARBDRLEAYv+rE4sgghsMQoi7+vfvv/e/PY8I/m8xderUEkQ0hIg6A4gHUPy/PacI/
vsoXbo06tatey46OrqJ6pD8Z4fjvz0BFYioDIAGzHyaiOYWKVIktnz58gM1TSvwudOnT38aGxtbJSE
h4YFQWzAYvHTy5Mm5gUDgaqVKlQY6HI48N7uU0u/3+48VKVKkar62vL/
MzMyfixYt2oCZ89oCgUDW+fPnNycnJz8ghChintpDp3dd1/
UAEUVLKZFvHAcCgRwARf4Pfq6bGg6H8YiaJzkAkIFAwBsVFeXWNE2E+qx/1na/33/
W5XIVF0I4Qm26rnu8Xu+22NjYkomJiXWICJqmgYggpfSdOHFibqlSpeolJiY2Cj17QghcuXJlY2Zm5
s6yZcs+J4QAESH//546dWqY2+2unJiYODB/O4BzOTk58+Lj41/
MN+aQruvDihQpstj0qOSBmQ87HI7WCQkJv3q93hkA+of6jhw5krt3794oXdfHAWj5//
UfIYIbDkKIOACdARSRUnYGgEaNGo1xuVz3hz6j6/
qZw4cPP1+kSJH4ChUqfEREeeHR3Nzc7Zs2bRp23333jXU4HI2YOW//8vv9vzgcjttD/
w0Y+2ROTs6xs2fPfl26dOnBROQK9TEzfD7fhpiYmOpOp7Nk6FqhPut/
A4Df7z9/+vTp1fHx8RUSExMfsPR5vV7vVrfbfa/D4UjKPzYzM3NfTk5ORlJSUj1N0/
I8DFLKqz6fb5eUMhAfH1/
N5XKVyP975eTknM7Kyvo1Li6uYnR0dAEqQHZ29sGoqKiE6Ojo0qH1CiCYnp6+OScn59wtt9zymNPpT
ArtG0IIZGRkfB8fH3+3w+GIzbe+cfbs2RlerzetcuXKHWJjY+sLIcDMGcePH5/o8/
lOCiGCNWvWfCYmJqZBaFwwGNy3b9++URUqVLi3ePHiI4QQ0DQttNf037Rp0/
KWLVs+43Q6B2iaFvpec9xud6/s7OxSubm5PwMou3LlSpw+fRrly5cvVbZs2VIAIgbL/
wWklMWFEMWIaM2AAQPe9nq9G00PSx6Y+Wr16tUDAB6wtBepXbv2JCnlCABWToALQFUowMxbieh2Rdd
OGKcXlfERcvNZkc7M64ioo6LvJ2bOIqLHFX2TADwEoJalvZvb7Z7v9XrnAOhhnbfb7W7s8/
neBvCs4pqFxcfM3I6ISlvajzkcjgaBQOBlIvqbYtw0AE0BVLS072bmH4joOesAZj4thHiHmT9SXG86
M/
ciomjLmKtEdB5Asev9QkT0iZSyDhHdYulKBlAaQE3F3F665557LjCzat4lADyVz4jK39f51ltvJSKa
oOiLIaIXLc3VAKwIM/XyzJzo8XgmIp+xAgAOhyMqzJgI/
gcghIiSUlYCcHLw4MHfeTyeMUR0v+Vjt95yyy1+AG8DKMDlYuYFTzzxRHUAKt6Dah8EAPedd97ZE8Y
+mh8ZzFyGiEoW4iuUJKINUsrOinXkZuYHrHu+Oe+dAMoo9oWU5OTkjl6v900Ye2j+viMOh6ORlLInM
09UzMULoLqlzQHj3bIfgJUTuBOAhMLjX6NGjaUA7gRQP19zQpUqVZ7XNK25rut/
A9DAMqxmuXLlegNoZ71efHz8zI4dO/Zi5lGWrp5er/
dsbm5uSwBlgd8Pd6bxlKD4nn963JAGi6ZpOaZV7fT5fIuI6G7rZ4joYwDWzR9ENIyZ68CywV8LzHyQ
iIrD/mDug2GQ1CnM/
IloCYB+qj5mrklEcYr2f8JYiLUs7WOSk5PnezyeMbAbK4cdDkcLn8/3LP4zxso/
ANS0GivMnOV0OpsFg8GOYYwVABikamTmW1XGCoyYe39mXqAY8ykRdbJuSgBgnhJrWD6fo/
qsiYXMXFT1DJmwGSsAphLRFinlZsVmmmreK14xboQQ4iIzb1DdiIhUY8JCCNFdStmEiIZY+3Rd32fO
XRbmmhHcHAgEAn5N08DMUV6v9xkA1hcaACwH8BHs4aJNAFYz83aV0R0OzHzFavQzcw6AM0RUrTDzNw
2HCWHWrY+IbIkDzHwWQCwRPWpp3+52u3v4fL7ezDzSMsyjaVoLXdebAVAZKwBgNfTy407Lfx8DsBbA
cMVnB5sck/
GKviRd17eobsDMmURkM1ZMjJVSvqX4d9oH4PH88wsZLF6v96MaNWosCXO9PzVuyCwhXdf9AJCcnNwI
gC3zhplnMfPTiqE/MvP3UsrPr/dezHyUiHywewZOAfgN136YVdf7gJnDGSu/
hDFWthDRcSJqb2lfkpyc/
KrX632aiEZZ+k4DaCqlbAXjBPXvYoPpubBl3QghWkspywOYWpgLmiG9Eor2K0KIDgDegv0ksJCIHgT
gVlzymKLNE85YYebVAHYBeLIQ0/7B6XS+BmBZfhe6iePMnA6DW1UARPQJMy+XUn5diHtdCy9JKZNh/
EYqnDLvGzFY/
gfhcrlyAEDTtFgYnlkrvofxnN5m7dA07W9EtPQaRr4KBxQeShDRr4U1VgC8A6AZ1F7SX2E/
OIKZrwBYTEQdLF0nXS5X64yMjAeY+VPFuNYAKsM4jP27SIcxd5uxQkTvCSG2SSnn/
4FrhrMa3wXQSOHtTjMNxdr5G0MGy4EDB1YXcg5/
GtyQBoumaTkAEBUVZf2HAowXWgdFvD+HmYcT0Tcqo0AFZj5PRD8DuM/
SnsnMWwE0L8y8mXkMgL5huneGCTmlCSEWwu4t2ut2u3t4PJ5OACZb+rxOp/
MxIqrFzLMLM0cVmPkggE+Z+QVFd3cp5SVd1wtrsZ9ULDQAABF10XX9JVgWHIAUZq4AY4OxznEbgAqW
Zi/UITkw8zYhxFQYG8x1z9npdHYMBAKLYN/
oLwE4qPLUmIbRmwDWF9aLogIzfyaESCWiGeE+k5CQ0AIAhBA3pJc0gv+/uHr1qh/
IM1gKgJkPwcgquUsx9CVd1ydAscbCgZnXwuLVNNsPwu6B+FeYw8z1whg5+xCePPye1VPLzNkAWuXm5
pbQdf0rxfw6a5oWUPX9QfwVwDjFfb5i5o90Xf/
G+l66Fpg5C0AwzPtqLjNrAB6xjLkAw6NV3zqAmX3m/
1XuiTcDbkiDJTExMRZAHuErH+Yx810AbPnwptt8EhQnChWYOZuIPgHQTXGtb8LwT651vTeIqEeYh+8
nZla9vH3M/
```

```
BYzf2Bp9zBzq4yMjAeIaJHlPlc0TWshpYxl5sWFmWOYeZ8TQjzNzFOsfUT0alRU1DoAq67XCDSveQb
hY6g9ADxJRE0s7RsB6ER0j2LMDwDusNwjC4APimcBwK8Oh+NZKeWcQsz5KhG1CQQCrwF42NJ3hYiWA
mihGLo3Ojq6j5RylcqbVFgw83oAi6SU/7zW50KnqeLFiz+UkZFx3S+fCG4ONG/
evBrwO1E1H9JMT6mKm5ICgx9XGM2gZUT0mKL9FBFZeR/
XBDOvAQBrSMfELmZ2Qb1vjCWiwYr2TjD4M98SUQHNF2Ye5nA4dkkpV1v7/
giI6ClmHgKL94eZf46KihoI4JvCcHiY+TIRXYDay7QCwBpr+N3c8/
ZC7fXPiI6OjgeAUDLCzYgb8oulp6efBgouRpOYmRTGMp8CoBkR1bveexDRaJVHwTQCChNCCM3tcSiM
JdNTE6t6mInoRRU5k4g6aJpWQtf1LxW36wDAay7EfysLyTyhdJBSTlUYJHMSExPf8/
v9K8jI2rrea56BwauwbTxkpGHWgeX3ZeajAA5CEf6DYayUVXguDgNQidpdJKJOuq4vKKS34ykpZQMA
qlDj9DBhvhMAWvv9/sVEpCRzFwbMfFQI8SaAaxorwO8GC4AizHxDC1pF8J/
H2rVrtwIFD3Umx+MwLAa32XcEhgfDdkC7BlbA4n02r3UOJtGzENgNYAuAnoq+vczsCeOBngKgFewv9
meEEFuYWXVQmBYVFTVb1/
U1UIeWC4sRzHwPEVnJssdcLlebQCAwB4X0NBHREaj3r5+I6H0AcxV9q1TGoxkRcDmdTg0A7r777tc9
Hs+/
7em9EXFDGixmfA4ZGRmHADCMmGFRqNM3N5qWeTjSkur6LwAYrnjhL4P6pXmtay0GUJqI7lV0HyCic7
Bn/QDAYCnl32GP1w4SQpwxDZL8HAomog5RUVE7dV1fi39/
IepCiDYAXlW8bH9wu929fD7f4muQVVW4BCA7jIHztpRSsxqJJuHsKwADrAOYeTsM17Y1FLQhjEv0sh
Cihemxso65Ft4motOqEAwzj4Y6zJeuadpjMLx6/
wmFyUtCiH7MvFjBnbEhZLBkZGTstArtRXDzY+DAgQHgd4OFmQ8R0TIovIDmaX4pgJeu9/
rMvIaZK8OeaZkBNeH8WjgOYAYRvRqmb1OYF/
FXzHwL7KGtj91u98fMvEJxgF2elJQ0PBAIrEbh9oBwmMHMlwBYPTzpDoejWW5u7hsw+DjXDWZeB6Cu
ousAgOHMrAphzSeiTop2HwwBwOjQnhAVFVVbCNGrMHP6s+CGNlhycnLSzdMjEZHqpXEKwPdh+sJhpP
l5q8W+GQbB6bqJaMy8lohSFUQwwCCILgfQVjFuNIAuRFTF0jXd5XIt13X9W1g2CiJ6NTEx8VtzIdpI
n4UFEfVl5hZkSa8249JtzFRaVQhECdNb84vqlMTMnwPYS0TvKebxDyhIbOYGfBCAVZJ7JzOrwkbQNK
2druuDUTiX90ohxEwAS60dRPQeEXVTeWqYuaWu688DaKPou6q6Uei5DoPeJmnwuuT5Q5vT1atXL13P
5yO4+RB6zpi5LxFNATBQ9TkimotCGCsANhJRtPUgw8zZzOwoZIglA8AoZratfRgctGmwGwOhw8oJay
ICgJVut/
sZj8ezBHbu4TZm7u71epeikJmdYbCciBYQ0UxFX5tAINAaYX7zcDDDV6qQ2AlN03oz8xewe6fnM/
NfFNfKBnCMiEoBv+8Jubm5O5KSklRE7D89bkiDhYj85v86iKg11MTJi0Q0C4A1je1a132fmR+EnUC2
B4Yex3VrewDYY3oG/q6aG4Dxqj5m/
gyGwWHVCljncDhG+f3+NQDKW4bNTEpKetPr9X4JO1G10CCi12GEbQoQfZn5HBE1B9CdFKm0/+KaG6D
2NHwNYCEAG3uemRczc29F+2kYYZGelvYjzFwqzIbZg5lrEFGf650zM//
icrn6SSmXwfJvz8yfMfPdULhtzU30XgDPKK55VRWqY+bzAHTVPIioNzO/
prpXOGiaFuI93bQEuwiujdA+qev6WagzhcDMa5n5qeu9pmkonIYlW5AN6YDg9Xj/
8o9h5oEAJlrXhOn1eZGZVV6XEzCSK6x70IGkpKTOXq93MhFZX+CpUVFRLYloChE1vt45XmPuP8MwtF
TJBl2JKJmI3i3kNdfBfgADjNTrzsFg8HOyJyp8A6B5mIP0KuTz1ITELffv3/9+Yeb1Z8INabBIKXMA
wOFwJAKYp/iIB8AHzPx6IS67gA09DqtgWyozO1E4r8UpZn4LwMfWDvMU8iyrc/E3CCGOEdFTljG/
uFyubsFgcBnsxtQKt9s9wOv1LghDfisUmPlzKeVqZp5jac/RNK0VDG0Pa1bSv8I/
oA6lbWbmtwGouDibiKipYiH6iOgtInrFMr+zRBQgolsV13qZmS+ynbwcFsycGRUV1c7v98+A/
TdfRkZdj4cVQwdJKZ0qbxEAhDFWThPRVdVmT0SvMvMTheFfMfMOp9M5h5klIgbL/
yzyeezCcZ52EtFjhfAa7yOi1QCeUPR5oSa4h4UQYhCAV6HO/
OnLRqKClSybBSNEazUGPETUKj09fQjsPDOvEOLxQCAwHIXj6IRDqtPp7Alj37KG3kcJIY5KKW36Uf8
CGwHcQQoxPADtdV3/
gOwk5t0w6ASqYraTyZIYYpJ4ceXKldxCzu1PgxvaYImJiVGdOL0AJgAYe73XMzMvdsHuvrvEzBcVD0
ponM2Fby6ovxLRNNUYIUQ3IhpnJbGaxNJPzHBQfvg0TWvh9/vnwG5970pKSurk8/
neA9Al7Be8fnwPg7OyXNHX05hm4TKPmHl2GHflEQCDiGiFYlM6wsy3weL6NH/
vZ5nZljpIREehJrbNczqdSwEUKu2aiLoEAoE+sPCizJPVz1CQA9lIWz9AlsytfHNXwUNG1sZtir75p
lrpdcfAzVBZIjPv1DQt1zSsIvgfhBAiCABSSpXH8QdmvkPRHg6/
MvNkKDzWzHwkzEEh7HNPREOklN1UeysR9QIwFGri7lAotIeYuZWUsom5BvO3XxFCNGXmVlAIif4BXH
Q4HK0CgcA8WDyezPwZEf1DSplSSOrADmYuFobb1xrGd7bu/
akwuEKq32g8gK6We2SfOnUqFIm4afeEG9JgueeeeE4oDADMXmB8bbOg3C+lZ2SOEmAPjHzn/
tXLYkIxXkWUBQ4nV9lAKIXoA+ABqcaMnpJTPwE728mia9jIzf6K4T1sp5etE1NTSnupwOJqmp6cPYr
U+SqHAzIdcLteTZFSHtoa+3jJFj1apPATXuOZiAI8r3L0XhBBPwjAirJyME2aoz5bmbfJqXlNwRpZB
IWgHYGVUVNSLgUBgVWFc1QBeJiOzwBoS+0UI8TEMTRVY+mYR0WJm/
kbRdy1uylooCHbMvJ6ZfzU37+tFmnmKqgQALpcrOi4urlCppRHcHEhPT0+KiYlRptEz82pmrnu9a8L
0AA6Hsa9ZsY+Iwhk+l1R7pOl9vJPs0gUA8KyUsjEpSPNmCGgY7KnDXYQQpUhBiieizrquVyqMdzUcm
DlbCNEsEAiMsXo8mflbp9M5XEq5CoUrNHkAQLqVDwQYqdIwDJYCPEc2tFauwi5mCmb+EMYBp4Dnh4h
iS5cufbf5mZtWm+mGM1iysrJKlCtXTqWfcYyIxsLIyb9e6/YYEb0upVR5QxYo4qAh/
Ap1Wm5vZh4ONdfgGQD3WhepGfsdoOv6ZOuLnYh6EVFbAN0t1/JqmtYsEAg0ZnXti8LioqZpLf1+/
6ewhz+Wapr23h9YiCuI6I4Q4SsENkrdt5NSzoBdnMrLzJeh+P2YeSAz9yE7EXkZFMRWALscDkdPv9+
/
AoUI55lG1kY2iMD5288T0VAppU2PBsByIcSbzLzGakyxodFyJcwzORkK9zozHyaiL0mdNREOPmb+Hv
```

```
m4T5qmwel0Fvf5fNedIRfBnx8+ny9RSjkvVE+KC2qxrIKRPGCtvXYmzOUyiGgwM89QHDwOs5EpZIPJ
ybJx/ph5iZTyHKtlAN5lZlcYI30cGzXMCqx/
InpNCHGOFZkzRNTbXHtfhPluhYKmaR2YuZs11AJgv9Pp7BoMBr+6hvFmAzP/
BiMspyLZjoLBVRxgGXOFiH6D2ps8B0AZqLNOkZSU1BUAatSo0UPVfzPghjNY4uLiLjgcjgI6LGZIZx
qAdwrhAfDCCC98rniZzEEYrRVmPgy1CuQIZm4KNbF0vLlwbHV2hBADzVitVYdlnJSyBDMPVcyhpZSy
zH9iIZrclJZSyuGwhx72EFFvXdcLtRBhlEBwQbFwNE3rAOANxQklB8BZlYvYDJPdo1jY30P9e5+Mio
pqEQgEZhSG+wEjU2k0DCOowNw0TesOYIr1VMrMW6OiogZIKb+xGmcAQEQXoU4xf5eZVQRgjxBiPArP
E5pBRAUIypqmwe/
3n09KSrJlOEVw80JKGQsgr4J4Pi2WeTD0qKyaSqlhuFU5zNwFxrNoNT6OEVHJMPvtRSiKwTLzz0KI+
aQu/LmYjYKwKqLqFzBe3g9bxiyRUi6RUqpC2H9n5u3/
qVIYRPSUruu3Wb3ZzHw+Ojq6WSAQmIFClGkxqQOfwlL/zeybxcznmPkNxTx2IbxH9gSpM1IB/
E66jYmJedzj8cxi5usvFPUnwQ1nsABAUlJSFyDPYJlKRFuhzhTyqsabp/juMEixVk/
JUmZurDoRm7Fam+uOmT9l5miojZwFAJaxoo4FgJHmhlDAWmbmL4nokGphE1E7IrocZpEWGkKIbrqu3
wNLcUJzwbRi5o+hDreEwz4Ah1XuXmbuIqXsFcYVfABqee/PhRA+smT3MPMOGP921o00g5mb5+bmPk/
2lMdrwSOE6AMjfdlKHuyl6/
pbsMSLmfmIy+Vqm5ub+88wPKc9sGd0gQ0hwY4K7k4OEQ2TUn5YiHmDmd9gZlvqp5QyPTs7O9zJOYKb
FMnJyb8B6GZW5YWU0gujzpfVUwtmPsTMQShC2GbY9g1YPJRsZOkJ1RgYlegDCk/
jUU3TXpFS2pIk2JB/
GA3DMLHiBxjqrV0t7Zth8O02KPiAHxDRQjZShK9bgfsaeBcG2X+65T5XiKhpTk7Os4Xca0BEb6s8qM
z8lRBiORkq61ZshEKoD8AuIcQ8siQiWJFPTBLm4SpisPxfgIiyAeh+v9/
LzDEARig+djzceJNn8hbsL5PvAJRXkZ/
YIMWqZKFXmYvmNUXfBk3TXoWRumvFfAC3wlKPiJl3aJq2gC1ZOiaeYeZd5gJXsckLBWZ+QUp5GZaUR
zbk/
VuSIXdt3SiuhZMwDDRbJWwi+hsR1YVi04Sh66CswSOE+EoR9jpGRGehSOEWQvxFCNEA6nTysBBCdNV
1fRrs4aiXiKi9NabOzOc1TWvu9/
snQ72JfA91rZa5ZKj53mbtIKOS+OuF2WRNPkAXxQviUHZ29m4iumnj1RGEh9vtTsnNzT0JAMFg8Aso
tExgcJ6Oq7ynRNSLmXuTXb01g4i8UBviV5j5DNkJuB4hxABd1+coPDJ7APQBsFRl5Jj7oDWB4hgz9y
MjOcAapp6radpoU1jT5vEsLJj5K03TFoXJ+vkLDA9vYTRsYH5eRQD+SQgxKcy9NkPtwTkO4JUwoeoC
CHlY/H7/
yaSkpE50ExZGvSENFgBg5iARFQ0T70wFkAm1K76blHIg7C+7PQCyoRYUOgWjjo11AewySU4qmeQ9Lp
erm67rS2Enlm42PQQF0u+Y+TchxFhd123GChnVPucz82r6D9SkATBZCLEBiuwZ0+tSB8DLhbheOozs
LFX14HfNU5yq5PpGqBfiTgCjrdVN2SBWb4Ahx21FDwCCDS2b6wYRPSWlfEYRPpjjetoKZGCxob7bVE
r5giKeDRiGr0qcLuQVe8DaYYa9+qBw6fPzmPl2xQvH53A42sTHx5cCEFWI60VwEyEzM/
NftCKCAAAgAElEQVQAADgcDpWxchFGWq6qgOtwZm6IMNwwGNIGNhDRDqun0fQadmTmSYqw9wlmbkVE
towbGETUN2AJjTJzlqZpT5AhKGklnX6TlJQ02AzPFiaErQQbmjOjzKKF1kyrQeZhoFAV6onoFZO/
YyUOH2TmYcy8RMEV2sHMKl5KhhCiLzN/
EoYjVwAhg+Xo0aPTiOhKYeb9Z8ENabD4fL5Eh8Ph1DTNZe1jo47FNij4E2b88XGyq7eehVHHQvUSTI
dRWdgaCjoF4HkiUpULP+5yuZr7/
f5ZsIc5jsPgQhTQ6WBDKOklZv5U8cD+MzEx8RUp5Qoiqur3+zFnzhwcOHBAceuCSElJwdq1awu0MfM
/ieg9KeVKBSdjmJQyR+WSNENpNpib0lAosmcALGSjkrJNuIqZtzKzSujuGIDeAL6wzg/
Ap9bwkHmtN5h51x+oGj2Wme+DXSdmM4BvmfmNvXv3Yu7cuQgEAgAAIUQ7k69kE4aDQdhVxZh/
ZuZdCBOzNj1MhVHf/
A7AGcW8AWBTMBhcEB8fXzUmJqZCVlZWYcjSEdwkSExMrArYSLeAETYdBfUpfxIbAwYp+lKg1h4CgJV
QGOJCiG5miRErSdSraVoTAGOgEKGDUfn4A+uLmIi66rr+HiwHTmbekpSU9ITP5/sH1OJrhQIz/
+Z0OrvBCBEXt/RNFEJsZ2abfMG/
uOYHJt2giqX9rKZpPWGExKxhtt1EVF6xT18VQvxFSjnxej1JmqalAUBOTk6gMPP+M+GGM1iysrJKsJ
FuLBQL0UtEE6HQJDF5Awmwq6NeBjAL4SWUv4Nd4jkTQFdmngX7A+Z1OByP5+TkvAR7uCebmf/
OzDarnIiGsyFPbeVP/
NSgQYMPxo0b952u640AYNu2bRgyZAhee00VhfodUkr07NkTnTt3zt+82eVyPaMiiTLzLCHEWiiEppj
5NyIKJzj0HDOPhCVkdvny5e/r16/
vWrt2rSo2vRNABUVoywuj7tPnitDcZCjCTQDmulyuaWRU0b7uOiZs1OXxK655DMBbzDwTAF5//
XU8//
zz2LZtG5j5CTbUdFXEwa0wQoo21zaAT8LErFcTUQDqOljh5n0EwCKoSxYsAdCKiOqZJ6qo3NzcjR6P
57oLVEbw54fP5xsVExNTAbAVQLwCw2i2bR7M/
KUQ4gfVsw3DWFGW4mBDLdfGcyOiIczcRHFAvMrMrYLBYFuyiGSaeB7AaNjVpQewQVR/
wNJ+SAjR3OfzvQ9FqZPCgpkzhRBtgsHgLKtxAeAbTdMmSynXKLwu18ICGHv7I5b2DAB/
kVJ+at3vzHUeD0W2lRDiSV3Xn0aYjCArmPk8G3xJ4CbWYbnh4t9xcXEXPB7PESFEAbckM2cJIfpLKT
8jKsglYiNVda/
KayCEeEdKqeLAAEaop8CJmJmRnJwcD+DHMPM7ffz48YeJ6HnFvUIKtwVe0kT0ipTyeYUBcVDTtFbNm
zdf+vLLLzfo3r07YmNjUb9+fYwZMwb16/9Oq5BSIjU1FeXLl0dUVFTofpg6dSpC5Ds2FHPb5+bmLlC
4bldrmjZW1/XNCmv+FyISMFLmYOl7wQzLVbS0H9yzZ8+bqamp3545Y+N9HgCQEApt/
fLLL5g0aRLWrl3LXq9Xr1Gjxtpx48YVv+eeAiWB5sJ4EVs9LhsAPOv3+9cRkS2uHg7MvJ2I1jGzNaU
```

9A4bnZHbodDd8+HA89thjqF279lBN0y5JKddlZmYiIyMDZcvm8XD3m8aXVcjpkqZpL6vCfOaY76EOo
4XDJQCvMvNs63MOI+SUR2h2Op2h03WiyhsZwc0LZp6k6/
pwAHH52nI0TWsrpRyl4Jls1jRtqpTyW8XlfgBg5bKE8JMZfrGuy0m33HLL2JycHJvWy+23375xy5Yt
xWCEkAuAiF5joxyHNRPzLSFEA2YuQG41PepNmflpKAqkhtC2bVv8+KNyywYAnD59GkWKGI5tTdM6Si
lfgj1UvYeZB+m6vp6IVHSDi1BIPzDzuqysrEPnzp0bffvtBUupCSE66Lo+BnbD45h5mFKFtgaxUR06
nOyG9f7ZAGa4XK5vAQRgFIy9KXHDGSwA4Ha7ezBzWyLK++E1TWsnpXxPccLeZHI/
bHn6ZhhhgIIIBmb+EkBb60tBCNF71qxZ3YoXL/4YAAwaNAjVq1fHc889h++++
+7lxMTEi6QohsXMQ5n5aSKychQmSynbkqUoIBviQM2klIPKly9f4PTicrnw9NNPh1yn0QAwf/
58PPfcczh06BBKlvw9VNypU14Bz3RN05rn5ua+D7uVvxdAP13Xv7XGmU1j5RzUmULvmLwPqwfqgsPh
eKpq1aq28Ix5vQDMUNmBAwfQsmVLVKtWDQ0aNJh0xx13VD516lSLvn37YuvWrShatCjY0DepDAtRlZ
kPa5rWQUo5T0XavQZOCSEmMfNsawcR9THdrHmnmnvvvRcNGzZZ8D8A6Xdc3EhEeeughNGnSBOPHjweA
NBieIdtvJIQYpOv6x4ow3wUimgwjHf+6IYQYrOv6JEXM+kcA1fI//
5qmgZmZiJokJiamFuY+Efy54Xa7Mz755JMfAbRg5vzyBc1gr1N2GMALptYSLH0/
AyiVfz3k6zsSxkj/
mojWffnll88Gg8G8xiNHjmDYsGFwOBz7mHmB4mA5C0ANsoh1miFssEW7xfR0PyqEeISZVeHoPIwZMw
aZmZkAgI8//
hh79uzBjBmGzpwQIs9YIaK+UspHYdFHYoNf2BaGZ9PqdQEzH1V4V4YwBgnxBizogRI2bv2bMHGzduzN/
XVUr5FFlKqph7w1moJRvGElEOM4c7ZNtABpn/XQBFnU4nypUr14eZ378ZeSw3pMFCRDnTp0+/
5HQ6izNzjhCipZSyG+xxzYOapr2q6/bwEwrUqQIihcvjvvvu2/
AQw899J2u69usFzPDtpE7TfX+Hoj2TDM2RhxDm9M1G7ZxbVH2Kz+YAaCGl7AN71s8pImoDowChl
aeTCoPLoSI2/wNAlvV6pjXfXtf1mZQmWTey4+Zfnmrv/PnzEQgH/
KeTkpIkgOcAICMjA0WLFgWMNOnM/GNMXBJCNJdSjoaaae6RhxDm9M1G7ZxbVH2Kz+YAaCGl7AN71s8pImoDowChl
aeTCoPLoSI2/wNAlvV6pjXfXtf1mZqmWTey4+Zfnmrv/PnzEQgEMH/+/
KeTkpIkgOcAICMjA0WLFgWMNOnM/GNMXBJCNJdSjoaae6QEM18WQoyUUk5RPBPPMPNQq/
EII6NrkpRyqyKEdYmZd5KafNtD1/WxCiPwshDiJSnlZMUcwoKIeum6/ndFzHo/jBTFAqdSTdMCfr//
itvt3nvdN4ngpkEwGMwmIui6/
pMQYhQzJzRX+J8FQis0DM59zOBy9dF1fDHsW5W5Mz2wGMZ+Zv7723oEj40KFDj2mahnX
r1nVUeHFXE5EPQF9L+zYxAW6Hwxggh2hBRKSmlyntZVq/
e7AWLRoEVwuF+6/38b1H8dG3Thr1k8GgMell08SkyofzxSfs4mIVJmCJwC8zJKHRdiVEN2LMmM4joZ6j
3tDkAVjPzD5Zr5SgOMADy1MGHhH5vh8MBPp9vZ5Q9SSwyLZxz0DZwgIBBI1zTtY
WYuB7si4AUhxGAp5UJrrJGZvzVjuQ8rLr2PmW9RvBT+QUSH2V7rB2lpaXs1TfunruspMBd9p06dMHL
kSEyZMmVn9erVu/bv37/jwYMHMWjQIDz22GMoU6aMfv/
99z+ybNkymyZJ9+7dP6xcufL8ChUqQzH3qqadw7tw563c/
UqpUqVsmTjSyfRs2bIjnnnsOAFCtWjW43W7k8Bhq8J06dUKtWrUOwfBojASQ4cOoX///
qhRowaXKFHC1bZt2x/
T09MLLLh27drlPPHEE94JEyb0qlevHqpUqYKX34ZE1d7ZeSw3pMFCRDnTp0+0+
Xny5L/
DINJZU3q9MAsaWr4LdF3PPXPmzEXkY9wnJCSAmS+wISbVcdu2bejRowcqVqyIg0bolWrVrOklO2Rj
/i6fPlydOzYEbfddhsaN26Md999F1JKZGRkw012Y/bs2SBD52TC/
v37Y91uN9asWQPAyMJqTJayNHjmyy0ePFiNGrUCP369QMzr65SpU8/QMzr65SpUpa8eLFjxNRycWLF8PtduPEiR
45JNP4Ha7i40bN67jBkz4Ha7EQp/
EdFzAAb17Nnzjt69bQWnh0gp31dWKYAVJwJYu+cJm9UmmZr6Fl6WUrRWeJA+MEJtt9z1//
vxnUsqbNl4dwbVBZtrq+vXrB2ia9duBzVQPS2NsiHzeaK3n4sNWjkoxqFzLrf4VkCmdwMNx5d2GbYr
MfuyYRxmrCTb40KIAQC+tO65M2fOxZdM4HG06fHNWKEKqxgXNdYnEngH4zT0d7OWgN3KcwWNbnSg2dt2vTTFn3/+Of
+wk/
Xr1y86atSoNTFZbvSxHh0BzB2QFwvULfQoxOdjzKqQpQOJGYBt14eMLgVHAS6aTnIZJxFb3T/rXLSZFRYQ2rqu
alXj/NawYcNVFStW3JL/UNK7d0288/vjjIU/8fampqejinfBtk23s0bFmq+zq+/nSHYrW/AGo+/
fTTn546dWp2cnJyIC3EG43W40bEjIZN1cyanHw7xBMENERSTR6KqTdHG4j5NF7AGBiGEVOf8/
EWLKKWAHANT8kIZn4M4BHHUcN7W2VcFTF91+yXE/UrQUn9P2EjV4T9LtnZLd/
QiX9hsINa7AQUZCZSUoZDUtaMRfRXdtnENCvpUGE0BITA4ZmmMXrKh2zXgEmrtUOKaxBR1auNtWzw
Ldj+7EL26yg6vhCBQ9Bd7jHT8hCs1WBuY8KDXMHHpMuLxrb4k84a5ZS+g63DM4mRFjQqAjvfTmCxQnY+
ZWeNmDiaCu6tfwtV1ejCgTzNcz0WuW+aW
ZNjYcEXqNvlGpDZ9h4CFJpBXPV3vnRkQSlJPPx6Yk5W/
UxSJTxKsjhTCvCNj2xmuWMdzQfdzOmuTahmCjBKuYUGqTUSoezVi6/
ffULtn2LI+SJSdOkqZkDbJyDT97u83/
uz4HwnJzs4bdtHydDXwF3PnsDpBqFHjt96fKxiYPkTAZpDr7ogbA7L/
Im3eSoHD7nwZKhPxR2eSAfF6PV8KqNV4bMpOSk/
N5FCuTHVlXeTsHNeN8Nl9nZ7z/
xMk8FcvAawSUlp9OqmoOBAlDnDMuPR+/+jm8xWTESZUhaSJ0FRU/
DvbwZpYoZ6BH9T7DUaNZR5cgXf3HhK4/
Cp7xlOnTnmK3Ks3w+s6Oli3G7B0HLw+AbRS8gY6w0Mhxp+/
izBG5+Ai8lQXG2xZl0Ef2t+Yx4y6DJt
4GAXGQ8/
ANBZ6Y6RHBwOcDQyB/ytKZ7Kny/+/
EmRUCeNRy9Oezk4qlRXuqwSw5dUnmG6R1eyMlasH/
ZwnFUQqsCUtkDGDc1Ys8Iaq6AMbyh1HTMVQ2xsNX/
yBJmjwqF9V9GhOSBq3/OUBBGZXIbQF82AsKrzj

```
XewEmEXnkyJH47bffMGLECEyYMAGnTp1az8zPlihRoviyZcvw2GOPoUKFCpg9e/
bmQYMGjYMiHZoNwTuV+vVuAH0CgcBy2JMyDkAh38GGWm4uLGKmZpgYAHY6HI5h1nF/
dtzIm51uEkFtiq9E9AQzv6cwPHwA/gZ15V6f+WdNs/2ViF5g5nXWAcy8/
vz582UbN278ECz8ikAg4D906FDM2rVrY+rW/
T3LddCgQZdgCMkN7tChA+bMmYMffvgBPXr0AIBnJk6c2LR06dL63LlzHaG8+WAwiLFjx0JKuYeZK1v
DCPXq1cPhw4cBAPXr18/
jsDDz7EuXLt1eu3btPPbq7NmzcenSJUyfPn1Ao0aNiIhGtmjRAq1bt8aaNWvw+OOPXxRCPF2+fPlFM
TExmD17NhwOB6pWrYqqVasGPv300x0vvvjiAiIqUqtWrTxXKxG9duHChWojR46snpaWhsqVf7fdDh0
6lBLGQNzYuXPnAYmJiXtefPHFhFatWsHtdqN9+/Z48cUXXy1RosQbRITZs2fD4/
EgJSUFVapUGdmzZ89VI0aM+MuUKVPQsqWRXPPhhx+iatWqmDVr1nkhRMnWre3ZvmXKlKlBRAUKT16+
fPkYEaXCdJXv3r0ba9euRd26ddOcTueDgUDg84SEhDwyb4kSJVCiRAn4/
f6Mu+66q1x+t3K9evWwePHiM3379nUA6LB582ZcuXIlz2AhoveYuRkUgnJsFJizFXwEsFkIsdw8yVk
xntT1hn4F0P+OO+4oduTIkZuWYBfBv4QOAHXr1v2A7LIML8F4mVn5bCGtkOdUFzT5JLbwp6Zp7XRdf
5OIrMbP7sqVK39PRI9OmzatwMY1adIkvWjRohm7d+8uT0Ro27YtGjdujM8+
+wwjR44cxcxvAwXWJIjo/
Tp16uzJycn5cOrUqWjb1kgKatKkCWrUqIFp06bhjTdsivbXwjFN0wYHg8GVmqY5z549izFjxuDpp58
GgBFEdLlWrVqPpqWlFRj022+//ZqQkHBb6ECwZ88eNGvWDN27d4cQomPbtm27w8zuuf/+
+7FgwQKkpaVdbdOmzd/ZqPllxQRYdLlMnGDmNkS0EHbuzE6oZfpXA/
gnGYVsC0DTNJiRiSYJCQlKJfg/
M25kD4t0Op0JsKcVPwMjDmrTtGDmrkQ0xequNHEAdmPlIhF1ZiPf3nqffW63u63b7XaXLFnyNst9st
LS0g7XrFlT5jdWAODtt9/
e3qRJk8HlypXLyzDJysoCgHeFEPOjoqJa3nfffVrIWAGAxMQ8o7rU9YYRmHmt0+l8u1atWvVMww4A8
P3338Ptdp+5//77c8mUmm7Y0AjLbty4MYeZe0opPxZCaCVLlswv5+w7ceLE/po1az4YCpf5/X68/
fbbqFmzZrrb7X515MiRXfJ9nzxUq1bNWqMIMEJvXaWUK5s0aZLw888/Y/
z48SGjA506dXorMzOzKABs2rQJFStWROXKlWcT0Xwp5eratWtj27ZtCAQC0HUd69atQ61atS4KIazi
VAgEAt8BQHx8vLVKNk6dOrUJ+eL6d911F+rWrXuRmR8OBAJjoBbPmhkTE1M0VFwuhAYNGhzbsWNHcb
/f/wIArF+/
HpUqVUKVKlUAYJGUUiN1WYK0MMbKr0Q0Ioyc+QdQZ0UcgOnpS0pKao+bOIUxgn8JCQAul8vKr/
iGmWOh8Hgy80Q2MnFU2S5fqowVZu6s63pPa/iImc+8+uqrPQOBwMu9evWimjV/T+wMBoP4/
vvv0bp16yKh/ZiIUKdOHSxfvjwNwFAyFZ/
NNQkAy5KSkoY2a9ZsFoACnsuiRYuidu3a+pYtW65bvdXkCnbQdX0+5RPj7Nq1K9jIwvuJmVUq5eOTk
5NLapqWtzk2b94cS5YsQceOHZelpKQ0gyHNkAe/
33/53Llzp1UHD2Z+k5l7KqgLWQ6H43EAH8Ke2HCImasp5raPiF6EuswBAATOnTuXcjMaK8ANbLDExM
Tcmv9FbGIBgOqwPCwmuhPRswBsLy0YWisFOACmu72tSZi1ptidioqKaurz+dolJSVZVWwhhBhSqVKl
qiVKlCgwv5EjR34/
fvz4Zj169MCWLVtw4VkLK5V6vV4uPL5jolJmZedy8ru1lrAIzH3Q4HH8NnRry9x
07duwijKrIn+ebL4oVK8bLly//
kYgmKPg7ANC6TJky5YoWLZpHzBs0aBDmzp175dFHH5127Ngx7auvCiZipaenjwQAh8NhzZD5jZlbEt
FcIqoGGJlP/fr1w4oVKya/+eabx/
fv3x+1ZMmS0PdHWloakpOTeyUlJR1zu93FBg4ciGAwiPPnzyM7OxuBQABly5ZVbbKHA4GALa9a1/
UrAFC1atUCpLfk5GQphGghhOgFhTYPG9lmVR35C3MY7QerVq06PRgMOn/
4weDEbdiwAc2bNweM1M9NRDRE8bvuZmZbeMjkEPRm5rkKA3segAcU/
057mDnP5R6a4pkzZ1QbWwQ3OYoVK6aq6PsrEa0mdd2Zr81nzXZqB/
ADEdm8MTDKopQnu+J4RlRU1GPffPPNhOjo6CIvv1xQNPvs2bNvMLO2cOHCIm63G6G/zz//
HLm5uaXzG/DFihUDgA1ut7utx+OZJYSoBBg8txCYOTMuLi73zJkz1/3O0jTtL6YnPi/
E7nQ6kZSUtJyIZkopU6xjiOh9APWLFClSIEQ0evRotG7d+ocjR45U7NZ782bdpg7948rrt3+/
btG8uUKVMedtXzd8moD2fb24UQrYPBYA+y1Cli5kMAEsme3XrKrCi9iNR6VOmZmZmbrl69ejXcb/
Jnxw1psPh8vncdDkdsSF8EyOOm7Ici7mpasFWgED5iI23vYWs7EXU2wxhWQyaTmZsHAoHboZDkZ+ah
UsqhDofDqnsxf8WKFQ80bdoUPXv2xK23/
i6D8PHHH8/1eDyLAdxXtmxZq4dip5QyiOuElNIDoLPJ+r/N0r0sNzf31xIlShTYyHRdz/
F4PLJhw4Z3QFG2XAjREUCLhISEvMWWlpaGr7/+GmXKlJn3wQcf/
N1qZAF4OTY21lYM0jzVNCeicbCnV34FoHyvXr1uA4CTJ08CABITE7MdDsehefPm7VeBny/
xUvXhwJCQmL4uLi8tIW88FLRN/
GxMTY6iGdPHlSVVwMhw8f3sPMdzLzGEX3JjJSsq2ZEeeFECO6dev2eqVKlbBB+/
XqcPn0aBw4cwOPHj+Ps2bMYGBjA+fPnMTAwgLNnz+L48eM4cOAAHnvsMdx///3Y2NjAzMwMzMzMsLGx
gZmZGZiZmYGZmRmYmZmBmZkZmJmZgZmZGZiZmYGZmRmYmZmBmZkZmJmZgZmZGZiZmYGZmRmYmZmBmZkZ
mJmZgZmZGZiZmYGZmRmYmZmBmZkZmJmZgZmZGZiZmYGZmRmYmZmBmZkZmJmZgZmZGZiZmYGZmRmYmZmB
1zbbtm1bKgD07du3XcjVWrduXRw8eDS9ADtPYrMQYlLv3r3rHT
```

```
58GJcuXcrreOedd95kZq1t27aqOjbPSCldsNQVOnPmzHkA6NevX55Rsn//
fgDA8ePHpwG43+Fw2BaipmntmbkTTHf09u3bkZmZCTZKz3sAtA5l2lSoUAEAvGlpaVOcTmelBx98sP
b999+P/H8ul2sOgCYNGzbEpk2b8u7DRqrf5wCedbmM/
S8krU9Er0ZHR9tSd06cOHFYSilZUYuIDS2LbQA6A8ZJTNd1MHO2EGKAlHI6EUW3bNkSK1euxNq1a1G
8eHH5wAMPDNR1fZbid90MQ2zL5qFjU9HTapQw80Go5fj3MHNRWAh5oRdVSkpKtuL+EdzcUCknT4JBs
i0ANkqTvALAVkCPTbVVsqtOp7ChY6RKKe7qdDp/
2bdv3+yKFSti4MACNtByZi4J4L57770X586dC63lva1atTrcunXre+vV+13lIRAI+Hfu3LkNQGs2Mz
RDgpmbN28GABDRz5cvX66xY8eOAmGicEhNTd3pdDqdsBBSL1+
+fFHXdZ2Ivka+FO8iRYogOzs7h5kvwpRxOH/
+fP7faJ0QYpQ5DmXKlEG7du1w8uRJ7Nq1628AxsTHx8eHEgrMMbOZORoK4wfACCGEh+xCp5eYORWKW
k6aprU3ZStU4fc8xMXF3ZmcnPwgM9sOSTcDbjiDxe12rwi9UPKdHCYys0qnfheAN5h5obWDDYXEWxV
W9LtkSNDbUs4AdBVC7A0GgythL171JYwKptb00v1EVEIIUenuu+/
GqlWrsG7dOsydO9fbtm3bXJfLddXj8TwQymbp3bs39u3bh48//tibnZ393fbt2/8ydeq/
rq9Vo4Zhd23btu2tDRs2PHbo0KG8Pr/ff5mIXtZ1/asBAwY4ixUrhieffBJLlizBX//
61wUzZ84c3qBBAzz+eMEMxrNnzx6DURTyH5bvesXpdA6OjY2VX3zxRdyPP/
6ITz75BFOmTAnNoSaAFnFxcYiNjcWOHTtw/PhxAOjOzOVDRFFmxrBhw/Dggw8Gx44de+bHH3/
st3LlSvTs2RN33HEHOnbsCABtVq1alZuUlBTVr18//
Pjjj1i3bh369u2LF154YS+M9LykoUOH4uDBg+jTpw9SUlLQv3//
Xe3bt38hEAggOjoa1atXx7Zt26Dr+nvbt2/vP3r0aGtJ+k+9Xq+vRo0aNgG6YDB4RUqp5w/
p1KhRA5s3b8bbb789YdGiRZNC4ZkWLVrgxIkT+Oyzz5CYmPiNw+GYYnXPmoaPX0GEDBm9FYiog6XLQ
0Q/
wK57cwSGVoZVOwZSyr0A4HK5bsrNKYLwcLvdT2ZlZW0G8vbJDczcniw6QmxUZu8B4GPrNdiovHyV7I
UEdxHRyzBCSFb9jxFJSUlfz5kz58d9+/ZFtW3bFlu3bsXGjRuxZs2ao//
85z8pNTW1IwAMHToUmzZtwqhRoy4vXLjw6Jdfftm0meeJqzJy5e/fubXFxcUWRz5tdv359NG/
eHMOGDcPo0aP3fP311w916dIFRITBg1V1Hgtg7uXLly/
Hx8cXMO6Z+fx33333lclLKRBaLlWq1N7MzMzoX3/99dX09HS88847+VOo902aNOmFu+++
+8Abb7xRLLS/z549G6VLl/
6tbt26XQDcVb16daSmpmLlypWYNWvWtosXL54kdVmCmQBSdF0vwHVho5zBMhUHjpkHSikrkSGlcE0I
IeB0OstnZGT825Wsb0TccAYLACQnJ/
fJyck5C4ABTCeiQYqFc8nhcPnnsAEAACAASURBVHQBsFhhlGQQkUvRvpSZ17GhuGjFy0lJSUsDgcAq
WGTos7KyPER0iSxSyYFAIAdG8cS7AGDq1KmoU6cO+vXrx8OHD/e2a9du/
bx584sX7AGNxPP3005g3bx569g3bx569ep1UAhxgZk/
zXcdLF26NKNYsWK7V6xY0a5r166YOHEimjZtihUrYiA2NrYngHIlSpQYlZKSgkAggN69e2PIkCG4eP
HiyS5dugRh8ovq16+PL774AidOnEfCfPn0CaWlpDdq1a5fneZoyZQr27NlzoWTJkkOfffbZ27NlzoWTJkkOfffbZspMnT85f
smC10+mcUKtWLWu1ZjDz1QMHDmwowIIG8Oabb8Lv9+/
+bOHHi62PHji138eJFhOZRsmRJ7N27F8OHD68MC2fK9JIchFoD6BshxF4YvIACc2DmObAXpLsEo9q1
7VrMfHT37t0vAICu6xGD5X8QFy5c2A4AOTk5H8IIPdpEMoUQ3XVdHwG7Dks2gN9gT0Q4xczdpZSLYU
+nne52u9/2+XwLL168WBkAJk6ciDZt2qBNmzbo0qVLEDBrRavHgxAGOtLF682L9s2bLM4cOHdxg/
fjzq1auHO+4w7CNN09oDQPXq1W2cmpkzZ+Kuu+5KXbjkyV29e/
eGx+PBokWLcMst11QL2ABgca1atawh3cuapvV45JFH/
kJ2IcddvXr1GjtkyBC0bt0a1atXR1ZWFv76178iEAjkMnPLZ5999r0ZM2a4rvF4vXnzRYwYMQJ7Xu
au2bNmmNEdA8APPXUU+jRowcGDBiAiRMnYtGiRcjIyMCLL76IiIgIvPTSS3jhhRcwZcoUvPjii5g8
eTIiIiLw0ksvYcKECZg4cSIWLlyIjIwMvPjii5g8eTIiIiLw0ksvYcKECZg4cSIWLlyIjIwMvPjii5g8
StXfktMTDx2PZ//s+H6ZTj/jzFt2rQDQoiEDh06ZKlKlOqjB4Bs/CdOGHYIYKLsPiimcjF/
+5YDC4VvGwzHS73QO8Xu/
XsGeNHINB9i0QMjHDVBuhcNEJIR5lZp2Zv1PMO4OIXlVxHq6BKcycRkTvWuaQCaAzEc2AZUOC4cpdB
GCF4noboqKiuubm5v4EywuXjLpHbcmizgtgORF9yuoSCJ8KISZJKX9UnPBeBDBGweMYy8wpRLQJdiy
HQmXXxDwY3Bgr92MFM+dajUoA+zVN+4uu66ut39Wc31AiGgV7ltg4Zi6p2kQGDBjwz3Xr1rU6fPhwt
OF5zsOvRDSXmVV5l/tgpJraiH4wTr+qlMfxUBRAhJHd1mDVqlVlMzMzfxBC3NW/f/+I2u3/GKZNm/
YBET3frFmz9XXFxcY0VHxkB47lWPUM/
wSINz8yZmqY9YpaauNfy+RVut7u11+udDruIZ7YQ4l1mfl1xn/HM/
JziwNmdjfTfbaokANPL3iEMudQGZj4qhOgnpUyxHlSZ+QkiGgm7Hs1JAINNWoGV+J7hdDobBgKBv8N
SUBdGhWcNltAtG/
L9QwB8o5ji3qioqKa5ublrrPNg5g+JqAfsBuIyZn4ZwBbFO0uJrVu3+k6cOHFk0KBB/
3ZF6xsRN6SHBQCIiKKiopJVxgoR9YVxMuis6LsKO2/gmBBiQDAY/ErxD7/
SNFamwmKsMHMWEX0Ki7Fi3mc91PHEblLKC1JKm+fCvOYwVqjpXgMriGib1VjB/2PvzOPkKMr/
3mqumd4xq6qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
DkGOne/aeo6ue3x/dEzfdNWHWH3HDWu/XixfZrqnump7uqqeeE4AQ4iiE/izx3dNjzHwtG8qjM/
ObqVTqsFKpdC+SC/jtzLxrXFhh5heI6GKtdSKxHjM/
4jjOhRzWA4rf23OJ6Ky4sMLMf3Fd9zYiMglTTyOsfWQSVh5EGM6+mrDCYbrwxQZhJe+67hSl1F2G7w
```

```
oiOo+IvoOk+W8mgE6TsPLaa69d8/
jjj+9x4oknriasMPNHzHyRSVjhsHbIaQiFrXjbTcw8NX4cYTXpkw2fLwJ4kZnPmThx4hUAsMEGG9go
of9NBABIKU3Cym0IgxRMFb+fhaGOjZTyoKg0RLzWz9xsNnuI53nnwBBqT0S/
qyGsXAfgOIOw8kMiegDAI7WEFSLaqV5hBUA+ElbuMmjVT6QwejQurLQjDOC42SCsgIj2CYLgIMSEFQ
4rtgskhZUVUsoTYAjUAPBBOp3evVQq/
dEwjj8iLGgaF1ZeAXAKhRXq6xJWmLl72bJlDwEYtBrXdVZgaWhoGO26rql+wrUA5iJ0MIvjIblT9on
oQGb+Y9zzGsBr2Wz2YM/zzkZSHQ8Al7AhmoSZ/w5D/
o7I2fNJZn7U9LJxWNzrPCRretTiVSHEzSYnUSI6mpl/ZBDo/iWEOIOI7ou/
iJFfz+RyuXwNJeuHzAEwGjXScXOYUCr+IvxLSvmdSHsRDzm+OFqI45mI5wohfhDtNOK/
1UuRacTkXzQHYSn2uBP1+0KI+xA6Uve9To+Ucs9yuXwFkmpvAJjBYZK3TWL9XhRCPABDjad99tln4a
RJk47faaedmk4//
fS+TZ4Q4gQAv433icZxqNb694hNSpG2apLhWbkGwGGmiRShinh3ANMcx9kKADbccMM7fN83hVRbBjE
jRozYClg9SggIn+HGxsYfwrx4vmTQnoCIjtJa70JEB8eaFrmuu5vneXvCXPfsIjYkoYvmyF2RXIhvz
eVyF2itH6FY8ELEndGGqa7K7MzcK4Q4NBJy4qHDFzDzfjCUtUDokHs1ouRvsXNO0Vqvb9hYzqewvpJ
pY3uQ6R0HUBBC7FIqlS6iZNmSRwFsHL8PzLxMCHEAh2n8665QT0SHlstlzzBPDxrWSYHF87yzXNdtM
dgbn5ZSnmsySyCUmBMpjInoAK31BUiq4ZZEuVb2B3CB4XwXIcyauxqRhJ14AaKd8uW9vb2P1tg1TAf
wAzIkEItMO/FjS4joPKVUwkufiL6rtT4MsXwKzLwEwOHR/
Rkea+uKXpjTkcxjsxihv9AOseNtRLRfpFmJCx4fCiH2jwp/
xbUXtwD4clyYYuYlUspDmPneuL2dw7D1n5C5EvY7HOYtiYegL2fmX5s0VkKIw5VS36WwyGScvyEUGu
Nq0w+I6Hzuk8OmD7O+8Y1vvPuXv/zFmTFjRl//mGI0Yf7OJKRGPgQ/
pGRW5icodL6N+x3cx8ybIhmyDiI6jYgO7/
M3AEBrDa11MvWvZdDied43W1patgOw6lkEwncsnU7v1dvbewuSad7fZ2aTef2XWmsXSW2ML6XcRWv9
JSJKaGsB3MbMR1CUAK4Pz1BY/
Tm+2D6Uy+Wm5vP5uw0bpqpmcygMUTK1IKLjtNYXIuZ3iLDMypi4kBD1ORLAL5A0o4OZzxBCrKQw82x
f2hAmbTS9ZwdH50tEezLzHkqpoxArgsjMc4nIQ3JO6xFCTFZK/dpglgczrzBcH8x8aTab/
UfkimAFlv8WXV1dowBcCPw7z0TEYtd1DwyCYAbMyeFMWovDtNZTKZmhsSuVSu1aqVQ+B/
Mu5I8cZiaMR3+8S0SbGTQXj+ZyuZMQxvab1PMnEdGRNXxx8obrdEopT+cwG2PC90NrvS3FvMmZuctx
nAMibcxn4hcRQuwDYFsiOj3WrwehsJeoRsrMe0cVTCfEjncJIfZUSl2DpND0dwAukvkPilLKfZVSVy
OpFn3fcZyjYDaZrEBYXynxG0b24kSBL2b+ntZ6BwDfMrTNJaJ3kSwv3ymEmA7gD4Y+bzLzq2edddak
eAXYKOT5XBjueTSOvQ1C06vMrJHU/
LwGYEkNIesCZt4EfSbmqsBSqVTyjuPEd8aWQUo+nx8H4G6OUj9UnwNm7iaiPSqVynQA2/
Xtw2Gh0REGrd3tzDzbtFEAsK9SqjEe0RLxBDNvbdiAzYvmlLgj7cuRNvsqiiVKi3iQwmrOplxanRw6
CceP/
4CZjzRc6wlmbkPS9wRE9F1mPsTQBwCuTKVSD7AhpQWAd2AQVpj5W9EmYjtD2xQi+gKFPnJ9WQDgKRj
SalCYn+kQMleHf42ITJmt5xDR477v/2njjTc+yGpY/
os0NzcvI6Idtda6zy62l4j2rVQqB1EyHLQW5yJMtJXwQxBC7FWpVFytdcKHgsNKzxPj5iNmXgqgCcl
dy+u5XO4Az/P+CMOij9D/
ZRIMNmNmXg5Dng4hxClKqcsRE8I4jG7KmB7mSIA4n5IJxwBgKjM3wexp3g5zYqO9IyFrl3iDlHI/
Dsunx0PwXiail2EQFCgsgfAdg1r0IyI6MAiCmxG7t5FW5f64mjrSanwbwIWGCfja6HrG4pdEdBczf9
8wvsOVUpci6ay9jIhmmc7HzD+PBKPEZAXgWiJyiOjoWJ+PmPllg1CyksMCkqaCdLcLIR5D6GTed8wA
gPnz5182WFNxW5JIKbuY+dWqwFLd2BHRtwC0cNKPqp1C4hrA2VLKy2CuvXYEwjo3jxp8KF5j5iaDSa
eAMM1D/
NlenEqldvd9/2SYn+85CKPhEv4xHCZMKxvGcC2Arxrmk7cQLuAJMxURXaK13hoGoQjAvel0+leVSuU
hJOfd92De0P2AiMYDMPmgnSWEKEfj7Es7gOvjG8fofGcQUStiUYQRLzGzg+R64XGYcuNvAPZJpVJjh
BA53/
fj69SgYJ0TWAAgm83O6u3tXcLMFQAgomO01uuhztAuZv5D9JCZTD2HE9EiAI8ZNCUvIkyiFLcpdlCY
fTBuxljBzLv7vn+RSYigMM3zBjCUEuCwGJ6pcN0pWutz4gITwoV7AQzRJEKIg6KkQrsbzneuEOItZv
6zoQ2G6wDACRxmDjb59RyhlNoLyToli6IF96x4Bw4djXfi0IenL20AduEwN0k8FwSI6FaTwCmlPEJr
fSZiKudIu/PP6L7Hx9CJMOrmIsN1vs3MJxt+9y4iug/
m7Mr3IFwIEuNj5keY+Ynoen2P9yCsJH6Uoc+PAJiy7z4F4BytdSLXUFVgWbFixTJDP8sgJZPJ+K2tr
bt0dXW9DqwSWM50HOddGNIUICySGDfpvgvgxCAI7jXMgz9zHOdhZn6E+tTgiVjMzG0UhfPGeBixuY6
jzOHlcnkSIs15jFcj7U7CP4bDiM+PkFyk70VYHDeuVVwphLgdZh+4O5m5RMkSA0CYdPPoYrF4Hww+I
wZzLpj5UinlQhiSmSKM6pwdf2c5LAdzvqkPM98khJjLBn9FhPnGlhoERBDR9xH6RQIIzYNaa6G1Nmn
MPvWskwILAGitK+3t7c/kcjkiordg3gUkYObHhBA3mWyuRPRjx3Ee0Vr/
HUkn0Q+IqNP0IhJRG5KROD1ENImIDoN513AdM+dhWPQ5jBrRSPrcXMTMU+OLdyRI3Y/
QThof2+la6y/XeBGvA3CrUup+Snrq1+JXCF+OxKJPROdxGOobd/
BsB3BBDUHhDwCa43049NvZCcAPYMgGyWE+l0SWKCI6Vmu9PyUdB/
8lhLgGZhMfhBDncpiSO36+nzLz1+M7tajtHpgLEL4khLiFDJFbAF6TUl4C4GbD+S6rofk5iYjOjf9G
zPyW4zgHArgDhmJ15XL5kuhzg1YFbKnNihUrXmTmipSy1XGcm4IgeBjJiLduJOeZfLTButWwYbkzl8
tdVKlUHqakD1oPgDeIyBSV9CcYNKtSygMBjIW5zMl7AH6ota61Ef0XgPF9D0Rz4euIbdw4jJ4zBkkA
+CfCyscJzQUzv+c4zj5a6z+QwWekBnc6jnOHUso01zwI4BoKo3tWe5+J6CcG8xAAzCKiS9icMuJtAI
8B2MvQ7xSt9QmU9CFCqVT6QX1f5dPFOiuwMDMppbry+fxYrfVDVEcVY2Z+U0p5tskGycw3ZTKZ3wVB
```

```
8CiSkSGdzDwP5jTK7yPp0AUp5X4IncMSO3aEnu5zYJakOwHkkQzN/
TMzf5GSzmgfENFlSKoWAeAKrbWAWYV4vxDiLIS24XqzHt5ORDPZkDkYwC0c1hVJRMJEwogpguBJIcR
8ipVNYOZux3F2AbBn3GQScScMIesc1nHKIqbdiUxr52qtjcIKgDM5zLcSV4nfFtm6E4JRNHkkVL0c1
hU6Q2v9B0PbCiI6TWv9J4OAeCHMGqsLEE70cYF4BRFNDoLgfCSdg8HMf5g1a1b1t4jXtbL8byCIqGf
YsGG9kSnDFLofz0lSZOa9mPk3SPqSPcPM0zzPu9e0eBPREzCncniQmfc1fP4YhJGbps3moqj9ZjL7X
DxFRP8XO7aAiP4CgwZFCPErZk4c5zCR4x0wz9NtUsrJSqmzYa7abuIJIcQPa2wCX3Yc53SEQkvcvP0
zZj4eSeFxnuM40xFqjUymqIvRp9p8H65CmMn9q7E+vQDw0EMPDUoT8TorsBCRjGyAf69htlgNDkPBD
o8yNMZ3GX/P5XIn+75/
P8I8HnGeIYOvBsIMg+PjB6MHDzA4iSJ8WI2hyABARHMp6cT6IgCmmGMpgHZmPpuZE8IKh2HGL5kECA
AvZbPZw6L8I6ZaSiaeYOazosRLcb+QJxC+9InvS0THMvNPkAxRXgBgNscieDj0R5ocBMFGMJjsInPK
DnGbNTP/
AsCbca0Gh1710wHcYLBzA8CVHDrZxVW9T0Xf6UpDnyfJ4BjIzL1SysOiukJxR+luIcQhkWYoPildFU
3o8bDm6rOayMwphNgVoW+MSXt3L4DFY8eOHQYARGQFlv9BiEgwc8n3/
bvq1Q4IIQ4HcLxhrlnguu5+AG6qMRc+AUP9Ig4LfH7VMGdcQERPaa0fNWw226SUBzHz9TCEFQP4JzP
HN24FhJs2k5n/
11rrkw1zxgoiugrmFBgQQuyutd6VDT5tNXgjlUodFuXYims8F0oppwRBcDdim1Eiup6IdoiblqLN64
GVSuU2JDfF86N5zZRgdJYQ4l4YNqpLly69FQCCIBiUc8I6K7AASI0ZM2bb+OJuIjLPHBzZ7RKp0oUQ
h3iedyvMzpFPmMwBCP0rTDHwv5ZSvqSUMoVWPy2lPJ8NCdsiHkYsdJjDUOTXDfZYADgZwGWGhfgZAD
NrCEUfuK472fO8y2pMPAmY+a1UKnUogL/GhUMOM0j+wvSdiOg0Dr304/
e8A2G2x8SOR0q5LzMHRHSnYShPENEmlMyncIXrurci1LzEOZXDqscJkwnChX0cJR2R50kpz2Tm2+Id
oh3Z9vHjEUcppc6CIXxRCDE1Cp+P34u/IHT+jgupzwohZsOsdTlIa90Is3lrDoB9iejHn//
85x8FgHQ6XV8JW8tgQ6RSqSaYzQUJOCwqu2nc74qZO1zX3bNSqfyCkskXgdAEYzLbvkehk2jcx+Qu1
3Uv01o/
BkNeEinlHkqp38VN39E55wLY1GAevRwGLQkz38hhDaX1Yse7KExRYNrQAcDeWuuRCHMefSzMvIyZJ5
fL5euQ3AS2E9F+Sqmb423MfDeHAQ+mtWcKgF8ZhM0PiOgAZr7RIOwtIKKfKqVMPol7dnR0LAaAqKDt
oGOdFVhc121tbGysayKO8mCcFv/
hOaxSOllrfalpx4zQmcn0InbDnFDoz0KIGVrrhw0P0kvMfELkxGba6c9CTJ0aXefvZC6SdSIznxM35
zDz20T06xoLvielnFSpVI6LT0q14DCZ3K7lcvl3hoW9TUr5Ha31nYbv+8vI4970Ij6GUNhaDQojvN6
nMMtlfBwvIBQ64jbrm9Lp9AVBEJiS8Z1NRCfCHFL8IsLKx3FVtSeE+JZS6laDlmQZmZNZgcKCjl+rI
dx+R2t9WNyvhpmfJaJ5SC4o7wshfs2G8gzMfJyU8j3TPQLwNIfFEAEAQoixUR+T87ZlkJPJZD7X0NB
QVxZUhAELi2HQUEgpDwiC4DgAx8fbmPlDZk6YxDksnFhC8t17xnGcE8vl8gPxNg5r+kwOguBMmM2c7
xFRDoYklABMWpAHiGh8XHMRcT4zX2Aw2wDACUS0hJlNc2gCDoMuJhHRyTAIh0S0v9b6R0hGgs5GWFc
skbWbiE4loiOQ1FotllLuGs0Nn4mNoxPAyVFG38RcCGDcZpttdgwACCHq9Vn8VOEM9ABqUalUypH3e
+pjPnoKgO0oFqUTSdiTEarNjjL0W8jMm1EyOV3C7hudby6A72mtn0TS4/49KeWUyK5pShr3PBElTFE
Ulis3RZn8AmEdjXjUynIhxFla69vi4+bQ6WxPpdREmP1JEjBzRyqV2qlcLh+HZF6SXgqzXybUthzmh
+mgsD5H/JxzTbs0DhMyPaG1fh5J08i7RJRF0rdoZi6XO833/
dlI+vz8DsAuRJTIpxBprR4C8OPY8SIR7aOUuoiIEn5Mpt8u4k6Eux5TSYXfIMxWGY8SWyyEmMF9ikF
G+EKIE7TWprIJP3cc5x6l1HNI7kxnc+hDtMrnh/6df2NQ7qYsayaVSm2glKrno/
cDuIPCauCrQUTHKqW2I6LvxdsiTWkmbu6J3pXlSJrXF6RSqf3L5fItJhOVEGJvrfXBhncFCEtrlADE
zSY3EtEx8Tk52pCUiChhpqLQkf4Mw6IOhFqah7TWz5nmeRNSyv2ZeWtmTkRAAjiMmQ+gZLqN16N50p
QI8wZm3j7eh8PEmjsEQXAuESW0vER0AoArDNqkXwDYkYh2q5YLiarSv1/P9/
s0sc5qWADQRx99dDVCB1UjzHwZM5cMNkgVOcUeD4NDJYACm5Mo1brOEiHEgZGAEXdsWwxg58jLPJEY
jpnfIaKNkHSoegzmejm3E9FnKZbLIPJrmBa9wIldlRDiEMdxGIbolBoERLSHUupzFHOKjTga4cv9md
g4/i6EuAdmJ7Z2g5YGAGa0trZerJR6EElzymIiSsWPM/Njra2tUzzPuxtJ58C/
ITT1JExekdbqMiJKVEsVQhwG4JD4vQUAMnjaR+d7MXrOEhmHOXTMfR8xp7hoDCdqrS83jGGKUuoqJH
1+7mxtbf1JEAQPIHmPZjHzPIMmbj4AVCqVulYty+Bi5cqVcwCs/
JiPvUxhZIop3Pk3zLxepD00kaqxqL+NmLBSNSuVy+Vfw5xeYR9m3ryGv0g7hwki4/
mgZkXnigvvC4no+Rrmq6uY+aj4oh6N8c8INUz9CUQ4XCnVa3r/
EdZKG4+kNnkxgHNMwgrCHDFjDMLKMsdxdlRK7VtDO34CwpQRG8f6/VkIUabIJ6m6iVl//
fXv9H2/7rT+nxbWZYHF7ejo+BcZEuxE/JWIHqewUvFqENE0pdQ3YTBLcOgl7/
ZDWOmJdgYzkHxJlwkhtieii2CuV7EwWoxNORBM1TSfIqJ3YM6A+AOt9VUwJJojotOFEG8ppR7Cx2uk
qkwVQvTWCM07h4hOQtJW+4zjOD8xFUGMMGUbvj+Xy033PO+2uMkEQBszCySFoseqlWENQskbzJyvMV
lBCHEhAJMm5Eyt9XDEkq99DIsAHAlgZryBmZ+XUt4GQ/SWEOI7AC41CJaHa62/
T0Sbxs71j2w2e1QUnRG/R09R6Fx9VPw6QRBcHfW3Gpb/
QbTWTltb20MIq7KbWAjg25EfVTxq5R4iWgKzEysAwGROYebnKBm9AynlgZVK5QgYsssCOJTCldQYvs
zMbxk2OvMQai7jPnUdCNPum3Ij3c3MO8NgIgbwZC6XOzISWuoNRDiTmZ+mMBdT/
Fo3MnMbJ8OofSHE0cxs0qwsBdCApGvAEsdxvqmU2owMqSEA/
AjhPBTfuP1TSnkd9wlsqAosXV1dd2Sz2YX1fMlPE+uywJLK5XJNzJzw8Gbm5zmsIWN6UX+ltc7U0Bq
AiBrqVQVGnz+YmU83+C7kXdfdUWt9LMJCWnHamLmEpEamgLDGRVzF+R4RXc/
mar8/47DQYbzuDABcLaW8VSmVyMGwBs50XfcfSql7KRlSeB0z/
x+SRRBfl1J+Wyl1Vz+EvbnZbHZKPp//GWLaJA5TbTPFUnsz83O5XG5v3/
dPQTIHSns0YR5V43qXaq1PMaiwbxBCvGQSbtcw9m4i2peIrjHc93lSyh+a6jwx8/nM/
```

```
F0ktSTnMvNXkQwLfR3AAaZq4QgrVz/CzCZ1/XP33nvv76M/
rcDyPwgRpR3H6WDmRDhzZLbZF8AMJCMdXxJCPMkGH6o1wcxvkiFPFTNP11p/
Fuaq9sdKKd83JT6MeMogpBc4zC2UqPUjhLgY5jQOT1Poz2LScr8FYF/P8640aWVrcFUul/
tNpFWPm8QfkVI+SES/
j3ciogMjk3NCgxMJgHETdl5Kub3WurnGenYlgJ0R2+Ay8ztCiNO01onAAQCYM2dOYmyDgXVSYLnpppp
syALD55pv/
FMld+8Lm5uZjANwT3wEw8z3M7JM51LffUJjka3skS4x3AdhRKfVVGCJhmLk30gJsGm9DaBOOC0w+hf
k7Eg8Zh5FAx8QX9oiHs9nsmUEQPAJDrhgTzHxDLpf7TblcfiC+EDPzY8wsDNqLxQ0NDZODILgdhkmk
xnU+TKfTexYKhSkm80ykfUhonoQQkwuFwu6IZYmN2u+poS4Fwoig3Q323ceklFcrpUwq8ZpEdutjkX
QqzjPzt5VStxkEt7sQCnrx+ko3I/yNT40dX97Q0DAZwM/
iQhiHRTZvgzmXT48Qom+SrkHpYGdZM8w8ety4cXvW0HhUHUHjmtzFRPRXDiPr+sMimJ3bf0dEHTBoT
4jodCKapZR60LAxqjram2rwSNN8F20GTJWh3wbQDGArQ9tyIppMRKeQOedTAma+O5fLnex53p+Q9NN
5FcClSqlEigchxG7MPK2GWRxI+u71Sil3V0pVTOkkIo3R5kjWZVsuhJimlLofMWGqs7NzDgBIKQflJ
madFFiam5s/
BwBSyrj5wxdCHNTV1XUXJUNf5yDMwvibT2gY1wJgxCqYRv4Jk4QQo9hc1RdEPoMfDwAAIABJREFU9D
4ZQvbWwLcBXB1/
qZn5cSLazqRZYebns9nsQb7v3wpzIa8EzHx3a2vrcb7vX2eY5F5FaF89NnZ8pZRyp97e3jNME2MN2l
Op1KRyubxLrXtkGNuHAHbRWk8wmZw4jLg5qkb3p5l5qGF39ZqU8uwoF0RdWiEgFFSjkMfVTIqRoHAI
EV0Xf/6YeS4zO5TMAvqGEOKviE3oHFXPLhaLUymW/
TbStt0Ec7JAIPQ9uH3SpElVLc6gnJwsa0YIsWljY6OpEOxUrfWuZA5EeIQN1c3XRORfMtTwDj1ERP9
AmOV2NYjoPCHEHyPNryni8l2Ya5gZ/ckiwWi/+LmieaMbhvxaHPr9TQbwDYPpphb/
zOVyh3uedyaSmXsXR5r7mYbN8hSl1JaGPjURQnzLcZwlRPSEwfTVSUSbxjVCHPpTTmbmKwxanIsXLF
hQTZo6KOeEdVJgGT9+/Axg9bLp0d9TlFIXUDL0dB7CSpamtMf9hpn/
QUTPcBj7vxpSyn2JqKdGBVMgdMI0vog1mIowzfRnYsffIKKNYUhcB2C+67p7+r5/
IQx1impQfRFP5FhNHw6jah6mmPNdNMHtxsxbxRfVNUFE+wZB8FmYE+uZ8AHs6jhOmohMGSTzMOyeIu
ZzmCBqNUGBwyKDJyil7kXSaW9NXItQAErYoIUQh0dZMeM28DZEuRNiY+gloh9prROO0FLKAxDuLi+I
9fkQYRhnLWHlYYSO5F9vaWl5Mjo2KCcnS20WLlx4LTNTfI6MtJnNiG20orYX4u/+xxHNARJJc/
MbCGvmmMwYF2UymV8rpf5G5jo8yxFmaa2rpASHSTJbEZsDokXdW4NG40CEvju1fO7i13lTCLF3e3v7
NogFFUS+M2dzGPkzNNY2XUrpk7lUhxEiOjWVSr1QLBafhGGOj66x2joSCXnbMPOZiPmzMPOfU6nUb3
O53Pjo70E5J6xzAks+n7+hVCptAawusDDzNK31VIMN0mPmp2FOwAVmfpb75K6og/
lEdEOkxl8NIjpAKfUOh0XBTPkPPJgFjFr8ipk3QdIJ693IFPQZQ592x3H2rFQqU2FwKjYR2Z738n1/
Z4Qpnfu2dRHRGTAULRRC7EVE7UopY9ZeE0R0pNa6gZnvrXNs3VLKya7rroh2YybhorWGSrmDmZ+gpM
d9t5RyKoA/GHxkXkD4O5nG8qgQ4teReja+gzqewwRVJhv4c/
ExRJzLzL+hWHglER3NzGORzMDZJoQ4B8ClNcbXAeDrfcxewwDAdV2bOO5/
iEKh8OVyuTwdSMyRN2utX4Q5GdqZzPyxSTjjEFEvko7+PjP/nJnviL8nRHRJLpc72/
O8W2CuUN+DsLZYXfljOEwnMQdh9ej42PbkMLzZNO4jASzRWtc7Dy0DMNl13cYahUZP5LCcQTza8wwA
D5rSFKyBK1zXnVksFmfFBTpmfi7SaMXH905HR8duvb293y+VSof29PSgq6sLHR0dyOfzr8yePfsPix
cvnjN69OjpAKC1rjf44lPFOpeHhYje3WCDDfDmm2/2fRmvEEKMZGaTB/
o+ruuurFQquxtUZO87jvPdIAhm9T3IYT6OWxBLlBSZe6YirOQcH9dRzPw4QrNJrZA402I7Kzoel4jv
aW1tPdfzvPtjny84jrNnS0vLPM/
zTkZMaBFCHDhs2LC3Pc8z5R95DsCWMdXtB42NjbuWSqXPMPNd8e8F4OBcLvew7/
ujmHnVQklE+2az2Sc9z5tjUNEugKFuCcKd1T2e531oaLsKwFuIpcKXUu7T0tLyfD6fv4zCEMH4dzoO
wAla64nMDGauHkepVLowlUr9qnq82tbV1fWDxsbGy4ho077HtdbLXnvtte+PGTPm67lc7qLoGAAgCI
JFb7311rUTJkz4BxGN6nvOQqFwC4Cdm5ubv1XtU20rl8sLHcfZs+8xZkZPT8+rWutjm5qaNlFKgZmh
tUZ7e/vzvu/
vOHbs2G9Xz1Xtu2LFijeY+dhcLucQ0ao2pRSCIAiUUs3MLIIggNYao0ePro69bLjflkFKJpOZ6/
v+0ZlM5qbqHMnMjzmOc1UQBE8Yuvw6l8v9xvf9ZRwLz2XmTsdxdlZK3YGYH1wkhG/
DsVDkSNO9ocEX74psNvt9z/
OuAGDKtbIS4YYw7ri7EoZM1ZVK5cPly5cfPWLEiOeB1d+7fD5/6nPPPbdyyy23fGzkyJFTAAypvsuF
QmHGSy+9tPirX/3qLalUali1X7U9/ncQBMUPPvjgDz09PYeOHz/
+ZMdxRvSZM9DW1vZAe3v7tmPHjh0ihFjVt7Oz8+WVK1duOWbMmDOllNnqcWZGEASVYrG4qKGhYTwAV
PPllMvlQldX145DhgyZLoRI9e2jlKqUy+XxQoghUspV737EZgjnXRNfBHD/
smXLsNFG4bQ8YcKEIxH6wA0qklnT1gHee++97z3++OO/lVL2/
cHqRkpZfaiKADQRpaSUq4SzKK4+AOC4rrtq5x4EQZfWuuK6boMQohEIw8SCIOhSSvUCgOM4GcdxVmU
WJSIwsyoWiytd1x3mOE5fYSEoFovLhBDpKH06AQAzl3t7ez9kZiYibmhoGOE4zjAA6O3tXaKU6mFml
lK6TU1N44jIjRboFZVKpYNDx1hyHKcxlUqNBEBa66BYLC4XQqRSqdRwIiKttS6Xy57WWjuOM8RxnCF
9F3ylVI/
WuhIOg4iI0lLKlFKqrLVWFEo31qFz3aATQKmhoaHFdV3XcRxkMpl5CxYs2ISZXz3hhBO+ONADtPx3u
f7665dJKdcrl8v1zONFAHAcJ41oHormth5m1q7rDgkPhadSSnVX5yHHcdKu67YAUEEQdFcqlU4iYsd
xmlOpVAYAgiDoLJfLbUKIxnQ6vZrAX/1PKVVkZjuf/P/
R47pug+M4gohQLpeXBEHgp9Pp5ubm5nEtLS3O/
PnzscUWWyzYdttt6wrE+DSxzmlYAGD27NlXf+5zn2tauHDhF7q6ukYAUE1NTdmhQ4d+UUopiA9vb3
```

```
zfN9/lZkVAOW6bsPIkSO3T6VSOWZGW1vb/V1dXYsBaGZWuVxu60wm883Ozs7ZS5cu/
Wf1zRwyZMhnWlpavtje3v5KoVBYSESoVCq0/
vrrf3XYsGHf7OjomLNs2bJnAICZqVKpYNSoUXs1NjZuWqlUljKzamtrmwUgX6lUMGLEiB2GDBnyRa1
1ZenSpXcwsx8JXa3rrbfePkQkP/
zwwzsA9FQnh2KxSKNGjdomCILOzs7O16v3QWtNxWKxcfTo0XuVSqUlnZ2dz/
a5TRQEAVKp1MiWlpYJnue9DKBDKUXlcjmVyWQ27e3tXcph1BSCIKBhw4ZNaGlp2QYAurq6Xm1ra5sL
/
HuWYmakUqmR3d3dVZXkqolw+PDhExsbGzdbvnz5A+VyuQMAWlpaxre0tHxJKdX70UcfPay1VsxMAND
Y2JgdPnz4LkEQtC1fvvwprTVXz5XJZDbXWhc7OzsX9r0GM9Pw4cO3TqfTY4Mg6Fq5cuVTzKyrbZlMZ
rOhQ4duWSwWl7S1tT0HAK7rDmttbf2GlLKpu7v7Xd/
335BSOrlcbmI6nV7lyFYoFF6KnodV37e5uXlcc3PzF3zff7ZYLHoAKJvNblF1ZFRKdaxcufKf1bE3N
jaOzGQyX45+m96VK1fO1lqrhoaGXEtLy5cjWz9833+2XC53EJGby+W2dhwnUy6X857nvRQJhmLYsGG
bNDQ0bMDMKBaLH7a3t7/d915IKRsymcxWUsoGz/
PmBkHQAwCVSqVxyJAhX9Ja9yxatOgWhGHypgKJlkFOEAT7U5gRdTLCeU43NTUNHzZs2JZCCFEsFhdF
84ImIh3Nlan11ltvB9d1M52dnS/n8/
lXiUgLIZpGjhy5WyqVyvb09Ly1dOnSWdWNjFKK0un0eqVSqRAEQXUjQ5VKhYYOHbqZ4zjDV65c+SwA
UkqR67obVecZDvNeOb7vP9PT07OMQ78bOXz48G2klEN7enrmtbe3L5BSutlsdmIqlVoPANrb2+f29P
SsiOYTcl13SCaT+VKlUmkrFArvIXyNKWoXQohUU1PT6O7u7kXVcUf/
d1paWjaXUg7t7u6eXywWPSKihoaG4alUanSpVFoWvfvVeYHS6fTwdDq9vlKqt7u7+wMA1XMRAJlKpT
LlcrnQ9zpSyqaGhoYRzEzlctkPgqCnej4pZaOUcki5XG5HGMhBzEyu6w6LNqM6CIIuZkb1fEIIh4iE
1jroc+0GAE2VSgWVSqX6GIwFMLZUKqFUKmHrrbfuXL58ecOCBQtMie4s/03y+fzXPM/L5/
P5eH4OAAAzN+Xz+Zme55kyyML3fVPdm5r4vr/DGtp+nM/
nTamf4fv+9u3t7QnzUEdHR6vv+7WcR2vieZ4pIdt/RD6fnxIVguwXxxxzzFannnpqIX7c9/0Na2VU/
E/Hbbp3VfL5/Nc5LCa2io6OjtZ8Pv9Tw/XP9TyPPc9LOE9X8X0/Ez/med4Jnufdb/
pevu9v53neVfl8frXcEYVCYWI+n7/
L9/1E1tB8Pn8+Myds9r7v7+B53tOmNgBg5ob29vZE3gvP875Qq4/
FUigUvpTP52s61+bz+WG+7ydSDTDzUM/
zfvFJjMHzvD09z8t7nrel6R2LrpfIh+V53oWe5yXyuQDmdxUAjjnmmP2nTZvm1xoLMzd0dnYmTE5rm
p8KhcJO+XzelPeqJoVCYaNCoWAyhdUcl+/
7F3d1dcUjXv9jCoXCl3p6ekwpMCwDwSe5eFvq57DDDttw2rRpxYEeR3/xPC+eAM9isfwX+G/
N1dOmTdt12rRp7f+Na1kGlnUuSujjyOVy9sEcAIQQLoCegR5Hf8nlck8P9Bgslv9F/
ltzdblcFhwWf7UMcj51AotlYHBddxjMtYIsFotlwJBSDjVEMloGIVZgsdRFV1fXcmZeMm3aNCu0WCy
WdQal1NsAvFNOOWVQJkuz/BsrsFjqIpvNSiIagf4lxrNYLJa1SiqVcgFkK5XK+h/
7YcunGiuwWOoiCILG8H+B1bBYLJZ1BqVUIwCttbZmoUGOFVgsdSGldJhZxRLjWSwWy0AjAVSIyJqEB
jlWYLHURZTISCul7DNjsVjWGRzHcZmZgyCwc9Mgx/
7Alv4gpZRyoAdhsVgsfSEiIYRYJzO3Wz45rMBiqYsgCBQzryQim+/
AYrGsMwRBUGHmFdUyHpbBi5VILXVBRIKI1tNa22fGYrGsMxCRQ0QjiYg//tOWTzNWw2KpCyJS0Q6m/
+WzLRaLZe2ho+r0wUAPxLJ2sQKLpS6EEExEUmtdHuixWCwWSxUhRMDMXUIIOzcNcqzAYqmLSqWiAEg
hhN3FWCyWdY0W68My+LECi6UuiEgB6GHm0kCPxWKxWKpEc5NQStnN1CDHCiyWunBdNwAwVEppJwWLx
bLOoJQqM7NvTUKDHyuwWOqiXC6XET4vlYEei8VisVSJTEHDhRA2IGCQYwUWS1309vaWmbmnVCpZk5D
FYllnkFIGRESwm6lBjxVYLHWRTqcDImpOp9N2F2OxWNYZIr86r1gsWpPQIMcKLJa6SKVSZQBkHdssF
su6ROR0O3zIkCE2SmiQYwUWS13MnTu3gtCVxe5iLBbLOkO0iaJSqWQ3U4McK7BY6mLu3LkVZm5IpVI
00GOxWCyWKsxcAQDHcay5epBjBRZLvyiVSu5Aj8FisViqMHOFmXthnW4HPVZgsdTFtGnTmohISynHD
vRYLBaLpUqkYRlSLpflQI/
FsnaxAoulLoQQzQCKqVTqywM9FovFYqmilLKalf8RrMBiqQuttQRgvfAtFss6heu6LQBYSjlyoMdiW
btYgcVSF0EQEICPtNadAz0Wi8ViqeK6boaIOoQQ2w70WCxrFyuwWOpCa60BjCEi+8xYLJZ1hiAIBAA
mIh7osVjWLs5AD8Dy6aBaEVUI0TvQY7FYLJYqRCSYGbAm60GPFVgsdRF54nMQBF0DPRaLxWKpIoRgA
B0AigM9Fsvaxar3LXUReeKniKhjoMdisVgsMVqY2Sa1HORYgcVSF4sXLy4xs8fM/
kCPxWKxWKpUzdVEZMuGDHKswGKpi1mzZgVENFwI0T3QY7FYLJYqlUpFASgHQVAa6LFY1i5WYLHUDTO
jp6enZ6DHYbFYLFVc19UAmoQQVmAZ5FiBxVI3RASttXVss1gs6wxRtWYBwG6mBjlWYLHUxbRp05oA8
NChQ23xQ4vFsi5RgRVY/
iewAoulLjo7O4cCaFdKpQZ6LBaLxdKHShQQYAWWQY4VWCx1MWTIkCYAzcxsK6JaLJZ1hnK5HBDRCCm
lDQgY5FiBxVIXROQC8KIkTRaLxbJO4DhOGQD5vm8FlkGOFVgsdRHVEsoxs01/
bbFY1hkcx1EAMHPmTFs2ZJBjBRZLXRBRJwCtlLKhgxaLZZ0hnU47ANRAj8Oy9rG1hCw1OeaYY54WQn
yFiAIAgdY65bruK8cdd1xFCMEzZszYYKDHaLFY/rfp7e1tFEJY37r/
AayGxVITZv6FEKKdiJqIaJgQgohopBBiLDPbHY3FYhlwtNZDAODggw+2QssgxwoslprcdNNNjzDzv2
o0P/1fHYzFYrEYcF23AUAbACuwDHKswGJZI0qpKwGs6HtMa71Aa/
3rARqSxWKxrEIp1Qggl81mrYvDIMcKLJY1cuONN97DzPP7HiOiB2644YbXB2pMFovFUkVKmQIAx3Hs
ejbIsT+w5WNh5quYuQAAWuv5HR0dVwz0mCwWiwUAtNbEzO1SSrueDXLsD2z5WK6//
vpbiWhh9Of9d95557sDOiCLxWKJEEI4RDSsu7vbJrUc5KwTAkuhUMjWasvn81/zPO+w/pwvn89//
T8ZBzM312rzfT/zn5xzsKCUulJr/
WG5XO6X74rnebf7vn+U53kta2tscT6J32pNz+TawPf9jOd5J3med21sHBPX9Fya+KTH3tHRsannebP
```

```
z+fzYT/
K8FssngVKKAQitdWWgx2JZu9DHfeDaa689iIg2AVBk5iKAEoBic3Oz7OrqqhacqhBRSUpZrlQqpa98
5StfmDt37mwpZalUKpVPOumkLgDI5/
MzhRBPZ7PZy6vnb29vzwVB8CwRzYsOHZrL5doBoKOjozUIgpcBjANwVS6XO7naL5/
PHyelXKi1npjL5S6oHvc8b0tmfpaI3mHmfVtbWxdX2wqFwsSWlpa3iagr/
j09z7sSwHZCiH0zmcyCWNvVALZraGjYramp6cO+bfl8frIQYkQ2m70lfs6Ojo7NiSg/
dOjQlbHz7QFgejabPSJKyLYK3/dPlVI+MmzYsHeqx5h5qOd527S2tj4Sv0Z0D7/
a0tLynKnN9/1MNpstmNrWhO/7O2Sz2Vnx457nXQFgad97Hh0/2XGcx4YNG/Z2n2M/BPDLPt/
jkNbW1ruqf+fz+Z+6rnvFsGHD8n3P1dHR0VqpVEa1tra+YRpboVAYn0qlivHfwvf9n2it3wJwAxEdn
svl/lbPdy0UCtlMJuNX/+7s7BxRLpdfJ6J7Adyby+UeMPXL5/M/zeVyF/d9ntrb23MtLS2e6fO+7+
+TzWbvM5znawAeI6IhABAEwROLFi06vLGxcVxra+ujSqn333nnnUMXLFjQWSwWpRBCbrvttpPL5XJX
U1PTdsxcmT179nVEJEeMGDFywoQJd5RKpSfmzJlzJcLICQFAEpEkIjlmzJjPL168+F1mFkQko7aGxs
bGEcOHD//
G4sWLnwPQwMwNUsqW0aNH7w9gaKVSKff29t7e0dHxw+nTp39Uz721WNY2xx577FeEEPcXCoX1Z86ca
dMtDGLqEVh+TkS7AUgDaADQIIQYKqXMBkFQYWa3vxcVQmitdZGZA8dxmhzHcYgIRAQAQW9v73JmLjU
2No5KpVJNAEBEUEr1dHV1vZ1Op5ubm5s3rfapVCor2tvbXycitLa2buM4TgMRgZnLhULhmd7e3hWu6
zaOHDlyVyllqqOj41nf999CmB1R53K5zXK53PZEBK11qa2t7b729vYPmFmPHj36/
zKZzE5CCCilOpYsWXJLV1dXGwC0tLSMHT169JFCCMf3/QeXLl36QvU7ptPp5o022ug4AGrhwoV/
7O3tbQeA5ubm9TbYYINjiSiltS4tX778Ts/
zFgDAyJEjtxo+fPh+WuvSihUrZubz+fcBYOONNz6ksbFx897e3jfnz58/s+
+9HDp06Khx48YdU6lUli5fvvyhjo6O5dW2IUOG5MaNG3dMR0fHP5cuXfpM/
HcYN27c9itWrJhbKpVWLbiu6zYOGzZs3KhRow4tlUrzFy1adFe5XC4BwJgxY7bJZDKTAKC3t/
e1+fPn3wMAY8eO3a6lpWVHrXVp5cqVf25ra5vX2tq66ahRow4FgDCrP8DMyOfzD61cufL1UaNGfWPo
0KHbMHNnW1vbY4VC4UNmFkIId8yYMfs4jpNZsWLFIz09PXlmJgBCStkwcuTIHYioEYCTz+dnlUqlHm
YWw4cPn5hOp8cxM6r/
dXd3v9fZ2fkBADFkyJCx6XR6VEdHxztKqTIAwczU3Nw81nXdMcVicWmxWFzBzDRkyJBNXNcdWj1PpV
Jp6+3tzQMQRCSYmRoaGtaTUjYrpcqlUqktun3Sdd1WAKhUKh3Vx52ZheM4jUTkKqUUM1cQvkufSjKZ
zLmHHHLIrwZ6HBYLAEyfPn0rZn5pxowZNqx5kFOPwHIWEV0I4CUAnVLKxmw2+
+VoZ4ZKpeJ3dna+rZQqDx06dHxDQ8MqtXF3d/
e8np6eDx3HaWppafkyM4s+i0C31lpLKYcy86pFTWsNrTUrpSpCiFQQBGvpq1ssA05RSpmSUgohBKoC
ePXfQohV/5ZSoqenZ15vb+
+i4cOHf9113cb4Z4gokFI6ACCEQCqVQqlUennBggV3lMvljk022WSX1tbWA6ufL5VKT7755psX9/
T0dG277bbnNTQ07FA9H4D5WuuX0un0QUIISCmhtcaTTz5ZaG9vfzUIgm+ddNJJywb29lkswNSpUyc0
NDS8ct1116UHeiyWtUs9cetHAAAznzxlypQ3mfn5qrASkQVwFoDPA7i6b0dmHpZKpbYpl8uziCjuLz
NkDdd8CMAe8YPRtTcFkKkKMlUBKNKorPZf1N6ptf6IiDbtcwzMjHK5/
Gcp5a5CiGGxnfkty5Yte3CjjTa6EUBj3/
MtW7bsJ0uWLHl9q622ulwIMbbv+bq7ux985ZVXbpo4ceLBPNed0PecxWLxDSllg+M44w1jXO3f1f93
dXW92NTUNLH6/
ar09PS8sXjx4ns33njjY1zXHdX3HmmtA9/3H8xkMttJKVfz5ejq6npOCJFqamraOnZfy0uXLr21paX
l883NzV+Jt/m+/
3g2m50MYNU4Io2XJ4QYKoRw+46v77/7HiMilMvlt1Op1EZElI6fr1wuv5dKpT7bt49SqvPll18+acK
ECUcOHTp0Z8P5iwAa+mjoVvVdunTpz9Lp9JDhw4d/Pz6m9vb26zKZzPHxMfQ9T9+/
mfmDV1999bAtttji6IaGhuPjn2XmV4QQX4wd7wqC4JRUKnVTVejow8UANgewV+Jm1YCIfsXMRwForP
ER0/u89Re/+MXLtNa9RHRgrK1l4sSJT/i+fw6AHWJtG0f/
rUZ7e3sGwPZCiE+thsgyuEin0+sTUXmgx2FZ+3yswBLVkQEAl5nvjASGOEcAmBY/
KIT4TqVSOY+IPlfvgJj5UQDbGxa9RQA+AyADAI7z8bIWM/cC+KjGmAHgINPBXC6XGzu3AWILQzM/
P3NNtvsGt/
3HwUQd0D8Uy6XOyyfz99FRBMMp93iYwe8+rXuAbCN4T6sFELsPXHixEsBjEr2hANgnxrnZCLa2tD07
hZbbPE8gGPiDUR0BjP/rMYwczW/gJmHAWyG0Lxo4rPxA0KI/
cePH785gJ1r9Km1cJ48duzYd7TWjxraZo0cOfIIk2BVA08IsfMOO+xwMIDj443M/A4RfdFw/
EbXdX8Xvw4zP4bQb6RuYYWZn2fm7Yhou3r7RPySmd8notmGc55dKBQOAHBuP88J13VtRIZlwDj+
+OOfJ6JWpZQioiatddNxxx33Kg BFROnrrruuX/Ot5dPBx0YJMXMAAF//
+tfPi3xZVoOIfsvM3zb0uxuhFuWkegfDzI8T0WZV58M+eMzsEtF69Z4r4o01CCu1mMPMIxEKR335fW
tr6yW+798J4Bt9G5j577lc7jDP864kooP7eT0T9xPRekQ0MnadXiHE7lrr7wDYt5/nfJKIvhY/
yMxLiOhUZr7E0PYDrfWZAP6/
I3yiRboZwEb96HYKwmf0yv5ci4guIaLZSql7DM0vAdgq8oOpC2beS2u9G4ALDW3LiGgzw/
EbiWgPIhoWO/6eEOIBIjrd0Ke7xhAWENFfieioescccZ0Q4gYACedjZv45EfUw8x/
rPRkRHS2lVABQKpV0P8disXyS3KO1HiOl/
CwRjREhXxBCbN3fqDrLp4d6wporAOC67k7xBmb+udZ6OhHFd7m+EOKW/
kyGAGZHi8hqFYCZuRNANxGt349zAcB9RDSxRtsHpoPM/
A4AL94vEkhOyOfzfwCwt6HPwZ7nnYV+CGe1YObnACxBTCgCACHEocz8BQBn9PO0cwBsbzjuSSn31Vp
fQ0RNsXH8nIi+TURjDP36FXXEzC8Q0UcAtu1HnxuklI8opf7Sn2sBuA/A5VrvxxPRahMXM7/
```

```
HzOshNGPWy6EItWlXG9ryRGTSct0LYEMAm8SOtwkhfsnMlxr6tBsEdQDwiejnAPrl5MrMfwZwhlLqE
SS/761CiBujcdbLKcw8xXVdCQCTJk3avz/
jsVg+SRzHuRaGeVxrDSIyaVUtg4CPFVgymczmwL99K6pEC9oJ8UUBAIjoUma+qR/jeB3AUgCJ/
ClE5CMMa64bZr4Rtc0izyGpPQHCxed5xHwKmPlNAAfn8/lLiejIeB8p5R5EtDcMu+//
gHlEdCuAE+INRHQ6EXVG360/
vMrMW5rV7A9XAAAgAElEQVQamHlPrfV5Bg3BdUS0LYAvGPq8g8gsVw/M/K4Q4n4AU/
sx5qdc1z1LKfUgEQ01tBsFJmZ+IZ1Of0dr/
YhBG7eYiAQR9SeXyI+EECuI6K54Q2RubDUcf56Z24jIZMI6nZkvM/
TpQG0t1kkm7dfHMFtKOY2ZZxLRamY2Zn5ESnma1vph1Cm4EdFvAYwGsHvkkIumpqbfeZ53aD/
HZbF8IlxzzTU+Ec1k5rimbx4z/3ZABmVZ66xRYGHmBiGEBP4dmhod/
zkRHQZghKHPX7TWh6LORY2ZlyBUWU8xNC9ATOPSp59RfR6p4ver0fY4gK0Mx4vMfAuSi+pKAJMjwey
7sT69QojJSqnPArjVdL1+4gkhzgFgSnt/
leM4j9QwcdSEmd9m5vVrLPp7RT4U+8T63IPQlLej4XwvmMwfa7j+MiHERcx8fj+G/
YHrugdVKpU7kdRQAKEvk+nZ+gDAAcVi8S+GMXoAOgCMr3cQzHyzEOIhpVQib0qEyQFmARHdR0THGs4
3nZl/Yhh7W9xstOoCREcDONvQBwAKHOZAil/nLcdx9ldK/YmIJsWaX5FSHqqU+ms/
fse7tNYvADgH+LfvmNb6vWw226/n0WL5JOnp6fk9Eb3X9xgRPXz99de/
NVBjsqxd1iiwEFGxvb39BWC1XBrfixa6xOTPzM8RUWsNp1MTBSK6CNFkGDvXe6jh78DMH5rU55HfzD
dhcAZl5n8AmGAwX4GIrogLJAAghNhDCLEzgItiTZqIDmJmBaC/JotaHKWUutxw/
EHXdX9WLpcfrbWw1WAxETXW8PuZysyjEHO2ZObnASwGkMgszMxzAfTHebpTCHGi1tpk/
qjVp4uZ9yyXyxfV0FC8DLMAm5dS7grg8rifTqQJWYj+OT0/6bruhZFZyfSc9ZrMoMz8SwC/
MHz+fCI6LK7tQOibVSta7ixm3h9mLVcnQhNS3Iy3vLGxcVKlUrnY4G+2KJVKTVZK3YDwHflYmPl5Ic
RFAFZpS6uRTvPmzZtKRMV6zmOxrA1uu+22JQDu40j9z8zvl8vlhAbTMnj4WJOQ1roIAJVKZT4R7Rst
JKZIk4UIVfU71HNhZu5l5jOZ2WRKaTNM7tV+75r8Kpj5kchRNdEvcuZtreEHMwNAYkcshDiImcfUMG
2dRkRvRtdcU3h2XTDztwCcZRjfq47jHFkulx+s4UtS63wrEP4WGxqazyWiDiK6PtbnXQCPENGphj5z
AIzsz3eVUh7NzL/tj5BFRN8iop0izcJqMPOLMDx3kaZrN6XUaUSU8KsgoldM/
WrBzO85jjM9CIKHYTD5ROdMOOwS0WlEdLHh47cR0XAkfYh8hJFCJuff67CGaC8i+hdivy0zdwkhdis
Wi982mS6FEDuVy+UfmO5RDd53XXeqUuqBvmMUQmgAmD9/vs3BYlkX+D0zL9Ah9918883vD/
SALGuPup1uX3zxxfO01vsC2DP+AWbuQqgOT0QRrYHTiOjH8UUwsucPN3Vg5rdNUT/
RYtYJg1NnpPXpAGAKO72bmXdEUiNzNjO3MfNf432I6BLXde+Mol4SJrH+QkTfJaIdkHSyXZhOp3cPg
uB6Ivpyvedj5i4ieh+AyW/lainlP5g57mxZIKKbiejHhvPNZeZUP30/pmqtT0H/
IoLOFkIUYTCJrUm7I4T4ltZ6Z5gdnmfD4Be1BtqEEFOCILgTZmHPCDNP11r/
GEnTzT8BPGsYW4GZyzD7rTxMRPejT0mD2LX+DGCb+HEp5QHM/
DnEnHOZuZuIJimldgbwg1hbZw2z0nLXdfcOgmBm3Km4u7v7ddO4LB/PmmpcFQqFuPlujTDzkPb29v/
7/x/VukV7e3u/UiXMmDHjfWZ+mJkXlUql36ytcVUx1enyfX9Dz/POYOYmU5+1QX/
v07qA53kt3d3doz3Pe8r3/c/8J+eoJ9PtTCI6aNNNN/
3rVlttlfANiYSVt9cQkZO8KNGpWusj4wsxM3fW8LeoOnuONrS/z8wPmDQDHObHuA/
mqJonALiICTnMfJMQ4nKt9dMGh+L7stnsEb7vzwLwpTV+yTogoksAvMHMN8Sa2pl5GwDHkSH8dU1EW
p+E4MjMf3Fd99wgCJ5DbKEkovNMfibR/XsLgNEnqMb1vw9gS+pfCO6fpJTnBUEw1/
D7vsLMI2tox04E0A7gNsM4XiCiuid0Zi4S0a7M/
FMiSkTErYEfMfMORLRL7Pj7zHxO3GE3Mucsq6FBfFUIcaxS6skapqg/
A9g93kZE3wawkJmfjHUJhBC7aa0bAMTrIRWi77yaQBIJONsw88VxHxgi+u2dd965CRHtu9NOO5332c
9+tlZ+nk8VN9xww+ggCI4C0AugGCXZ681kMs4WW2xx9tKlSy9buHDha5GvW1EpVdxhhx0+/
+yzz84+9thj47XAdtRan93Y2HhM31pXvu//SGs9FcBdjY2N1/
Zty+fzB0fPyRPMfGTf+mee530DwDdSqdQfm5ubl/
U5fh+AvZn5uNbW1tXmj1r1wwqFQlZrfa8Q4ruZTOalvm3M3Oz7/n0Azsvlck/H+/
q+v182m01s4Gpdj5mbPM+7T0p5Zvxa7e3tmyilJuVyuWv6Hs/
n89OI6EIiOsZ0rXjNr754ntdSrUEXJ5/Pf621tfXZ+PHOzs4RzNzat/
5ZdK4vMPMljuNM6VsXrKura2SpVJoF4I1cLnckEXUzc4Pv+3MAbB1ttp/
L5XL7EVFPNOaNlVKVvr9pn+vsDuDEbDZ7GMVqygHm++p53ueFED1a63sAvJ7NZo/
ta5qN6u+dvmTJkt+
+8sor5UKhIB3HkePHj88sWrSoR2sthBCSiOQ222xzhOu631y+fPnVb7755vtEJIMgWFVzjIjkhAkTv
lYqlYIFCxa8rpSq1h2TRCQ5qkWmlJIU1SRLp9PNRCRLpVIJQBOANDM3ElHjhhtueLgQYn1mdiqVSnH
FihXPVCqVBcz82xNOOOFN028Xpx6B5XYiOnTixInYaKPVN8zR5PYC6jQDRX3OB/
AFg2q6HYCGOXJhPsIibvFdbzuFEUk/
NVznIyHEhcz8O8P5XgcwD8mFeJbruidWKpXZiGldmPnZXC63i+d5dxPRrrW+X70w891CiMuZeVa8jY
h2ZOYJMIfSrom/IRZ2HfEkM08loqdgyC/
DzIfHhbPIrHRHDRNRLa5CaBqsu6IzM7+QSqX2rFQqcxBzsuUwQkuS2UH0N0T0EIeO1PFzvgVgnEHgX
NM4phDRAQC+1Y8+N1GYYXN6rKlAREdqrW81CGAvwSzsLpZS7qyUeghm5+CHmXmj+L0goh9LKWdWKpU
XDNc6TAjxrlJqdl+fGw6LmL5GRF+JfR7MPBnAHvHfnZkfa21tnXTXXXf9y/f9z+
+xxx4YMmTIjFwuF//unzpmzJixhdb6egCNRNRYnWCllNlokq4bx3GYiAgAK6W6lVJdUsp0Q0PD/
2PvvaOkqLp34Wef6u4ZGMJMj2SRLMiriAkFDGAgM0gUQQQMwIuSVJRXUEGSCIqgCGIgqBjgVUFAomQ
QkSggIgw5z3TD5O6uOvv741SPM1WngfHe9d0fd929lkvtmqo+farqnB2e/
```

```
TxJ9DcDspWbm3vMNM1MwzA8pUqVukkIIQzDADObGRkZe8Ph8Hm/
33+LzeIKKWVOWlraOtM0M5KTk28uUaLEv6LXy8nJ2X/
27Nn1RGQlJyfXTUpKuic7O3vHmTNnNrHC2VlEZNWsWbNHXFxcdQC4cOHCd+fPn/
8dAAzD8NSsWbOPx+MpAwCBQODHM2fO5DsZlStXblqqVKn7s7Oztx89enRxwd9bpkyZutddd13KuXPn
FgQCgaiAbb7+GTObOTk5u44ePboEAOLi4opVrVr1WY/
Hk5SZmbnh+PHjPwNAQkJCmSpVqvQhIg8AXLp0ac3JkyfXFxjDAwkJCfXPnj37/
cWLF48XHEPVqlVbe73eikePHp0TiUTyGW/Lly9/
GxFRUlJSy1AodPzYsWNfm6YZpenwVatWrZdhGImnTp36/
NKlS+cBGPHx8YmVK1d+kogSIpFI4NSpUwvD4XAuERnXX3/9o16vtxwraZnguXPn1vn9/
lt9Pl81QHXSRo+lp6f/xszw+/
0NhRDx2dnZqdnZ2eeiG73X600oUaLEvwAI0zTzcnJyjtkkeMIwjFI2K3pSOBxOM00zBLUOemytsnyJ
GymltCwrTBps5jVk/
+3bt6+WxNVpV3RYvvjii1XZ2dkP3XHHHahevRBT9yWoLEVRou9PiegCVOdDwc9ziCgdmvZlVsRcp+F
Y5O1Fd0QM3MAlAP2Z+WNyAxPPEtEPcLQOM/
MBr9f7qI1dqOo49qfH42lkmua7GnzAP7FNzNyHFPuo00HrYY8/
VndKLFvCzA9pHtw9cXFxLUOh0GK4sRxLoCQVnHiIDFL6US7uD1aAUxfugpnnCyG+YgV8vipj5pPFih
W7Jzc3dw65QbZHAJyCnrvlGyIaL6XcqHFKDjFzQoyMTCz7D9R9eLkIY18uhFiqc4iJqAMzT4KD2p4V
lkrHZ5RBRPfaWQ2XM8yqFT/DmfEA8LHX6x0eiUS2wl1+
+w8RfW2XS51YnCXQlHaJ6ClmLgbleBa0w8x8uxCi/
bZt22YfOXIELVu2RIkSJcDMk5OTk19wXutashkzZtQCMIuIbgawCwBKlSpVOy4urlD2KSsr64Bpmpm
lS5e+3Y4oYZpmVjAY3AcAJUuWrCOEKG1vJJBSIhwOX/R4PInR/7fP+f/
19/0/+z9nUZA6KXmPiGmaGUIIGRcX5xdCGFFdLwBWVlbWPiISpUuXrmsYhiBbKyw3N/
dgRkbGX2XLlm3k8/mSCmqN2Q7rjosXL+6+/vrrH/N4PMUPHDgAj8cDIrIsy7ro8/
lKG4bhMQwDlmXl5OTkHCxVqlQNn89XsuC1TNM8HwgENpimmZWQkJBYrly5Vh6Px2s7xnknT56cxcw5
1atX/7dhGMWFEAgEAh8fO3Zsg5QyfPfdd4/y+Xy17b/POHv27It//
fXX7gYNGnRITEwcVlD3zNYnu7ht27bc06dPpzLz23369LninndZfvv09PRGv/
76a8Ps7OxCbc1QgM710DsrF6DHdiyyszEzNMeOQoNRsPEYOwG01JzzGhG9qjknTwjRm5mnaJyVHCKa
BXdXUpoQoptpmgvgzkBcEEK0ME1zyP8OZ4WZ9xuG8aRlWUvhcFZIYXr+sCxrPV09bXx0I7xb46wcZe
bWeXl5n5Gbkn8nlKPiwmoIIV6TUo5zjsG+H7qsxUYAk6WUq6523KzAsimhUGikxlkJMPNOO+PhtDWG
YYwwTXO9ZiwnoBSVXc6KXf5wRSGs2uAzAIy/
qoEr2yuEmMGqBbyQ2Zv+YLidlRWxMnOGYXSwLKt3jOOHAZzWZCQXM/
NL4XB4NRE5nZWPiWgGM2+Dw1lh5u811wKAsUR0kpmXOf4+y+v1tpJS3iml/
DS6ALNqzDjm9XqvedVmIUQVZm7MzFv69evXJBgMDoyRmf0RwGNQ2d6olYDqovJCT0kQC7cShMpG1gf
+dmKYOcuyrE+FEIOYtdpo+f9dcE3Oy8tb4PV6WwEoXvBvQqHQ5oyMjM1+v9+JXwrv3bv3iRtuuOGh0
qVLF8qShcPhHZs2bXrxxhtvrF+pUiVXl9/Ro0f7MLOsWrXq+wWDF2bOvHTp0tzExEQtgSYzh4nIV/
Az0zRPmKa5Lz4+voXz79PS0kZnZ2efvOGGG6aSrT2WP3nB4ASfz1etRIkSXaJrDintsd3nzp37sGLF
ilOielcFMlvIzMx8s2TJks8IISoWPE9KuYWVqvrdBT8npXE2My4urk/Bz6P/
duiDRe0YgPlwYMag5G1+I9W56dwjPxRCvCGl/BUObCkzV4IikHRVH5h5eVxcXM9QKLQhut/
dcks+fNFgxRBfcJ8vDhXc6KAXZZl5n2EYiyzLWkNE3gLH4m+++eYH7O/
I31dr1KjxbIMGDbYAuJ+ZC2Z/
S5UtW3ZyvXr1niaiQgkK2y4CSIxEIolSygp+v78eriJIv6zD4vV6DwqbKarAC3OQiM5C08HASpxQl2
b+VQgxS7fAQ1HG61hYQUTzoNEoYuah9ucu4JENwhxBRK5szWU4QdpLKT+yI6yC35NNRA9KKR8iohG6
MRbFmPl0fHz8IzG4Qr6Ji4ublZeXt8vpaF3hmr/
aG5YTqJwuhHjYsqx3yY1pOQG16N7s+Bys+EJGkRtDcZGIXIuvnX16ynYgrnrc9n1qQkTPOK6XS0Tzi
Oh5zWl7AfQyTXO5xikJQmWmXL8JqsVbRz64XgixuIhZoXNCiAFSyoUah240gIcB3O/
4fAU0zMUAQES9LMvykx6rFGTm9eTommLmAwC6A/ie3KzMq/x+/
6BAILCWiJw8NktJr0U0D8C3lmVtJodIKRF1M00zjpkXEpFR0GFh5l9LlSqVpvtd15JJKcP2vfRevHi
xk5RS56wsAtAc7rb6Dcy8kYiKBEZm5u1UAPdUQBvtS6/
XO6go1wKwtFSpUnejwEZSwBpVrFjRBdIGkFWuXLlycJQzWeHWHuzSpUslIhrpPEkI0bl8+fLbLcv6R
ZNpLVmuXLnLsX37HP9/
AcBH0FABABhRtmzZz+31zaU9VrZs2Vd0X8DMNcuWLftRjGOjSpcufRsUCWJB2wsgHTGESOPi4lx70G
UsHcBExJAT0azFALDG7/cPTE9PX6l5Z2EH7bpM8+8+n+/
JUCj0I+m7Y7NI36UZi6RyGYBvpJSbSYMlJb0mYEBKWc+5jtt/
P5uZP9GcE2Rmg4jg9SqfqGrVqq8y82QiiiVPAuAKXUKlSpVKCwaDy4F8h2Ux1M11LXrMvDqGs3LAMI
zhUkodMPI36CnjwaqdWOesTCWitjFu0LOssAguADARvcvMAzRf1R0qfe4CaBJRZyKqTo4W4H9oQZ/
P93AoFJpEbq6QVR6P5/
nc3NyViNEhpTNWWA2CoxxgZy+aSyl7k1vb6BJUBODi94Bqre5Pbrr5S9BEisx81uv1pliWtUBzzuXG
/
SYzS1KgY6d9BMDlrLDi3mkLhaup4ziWA+AP6B2wA9CXGv9g5nFSynlFGHe2EKKrnZVxLgRfQd0LJ4f
NLijtIh2I9k0i2kcaJt3oNTXOSobH40khomnkLi/
t9vv9HYLB4Fead3ETM9eAuzy0npmHsb5Ff3hcXNx2Zl4ZzWZFHRYp5U6/3/9EjHFfU0ZEIQDwer1+K
eV8zZ/
```

```
sgJq3Qu+Mnc0dQkQuraYr2NfkBmnDXmeKhAliheG6Afpn3AXkLPBdQ5nZmVUMGobRkplLAlgN98bWz
zCMdVLK1VR0XTfn2HKI6BVmdgWCzDwrKSlpCjP/RA49tStcMxuAFePwTCLKhZso8yQr/
imdsxLQfAbEZtrOFkL0BTD6KocMZj7p8XiiTOquZwJqz9V1v54B0CYSiXyq23ehmNuLoqn0u9frfQH
AKhRNO24SaTjMoNbDFk7Hx16rObp+Rh31cDh8+ErOCnAVbc2XLl06AgC242KRPk2/
GDEiWyFEXynlV5roe4/
Om7TtWwCtnB8y83+JqAz0DtMo+yVykZ4BmCulbAWHM0CqjbeV7rtIpfaDUsqvY4yxSMbMrSORyBNQ2
jQFbZ/X6+1qmuYCunrCPUBlSU7HcLS6SCnvgkaF13YSdd76RGa+Bw4mYI5BG8/
MOUKIlqZpvgO986M1VmDj75hZN6+TnBu0bZcANJdSToK+TXkzNK2+AH4HoOOvSTcMYzARfUVFAKsRU
VdWAG9nCWYzgE2aLFwqgFIxFt0v4uPjP7IsK9ZmNxOqC8o1BtM0/
w2lkF7QTsTFxbUMBAKT4RDGZOY/7ZKYM6t3KC4urisRLdY4nIuSkpKm5OXlrS44/
qjDsnPnzr6kAMfXvLHCw6FYsWK6NvxDzJwGTYaMiEbZz2RR2vdnMrMLGM/M/2XmogqnbgBgQr/
2pgGItQE8x6obrtCGJoToJITIJKI1zueBmUclJSV9GYlEVqJov1drQoh+zPy68/1jBe5+KhgMzo8R0
WvNdlYu6TIKzPxfAOvglk8JEtHXRORSqWfmswB0iuSxmLYhhHjCsqzRuErJCzuwbGNZVmvdps/
M85nZ5cTYmZPm9v6lc7QOIwaHVIxxnAXwRCQSWaTJXF/
OXoa77BV1oivC3USRRQrDml8ZKZBZvCr196tWay5WrFgdaBSCmXk5M5fXLMoXmbkrK+0bZ9bgEDP7o
b/
xawDU1lxvBxEdgHvDB4AviOg3aLgrmHk5gGrOqBzAPFYAw+6ac8YQ0Xoi+kmT9iyqMRF1EELcCKAQ5
oaZz8XHxzc3TXMaYmSatBdUTsQG0rDBMvMz9j2b7j4TP8U4Zz6UM6rDNjjTuAAAwzDaSil7IkYaNca
49xcrVmyQlHKxJpqfBqATNM6RYRjNiGggEXXUXHZJjMhkHzP7NR5+LoAelmXNQhFEEJm5L9Sz57xPR
6HSv84UcJCZQ3BgWWxbz8zPhUKhn2Jkpj5nZtdzSUSvMXNdZ/
nIzro0C4fDz5JDFoCZz0EJizrve5oQolleXt4cuDMH+5OSkroHAoEfNNmsiwAQCARCmnFfkxbNsDBz
oRqfHcWuIj0QOsoN1ORqv4cVfUEz57NfIDt91ZEtKyD2Pt3YoBz8E7pnixSFQW+4MzIDSpcu/
UskEvkJbkmMj5KTk0cGAoGF0Eib/
AP7t93iXdXx+T4AHQOBwHQALkzL5YyIzhGRs9QDAGsBfAI99cFUaDZcABdINYE4N/
3fEVsq5jFmfqYoQadhGE9KKYsx8xzN4cWkSDRdAZVhGO2J6FFmdpVhoIKnokiQ5BFRZ7t0EyuB4DIi
eh3Ak3B30x4kovPQ72en4MBMRgOgP//
8c+bVfO8VHRav1yvsf+uItNYKIU44SzB2qrQjgPfgnrwTADJJQ0RmR/
85cL8Uh4loNvQZg+VCiMn2puu0naTEE51U5OuJ6Bc4HAjbvoyLi/
tASrkKRRD5u4z9R0qZw8yzHePOFkK0yM3N7QMF5LtqI6Kvoc8kjYNaxH5yHmDmX6ABLzPzSgDL4ejc
so9l6l4YUi27N8ZIBcayNK/X2yE3N/d7zb3/FqqDqarmuzqYpnk/
9OXBn6EnMvzTTjm7sitz5swZM3369I9M09QtbrFsEoBScM95EMAIKAxIwe/
PY+ZU3eLFqlU7BcBn0GemljJzc41D9wMzHyZNV5xhGO0ty2rIDnyWnX6dqXFicoQQLaSUL5K78ygdQ
IuLFy/
qUtQXzpw5M9W+xtWQTl4TJoQIAXA2FgSIaDI0QqRQeK7NKIKgJyshyjpwdyBuh8oCXrXAq70puDodC
9gy6FmhP7XxBoXWayL6xO/3fxAIBFwK98y8wO/39wsEAvM0Jch/
YuMBVHE+d6xoFFoJIZ5C7N+lNbukowsMdgJ4HQoAW8js7IQuO5AFYCscUh6sSshaR4CZXyLV1OBaiy
5j4y3L+gWAjtvmJ6jnRJcl6c7M1zOzjgNpB/
SZ5pgmhOhmZ9uKQkI4nZlvhzuzdxGqA1FHDbFBk+EFEV0CgILt6Jcd7+UOBgKBG6pXr/
444HqZwczbmHmezssTQjwupRzsnARmzmBFAa+l9ielluy86UEiGmN7w84xbDcMo7+U8gfNxnqcFcdJ
V8c5f5ECA+mutxzAc+Fw2NXa/
E+MVRv3cuj1hjoBqG97qkWx6dBs3gDmejyeOUTkJAiLbpK6tPFOIppCGowOq/
ZvHfDqNWa+AH0GJ6Yxc0okEhmtWRCXQ6UDdS9af2aOJyIdg+UWItLp7Jwloj91LyAzv/T555+/
MHz48Mrbtm277Hg///
xzHDx4EMy8gIg26MbACvyt0y7ZTXp24gtE1BLA0BjZoo3MXIvc+IA9RDQHDsfIth5SygTWqHgT0Vho
SBOJ6DFWxIQugCQRdSCibs73mpmzDMNoW7FixcfsvysSP8n/
ZIvKj4RCoSCgHF4oHFUsPqGPAOjwcLFsDREx3GWlQ6TMmf29nAVIYb+0XW3MPBmaAIhVl1qa5rnbnJ
SU9Gx6evq3mizchuTk5M7BYHAS9JntotrXAPZAQ2shhGgB4FZ7/EWxNaTHcBwyDKOv/
f46sRwzpJQDNEEBiGgu3FnjIwASSd9UMI0U7YauEyaWLU1KSnqTiBZqKgmbmdkDzXpNRK8JIdJYIxf
DzAeZWStnE8uYeSgzd9Zl3S9ji1mVSHUksu87s7+2LYFGv4yZc5j5OADUqlUrhWPrquXblcQPk2yiG
qftBTAY+sW6PzM/
Aj2B2YoYJYmoto2uZj+I9XLhRwE8alnWt3BEJ9HraSYvIIQYLaXUEbLtEUJ0bdKkyRG/319/xgxd9/
XVGzOvIqI3pZQ/aVLAzxqGYeoevCtc81NovFdmXhkfH/+qaZor4O6cOkFEFaMvrWma8Pv90X9u8/
v9iwv8P5o3bw6ohdSVTmbmz5h5UYxsVkwjop5E1JpsAHBGRgZOnDgBqI19N/
QZprcqVqw4ctCgQbpNeg+ACnCUGu37/
gP0GjwfCiHqjB07NnnMmDG4667LBxTjxo3DjBkzzno8nkk6YC4rEdARzjFAOYF3a/
4+RwjRklRHnCtTCJUOL0FuMHk6EY2UUroUwYnodWY+zMzfaK73IYB+Gkf+OQBS57Dbf18W7lo/
DMN41DTNoQkJCbUB4N57751+NQvMtWCGYYQAwLKssBDiYcMwugPQzQ8AfMx68H4s2wUVsTvV6NOgum
SumjHbzhoOYWYtBT0rEHcvzaE9RLQQgLOz5rjH42kXCATeJwc43w5y2gaDwcGs2Kv/
V22NYRiTdWseEXUhIsF6XNvlbB0zuzBtrDr5Hrcsa57T+WcFYWiiCQoAYCwzO/
EsF+yyiQ7b8S0zfwl9IKE1O/v7eDAYnAX3vd8H4HdN1hNQVAU/
WZal62g8BuVQaVniY4xjFhElo2iO6O9QHFguCRdSHWW67rZFiJF5IqKDJUuWvAUASpUq1ToQCGy/
ePHiZTOBR5IAACAASURBVMtZl3VYkpKSdp87d+5LAODCbc1tAXym8TjHQ6XOXY4Hq84KLZsdEU1g1R
```

```
LqtP7M/Drcm3C6YRiPENHbukiWiN6SUuo4WobZXqBzET/m8/manT59+qM9e/
YklSlTBqtXr9YN9arMftl7Q7WROjf+8QC2xHjwLnfN70lpDjlxF7vj4uJ65OXlLYabUyXN9tbzS1uG
YeD777/PfPLJJ5+bP3/+qYoVK+Lhhx/GokWLsGjRIowfP/4YNLVMVq25bzDzUl1kchmbBNU+n79JP/
DAA5g4cWIGKU4cHVnblwC+9Pv9Oj6fw1DdOFWdB4hoOvTp5GUATjPzM/fccw/69+
+f304XyyzLstasWbPUBkM7f+9EqPJQoTEw81+sGIpdRkSPWZYVx8xzNYdTAZyHXu/
qFWb+RDOGLzwezwLS46y+hoponI78e0S0iZl1XUnTmXmPrktGCNFZStmBiDraLAfweDx3BYPBBbrfe
q2Zz+eLYlg8hmHskVJ+C3233jpm7hYj0tbZESj8hCujwMx7UDSdKwghBjDz6Bgb01gop6jQ+sAKhzM
BDjJA2/lJsSyrHxxdeXaWsiUzN/
sHGQ+d7TMMo69pmt9p1t7+AH63LGtpEeYVALYAuFlzvUtQgex0uEGfB0gJ5LoyWsw8BnoH/
xDpcSkbDMMYQUXoEGPmDK/
XmyKEGAR35v8UVGeNrktssWEYE3Xq8cx8jlWLsM4B08oY2MH0DhQhK2SP7z/M/
LHm8AxmfoIcgGdWcINYz/hPAOpHQbdSShBRbcuydqSnp8d8Ly7LwwIAFy5c2E+KpQ/M/
Fd8fHyTUCj0HrnrUV9AeYiuSJCZ5xCRVnkWKppzpZHs6LEr3A9drmEYzaWU3aDxDoloJDMPcT54dvr
+DbiBbUHDMB4Jh8ODN23a1EUIgQEDBmD06NHIyclB8eJF1rO6YBhGG8uyZsNRB4XiWvkgLy/
v1yJ6wysBXA8HHoiZTwJoEwqF5hKRc7O7ZEcGhfAiRIQmTZq0eeCBB94EUKlYsWIoU6YM7r33XkCBo
XXYjj0+n6+H3SFw1arRUA/lemYuRAgkpZT79+//
lZldGTpmXiGEGGFzAThBkOdIcQDpOE3GMvMAchPX7WHm74joqkBdtl26ePFipG3btq00DufXAOqSu7
R1zl40dF1H/
UnxdGzXHEsD8Cc0+CI7ankNbmDbKgCvhsPhzURU2nEs2p7sFL9cDOBdKeVWzaK30uv1TjFNc7Nu7FL
K2rCDEAdxXIv09PS6ycnJV6UD8j/V4uPj83Jzc0FEnkgksgwaPAQrwq/
6RXDW0wEMtwO1QgeIaBViKHHHMlL6a/2JSAf6/
ADA7c6NmJmzDcMYIKV0bTJCiCeklA2IaLTjnCwiaiaEqGk7bv9LxsxnDcNIMU3zG3JgyojoHZvuYku
MDTfWNbfZ76Ur+0+qceANALr3MwjNBkpE70DdDyfJ4kpdtoMVVUI30zRX2FmKqzIi6mpZ1s3sxp9cs
u+DK63PCnvY37Ksn+EO3C/
a57oEgaGyIS4BXGb+C0oNXpeV1RorvOUTdrevc337CQp87gxyNxNRdehJZOcx86NElN8lFE2IENElI
cQBzTkAiqDWfOLEic+8Xm/DcDjcCe705hohxFxonBWo6LYu9BHLPCgshzO1/
xkz14GmfZlUy24t1hPAfSil7ALHJLEipOnpfGHsY20sy3oYwLDVq1ejYcOGeOSRRxCJRFxZlpUrV6J
Vq1aoVq0abrvtNvTq1Qv796u1+vDhw+jcubMsV64cKleu/
EfHjh0fWrp0af65jRo1yqpYsSLZnSGVAKBWrVoYOXJk/
t9MnjwZDz74IH766Sc0btwYVatWRevWrS+dPn2aBw4ceFft2rXRqFEj2Ne95PP5mhHRBClls7Fjx6J
p06aoVq0aHn/8cZw9e/
ai01mx56+jlPIpuFHcx5m5ZDTKKVeuHBYuXIg33njj0nXXXVd+zJgxPwOo9/
DDD6Nfv8JJDOfvWLlyJR566KGcMmXK3Fe/fv2F0XmaP38+/H4/Tpw4IXbs2PGw3+/
HuHGFiFJ3xsfH95JSLnGmYJk5Z/ny5al+v7/
xL7/8gnbt2qFKlSpo2bIlvv32228AdCeiUqFQCP3798ddd92FypUrc+3atYt/
8MEHM6MYrMmTJ0PxZf1tgUAAzz//PG666SY0bNgQ7du3/
ywhIaFEyZIlCzkra9as2d28efPG1atXb92wYUPMnj07eigaybi6PIjoHWb+Ukr5EzREhwB+hp7JeR4
zd4Q7a7a3WLFivYhoqeb+7gZwAO5y7J6kpKSnSLUvO+f1LyHEs6ZpLnaOz856ZqIAsVc0w0JElhCi+
bXurABAly5dLAAwDKME9CWaTaTIGYvSxdMfwFTNAv8tYjgrrACfOhsrpWyqyyYDmEeqy0nn8PazLGs
83FnZV+zjLideCJFCRMKyLK3QYVGM/wZ3v6lx8JcnJSW9REQ/
UBHal6GCYhf3FKDWNmZ+Go4OIztw+wt6Z+UTZr4RbgD8+hjOynkhREsAn8TIvMSyYUKIczFKu4Ohl0
H5Mz4+viOABdB38KTGcFbWQ+OsQAVHwwHoupJiGhE9zoo53hm87YHKaDmJMrczs4EYmmgA7o7uMw4i
ylxmbhFL4BK4CoeFiEwAyMrKCkgpb3PWvu3yx2sxShy7oYCGOsDAJlYgIWcGZTmAk9B0wTDzs0KIs7
o6KDN/x8w1nQ+/
HV3fCT2IqaMQoiyADy3LwqpVq3DvvfeidU3aqFixYiGHJTMzE4MGDULp0qUxdepUDB48GBkZGdi3bx
8AYPjw4di2bdvJZ555ZsvUqVPjypcvj7Vr10bH8Nfhw4f/uu+++++++++++
+7FFThLDhw4gLfeegvvvfceJkyYcH7Lli2lO3fu3MwwDKxatQq33nor+vXrh02bNnWJRCI9AHR7+
+23MXnyZNSrVw+TJ0/
GiRMncrp27Vol6rUW+L1DWIE6C0kMRCKRPGYOkQMANnnyZGv27Nn7R40ataNTp07ObJHWMjMzMWDAA
Hnq1KldM2fOlEOGDKHoPD3wwAN47bXXXXXxl133XVW27ZtsWjRIvTsmT+Uo8ycEgqF/
qtbwIhoUWJiYkMA6NWrFzp37oxNmzbNM2Tw4YN6xAOh6sCwIwZM7B48WL07Nkz1KNHj4mdO3euvGz
Zssvqt/Tv3x/Lli3DwIEDcf/
997+fnp7e5tKlS4U2mnPnzh3p0aPHjYFAoPKbb76J1q1q1b4+WXX8aPP/4YBpDlnDsAYOb/
JiUlvQRggS4NDeBzuJ1/
MPNWZq4Jx6LDzGeIqE1ubu5cOJ5nZj7FzHOJaJDj87M+n695IBD4Eu5nL+jxeFrbXEPOBfELqBbJzw
t+GF1gzp07Ny4xMXGF5jddkyaEMO1FtpDZ2c06KBqvRVcAI+EO0hYxs845BYA00hN9fQnASxrKAVZA
2uWswZiQwu89TQ5MlJ3t3sp6duceAFLt0sNVZ4BjGRF1YebmcFBHsGq86JKenv4ZgKZFuOQRqOYMFz
EogOeZ+S7nd9m2EXruqUXMHITbwd/FGgCrnWlozqorSMdYqzVmnu/
z+eZYlrWIHOVbInpaSvkK3MHCWcMwWoVCoRmkBxWvh8a5ttcOXckrD8AAIpqhcaJjGhE9zcw94V47T
gDYBDem8jgRnSY9jm81q+7CfEemAA8LiOixKwVAVywJMbNFRChevHhZy7K+K5jetOujzzDzD86XzV5
c50NPu5xqb5DO1P5uqMXdlcJk5jeFECullNs1E74ZqtXQSWq3hZSOgguhTESDpZSniWgLAGzduhXp6
em47z71p02aNMGKFX+vxydPnsTs2cxcuRItG2rnu8Cmy02bdqUWaNGjUNjx45NAYB27fIpa9IMw2h
```

```
x/fXXb01KSroii204HMbXX3+NChUqBO+6665PR48e/Z+KFSti8uTJICJ07doV33zzDf7888+HGjdu/
HJubi5mzJiBTp06YcqUKQCw+Z577mlUv359/Pzzz3jooYei8zeFiI7D0bEkpeRQKJTtXNgA4M8//
wzu3LlzYfny5V0gzFh2/Pjx0Pnz5+Pee++9Gu3bty/lmKdXBg8e/
MjcuXONcuXKRctQ0TlqZprmZOhrnvNQwIEdO3YsOnbsCACLu3XrlvTiiy9ef+LECdSoUQO///
47ypcvjwEDBvRjRfLmovUuaPv378eKFSvw3nvvoUePHqOEEKk5OTkD6tQp9M6nvfrqq4dycnKqzZs3
D7VqqanKzc3F1KlTuW3btjqW0V+Sk5M72ZwSOhDdF9C3xR4nRchW6Jll5iwhRCtmnkCO9lJWYONxcO
MUsoUQLcLh8AhdtEhEj1qWNZIczMsAFhmG8b5lWVud50QzLHv37l2nGfs1aenp6csWLVrkCYcLd1ba
pbeb4S4VnNM5qED+At9HE32vhSol6hwBrf6a/f3richFNc/
MvxmG8bZNv+A89h4z30oK81ZoDIZhfGBZ1s/OMhWA/xiGsdQ0zc1FKc/
EMlJq33HMPMExtgyPx9NGSjmQFR/M1VoAioX1Wc2xCVBZFx0mYx3peZq2MPMS59yywmgazkwkoDS/
mPk+aLrrLmO7DMPoGwqFVmhKYoOllI9pSnkZRPSIlHIYNM0rsUpVULieRN39E0L8m5nHQZ/
ljWXjoVTvC3WWsSLpW0BuPqhsAD+THvi9lxRuplDXYjQACgaDy/1+/
xXxQFeTYZEAULFixfbOl00I8TgRfeycINubew0aZ4WZM5n5iGbRPUlEb8ZwVub4/
f63pZRL4Y50DrMS/
3Oiu1OhPHKd5tFUwzCWEVG+0Nvq1atRvHhxNGignNnGjRvj7Nmz2LFDqazXrl0bderUwYQJE/Dxxx/
jzJkzBS/
5UdmyZdekpqY+OGHChPysCzPnGYbRSkrZVeesODMggLqBFSpUAIB3APwnMTERFStWzBfcOnPmzCQAq
FGjxssA8NtvvyEzMxNNmjQBKzKpRuXLl0e1atWwffv26Pd85/
F45rFifCxk4XA4r0SJEq7o0TRNq3bt2puL4qwAwI033vhstWrVcqdMmVKu4Dwx82xmrq1bPAzDaGVZ
1iDSgLLPnz9/
hJkLtdBVqlQJrDh79t5www2NASAnJwcA0Lx5cxw6dAi9evWatHbt2irOdnynbd6sYBt169b9UQixhp
nnFCtWzIldeicYDD5SvXr1fGcFAOrUqXNh9+7dcZFIxHnZw16vt20wGBwEDQiYmb9nZh0JY44dBLgc
bMMwOkI5OK6OKiIazsy6zp72UKU/
3QLbXUr5MByZTGb+1TCMl2xxTpcRURYANGjQ4HVmvpYl7QvaHxoRu6+I6C7NxnWUCovJFbRXpZQtnG
sbgN32XOnA7OehX4f3CCE+1DkrAFKFEM/
GYOFeQqp9uZfj80NCiKFSyqXOdZyZP0tKSnrPNM2fSMOV8Q9suhDiF916YxhGJ8uyGrC+ySKmMfOH0
DsrXwkhfoNGeJJjSL+walsfq5nbdKjsvqucQkS9pZReZ4XhChYE0M6yrI81WaFJzFyHNMR/
dlmuPfS/d10MZ2UPgIiuTMXMQ6WUz6MIDMWsWHZ32UFfISOi2U5nxf58ns5ZsZMX70JDsRBtfjh+/
PiGqxnXFR0Wn8/nsQfjjAyes3+Mq1QghOhHRG/
orkdELtZNVrXOQazaduE4tiI5OblXIBD4TlMquMjMH5KDEp0V4dnP0JeV/
hsXFzfeNM1lKFCTXr16NR544IH8FFU0MxEtCwkh8NVXX6Fly5b46quvUL9+ffTv3x+nT5/+GcAHa9e
ubTpkyBBs3boVTZs2RUpKCj755JMRlmXVgoaBF6pUppsiQIH1XOJeRPTuH3/8sa/gZ5mZSi6kf//
+SE5Ovjvanvznn3/i9OnTALDZ4/
EMi7EBrYmPj3cx+ZICe3Lbtm1dkgVXsBFer7fLd999V6zgPHXr1u1samrqKY1TCWZuaRPDuTbVUCiU
l5iYWJYc3QPhcPg0KV4SV0TVqVOnSaNGjdotpUzu1asX7r77bixcuDDmgDMyMgAA+/
fvn8TMrro9KfD38IyMDKSmphZsCcegQYPKmKaJc+fOFTzlomEYLU3TbMB6UPEqIrpTF2kT0QFdKpWU
TMRNzPyC5npDAbyoud5wKaWP9arDk9RlXe2J+wzD6GY/
K7oSyDGPx1MCAOLi4u4PBAIbs7Ozi0LA9z/SkpOThzBzGACYOc2+523hxqycAJAF/
dy8DyCJ3O3BJwEc0WSxAAWYzHZej5Vu1mAp5WzNOWnMnMKKHdUZBO0mom/
gDhSDAHrZHWDOTM7S5OTkp20qfF3poai2lIgmWJbl4oOC4q6xoMc6xjT7OdU9+yuFELN0nW2soAou5
4tVy3M/
AHMdn+cx8yKNswlW2mc7WE8fcLlxPwrgeWeGAoos7hg0wYwQojOAaqwnhtsMzX4L4Bgz74ResmYygI
akxz/Fsi0A3rWfJef15kAfAM1jZlfG2M4M95NS6ihQosKOwFVUe67qj+rUqdN3z549zo+/
AHA39LTU/
5FSPkkx1HGhBxj2llK+RW414J1+v79DIBCYCkBHQf0aVDqwkBHR18ys8043er3evuFweCUKtKSePn0
ae/
bswZ49e+D3F86YrVq1CkOHKsewSpUqGDNGrQVbt25F9+7dzWXLll1KTU1dVLJkyZJDhgzBkCFDcPLk
SbRu3frIG2+88dLTTz9dpppGL2CHmVmbUrYsS0LVnp0b0DeGYXyUkpLy6/vv/
x1M2NkYDB8+POfuu+8utLEnJSWlklLbXUoONDsr9LlugZoLYI7H4xmpGXdMO3XqVJS2uk3BeVq3bt3
Rxx9/PGnSpEnDp08vzDVnb8SlSMPeCmCDEOIen8/niuJ///
33Wffff78uoppPRPEDBgy4FQCysrLwxhtv4Omnn0adOnVQu7Y7eExISDgHoNxdd901Fw5m49TU1F+Z
+WkiKlGhQgXcdNNNmDBhAiKRSLhGCWFED4AKFPm7z2AmVvZ7cvfaBzSzYjNanoY+pr0KFadGy5iOK
j26sfgbq/
+jIh2MfO3mjH8aDtNyxyfnxBCtLUs62vSaHyxUvEtF30m7OzgTVLK0gBOa8Z2TVk4HD4BoIZpmm94v
d5pznmzy0DboSHMghIz/MsZfdv3bRE0NA/28YOkIdcUQnRn5s/
J3SaaYxhGC8uyRsEtp3CKiIZLKec7x05EvewMRVXHEHYkJSV1DgaDHzPzVUtsXMb2xMXFPWPrTzkbH
6b6fL7V4XD4l8sEai4jotellM85gxaojMIblmUt11wv1c76OzNJWUTUWUr5KREVWujtAEjXUvx5fHz
8jLy8vO1UBDoHUqXBW+DOKvxORHNZjyEaYFlWFikohdN2QunzOJ3UACvsmosbhZX2XhiATv8vlqUS0
b+Z2bk+AMAyItJxqixj5vtJg42xn+WRzmc5al6v9zYAKF68+FWJ/
l7WYQkEAm8dOXKkHlCI6XYPgLPQ0xrPIaLkGF7qn6SXtu9Pqt7pxFAc8/
l8LYPBYA9oWCXtyHKE80G2x+ByVph5v2EYKZFI5CtSNMr5tnz5cgCK3bR06b+DqgULFmDu3Lk4d4d+6c
q7OkQYMGZyzL2pWcnNwCQKEsRaVKlT4tWbLkuRMnRMnTrx6/
```

```
vx5lC9fHvHx8YhEItG2shKZmZklcnNzC13z+PHjvwkh7oCjrTIjI+NcfHz8i3l5eRuEEIWivlq1aqX
6/
f6qlmUVL4AJATOfMwzjEcuyZmoyU78DuEHzAq7zer1Dw+Hweuf8RS36OwqMDVlZWTIrK+sS3Ay8aU2
bNh3arFmzrws6vV6vFwcOHPgVSnJBh4XYDcD0OshSpJRhAL769esPdJ6Qk5OzG4qgK9/5KVGiBHr37
o1Zs2Zh3759Oocl7eDBg30B/
HDw4MEqN92ksqmWZSE7OztcpkyZqgDKAsCdd96JjRs3on79+hcTEhLiiMilscTMXXw+36FIJPIbuQG
Uu1nxJcTqLNAh6ucJIX5mZt0czQNwozPVzMwrDMOYZlnWBt0iT6prySndEGTmFlLK92JE2an2tRILo
voNw3iyZMmSf8T4PdeUSSlzAMAwjGnOY/
ZGNwcaziBWoNwfoNrdCxkRfag7xz7vZ906CaCLlPJtXcBnSzC0c0bsdkb5WQBzyAHqZKWB9RLcoMkj
Xq+3xcWLF19ivSZNUe1ofHx8q7y8vC81z/
ji+Pj4t0Kh0NZYG1cMe5uZO5C7O+WoYRh9TNNcqAnsjtn/
1m2AnQCMIjdeby404HcoFt2BoVBoLRVBFJCI3iGiS5qKQboQ4iXLslxOJYAJQohfLMta6zzAip3dgJ
57ajQAF1cOM/9qVxlcz3MsY+ZMIUQHZp7tnHNm/
oVUR5Kzo3cbKWJSXUfq01LK9s79tqBFKxo33HDD85mZmW+WLFnywuXGeFmHJS4uboppmp1hb6B2euc
7XV0Lqra2HBrWP1akMzr+jrFQnBpO8O0lr9fb0jTNW6GngB9LRD0AOLMUSwG4KM9ZqVFGF2QXunvVq
lW45ZZb0Lp1YefR6/Vi7ty5WLVqFapWrYpXXnkFnTt3xr/
+9a+8KVOmvJ+bmzu6RYsWRlpaGtq1a4dmzZqhVq1av3322WdrTNOcdfvtt6N8eXXf69ati5UrV0Zyc
3PN9PT0Cq+++iocdfMfvF5vdXI8yZFIJLRu3bqf8/
LyFsFRg2TmkwkJCZHBgweLiRMnomLFiqhatSr27NkTGjduXGDTpk2vValSxZmZSmVmHzmEwph5v9fr
7RSJRL6ly9Sx69ati7Vr1yIvLw8XLlzACy+8kCWl9NSuXfteANi0aRNeeeUVdOzY0czMzJxes2bNT1
etWmX06tUr/xp+vz9127Zt/rVr1y7NzMxEmzaFgrtjzHxIk0bFrl273gUwzDAMVznl0KFD/
23QoMGkLl26oHz58rj33ntRoUIFfPLJJ0hMTNQy2zJzyjvvvPPv1NRUTJs2DXXr1kXlypXRp0+fU+F
wuELJkiXzsVlPPfUUZs6cyb169UoYNGiQNxwOY968eahTpw6GDh0KZh7q9/t/
DAQC68nNlXHYjtB1WcJYtoaIJkop12kWtzUAMuAuee72er0DIpHIWo2zki6EeFFK+Z1mU2tNRAOgx3
udISIBOysUzbBkZ2f/
nJiYqJOcuCYtLi4uORQKuXBlrFpih7KiRnCetsMwjElSyuXOA0T0rpSyny6bwIorx7UO2RnHZ3ROIy
kMhV8XSQshnmTmt+Eu90yEavF1YqKCHo+nRTgcTiEiHT1EUS3o8Xia5+XljYO762eXz+d7JhQKLUfR
9JJmkwKjOvmlAoZhdDVNcw45gM+sCO8uQd+J2QNAZ834FjNzAyJyEu79YRhGR5snpiiCj4uY+Qcp5U
rNve8hpZyucdq+EELMlFL+4gwi7d90GhosDhENZEWs6rQjUIFbkXh0hBDt7FJUoTm3g+zScPMTHSNV
0tR1AY9j5uKkB+AWMo/
HAyklwuHwR7hCNuiyOf+EhIQzu3fvHlngo59iOCupAF5jpfjotHQiStBEnPNYqQrrVGlTIpGIYVmWa
0FkJSJ4B9wp0W3MfKfze+zoqBlU9P+k83rhcBhr165Fs2buvaRBgwbw+/
1YvXo1GjVqhJdeegk7d+5Et27dIidOnBg4cuRIY9SoUbjuuuvwwQcf4MSJE+kDBw6slJaW9ulDDz3k
/eabv0uAQ4cOPVqjRo1LderUuemhhx5CmzZtcMcdd0TH+CuAgxUqVHC+aOnHjh072rhx4/
vgKBeYpnmJiM4TUe3nn38eL774IqZNm4bu3btJ4sSJR1NSUv6oUKFCL+f1mDngdEgikUhICNHKNM0p
uEKb4bBhw/Cvf/0LN954Ix588Ix588EGuUqXKgsaNG+enAqPz9NVXX+369NNPX/
30009LjRgxAqNG5a+LPzRs2LBbw4YNK3fp0iVhxIgRuHAh36m+BKUordPZeblWrVouBVcpZRYA3Hzz
za8SEaZMmQK/348PP/wQzz77/wQzz77LDwej7l48WJUrlx4rWTmrnaE22PmzJkoXbo0mjZtiptuusm6+
+67T9SrV6/
Qu1GyZEksXrw4nZm9vXv3xuDBg8HMaNWqFQDMSE5OnhQIBD53pvihUrY7iuKs2PX3gbasg7MssJ+I1
sBd/
073eDyPmab5rS4aJKKnLMuaA0eXgBCiE1TAoAMHZxJRLgpEdtGk186dO3Vg0GvSAoHAl8WLF68IuIH
wpHBXL2nS3YeJaIiOXI0Ut0dKjGzCOs0zEi391SI9G/
gIIcQfUEyozvOeYeY+cLe5LyCiJNK3Q7c2TbMWaTTE/
okxcxvTNJ+EY31l5pPM3DYUCs2BftNPjXHJpUKIABwONDPnElFHy7Ima4KqS0SUCr2zMoyZy5FbBHQ
rlByGsw34wqJFix4bM2bMglOnThUFx7dbCDEawCLn80JEvaGEUqsvW7YMgwcPjo5hhc/
nGyqlXAE3f1gGVBlZp3z8qpRyANwZjywAz5GmeeVyRkRPsmq5d875OSg9v5scn2ewAjU30VxunhBiD
TRAaJ0ZhhF9764ozXDFYuKMGTOeIKLPS5QosbBly5ZN4ACiMXOmx+N5xLKsL+DmVMkjohy4W6k22nU
3Hfvo4z6fb004HN4GN7X4CiI6Bgd62k6ZxUEj/
U1ETaWUtWJ81z+xflDz5sz8HI+Pj2+Um5s7i9xKpGeIaAP0acdDRDRVU//
OMwzjXsuynnd6qfZDuUkXpQHoQUQZzOxCmuoiuwLfk0JFF2IcwMzjNc7oq8z8sCblvdnr9baPRCKro
RdjnAC33gmgmDwTATyhOfa4Hf3qtI8ydJsGEb0mpfyTiL51/P15IloAPebgGNwkbgCw1O/
3t05PTx9JDqA5K7Xkr5wL5eWMVdfIgwC+JTen0HkiehNqPgqZYRh3W5b1OvTq1c8AeJkcJFN2tL5PV
09n5lwooT1nZnTz/PnzGxHRk3369PncwUmIOgAAIABJREFUed61aIFAYNGqVavaBoNBPProvoo/
lOmS1J0B1u3EoagPZQWD7nM7EQao1s4vweOzBJdN4HAHOJaA0zzxo/fjwmTpyIlJSUKDHhR1CkYr/
BnUEZZ3+XEwS52f7HVbYnog5CiFOmaa51Ztr+iZEiokx2rq/
MnE1EjVixjvdynjd58uQDo0ePrgOoYKB69eq444470LNnz7316tWbWb6VwP7e9qb+MjXU4YFJOzDoczn
RRXjRNQfxSKR8TJEZNrGMZ9n3zySY+XXnpp0NKlS3HPPPfQ1kJMQ5SESTYzgQryYlJS0Mh8M/
wZ0+3AeFUXA6K2dJtRnqKKsfZ+YSl3FWLsX4XGukWrOOw+GsMHOm1+ttkZubO8bprEDxB8yH3llJJ6
```

```
LRMV7OTpZltY3xwC6JkVJ+TQixX0qpi8T+G+Oczsx8yz9wVl5l5uGajNandqTobFvfbzsr30LvrIxn
Zhc2hRXxXxo0zoo9N8NjOCunY0S4X9jcFc4ugRxSOAWds3ICemdlV1JSUpdAIPC401mxxzeriM5Kjs
fjaUtE0zTOSg7UnOsUhB+3LKsn9CJjbwPoq9kk50kpV+mcFXvsFzTOylEhRBtmzrUs6/8ateakpKTH
pJTZBT+zM1JV4XBWWHU0PgaFDajiOLadmdOhd1b+IqKI5j6sE0J8yTYZ5urVq1GmTBmsWbMGoVDox6
SkpKFQm7Ez+l5ASqbC6awchlLHdTkrAPoLIfZalrXif4ezwswvseLT0q2vnVjhT3ppjn3u9/
vrAMCnn36Kjz/+GE2bNsXq1asjLVq0qHT69Gld6/
BzdhCkyxgtgN5ZWWQYxixn+zczZ0Kxx7qy+0KIrlLKinXr1tUJ+WmNmXPt8z4BUCUYDGLjxo0oU6YM
FixYcJYU/
qQQHYFlWVZcXFybSCQyS+esAJgZY+6+llJWhsZZYYXrfAFFcFagsiFrnc6KbZuh7zyaD42zYj/
jPSORyCLonZVlzOzK/lqWlZaWlhaTjr+gXbXDIoTQER49L6WsE+MhyoC7/S+NFNuqruPhY7/
fPz4YDH4DoBBIh5nPsup8eM3xeTYpXghdf/
nLhmEcZr3QG6CipKum2oYC1n3OGqViIUQ70zS7xMiEvEsKVAzHsVwodkaduNi/
iahcjE3wE+jVjT+WUs62LGsJufELi0lTZiGiIUKIHC6iajSAaazErpzArJVElGqnPwvaCQDNI5HIVO
hrse8wc2/NIroFscuQI6SUj0Pj/
NhOsa7ddr1hGG8S0Y+alO00aHgCWPGi6Grvx30+X8tAIHAL9Gqt01jRhF+12aDKF6BPAQ8hovGaezs
WKi2sc7R+APAvcpcg1jHzWCJygm+jdgL6AOAjoUAsefYi/
H+FEVFuRkZGPsOmvfAfJiKXKrIQopuUcgTcJemTUN1CrtZ9qMDkFBxYPVY4iVeiZaXTp09jx44dGDh
wIDIzM1G/fv2Pg8HgV3DzgmyxnRznxn6RiGZDT6Pwls/
n+86yrBUo2roXy2Z4PJ71uvWViJ4SQlTQrV/
MPJWZ83EKd9xxB5o1a4bXX389MGjQoIG5ublJ0SaIAjYRQAL07bRfk76MtsXr9Q6z10Pnu/
4+9NmnQUKIM1zE9mUAPaWUr8Eue61evRpCCDz55JPHdu3aVSYnJ6eQEK9pmnlpaWkX8vLyxgJwlZxs
58G1xrMCap8mR+u8bW8TUTvoKfxj2RZmHhcjw7paE3wDqlNIV96+YBhGSynlTN0YWKlkJzvXL2aek5
eXl0qxuY0K2RUdlltuuSUWgnw6EW2CnrAnyxnd2ht0T6h0tvOFWer3+/
ukp6dPhoPZz458R0PzEhLReehv0HTDML63FUB1kcQFLgLpFStWySjpkrOzpgczV3JuqsycJ4QYwcz/
0V3TZh58E+5y2QRmPhrD451hb9JOWwpgKCmtGGe2YR0AXU5zupRypWVZ3+vGdxlbCOBWTQZgvxDia7
jv00VmbgHl+etewll25OR0fv4SQrxD+lrsxwCq6DJGUG2DOn2NQ0KIXqZpLoS7g+ADuDucAMVA6my1
j9ZvW0UikTjSq7XOAPC4c6G8nJECVT4C/Ry9ACXd7iwJ/
ADl1Onewb8AhODOuhwyDONZe9y633YescGR4yORyG7DMEyiIvSmXgPGzCEACIVCr8fFxX1hR+3Ov3m
WmV3ATVaMwiN0Dg4rEs2tcGddLhiG8aRlWV/BXg9Xr14Nn8+Hnj17HiSiC7fddluhEt/
hw4fRrl27nAoVKtSqWbPm9x06dIjqiiEvLy+vefPmR++8887RVapUQbNmzfD+++9Huzu/
rFSpUolq1aqdQIHou3fv3mje/O9X6JdffoHf78e2bdvQtm1bVKlSBU2bNsXvv/
+O6dOno0GDBqhTpw5efvnlQ4ZhvGtZ1rLoBvTNN9+gXbt2KF+
+fLh69eovb926VReUTgDQ1bmGsiJM7Na4ceP/AH+TQALAww8/fPbhhx+uO3/+/
LcbNWqEZ55R29G2bdvQokWLE9WqVevq0PUCM//
ZtGnT2e3atdvaoEGDMtWrV0e3bt1gdypOgu3cZ2RkYNiwYWjUqBEqV66cV7ly5Tbbt28vlH3Kzs5Gt
27d8nXLtmzZ4vxNw4ioDRXgFlu9ejXuuOOOvJtuumm6lNIoKPHCzNkrV65ckJCQkA9IbdKkCZ577rrn
o8QWfffZZit/
vL20zlwMAnnvuuUC9evVqMPMLixcvxpNPPokGDRqgevXqeOSRR06tWbPmZgD37t27F36/H/
PmzYteLwMAPvzwQ5QrVw6BQACHDx9GSkpKTpkyZarXrFlzd4cOHRIL6t4x81ZycKXZn2+DkqlwwkLy
hBCtLMsaqHNy7Ov5NIHTsri4uFe8Xi8xs6vrUmeXdVgCgUD/
4sWL6wa+iohevUw62aWJQUTPsBIsdGZD9thp9edIiUAVHqAQwwGM1iz+hzTXAoCFPp9vlGVZK6FvbU
tjZqkbo86Y+aRhGF1sWYJC6Swieo0U3b2rlk+K+OkVjYMT1fTpSe72um+EEPPhoM+3z/
mElcKl83o7kpKSutpRQSFgGyuulUpwz8Oy+Pj4sQCWxyibaI2Zt0M9M05djgsARmlqoHnM3EoI0Yw0
zIgAfrQdFScgL42IBkkpdUSCy6FQ8DqenR3M7FLaBRD0er0plmXpBMu+YMWk61LxZuY4ncNrGEYHIj
ppCxo6QW+zoTozrpoCmxUxVQno0/hvA2jtdBAB/
M7Mb8eIBtNIib05nZ9LADqapvkl9IrEWXQFWnYiqhQfH39dxYoVY0rAX4vGzBIA/
vjjj49CodAiuEswY0ipz+rKCP05BnMrKWXmQlG0Hby1tyxrOgqsYatWrcIdd9wRTkhIeLhu3bp//
fHHH4VKBa+88kpk+/bt58aMGWNmjQJBfXKXnzxxS379+
+v37t3b8ycORMNGzbEAqFViQlJT3Tvn37FCdNQCzr2bMnevfujeXLl+P8+fPo27cvZgjlz
5qBPnz6nP/nkk5qLFi1aC/sZX7NmDf79738jGAyebdiw4Yj777+/Ayebdbw4Yj777+/+/
ZufOnXHq1KlC88fMbXXPlxCie1ZW1mtjxoy5ITk5uaCsyZZTp06dlFK2Hj9+PF544tX2F36/H/
eOHUPnzp2rMHr06HxdryVLloCZz3k8njZjx459jx459tnXr1iXiXHjh2LiRMnIjc3F48//
njQsqx2sB31Z555Bt9//2tatWr1R5kyZfrfeuutjc+cOVPIiX/
jjTdw5513Zs+YMQlSpRAr169EJVwYOY59nubDza2LAsrV67khISEZe3btx/
p1KQzDOPRChUqlCtRokT+unv77bdj37590Qx19YMHD5ZJTEzE3r17o99zdt26dYE2bdpYE2bdpUAYAbbrgBT
Zs2xdixYzF8+PA/MjIyIq+++morKSVuvvlm1KhRA2A2vWrAErbp5SAPDzzz/j3nvvhd/
vx7Bhw8Lbtm7Zcy7Ybb1x89913jYLPERT5oK5LNNXeg6s6DxBRZ8uybotRSThAROfgdvJ/
MwyjeygUWpycnHxb8eLFr0oIMYahplLBIPBsc5Ayq5TdbLJd66K6peVOFdHTa3umM/
naxYMBptAAyQkxTj5PNyL/zHo006/
GobR29ZtqKoZyiUoNLmO80I37kwiamlZ1kdE5BSimwUV4boohVlpiQx0Oji2vS2lrEdEzm6cjV6vd1
QkElmnSft/
zcz3aLInR7xeb4tAIDDFmW1g5j+IiOGep999Pl+vvLy8fNXoq7RjRHQAbpBaHhG9QBoKcTt9fr2u7M
```

```
Wqf/
80HGRN9vV6Q+GEnE7EbiHE1zFKWDuY+foYDuKj4XD4ZXLjalYQUV1ycAiw0sQIk14v5onExMTVgUBg
rdP5YYW3uRVFqyF/bhjGHhus5zoGoKIm2klnxa/xX93vhQITuqj/
hRAdpJSjNZEOAH2gEcMoLi5Oh+m5ls0EgFtuuWWmZn6+IqKTUJmzQsbMQ+3yqC4rtRYabIUQoiszDy
y4HobDYaxcuRJVq1adKYSo3rdv30YDBw7EgQMHENW12rhxY2ZKSkqpp59+OgkopFf2QXZ2dp8KFSqg
f39VGbQzJzuTkpI6BoPB2YmJiboSn9ZGjx6NDh1U1ea+++7DmjVr8NNPP6FUqVJnQqFQs/Hjx/
9+6NCh/
JLrtGnTUKZMmdDGjRsbW5a1BYDnwQcfxKxZszBixAjYmeR7NE436tevDwDfA4qAccaMGVHpjf1ENLR
u3brr1qxZg1WrVuH221Wj5CuvvLI/Kyur7urVqwvper3//
vuyTZs2LS3LGtmoUaM7GzX6G+aRl5e3acCAAY2PHDmSVLNmTfz2229YtWoVpk6derxnz573jhgxYiE
A57qLJ554ItCvXz8/AJimiZ49e8LWLVsPYLNz3du6dSsCgQANGTLkYSKKL6hJx8yPSSmL1a9f/
5GjR4/
mn3P77bfj888/53A4HIqLi7t99+7d6NKlC9auXQtmzrAsa1ggEJh9660qrqtXrx7q1asHVtxmH9xww
w3THnvsMaSmpqJmzZpo2bIlZs+ezZZllfJ4PMjJycGGDRsKknlmPPTQQ/T888/
XBv5+juy9PRHuzGsaM18gvaBhX6iSpyvTzIrK4Ve4u8f+tLXjPiWiO71eLxITEx8KBAIt/X5/
rDI1gMtkWIgoyzCMBlLKfDeZmTMNw2gJVX7QtZ7qbBoRlSeHMCEzZ3m93paRSKRCjChxupSyDRyIYj
tlrVssD8XFxaVIKedpHKNoVHPEeb3LmRAihZlfdKa5mHmFx+MZx0qcrNDNJYWz6QQ9sPRbqJtbCONh
38De4XB4Idxp/
8UAKmiud9EwjOaRSORZzfXOA9gPh5Agqxa1NuFweDYcOKHLmV2WWwm9EuoAKCrwRMc5L0D9Vh2GKJW
IFkLDLGn/
ljfhBjSeJMV6qePl2cXMCTGyA09IKR8kN4BtB9Tz72KXJaJ0nbPCzKP8fv+XtvLxA45jK6CYNYsyr6
uJ6BO7w851jJlToQEbCyEeI6LpMRzihdA4K0T0lJTyMWi4VopqzJxz5MgRl+jetWz0N1av0NyxIsya
D72z8hkpokyttgsz60j4BjDz3XCA8Dds2IC8vDzUq1dvs5TyxyZNmgBAwei8R4sWLbKWLVuW7NAr+5
6Zm7du3dp36NAhDBgwAGvXroVlWUc8Hs8jwWBwHPSYN1iWZek+r1Tp7zimVKlS0X+yhRCtb7311lEJ
CQkUJb00TRPr1q0DK+6R5URUlohw2223YceOHSCid6AE9LRt/QMHDvxy0aJFmDJlCm6//
XZ0794dK1euDAJ4mpm/
FkIYt956a76zAmDJ9u3byzl1verXr49t27ZxdnZ2BwDdQ6EQ3nrrLTRq1AhlypThpThAQMGNAb+ljJZt0
5xMQYCgfaWZU2DXs0Z9erVy3fio/piFy9ePA7gY12QNnXq1DXFihXjhg0blgD+1qSbN2/
eRKiGjUXOc2655ZYTlmXRvn372kQiEezZswfdu3fHwYMHceIkf/
s37//3by8vPw5CIVCePPNN3Nq1KiRULZs2WmPPaZub/S3NWnS5FhWVhb98ssvJQFg/
fr1iEQiaNu2LYio41133ZW6adOmmgWfIyj5iFzo99atOmeFiN4xDGMlES3WnHOJiL6HhkrEBii/
Qjb21TAMkOJ6crHWu8693MHSpUv/
tWvXrqEAEAqFztrEMvcDGH6lC9u2BKq7xwVmFEK0MQwjw+aacEaJP0IxsRZ64e16nK6EkUb/
H3vvHSVFtbUPP/
tUdc8MYZjuAQcVRMwoeA2YuRcvJkBQkaQg4YIooF5RFDCCioIoJqKCgiQlGEAlioISFEGRKDkHgeme
YXJ31dnfH6d67syp08Pwrnet3/
Vd316Lpat6uru6u+qcHZ5AdFs8Hh8K1Y43xSr4RYiShrfBNTFsdBsty+rruu4Sw6Y2VkpZP8nNudob
oek/yvFgMNjGcZxPDSOiHwEUwGzg1dJ13WugYUZYAZE/
1xNKVuyGO6Bow77viBULxRhCiBlsVsMc5LUB9Yt8DIBFzOy7OaFYU2/
CYIxJRI9DbdA66PoklCv4RNJGg6w0SwpNbUyvjR8gP934IIA/yOziuh5mwOnUzMzMIdnZ2a/
Abxi4joiiSTYuYzDzVtu2n2XldK5/pq1E9Jl+3gBARN2klE/AoGvBzN/
BkKyw8jSqATNO53RjU1FR0aHKzpz/
KlGlSpVaAEpNRr3IFkIMk1IaE0oAC2Hws2KFHzpb75Qy87te4fSs/
pwRI0YsIaKTo0aNepWIqtepUwcXXXRRImF5npn/
OXr06HPK+pU1a9Ys9+eff76MnZg5MnT6Jbt2589tln2dxowZg5MnT6JbtzCrhxcx82DI4PiYLIu
oIoLO+ruTl5f3pui5OnDjRMRwOX5Dw2Zo8eTK2bNmSK7rky79+/
fyUA9OjRo3OTJk3OsXzJgxAxdffLHs2bNnYeFOAEjYb5SNDRs2jGVmk4P2O/
v27bvh5ptvJt2T7s033wwSkcnPLdKoUaMp1atXx+bNm7HhwwaEQiE0atQIE1atXvffuArVu3hsPh
MC66SEHzHnroIXfixIkrnRrrYydO3dC+2zHb7755uNZWVn47rvvAKiRXePGjZGRePjZGVlfU0Mwdnzpx5bd
nrqGXLlvFVq1ZFYdawmQezVMJnGRkZL3meUToTuMjrgvu0naDwQ1ehjHyFEAKu67q2bZuYtOXilKDb
WCxWAACHDx+eT0Q2mxk+pviNlP/JWMNjnaSUvxUXFy/
UxxzMvJaZI9C+JO9GDxgW90LLsloCeCDJpgoAXxra6knDwxS4hrn0Ptu220spP4ffv+VzIvqTzAZ/
24QQzwP4SDteaFnWnfF4fBj5zal+B/
ATzCDMDt6NNN1w+hNguFCI6D4oipqJTZILIJmt8VTT9+otvrfCz2D4ipmHk/
Kq8YGzSKmG+pyFSTGFLoLh5hBCdPMqNb37tAfAVpj1CGZZlvWDPj5ipc3yBczGmL/
AkNQy89JwONw1Go12J81oE4pNsgpJqlhTsNJs6OK67iwAIe3hA0Q0FOb7ZjgzXwMzffk3mMHV84UQP
5jGcv+DyCGiVgAcMlgT/
FUjEolcXr169UYAwGWE44hogJck66OCnbZtPwPAN5r0upvV4WdIfgnFsPCJtTHzy2vXrr2QmdOzsrL
qJzbh7du348cff3cff5SHDh0KEVGPatWq4YnnnnnnnnnnnDnn3n3+ONWvM3348cff/3/
2YPHly0VdffdW0QYMGu95+++3+++/
a8Hly0VdffdW0QYMGu95+++3+++/
a8T2ZkZLSpWrWq2759e8ybN6/03/03wcffLCoX79+bxvWUABYsGLFiu/
```

```
0g0SEwsLC7woLC8+Dv6P8KzMvJ6IeCV+vxHu988470/r27fvUvHnzUKtWLezevRtz587F/
fffX9iuXbs3a9eu7dN22r59+zQAKCws9JEivHFU0uv7yiuvHGi4Jmbu3bv3hm3btqUuWLCgNJFKjPM
yMjL6QLvXWQGyRwohnrvuuuuwZcsW/
P7772jcuDGY+ZUrrrjC3b17d72NGzeWdld2796Nr776yurTp499zz33VEtP/
0/97olofieEaNy8efPShGXJkiVo0KDBGiJaDeCTstfR2rVrC3Nzc3P79u17lcHZfj7MHdlV3nr4iT4
WBwAhxDgy4FGZ+XMhxE7WsI62bSM3N3d9enr6KanNlXG3kwCQkpJSw3VdI8jWEAeEEIOklB8bHnsmH
A5/AgUs1S/KfUKI5UTUzfA8IgMAkog6SCkvSXJjAMBMmA3LksV0y7KWww+kjRJRG8dxPoI/
E10phPiaFai4XLAS++rpuu50/SInog6u6/4L/
qp4FzNPhZlm+3QwGNzEZmG4twH4kgvv4nHZoPfCzHmstBRM+IUFMMu1zyGiWnqHgpnXBoPBh0jRZX0
zfSJ6kplfJD+DbI43evTRFpn5QSllb/
hdSo8D+MY0mmQF6Bppul6FEBNgqDqhNnyTNfsWImqbk5Nzm578QHWLZiV5PWN43aJ7pZQT4B97nRRC
PAlzsjKPFObnUcNjuwCca6jot5KS9zcltv+TuIuZc2zbTsvIyKj0aPW/
OU6ePFkTwFceXbu0w0JEI6WUA+BPkiNE1N5xnKl6Z9hLhgsNRdgay7KGQ+kx6TElMzNzJjOfO3DgwH
Kb/qBBg7a7rit++eWX/tpzss8999w1Xbp0Ce3fvx/
Hjh0rfYCIOlxxxRVpo0aNukVKWdryT0tLg+M4ALCCPCyJ5jJujL179653Xde4dgDoSESv3XTTTdbRo
0fRpEmTxL+vOnToMKJ3796m9XAtEfVt27at7153HKdHPB6/
umHD8ttCSUlJAdQIZjCgfL0OHz6MK664Ak2aNJnepUuX4a+88sqLTZo0QUpKSqlydn5+/
ix4ndwEgNWLAVdeeeUvgLIS0c5vCxH9mZaW5uuybtq0aTwAWJalJx5LmdletmzZdYDypJs3bx4+/
fTTnddff33bdu3aRdavXx/
Uv2+vMBkAKHr3pk2bsH79eoRCoXUAzm7SpMkZGzZswJYtW0oTlmXLlr0NAA0aNChtOyU+29GjR7+EV
zi1aNECGzZswA8//IC9e/
ciNTX1FajJRbmoW7fu7G7dutXUryOo7r5ppLnLtu27o9HocJg7L29LKX2dXGbeBuAN13V9WL0TJ058
XVRUlLTDXzZOyX2WUkoiQu3atZsbRje+YOZ8y7J6SCk/
0jdBZv4wMzNzeCQSmQZA3+xOQol5+bwyAEDvrHjRWwgRk1JOMTwGqGTldPxbVhDRSNd1l5VtDbOibd
3jJUV6Nb+ZiEYkSSAKSGF3RuuLGIA+UN2JPtpzjgohXgNgojWPTUlJmRaLxX6C1r3wKrd7AeiJx1hm
/
p6ZV5EfQF0A4HCSccpaImqovw8UjfYAAJ31sy81NfXukpKSGTDjd55j5h5EpI+PVnkdD9+myswveZ0
nHVCcL4QYw2Z9lr1CiIccx/nGcP29x8w+fxdm/gPAGYa/
P0pELQDU81hiZR8rhvpdT0twz7Ksdp6Ohwnr8pCU8g34v/MNzDwd6nrWz/0IlLy43qnZ6bFXZpsS/
dMNbzR6QEq5rWrVqlm1atU6NxKJzAiHwyZa918m4vF4jIg2k+f/5P3GC5j5RtN9QURtWLnPmh47AT/
7ag8RPeg4zgLD9bU0MzOzW9euXZdNmzYNvXr1KnWLZ+Ydl19+
+XtjxowZvXTpUjRp0qTUr+ycc85Zf84553T4+OOPcdVVVyErKwsdOnTAiRMnRMnVqanp1/Rr1+/
5yZNmlTOQ+vSSy/FsWPHsGPHjia1atXC+++/j82bN5d2AJLEvP3793NWVpav67hy5crPiKgvgJv79+
+PFi1a4OWXX8Z11123fezYsSsKCgoWDxkyBGUNWaHUZe+VUn6ekpISBoB169Zh7969Zh7969+OKLL5asWbPm
hf3794deeeU/tWcsFivavXv3Ni7j5dSjRw9MmDABHTp0yLYsa17fvn2XzZkzJz3h63XhhRciGAyW/
Prrr51XrFgR2LZtG8aOVTXAZ5999vO111779bPPPvvTli1bMHDgQBw5ggGS1a9fGhx9+WNyqVatjDz/
8sMmeZFi9evVMhe9GItoOoE9ZTzpmPiKEuPW22277aM2aNeE5c+bg2+/
RefOnVGrVi0cO3bMWNhbw4WN33HFHDSLCVVddhbFjx+LIkSN5PXr02EJEPRo1aoQvv/
wSBw8exMMPPwwAb9x++
+21qlevjmnTpiEzMxNlP9uBAwdKu7xNmzZFjRo1MHDgwOJAIHDw9ddffw9AqKzv3dlnn72wfv363RL
XUcL3DgrfdyYMztCeW3gnmEeN7xHRA9D2IFa0/4c9J/
FyxSoRPZ6Xl1cfSTBEepyyw1K1atUgAAghKmWtLYTo4i26uqz+kszMzAcjkchQmMGb75HB2KuCeJ2I
fqqg6zMXKkPUF3JjMPM2Zn6YmefqX6plWYlxk55RHhBC9GNmY8JERB2gMmj9hn8dQB6AYdrxqGVZjz
HzW4aX+yoUCg2KxWLz4a/MP5dSXqEfh1p4hzHzN6Zkk4iSUdh2kUKL67/
hDigROj1ZyWXmliUlJSNh9iIaB+Aa8jsL74AyyfoQUJLVn39e+nNOEUJEoSV0XrzkVb965FqW1YGV7
YMOSJ0CoL3he9gXjm9pAAAgAElEQVRLRDHSGFOsMD8tvP9fpG82pFSPTTTkiqKL67odYRaLSrjqnqs
9dALKg8Q3ivWSfCI/lipKSsF4AszU/tMKZh5q2/Z8VsJVWUKIhL7HvEgk4pv//
5UiMzPzZDgcbllYWLgNAIhoFwAXGmDde+xfzPx3GHBCUOPJcskKK5bhvQCm6tcXgE0A7o1EIr337dv
X9Prrry9NVgDkAHgzPT199C233IKHFCxciMzMTo0ePxpYtW7Nq1Sr8+ffvP/
hw3wZs6cCSLsFf4AszU/tMKZh5q2/Z8VsJVWUKIhL7HvEgk4pv//
5UiMzPzZDgcbllYWLgNAIhoFwAXGmDde+xfzPx3GHBCUOPJcskKK5bhvQCm6tcXgE0A7o1EIr337dv
X9Prrry9NVgDkAHgzPT199C233IKHFCxciMzMTo0ePxpYtW7Nq1Sr8+ffvP/
hw3wZs6cCSLsFf4AszU/tMKZh5q2/Z8VsJVWUKIhL7HvEgk4pv//
79uaSkZFfz5s1vNnwXkwBcVr16dZ0VeJAVLrFPWU+6xNohpXyTiJqV9aQDgObNm08Ph8OyOdOWQkX
+6uuugp5eXnuGp4dOnQBgEaNGHr1q3Iy8tDw4YNyw3Xq1Ok+ffp0+ffv/
4oWLduXSltPSUlBX//
+9+Lt23bltqpU6cq8OjzCd+7zZs37xg5cuTtG5IbBZoeZ75RSXsbM70ILVgD0u+DvSALAE1
LK8eR3dB7DzOsuuOCCR1JSUirlhn1K8acPPvjgDmZemPB6qCiYuRcp5K+uO7AFwA1EdD8MaHsoEGYv
VF6BcSYRDfLcLU1sjiVEVBOVZ2xkQ220U+EHM/
Zl5osMM7lcr9qaBAOymoh6MnMD+De1WUKICVLKJdo5F5FSbBwD/
6b1WygU+oenetkKALZv347rr78xYuzsrJKgbRNmjTB1VdfnT127NgG8Xh8EczfwzyUGfe
UlJRg3759uPDCC49Ctb11CmIEwIsw08+bMnNrw2cFFKZlNylAbdnIFkLc78lmhwEgKysLgwYNQr9+
```

```
ZYKIUYzs0/
UjpTh3EBDxwpCiFtd1x1AftDzN1BAWp2ankdE6+F3swWAVkS0Ukq5mvzmaKOhWq+mmzNZPEtEVpLR5
fNQybVv/CaEaOe67ihDApboAPm+ByJqxswDkByAfjoxkxVNfzm8xPvbb79FjRo1EtV733A4bGJu/
aVi/Pjxs4moXbt27YaSH6cEAKOFEPM8kzo99sCgCSWEuEVK+RSAcps+K/
f4a0hR4E0Mi0eY+Q19xAflLNzMcPyTQCDweDweXwWzkOZ8ANfBj6tJFvssy2rvOM7X5GfeJVRn9Wzn
OJQH1jT49aCKbNtuKqXsyBoOBorhN8UrAMpGLjO3BDCJNCFIVhiwG13XHW+412cCyIIm1MfMO1JTU2
8uLi7+kvy09VxSEhqmjXgRgIPkN048CeAlUtg6Pe6EuvdMo+KvmNkhTR3e65Q+QUQmA8CVRPSmaT2E
2p8e1ddrZi4aNGhQ9wkTJsz88ccfcdll5SbqC5j5AvKTPKJQoyDfOkRE9xLRPtd1Vxg6tvOgilvTPv
M+Mzc1rKHzoYrRdZs3b665f/9+tGjRYlw4HE6eRaMSHRbplVKFhYXbT/
GnrxHRlfBXj8cBNCeif8BMDZzEzPeh8snK6mAw2M9jF5mSlZ+9/61UssLK7OpOqK6Hnqy8AdVu9wGI
4JnuwUwDSzB3ym3gzPyTZVlvmtRlhRD3s9IrOFd7zsFgMNgyGo2OgEHTwXEczJgxo9zG5LquO3/+/
LnxePxDGL4HVvYC5S7KJ598Et27d5dQoE/
fxU8KLGuinT0A9b35khVW3irL9WSFlfdGJynlWGgI84KCgmNENCQJM+NJKWWvJJt0d9d1O+sLGCvDu
arwg4MBYAnMyUrfUCi01LvG9BttBtRidDrJygQiOpgkWZnAzDVhBrc9KqV88TSTla7M3BH/
O8nKaiLqTUTfoEyXkIgS4NRX/y8kKwBASrMIUMmjHitSU1NHmJyZoRJ5X7LCzPe5rtsV/
mSlgIhuE0LUYoOaLhR74mU9KWHmn5j5GkOysiIUCj3kFSamZOUbABejksmKtxF3dhxnmp6sMPNsVor
AfbXjBZZl3elt+CZX5nsdx7lST1a8a3iyIVmBt6GPNCQrBUR0u+u6rxuSlR+YOQC/
qnA0EAi0Likp+VBPVlgRAR6TUpruzd+IaJ2erHjnNwhKfkGPvsx8KczJyq/
MvMeQrBQIIR4hIt+95HX+nzath1AbfkdDcYljx4498OOPPw5v1qyZnqwsB5BmSFbgdYtMmMWniOh3j
7auJysJcoVpv10F1ajQ19D1tm13g8LU1ASU4B6APtnZ2Sb18tKoNOj26NGjS5LcYIASVjoG/
4VcJIRoadt2bRgAP6yEu642tIqMwczbgsFgm1gsNsfwJQDABiLaTqdBLxVCdJZSPgj/
wjKbiLZAKY3q0QkK/
Gi6OacR0bfsl9bfKYTo7VUt+oyvIzN3Jz9TKDcYDN4ei8W6QBuNSCkjAHDHHXeIDz/
8MAGoAzMX7d+/f0/
jxo2vhGZz4MWnyb6fkpKSYkP1ASJ6Wko5TB+nkDJbLGYzIG+fEOJdInrT8Ho9pZSDYVhgFy9ePIeZP
zW81xAius10c3qJwDnk16PZ4bX4bzY8ZzJp2kBevBEOh8d5CPjrtecsYcVkOh2/
jgVCiJmmsaFXvW1IkhCPgbomfVRDVoJMJsPHocxcGwZ9m4qCleeVHnuDwWAb77x98+WCgoId4XDYtL
n/
JSM1NbUm4KM1A8ABy7LuLioq+gx+raFimBWNnyeic8lPHnAty7pLCFHkdYF1xuO7UMDzTO34dlLeYl
na8W1E1Doajc6GuTBZ5J3z6QCkO0JpZ+mJwndE9IOp+2RZ1l2O4zxNfnd2MPODRCTILCw5jhXlXn9O
B2Z+WL//Eu8F5UjfXnvOH8z8q+meZuY74/H40zAn8V2Z+WXyK37vJ2WG6qOgE1E/
VuQBHXT9DjOfIINFA5TY6adkUIMF8C+v+NXBvH9alvUIKcsVfZT9DBQRwSd50bNnz4VXX331h0RUf9
So/7h2MPNWAIdhWA+hiiqT99lYy7I+klIugl/
V+2co+w+T7MYxAGfA77l1KCUlpaXjOBMSjwkh4DgOmPnzzMxMn5FU2ThlwmJZFgNAWlpaCGYA62pW4
kW+C08I0YmZT7iua+Kfr/d+BBP32xTHhRDNS0pKRkEzEfNiL1S216WSrwdmfpKZL2Y/
bfd7T3vERFtM3JgmHMJSAG+w38o8wsxdWLFr9KrlSSHEtTAwmUgptDaEljQxc+GhQ4c+AoD27dvj8O
HDmDNH5ZKWZXWpUqVKWv369cstYDNnzkTTpk2P161bt+Ptt9+esWbNGgDAoUOHEA6H8cknn2DPnj1V
wuEwWrdujezs7ISM82fM3JeIznjsscdKvUaYebKUcumNN944Z8iQIaXvs2DBArRr187JysqqedVVV3
08dOjQBN4BADBp0qTR4XB4xs6dO2989NFHUadOHWzduhXMnO84jnPbbbe1IW/
e361bN1x55ZU4cODAh8xcC1pS6cUMIcQOrztVNk5AtdtN3ksz9CrH+17nhMPhAZFIZLzh9/
gNAJPZWTVZ/
GpZ1kuu6+rXAwD86i2IJh+gpQAsmOnLOUk6i58B2ABzgl1RnNATaABR27bviMViI2BIemOx2J/Hjx/
fpB//
q0Zubu4F4XDYl5R51Xdrb8xoSuR9RACvY7wdgIm631MI8bu3+OtJyWdE1BSaBpA3KnCgdXFYsQ9vl1
K+BfNGvAxAPsxrpTG8ddCk8fM7gE9guFZJCRLeoScQXgy3LGs9GwxjWcnam1hETwshLoVBJoCIujPz
5dDYk953Mc2U+JMCi19v2oyZuaP3nHO1h3Kh1nHfngZgACujVr1g+NqyrAVkEMpk5Q79Bgz3Jqtxaz
/4cYmFAB6XUn4Cf1I8Amp8Y2IMfpWVlbX8gw8+yPj++
+9x5plnJl7vGCmBN9N6OAVK7FSPr0OhUH8p5TwYFNNJgY1NeC6QMjPUcTD5AO4oKSl5DmXWVyKCR80
3YTfLxSkTFsdxJACcddZZ9+hZKCt9kRehPjC0x56ybXslKzVYHfi3l5lPoJI3E/
8HAPlokhvjOBQV1ATETBbjSdmz68DXTUKI4WyeF44looAhwQGATZZlPQwF9tX1RzoR0Vj4f/
SxRFSot0q96MzMcdMNAGBwnTp1+gDAGWecgVtuuQVjxowBgEFSyuKsrKxyAL+E10dKSkpw1KhRVLdu
XSS8PmrWrImpU6f+duutt6J+/
fqYN28eRowYgQ11q9fj4yMDCxfvnw7Eb1dWFi4aMuWLbjySpUbrVmzBt26dcP
+/
fvXjR8/3rnvvvto3LhxePnl0lxiXGpqajoAPPTQQ0hLS8O7776bUKxsJ4SwqlWrdiYAvPvuu1iyZAl
Gjhz57TnnnPM7zE6tK4QQk/TuhbfRjCazf9FCKL0SfQS5KjMzs30kEnkO/
g7FHgA7DC3oimIPEfVwHGeeISHYI4R4hs2aRruFED/
ALLoEGAwLAfxmWdb4JNdKRbEfZlDuXfF4vA8MKpXMPDkvL287/R/
SYXEc5xsAgYTYV5noJqWsjTIiVxUFK4+1D02/
AxG9mJGRMdsb3egdj5WkdFHKgfO9Bf6Q3lX0Rgi3E9G/9K6i9/g6IvqVzJT/
YlaaVvrxV4joVv0aZ+VH8w4ZTEiZ+SVmToN53Z3OzGNc1/2a/
GOslYbuE6A6O4fZwP7z3quENT0hVozBV2EQooQiZuSbNkIi6k5E90BjfXrfzwA2aEVBJaFNYUjomPl
```

```
V13V9HnDeew1i5tcMn2koKaiET0eKiJ4E8A78o+eZQohFMGNBfyeiF1599dXnWrZsiWAwWPqZvE63T
yYDwFxWyst6d2ddKBS6LxKJmDqsu0kpn1fUHPB1HoUQd3oJZLm1nIjgui7C4fBK/
Tm+1zjVH2RkZKR7b6ZfdMeFEA9JKT81VBrvh8Ph95PcnLkAtpJZZdQYRNSBmW8ybexe9joYSSpLVtR
dPb4WQsyBwiOUjQNCiCeTzKrnQVF6TRfeEdu227quOxNatk5E3YjoGfhbtvOgOgCmC+9Z27bXQs2fy
wURvUhEfROsrVgshl69emHz5s3o06dPDgwgvuHDh0cyMzOLFi9eXOOee+7BxIkTcd5552HSpEkIBoO
/
tGzZskGtWrWQlpaGJk2aoEGDBgAwvUGDBpHDhw+fAyivjs2bN6Nly5bZEyZM+A3A15s2baoOoFQj4J
133kFGRsbBNWvWpLVp06bG008/
jSeeeAITJ07EkSNHFhHR2vr163cFgLPOOgtvvPEG2rZti0Ag0BVAR8uyCABWrFiBV199FQMHDvyjWb
Nmb5tGTsy8g5mfTqK1MjwJi2gVM2fATz3dKYRoFY1Gu8G/
8EWZeRk0KfVTREQI0Z6ZfTgAAFGP4jfDMBIoADDeVHkmC2b+UwjxlJTSpPFR0fOOwKDoywr/
0iTJmApEdGUgEEgLBAKVBXD+14dlWY9IKR1tHDQsNTX1RyIyYQd8wcxbLMsaCIP0OjN/
HAqFXolGozPJP/
bd5SUQJjPJTaaOHhG1l1I2TrKxb4VKFp40PFZMRHnkxyFMJ0WLv0/7+5NCiGellGMMrzVJCLEBanSp
P/adbduPA1isdyJYMWt8dhhQwnqfwCyGOcWyrBXe4+XCSwZ8WBKv6z/
PZHtBRP+WUp4PQ7dBCDGIiIYaxj2TmDkVfkHTg8zch4hMhQmgOjLPGEZOM4ioGAbrDVJSCc8Zvrt1A
IZKKX2JETMfghJP/VI/
DyHEMzCr0/8AIEx+pui+YDDYIhqNvmBoEBwnoimm66uiEEK0hxpF+bCOR44ceR8A3nrrrVPKL1SYsD
Bz1YYNG74OlJ/tsvKW6ej5uuitzcXhcLh3JBL5AmYgzg8wt/
aTRR8iCrIBwe3FEzAkEV5kGy68tcz8muu6+sKSy8wPua77MQzaI8w8DgZXZi/
Db+k4zpv6YuRVBe3g951ZY1nWa2y2sJ8UCAQmOo6zSD8PVuqyLQDUZ0+R03Vd3HrrrcuDweCukydPv
geU/60cx/lt3bp1GS1btiy9GMjz+li5cmU+EV1g2DgXM/POO++884Lff/8dgNJLuPDCC529e/
e+dsYZZ9wFoO7GjRtRu3Zt1K1bF67rYvHixbJZs2YOyoz5brjhBhQWFuLtt99ezWVwPQn/
C1L+QI0TleKff/6JXr16oUWLFieefPLJrqZ2MhTQsSsRzSCi6tpjbzBzT72qYyVcdIz8c/
GI5491DSunZT0+NVWxycLbfO52XXc4zHo0nV3XfRcGEKQQYoRpE6oovJb8RJg7L8kiG2aLi4Hecb3r
WDb+Fg6HG9eoUaNxbm7u6WB5/
msjIyPj2+PHj6+wLMthxeCZHwqFhpWUlCxEJWjhrLSTOnmFjl5Zfp+Zmdk9Ozv7Q/
hB8yegOne+4o2VOagPw8HMvQAIMijmQlW+Q5O11knhDPWKfTkz74JhvOAlA+8Z7qXFRDSJ1RhSj022
bbePx+MzyaCCSkR1DAnT6kAg8CzMjKnvLcsa7bquT+cK6np9Cv71er1t28OIaL6+thHRYGbOJoOEBh
ENllI+AoOfGynwbbknpXmWDcimmJ4DgC86Y2ddIzmCla2Jaau0Dhm7ga/
8OYBy7I6sgLG6liqPNu223jr67na855n5kfg30t2QOFZdNJBrufx1xb+zmIugJGnu0Yx81PMXCdZIX
b22Wc/
DABXX321D5enR9KEhZlTo9HofNu2LwHKb4KkNB5e0FuVADaGw+F22dnZs5J0UBbADARNFiOYeYP3I/
mCiHp63QvfYs3KL0bfFPYBeJyI5uo3IRF1hdIIKMfIYAXcHASDaBcAWJZ1t7eI6J/
rU1LANf34LiHEw47jfGFYCBYB6BeLxRbAzxaaA+BsaJVYcXHxYdu2//Xcc89VW7BgQXD37t0o4yK/
69ChQ7OllGLq1KnlvDcmT56M48ePp8KvU/
MrgFlENDihDbBz506sW7culp+fv2TYsGHtt23blhaPx7Fp06ZSYaoTJ058KqUU5557brnzrlq16mEA
uOSSS8pd/LVq1QIzfySltKkMEM1xHBQWFvKvv/4633Xd2YZ2MkjRv9+Ff64/mZn/Cf/
Nnk2KluvDCTFzK2ZOpuI8HmYdmKRBRB1ZCeSZrv/
7AQwwLeRQPlS9TZ+3gvfq4S0ClXJNB1TVDEDqiTwU6G6HqfVvCiml7bruQk8p9i8fjuMUFxcXH8rMz
DxTCPFAJBKZg0rg65i52Lbtu5l5LPzd5M3MfE8kEhlGBssOKOsNk6/XdjI7ar9m2/bGJEn8CQD/
9gorU/wGPz5mKzN/
TWbxw0FQIwQ9GfgNqqNtIlEcYeYWruu+S5W0QvHW106xWMy0EW8lov6u635juC9eZ+a28K+Tfwoh+n
seN7q45ltQ2B5TF2eUlPJO8rNnVgF4HwY5ByFEN9d1X4cZhP8pgIsNRewOIcTLMNg6AJjnrV+64W8x
Ed0tpZxgOD9YltXOcZxBpHnvQTEQmxrO7zhUcujTUCKiu2Ox2DlQ2lllz6GIiIbAgM06RYwVQmRzBd
Ygidzi/PPP/
4WZ9QK0XFTk1lwMBRZVf6iUq8HMD3pdg3ICYcx8lJnvjEajrxnaSICyvK90Z4WZ59i2/
RGZDaNARI97ku0+BLx3E+hZbS4RdSUFdKyl/f1DzDyI/
MyjE0KIB72xl68iJaKuruv+DX5NgtVepa23HE8QUTtm/
lhPjKCAbR2I6BND23gFEe3yNupyMWXKlJeklNN69OiRlZGRgYkTJ6Jq1aqIxWKFAIbUq1fvtfT0dJT
1+vjss8+OzZ49+9D48ePLDe3j8XgMwOBE9dawYUOkpqZi8+bN+Pjjj1e3bds2q1GjRtenpaVh06ZN2
LRpU8IefnlWVtbG9PR0nDx5suxL5s6cOXMEANSqVatcVZWbm/
sLgC36Ylm7du3YZZdd9uqhQ4e6rlixwkQZ7yyl7KvfnKzE3TL0Frr3O0yAwfhPCNHOsqyjUsrFhg18
GjObBA4rij5EdEWSjsxjzHwHzAj9eQBuMlwTFcVwKWUr08iAKzCyJKIc+KvBhUKIWabCgJn/
ZMWGKfsa8NaF8+Px+OmIPf7XBhGJxOd0XfdNqiReiZRM/
9PwYyGOMnNzIUR3GAwSoYo3n0wBlIq0yefnU9u2P3Zdd76hQxHx1oYxpnWKmdfC3+0+IYT4gAyMFm9
j7wh/IryXmftCjW/
0iv0kgNu8z+sbcySJE7Ztt5RSfmBYe497gp2zoF2vRDSRmS80rAFFlmU96o2B9Gt8nMdK8gHgvWLwP
MOGv0kI8RgMnXWo+7mX6f6D2uuy4S9WTwghHnRdd4rhN1zJShvFx34VQnT0imKfKKe3H99OGjvK65I
XkcYI9Y69R2Z8X2co0UJf50wI8Swzn9a9zsyfCSG+YzN5ZYt+LBaLzSeivIpes8KRUDgcblNUVLTIe
4N8ViChM/
QFmRUotjkRdYahtciKS26iABuDmX8C8KRpLOLF88z8zyRVyB5TFgoFYn0bWrZJRINJGbqV61x4n6mj
```

```
p9Dn20i8jbbA0H49ADV71r+jIsuyWjLzqzBTvVoIIUbCL7q3FWp2awT+tWnTpjOAG6tWrYru3btj+v
TpcBzHWbdu3XcA3gOA66+/HmW8PiL//Oc//
7zlllvObty43L1WfPjw4cMASv2fAoEArr32WkyZMmV+fn7+5c2bN78KUL4Xv/
76KzZs2IDLLrtsv9cSffX666/H6tWry77m/YFAYEBqaqou0Y3Dhw//TAbK83fffTf9m2+
+ubhZs2Z45JFHyiVAXhu3kSFx20AKsW5iWr3FzLpoHVixvb73hMD0Nv5XzHwL+cdNFcVrAPLZME+HY
gjUIL/zNwD8xsxVYabIJ4uvSLlQm2jZkWRdGm+R0HErvxPRsCRMpr1EVKK31QEkmF/fhMPhSgFS/
9uDmS0iKsnOzn45STfEFI9A4X3KXY+sQLEtiOhmNo+yV8FcvEWhdJ90LMQqAAMdx1kIvzNuPikBS6M
mFCvcw0X6cajWvqnq/VRKeRn8CU4Uagw7nQwsNcuy2hDR5Zzc000/
r0LLslp6IpCmTbWd67rvw98d+IqZc5Jc+89LKd8ydMkn27b9guu6C+HvKH9PREXwM/
J2WZZ1r5f86J2ft6GE+EzsrJ1Qyegj2nOKvcTjPfJjU/
5g5hAZJBsADPCA36ZO72ukSCC6vs1WUpgaH4WaiF6WUpru2WeFEKs9rRUfhZqZ+8FM4U8Wq4hokpTS
BHsoR5FOdFhc1z2lFtspQbe//PLLOwCwe/
fuMVC0SR9ehJT1+JUwzL5ZocxrG25CY3iztQ5ENBdmUbZRUEqGJl+H3axEuPTz6w6VSJUDezHzR8xc
B2aF0U5SyudN7Xtm/kgIsVAX8/
GSuqVQqr36693num53+BOSk1BUr3+xn320z7KsF2AAtm3dunUQANSsWfMfiWM9e/
ZEQUEB1qxZQ3/729+awLs5+/
fvj5UrV2Lw4MHxRYsWHfv8888b3X777VixYkXiHAoOHjw4sbi4+NwFCxaE586di/x8Jc2Rnp7+0/
bt2y85ceJEKMEGatiwIWbPng3HcVC/fv0XEqC8/v37Y/PmzejZsyeef/
75t5966qmRH3744VkPPfQQQiG1TsTj8aMA0KBBA19i6ziOW7du3XpE1H7UqFHIzc3FwIGl99YUAAeh
Vave6O8TGISavGSlp6GaGRsOh8c4jrMA/
gXxR696O51uxxQhxFKYK7FPAKyHeV59gJl3VrZ97sXvzLxMX6QAgJX2QbJFZZ9hQdxPRI+zchrXF6n
dzLwbBmAuEaGkpORkOBxu5XVi//
JBRCI1NTWDKmkP4hUqLsyFRDtmPgtmzNsfzGxyBC+EUh7XN9RdUJ3aufCPQIuFEK2ZeSDMeMGNpExK
df+WkcxsAmEuAxAnIpN4V2eodUgHrAOq6xmHn8SQNEiZ1t5kWPMghHiAFVBV75b+DKWQalLU/
oCIHoV/HDwrHA73dRxnHvzd+A3M/
Ds0tgszHxRC3Oa67tuG9X+eEELC3EWKEtFoGO51y7IekFL+G34V4INQmCRTsjIFSrzRp2EDBVFYDf/
optDbM0yK5C8C6K3vxcz8kW3bH7iuu0hPRkkp+XaGeS82htegeJmZTd5n35GyQiklIyQSlo0bNybDq
ZbGKRMWIQQBQFpaWjqZ6Xr9SEmOm2ZyUa86q6yKbXYgEGgFYCLMN+AnRLQbZhXB/
cxcRa+KSUku3wZ/Nvw9gEMwJBcA+kopO8Pcglts2/Zw13UXGDbCBUmq6EegFhuf7LAQ4h5SEt2vag/
lQimdmsB1w2zb9iGqzz77bNStW3c5M1tVqlQprQrKen306tXrkhEjRqBx48ZIeH0QUYeZM2de3rVrV
/Tp0wePPfYY1q1bB2aeU6tWrRWHDh06r2HDhkhLU2/
ZsGFDrFmzBhkZGfsuvPDCtxIV+DXXXIOZM2dizZo1hyZMmPDo1KlTG3Tr1g0vvFC6B+Tu3r3bRBcHF
DsGl1xySTMAOPPMM/
HKK69g5syZ+OSTTzYKIabr1xgr8PfrMINEpzLzrXo1A2B+OBx+JBqNzjK0gDdDVbgVOsJp5/
AdgJFJOhTLiOgDmI0di1mBF03j02Tv9SczjyazHPhx8jOSEs8rgF/nIY+IunhOzjpw/
ggRfUEGITAAKC4u3ltUVHSisuf9V4i0tLQz09PTfclZkvjSK0xMyt0PQQH4TZXlEQBnmzpgRFQIPxY
vatt2K2aeCL8fGbwuQ2cYNOY1rvkAACAASURBVKGgxjdB+BPOWczczbBpbSOiX2GmqnaBUgA2qUU/
4zEaTaBYY7DybHNNHR4ieoKZ74G2XrOS0BgObYP24kcoM119hDU/
HA53jEajH8JPHd4NYBH52XDHbdtuJqV8Gn5G0FoAP5uKBe/
cB0spTSzSp6WUV0LTLGHl7u2SJtLnxSrLsoYCMK2XKyzLepuZTTL+/
TxQvx7jpJR3wb8OLAbwRDweX2SYTMxg5uthJg8YgxVbqR8RzTQUQRuEEF9CG5W5rhsFgOzs7FM6Np/
SS2j8+PEtieibRo0aFV5yySX6jTZGCDE3ib8GoOZ4lZWELrYs6++u6/
ZJ0pKdL4T4KEmL6RhUcnSxdnwSEf0Jf1W+BcBEwzgHUBL9AmbO+u9Q3Zil8FfmK2HQlfGq/
GUw0B1J6SgckFJ+q51fkbeRjYK/qvpcCDGFDbNYImrLCojWyXDu38NsTPiAt7F3197nJ4/S6EPae+/
VXUr5nH6Rs9IW+TlJVfA8DNUHMy+ybXuw4zjL9Pdi5q2WZXX1viM98e3rvZ7eVfgG6jfU2+6/
h0Khm6LR6JvQdE68TuAuAP9A5WODZVltHcf5njTMlHfeXTzPKJ8BJ6k5vEnPxxjeiPIRKeUoQ7fyAD
PXMv1OFcSdUN1SfRR1HMox3US3B4DXZ82adSkRXfnwww/r1exfNiZPnrylVq1aDW64wcQu/
k94m1aCsqsvyK8LIWZJKb+DH+ORR0RSP+5Fruk4KY+u3jDTb9sxc4MkI5gTUAwQffT8s9c51JOYbAB
vwV80gZUs+60wjz8m2Lb9rOM4a1B54PergUBgeiwW+1kvLqHM8OJ6EsHMxyzL6uRR9/V76QAzC/
KbS/4eCoVuikQig8ivznscwGz4ldlPEtFNzNyc/
NiePUT0XpIxGqDGJo8bCqQJAL6DgZLNSszNVGTsZeZ/kBJ603/D7aRIL4sM7zUIan/S8VSfA2Dy6/
JsIKKmUsqZ5MdszYcSLDRZhiSLiBCig+u60wxjr4NENAD+LtzxJUuWjMzJyRkupfxnnz59llX0Bqfs
sFSrVq06AFiWpScr8wF8mqSyBCt9lEprNQghOjNziyTJyioAw13XNbVYC6Da3Xqy8q2nE6AnK0eg2E
CmZGUmFAbFlKzsI6K7ob5wPVnZD0Oy4lVZ00yZMCvK868mdoplWV2gJKH1ZGWdEOJdT/
2wXBDRv6SUf4M5WVkJc7foaWY+05Cs7ADQn5X6pmkTHOhVaXqysgjA7CTJyhvM/
IzhHLYA6O+67leG9zrutVJnwr8BPA3VudJn+muhRkd6srIvGAw2j0QifeAXZcslot9xesnKPiHEPa7
rztKTFSg/
pg4ezdXkFj5TSmlSnEwaRPQUKwlxvTL+k5kzTidZIaX6+Qj8yUoOET2I5LTm4QAezMjIuMir3v/
PRElJSX5ubu43XAFgGcBeTxxyjiFZmQVghpegmpISMh1nBQo3/
f0DrAxFfdcJKSp7milZ8Tp3O+FnOB1IkqyAlUiaL1mBAvFeBXOyMj8UCj0Zj8e/
QeWTlWlCiJHxePxrQ7LytXeOPuowEbV1XXcczPdSdUOyciAlJaVFTk5OOz1ZYTW2nw+zH9ItQoiLDc
lKgs6bLFkZzcxdDAnEAsuyPjRNH1h5IvmSFWYuZOY7oUTj9N8wWwjREUo3R08IJjNzY/
```

```
iTlZ+g9q622vFDKSkpLbyOrS4WuA4qia10suJ9noRRq/49RIUQ/
4ahO2ZZVqucnJyjgFk5Wo9TJiyXXXbZi94Llz28AWrxMqkYghUN63QAiwMA1GAzYHETET0C4DPDCAZ
Q4B4dfLsZymVWV0UsFEI8B3Ux6LESiqrnm/0xc14gEGjh3dg3aY8Vw7wI/GTb9jNeh0L/
jqYAmOhlyfp8uYfruvfBf+EdhEKm+74HVhYDDpnpib+yAfBMRCOJ6A/
DzZkDoBsRzYB5gRgH1RrWE6ANtm0PhoH+zUof4CHDIp8TDAbbEdF0+Jlbxcx8j5RyFLS5OTO/S0T/
hPLSKBt7hBBzoSnVJn6/kpKSfxg+L7z2vqmtnixyA4FACynle9BGl94Ce7f3mU3z/uVe9aR/
F0mDFJ2wF7T5PKvRjTide83r+F0LP5aqSAjRXko5AuaO0AtQyX9mtWrVLg4EAqej+/
JfH8wczMvL22KoNBOR430/H5Mf37SCiF4D8C2SYIgMXbHEcd+axorcUAsGrAYR/ZuI9sGMlwIR/
UR+D6xiNo+HAEWz9/nleMVWAOYC6LdQKNQxGo1OJf9Y1RjM/
G04HO7iiZ7p98VvUAXwcO05xUKIVsw82DCuSIQOiD3JzC1isdglrOkqecnhEtJUdlkpCt/
muq5tEpoDMIyZk1lezGPmBuTHoPxuWdbjjuN8maRDbbz/
iagdEd1DftZPETO3klK+Dv+I5gdSir46+HsrlETFE9rxQiJqUVxc/
DTUSLHsYzsArMBpWNwAgGVZ97KSOjFp73Rn5pHw08yHOI5zRcOGDRMMzpRTvU+FCUskEpkeCAQuBcr
Rmo8JIZ4E8Ll+AmVO5HRa0+NZaa2YZMr32LbdVkr5KczCPF+SH2F+jIheJ4OeBBH1Z+bX9YuF1fz2T
ShrdF8IIVrF4/
HOMPPWTZ91J4AOrut+ZsiEv7Ms6wkiWmDIRJ9n5osNF16xEOIBKO6+bkA1VAjxK8wAv60A6hqq8snM
PCVJ5+d+Uq6hJpDVAlbjtwe05xwE8IDrujP1BAyK0XIXzNXlnfF43OSSnbhxH4N/
9jxPCOHAn2DkQFVBvqpTCHGX4zi1iMikpTNTXxxOFczcIh6PPwoDLVUI0coblZkW8o3MnGXY8Cp6r0
nMfA0MtFRS7IZKu0Yz8yLv99MTumIhREvPM0dXvQQrc85yizwRBSORyOkkef/
tEWDmbE6i4CmEaOu67qvwbxY7LcvqL6VciNNz8DYGe6arpmqeiF60bftbk9u7Fz/
ATJtnMjB7oLoqD8Evy/
4TVFfBJwXAyj2+RU5OzkswEx9MsTEcDreJRCKj4JfDOEQKqDpWf5IQ4j5mbkunoYpuWda9wWBQstla
ZTUZPMSEEHdZlnWUiExd3glQSZ2Jefc7gGLSQPPMfMiyrPau684xrPFJw7v2bBi6XUKI+wD0MnRDDk
IlGI9qxw8BeMk0SbAs6x5WVGgdv5NNRLOJyMeqPMV5d5BSdoUZcnC/
lPIZ+KcFa73f6J0qVarcCAD16tXzCSXqkTRhiUajTQF04jI6LF6Hopc3mvnfEIxaIIT4EAbeNxT4qa
XjOB+YFlEA37AC05aGd34DTFLSAAaxombpi0qElBvxx4bnAKrCOB9maWNTRCzLakEKbOmbPwYCgQ6e
54S+8I1lpbLpYx14JpJDDd/
DuEAgMJUNeBYoM8jq8HcuvkhJSRkElUjoWX4nUnNGE8V2A4C5RDRYe708y7LaeAmnDuj6iZmv1s+hz
HvdBbOQYF9SWjR6gvgbVNJkYsgMYINfB4AHbNv+k5WypP6c2TCYrFUURHS3EOIaGADUUNdKa7396r3
XQWaO0ekBepcSkQM/5TIXagxp6uAke63tAObALPx0DytFTpOL9/1QG1fpGJSI4DhOPBwOGzWS/
qIRvuCCC1olSV47ua7b2dB9OUFK2Ozr09mYkgWrceZHMLBtmPntYDA40QNHmrRWfkGSkWaSLs5kr9O
mG9TtALCNzM69Cff4e5IldobYFwwGb8vJyWkH/6Z6UgjxXBLp/
wehEikTwcIYRNTNdd3t8Xh8IfwF0j4ygMiFEO2JaL3ruj43Yqiu+x0wdM3KJAodtOP5lmXd47qub/
2vKFgpnC9gZt+4H0AfZr6MNLgEq/
HlZBgcpS3L6kfKv65ckIIOnEEGSQkosovvtU5x3g+TIo34NKu837C1qeMnhHiamctpCp1xxhn98/
PzK7yPkiYsoVBoOTOX/
hhCCAgh+jLzO6dTIVYQG6A45vMNHY98IrrNcZwXYLauXsrMf9Of53VQ3jC0yEcDuFvf8FmNrnox8we
mRQDAQCHEiSTdH2NYltXccZxH4J/75niPjYK/
CvqSmeeRWW57ICvRIN2AamogEBjsOM58+Nuih1mB13RsxfcAupeUlHwJf3t4IFTHwIR1OQbl1eQDYg
oh7nZd10RB3EpEZ5MyddNfbygpN09fcuZVBLmsyTh7ldhQmFkCfYjI59dBRINt214Uj8fnw7+Aza2g
/Z8s+rAKEwr/
WQChJMlUMRHtJb8gIKD0LXzBzH8IIX6EgcXGzGugUfQrClZgwiFJuo5tiOgCGMwWiagrM9+rV5BFRU
U7pZSnBOz/VeKtt95KI6La6enpPsdmAM8AqG/YLIqJaCgr483/
jc7KQc+LyFe8EdHEcDj8YklJyQL4abuAMuc00WKTvddiKNyWnqAeh6JCm4wJAaBVPB4/
D8kB2XpEvVFsfTazSJ9i5pGGrsazALYmeY4xmPkl27YXQBEiTKMvU8e4d0ZGxhwp5Vf6yMkrMM4wvR
YrUsQMmA1Z27uu+yzMna5ksTwQCDztOI6piBwB1T02yYlMIj+gGET0b9d1X4Ef3/
eylPIIzJOEMWzQq6oomLm/
EKIIhmKeFVi7NswjxReklG+Shz0ij9acnZ09p1q1akcres8KR0KZmZmz9+7dOwAA9u3b95iUcihOQw
Y8WbCScO7ECr3swy4QUUsp5b0wf9gNpHRd9M34WagZu754fMnMZ8JgLuaZNw5PUh2NY+avXdf1sZIq
iNau615laLWBmVtKKR+EBqJj5p+I6GUo0J7+nEmsgFQttOOfh0KhPvF4fC782gI5RHTccAOuC4VCdx
HRGEPGOxmqmvF936xAzf+GQQuGiLqxWWXxT6gkyre4el2NBaw5LHuPfQGFI5quHS8kooeZ2QfmJUVb
7wn/dTklIyPjDa/
aOld7vSVe56eydHsAGCaEWMPmMdpHADbC8B15sQr+hDNRpZlwQieEEOPZ7NkxK0knJGkQ0XBW1Fj9/
e+DSphMCdhjzNyINNo1M8/Ozs5e5yWc/yfitttu6wf8Z+ydCGb+GMrOwwRI/
URKOQyndw0Zw1vz+rquO90wepgRCoV6RSKRz2DufEaYOdOw0SWLzVDXkGlz2pxsPCqEaCeEKGKlPFu
pYOZWsVgsH0oZt1wQ0QuksDM6MeNNVqahlaZJA5gqhHgnHo8v0de9ZEFEQ8Lh8PvZ2dmzYCBMALCTv
RYRjYHBodrrSrUzjZ0qiN2BQKB9PB7/
BH4yx6eeM7Op6zKfmbsbjn8qpWxt6OROsyxrHszTjJkAHjAkjkmDmV+yLOuHJOv4O0KInUjCCCWixq
bibc+ePT+d6n1PCbo9cuTIbgC44IILBhuShNMOZi6wbbsNERl9EYioAxGdR2YA6S4AedDAlqzcfDvB
P5L4BQp5bmrR95dSPprkovw6JSVlKBEtTNJ5MUUfL9s0aTN0JKLLobXbmHmbbdtdmfkLw/
ssJyJL3zAArMjMzGwbjUY/gkGdl5XJny5O9EcgELgjJyenH/yCRyuFEL/
BLB8OIcSjRDQcfpZOogOis7DyAZCpC8fMa23bfs60GDHzGiHES1JKE/27JxRzRW/
```

```
ZjmcFeNPlsb8Ph8PdotGoyeZgJRGddZrX8nQA4z3tHZ8RnG3b49ns7wIoQKavFc3MWyo4h5eklL7Rj
deBOx3XaEA59w4ynPdDtm3/6n3f5RD1pEC+EhpbjpmPCCEeAsAAMGTIkL980hKJRG6yLOs1wJewrLY
saxrMYmg/
kJIkMJEAslkxESsdRNSPFbZOL5y+CofDnbOzsz80dQNZgWntyq5RrEbOT8NTwNZiDJJ0BYjo38y8Tk
rpu/6ThbdpbyJlQFgOP8PKxLUH/EZ9Y0Oh0Ave+lApyAErNujjrJg/
lVWLHhMKhV6KRCLDDetr4vyNowkviTUxWYcx83mkjdJYgWXzk7zWSdu274zFYsMNRcj3QoiRJrySt8
Zfa0hSN0MVrL7Xsm37VSnlQv05rLAkTXF6ifebKSkp45Jgqb4UQkz29J30yCGlSF5uDM/MUe+/
p2QennLBCYVCZ0UiEQQCgf8VkzMius9xnAFE5Ot4kPL6KTBtWlCVxC79xmUFUmsMPyZkjxDiKzYzj9
70NhEfMJKZ1waDwR4lJSWLYG6/muJ127a/dxznZ8NjzxFRATT2DDP/
GQgE7onH49OJSE+0tpNiAnTVju+wLOuu7OzsV2DeuFbr7XsA+9LS0m4tLi6+HYAOSN1NRB9xGRdlLQ
ZKKR8honO141M8j4jl+hNIYS5M2gIHLMvq6F3k+rW0KxgMdo/
H49+QNs7zRiwdiEgXrfqKFcBaH2UkDOfGQBNqgsLAEPzsoqTBzIuEEI8y84/
kpyFuBPCE4zhLTdUJK8r2lUSkH19nqjC8eAbAi/rrMfN7rEwVK3vqgPq8LQwb2rBAIPC54zi/
6I+xYmCth7kq7sjMfSzLCrqui3r16tlQWg1/2SCif9aoUQMpKSllE5b9AJ6WUpoM/
j4MBAKD4vH4StIEv1ixUFqRwnnp8vDbyIzFGwY10tTZFctCoVCH7OzsIZTEKsC7RipVFbPC97Vg5v6
GpOPZcDg8LDs7+zpD8v9GKBQaFY1Gu8LfDS9I0tnpEwqFvszOzl4C/
7o8MzMzs180Gt3N5Uer88Lh8CPZ2dnvEpHOvCsyJYfeOtnOdd2FetcYys9tKflHJtPC4fCj2dnZHWE
YSTPztwDO0X9b77EvAFwPP6ZlJhEdZcOomIgeFEIclVIu1R/
zTAvbGn7fX4UQT3kJhn5/5hFRJvzkizxSPnkjXNeFlBLMDNd1t23ZsqX/
RRddtJiZazIzpJSQUiIWi209cODA+3Xr1h2eWFeYufSf4zg5QoiMssfy8/OXbt68efvll1+
+KhAI1EkcB4B4PP7n7t27/6hfv/
73RFSVFNYtcR4oKirKDwQCjyXe33VduK4rCwoKlgJoh0pcyxWufidPnrxox44dP69duzbjjjvuQHp6
ZZsNSd5MZeqXwABYJKJ+nobB6iQVw5fwo9J/
YAVkLIciZ6UBM5iSa604MICEAOwJBoM3xGKxiTAbk5lihhDiUSnlL/
C7bE62bXucJyxWpczxQiHETZ70v979yWHmJYbMP1sIcS0z/
4PNs90f4bcKj1iWdb2U8kw9ufBGPf0AjErSChwHlbC10p73XTAYfDQej6+EeZzhC+/
z3iilHGxol+YC+Dszf6QvlqwsEPbqSScrDMcHpGF+vATmGlLYi1e0x3YQ0U6chgEnlM/
PzVDaMnqifAwK7zObDLLarCjHPjdsVsDKhkm+87He+emI+kkAmpu6VhWFt4jpCeCccDj8r2g0+gP8l
OxJUN9rOUMo77GhAEBEz69atSrv0KFD1W3bTu/Zs2eFZmV/
hYhEIoNmz549rG7duqhevXr80KFDk2rXrt3esqxyv11JScn2Xbt2TQOA88477/60tLQGwH9m8MeOHf
vk2LFjm84///
x2aWlppd9tcXHxjp07d35Up06dG0OhUOsyx7fs2LHj47PPPvu6zMzM0lFMLBY7uHPnznHxeDx26aWX
Ph4MBn2duGg0+nmVKlUuSUlJKXftFRUV/ZKWlnaNntgeOXLk/
aNHj24OBoP2hRde2CMlJaUhABQWFq79448/JgFAjRo1zjj33HP72rZdK/
FaW7Zs+cj7jHzOOedcU6tWrdIOwuHDh0cBwFlnnfUYeYaYubm583bs2LGgXr16N2VmZj4AoHRDKykp
2bN169b3ABAzU506da7PzMxsX1xcvHXbtm0fA0CVKlVq1K1bt0swGCzdDI8fPz4LgDzjjDPuSxyTUh
YfOHDgo4KCgtzMzMzza9aseS95Y0rXdU/
u2bNnuuM4RXXq1LmlatWqf2NmFBUV7Tl48OA3AMiyrOBZZ511ZyAQOCtxflLK/
IMHD37BzKJ27dq3BgKBrMT5O46Tc+LEiVVZWVktE3/v/
VbZx48fX5mVlXW7ECI18Zj3fntzcnL+EELYNWrUaJSSkpKVeDw/P3+H4zjF6enpjRJ/
732u2MmTJzfbtl0zLS2tbplzAzNzLBbLtW07w/PyKpuYlDDzKWnB/
y8iEAhASllCRMXBYLCGZVkgIliWhfz8/
K3xePxHAA8x89DevXtXaI1xqoTlkh07dvyydu3aai1btkTVqpWWjjDFOGbeTWYdjFdSUlLGxmKxn2E
GOX1O/tnqLgB/wM+gSCQ/rxkqiZXM/
AsZMCbwNnfXdR+HGUxliuWhUKhFNBpdCD9CfxkUwn0FtHabEOI2KeWtMGf43+kjBGYusm27qZSyKjN
/b3iOqWLPIaKbLcsq8jo/
um7GAKgRlUlPYyGUdLUurrTFsqzWXkVTqVmxF62Z+RrSxnysZveJ70FnCy2HohTqfk07iKg/
NOVgVoZzTQBcyRpImpn/JKKlMGOiksUu27avcxznFWjGY6xEppq6rjtcT5a9iHpVoQ44/
g2qDe5L9LzKrp7he50HlcCYZNFPN1aHQqHbotHoLPh1WBYFAoF/O46zGn6w3k9QOkhvAMDPP/+M/
fv344Ybbmh8+eWXr/tfOK//
5zF37ty58Xj8okgkki2llGlpaWdUq1attCPiOE5eTk7OJmaWRESWZVVJT09vQEQpAFBcXHywoKDgYO
Lvq1WrVi81NfVMx3GKcnNztzCzS0SUkpISrlKlyrklJSUnCgsLDyVeLzU19Yy0tLS6rusW5+XlbWMl
XU9EJKpVq3a+bdvVmFlKKd14PB4tKio6QkRUpUqVcxKaOLFY7M/
i4uITaWlp59i2XZqoFhcXHykpKSkFdxMRpaWlnUlEqYWFhfvgjfgS75eWlnY2ABQVFR1kZir7PMuyq
qSkpNR0HCcvFovlAIAQItW27SoAKBaLJdr7FAwGMxLnxsxOUVHRkcR7Jf5GCJHibWaUOAYAwWAww7b
tqvF4PM9xnDyoJKNKMBiswcwoKSmJSCljiecRUTAYDGYwc+IcEp0/
sm27GhGJWCxWmlwnnuc9Fkz8xszsJv7Esqw0IUSQmdlxnHxmZiGE7dmikJSSHccpICISQqSJMi06Ka
V0XbdEez/bsizbdRNv8f+HF4+zGhEu6d27t0m0tTQqHAmlp6f/sWzZsh8AtLTt//
m4mpUC6nIiMnkfjAuHw69Fo9GVMKO7F+rJilc5bochWWHmp1g58eoz+20AviWNllvm8dZSyjtR+WRl
cygUah2NRsdDS1ZY0Zf7mNymmbkDM9eFOVnZqicrgGrFO45TCGCpYbywTU9WWOGE7iCiQ55stp6UjP
U+pylZ2QjVrSkHNGTmY4FA4N54PP7p6SQrrJDkQQA+TJKnbtwZ/
mRlFxG9ywqUXTYilmX19SS69Wjnfa96spJPRF/
```

```
AwIKpICKWZTV3XfcBGFxSiaij67qPJklWwMwlhmTld6hExZSsbCU1dtNBd6uZuRr5x2H/k9ht2/
ZdkUhkNBHpycp2y7L6OI6zBAY3YCHEAmYuLTQS12AsFjNhOP6Scffdd989ceLEeq7r1geAwsJCnHPO
OdfVrl37pVgs9svGjRtfl1LmA0hUwnBdN71hw4YvMXPxypUry6k45+Xl4fzzz29z5MiR1VLKo4nnFR
UVwbKsqvn5+QWJv/U2YG7QoME9Bw8eXJaTk3PCsiwWQkgpJZ88eZKbNm366smTJ7/et2/
fb7m5uXlEJIUQXFhYyE2aNHmwpKRk57p1675lZi4qKpJNmzZ9PC0trW9JScnEZcuWveZtttJxHA4Gg
1xQUMAXXHBB+vbt26PBYJAty5LxeJzj8Ti7risvu+yyan/88cfJWCzGlmXJ6tWrc1FREVvW/
8feeYfLUZV//
Puemdndm1t3N70RCBJREDGAYMGCUkJXkE4wgdAUURREmoLSxEIRSGih9xCa9BJBJImUNDSm95vcu+3
WLTPn/f0xs/
ntnTmb7ELCxng+z5MnyTk7M2dnZ855z1sNecopp1Rc8NLLLP1bIcTeLS0tS6v5TdLp9HdbWlpeKW1L
JBKfE0LsFY1GNzp7Tpo06Sgi+vF11113oWVZa+vr66vyIUqlUvsT0byWlpZAxF4qlToKQDoajb5Z0j
aKme8zDGNCc3Pz4mJ7Mpm8Be68utI0zS81NTUl/OdLJpNfj8Vib/m+06/
JTQj482g0erfv84fDrcr8cjQa3RiBmE6nvy2lvAtAZywW2xg+zcyNqVTqEbgFXp/
3nWscMz9sGMbElpaWQDBJIpEYQUQPCCEmtLS0LCk9JxEFNKmZTCbmOM5VzFyIx+N9lADJZLIZrgvCy
QBOKR1LMpn8AjPvG4/HpxTbbr/99hmmaXZjM2zWIP7MM8/
cuG7duvOOOeYY+BfLSmA3edlPiehFRd+T8Xj8mGQy+QIU6Z+9nd3nFWrtV0gdKXEdXJV6IKUxgN9Dn
YMCRPQ9Zs7BjVDZrCMyM6+PRCJfymazJyo0RikA32Tmxyhos/4REc1nt7aQ/
5wB9b03tvMty3okl8u9R74U1FymFoUQ4rvNzc1/
T6VSbyNYofo175jAIsiuU94V5Eutz24W1K8w8zVQp+lWwsz3CCFuklK+Q4rsvN73+6OvvUMIcZqXUb
SxpL1bCHGolDLgrM3MZ5qm+aFt2zMUppZr4PqFVDrmbiHE14mov5cMrM/
zQG7J9ij7wq5LWIVgRtqF5Pr2qHxnEuxmKfYn9loM4CNUV8ujHGnTNL/sOM7x/
nF7z91X2DXJ+TNGg5mnkq90w6xZs7BixQrstdde+48dO/Yt/
zHbE5lMZu+mpqYF5BYnVJJIJJri8XjHpzmuSkilUt8sXWhrRTKZbI7FYpmtdf6JEycebhjGfVOmTKn
IRL01SaVSP4SbCfjDKo9riUaj6Wqv19HREVcJRlv6Oh+XLX29zapN1q1b928AeSJahypKTHskyK2Bo
gqFez4ejx+TSCTuhHoRnAPX+cm/iM8rI6w8xMy7kBuNsxF2k9TczG5a/
QBE9FNyCxD+jYgqEVa6n8mVawAAIABJREFUiOg7uVzuiyrzFrkFCG9VCCvXGobxsuM4KsdcqIQVALe
0tLTcmUql3lIIK8paFABOamlpeTWRSDxBbh2Q0mP+DaAeamElC+AKAKoMmz+QUv6YiKoRVl4Lh8O/
8oqc+XfitwghVjBzIMROCHG+lPJW//0gohNYnaL7egB/
dxznbYWwch0zn1+NoO2lmJaO4zyleB7+AtfHSBVlAXbznfgdtZfBrW3kd4YuHhMm14mulASAl6FOTl
c1RHSk4zhfVQlZhmEcLaX8nUpYgRvlcVq5837wwQcrt8T4tmWam5tnb+4z26KwAgDbgrACAFtTWAEA
IUQeFWy+Pw2i0WjFuWN8x32sRb0aYeWTXOfjsqWvt9kFGoDBzEkhRCCB1abg/0/
KdicFnWjfjkajx3iVNFUZFZcDaFao1TNQ2/
LfBrCWFPHvRPQnVuezAFzTyHTPG7si9bZhGEcys2R1GOtJ7Cbf8cf1PyCEuN5xnL+iQkdVuCGNP/
bUe/607OVqUVwUi8UeSiaT15HCmZeI2inoTV/
kV0QU8Pshop8w815UJlJBhWcSOz6Xyz2FoJnvGcMwHlAJK+SWZ7+QgiGFlzDzkQim9X4CrhDxCoLJ8
/4E4MxKf1fv+qeapjlXSvmc//6yGy00jRV5B0qO9z/n7QDeomDkVukx/
rIJvXAzTm4RYYWZj2fmJmYOJI2Dm2vlEJTX4ijLyieTydcBwHGc//qwZs1/
P7ZtW9hGBBbN1qUSgaVBCNHrVcyt/MRCnC2lvIaCkQ1zotHoOM82p6oKm/
bMM6MUfapY8cUAHoGiUBi7oaA/
Ch6yMUTtV8z8CiqsKs1u5t8PALzkX9jh1gH6NoKhtC96Rb+eR9BHoRzvR6PR45LJ5GRUHq00JRaLXZ
9KpcZDkdSI3dTsqkyeAPB7IjoHwfswRUrZXc7vpwwpIcRBtm3/
yS8cMfMs0zQvdBznOcX4pkkpD6NgwqPpABy/YMvM74ZCoXOZ+WXFM3af5/
dUTYG+X7a0tDyRz+dfJl9+FGb+l2EYl2yihksAdqOwJsMXmr45hBBXQ+Hf9HEgN7vtWrimzj65VtgN
ZS+wIjNvOdh1JD7VcZxer8naEuPUaD4JpmmGoQWW/wk2K7AQ0bB+/
foNQ+WaAbCbAvgUhVlksWmaB6TT6T2JSJXZtRdufQ5VvgIVSWa+BIoKy3BTr59YxtTyTiwWOwXuYli
pEHFxPB5/
XEo53b+gAXiAiEzFojorGo0e7Zm9AnlnyrDMNM2D0un0z6EoPlaGZ2Kx2JnpdPq77KtQ6o1jDZWpqu
ppigI1ReBW4n6B1OUCykJER0kpj0awQOIiwzBOsG37OQRzCMyEq1HzmyXmE9E0BKu4LopEIt/P5/
PP+J8Vdisv747qzJe3xmKx67zoGb8Grx3ABMdxpis0KGURQlyPyutPAXC1QuzWu9oS/
J6InmU3oZafN737WmmKdbBbt+R7UsqLBwwYcDAAEJGxmcM0mq0OM9ejss235r+czf7I4XB4JyFENar
fB8nNVOuPdmkTQhxYKBQGsaIQHQAQ0QZULkAAwKmkKOLEzO8x875QZEv0Fs7DU6nUFFRe7+H2WCx2b
SKRuAfq8OV/+M1OzLzIsqxxyWTy3DJmrwDM3GlZ1qG2bR/
D6oR3Kt7xSr3v6TiOP6oGgCt0lrneu57fh79e0wdCiBullKqU0GUhovFEFPE70gJIWpZ1hJTyfgR/
31Vw65r4K552wPVB8Ztg0qZpHprL5SYT0Zd9ffOJyILChLYJHvESVv0Z6urLxxPR7QohdVNcxMwVF2
0DAHYzaB6KCrV9m+H5cDj8ZynlywqT01oiupKZq9GYZoQQhxDRL4lo16KgMnLkyFFbYKwazSdlNYBF
tR6EZuuzWYHFMIxRhmFUJL16UT3LEUz/ngFwgGmavQACob4ebahuV3wSM/
8UwYiMdUQ0UhF1AQDthmEc5DjOz1F5To5nY7HY2Z6/zWm+vsXkZhf015BpE0J813Gc/
VUCVTmEEEfm8/ndoS7wF6AofKXT6cHs1mho2PxRG1lFRIvgCylm5tVEdIGU8nGFE+umuMY0zdmO4/
Tx7fGibg4sFApXAviKr68XwDJSpB0nt87ITb7PZ5n5ENu2f4VgQrv17JZUV1asLcMLsVjsBE+oVNVW
OUVKeT4qT/
kNAJfCfbaqyQz9PBGNJkV2zWrxzFfn53K5GVAIP4ZhnMfM91b6rHhmoKM9AbqPYDty5MgtpQ3SaD42
Qog2Itpt4sSJgarKmu2LzQoi3d3dhuM4m42PBrBcCPEwfGpwL/rk0Gg0ujSfz/
```

```
91EzvViiueEtFlcLOF+nflC+FK24FzMXOPYRjjvFwrlYa5/
iMajR6XSCSORdDfJgm35ksf4cKL3jmQ3LBYVT2Fct9pgmdWqmjny8ytQogDiUh4fjgV3z8v0uklAKf
42jsMw5joaUIq9v9g5mnMfFs+n39dYTb5vpTyeFLU7CA386xKwLgFwE/
hM0MKIU4iosP8gqPn4P0yER1U6ZjhaqaOSSaTh0JtUrwWwK6o3IcIcAXN3VCdgPM23PpY5fyLqiElh
DjHcZwXoNZUXiulvBSVl5wAgPHMfANKhBX2sm+uXr363k8yWI1mS0BEYWZ2LMv6ZKnYNds8mzX1MPO
yzs7ONFxb/
qHeDtzvlNhFRJcwc2CBJqIfxGKxvyeTyedRnaq+HPebpjk5n88v94WrJg3DOARAVEoZyL5JRD+wbXs
nIrpZcc4EfLtRdrO6HppMJr8IIBAZ4lV6vsuvhTAM4+jm5uYlqVRqSRURKtcJIeZ7Kfz7dHjRLseW3
nN2k3kdEo1GlycSiXeJqBozGgDc4Wmn/N/ph1LKPypMSClmLpAijJqZ34tEIj/
OZrOv+KN7PFPYWCgcouGWTFeFV79Mbi0Rf5mDn8GtNaHyCzmN3QKTii4l8wCMS6fTuzDzo4rj/
go3rL4ak9gLcLWLgURzANqY+XZP0C7lAwDPwycMF+tvAK5wwF6ismJbJpM5u1+/fpOIaM/
Sz7W2tl4cj8fvFkLsyG468Y11Q7LZ7ALHccaFQqEvFNtK/
xSvUfqnvb19RjgcviYSiYwurU9iGIYEIFasWLGiivuj0WwV8vm8YVlWxnGcT5SKXbPts1mBhYg+ZOa
THn/88RdbWlrWd3d3t48aNeqkUCi0cVFbv37909lsdr/hw4d3Goax0ck1kUg83draOnbatGknf/
TRR+P853YcJ5VIJF7r37//
YUKISEl7p5Syy7KsPtEfuVxuxeLFi5cCOLe5ufnhoUOHnlQ8bs2aNU+n0+nxADB8+PC/
NTc3b9y5JxKJ51tbW/
eOx+OjBw0aVPD8HAAA+Xx+7fLly+8dOXLkEZFI5PPe9TtWrlz5Yk9Pz0922WWXMy3L6iOUtLW1Pblh
w4bdR44cOa+xsXHjzri9vf2p9evXfxXAVwcPHjwzHo9v3J07jpNatWrVA8OGDTum9Hv19vb+a+nSpd
kxY8a8ZJpmnxeup6dnzrJlyzrq6uoe32GHHU4v3tvW1tanEonEUZMnTz7qjTfe+M+gQYP2JC+9NAB0
dXV9YJpmSyQS8dekQTKZfMWyrP2KZRaKC14ikfgrM58aj8c/X/p5AFi3bt3LRESDBw/
uU3DRtu2uVatWfThkyJCZ4XB4OJfU2Ojp6Zm/bt26vUaMGHGsZf1/
MAkzo1AorAfApe3ePeru7OxsaG5u/
krp9Xt7exdu2LBhzwEDBozt169fn8W8q6trfjKZPJKI8gMGDFgVDodHFBd5ZkZHR8eHjuPkm5ubvwT
AtG27N51OZxzHebq+vn7HSCRSz8wgrxaKbdvZjo6OYXV1dbeEQqE+1/
LGmGM3nXpdsc22bbtQKOxtmuYBVFJErPi34zgDAKhqZOyJjyfElzMZbsqJtuKCjyV8o7MzWCqoX79+
H8AVRHWUkKbmGIYRAtAP+nnc7tnslvT222//
LtzEbnsVPy+EEE1NTZ8jtz7Dhp6envXMTIZhhJqamnY3DCPS29u7oqenZ03xPOFweHB9ff1OAOA4Tl
YIYXV0dMy3bbvXsqx+jY2NuwohLADo6OhYwMyioaFhFyGEAQBSylwmk1nAXo0NADBNM9LQ0DAmm82u
yeVyxQQ6BACRSGRAXV3diGw2u76np2dtcRymadY3NDSMJiJDSlno7Oz8j5TSBtz6FeFwuH9PT89qKW
UOAAkhzPr6+p2EEGF2U2ivz2azbYBbHyIcDvcPh8ODstns+pIxgIjINM2Gurq64czMvb29yx3HyROR
6Nev30ghRMRxnGxPT89KwH3p6urqRhCR4S2cPb29vWuK5xJCWOFweHChUEjbtr2xXHnxvkcikSFEZD
iOk8tms2u979O/tKZIoVDoKhQKCa8vVuwrFAqZQqGQEUJEwuHwgNLnIp/
PJx3H6fHuXVNR7crMnMvl2pjZFkJYoVAoTl6iNSllPpvNJotjD4VCUS89P5jZyeVyCWaGZVnNhmGES
66V8s5XZ1lWQ/FcxRogRCRM02wsOoEzcz6fz/
cxVxqG0a94TilltljPg4iEYRj9bNvu4RLJyjTNSHFsXrr17mK/YRihYl/
xdhcKhSwRMRGFvHGwr2aIKYTYruuFCCEO8KrPHnTmmWe+XOvxaP63mTRp0reIaDqAAyZPnvzPWo9Hs
/XYrIblrLPOegXAK7fddts3i22O4yCVSqGxsbGuq6urmJMBtm1DCBEbMWLEge+//
36fukG9vb0YPnz4HgMHDhz/4YcfXiyEsAqFQhcA5PN5RCKRIcOHD/
9+Npv9T1tb28sAYFnW4F122eVqwzAGLlq06OxkMrmq9JyFQgGFQqG+t7c34GPT09ODYcOGfWHRokVz
S9ullNzY2Dhy+PDhx7e2tj6WTqcXG4bBUkp2HIe7urpYSsnFNgBsmmbDHnvscaOUctWMGTMuLfZJKT
mfz/Ouu+6619y5c2cRETuOw6ZpspSSmZnHjBmzu23b5ty5c/
8ppWQhhMxkMnzQQQedsWrVqmlLly7dYNs253I53nPPPUcNGjToSSFEZs6cOeOWLFnSGYlEOJ/
PcygU4t7eXs7lclxfX8/
ZbJaL9T06Ozv5wAMP3DEejydt286V1sRIJBJnAPgzEc2KxWJ9Eq8lEolJAL4Sj8dPK7Ylk8nd4ObtG
AXg+lgsdhEATJw4cWchxGXXXXfdo8z8CBGdFIvFni051wgieo6Zc5ZljWtqamr3XesxIhrDzCfE4/
GPSq53P9xCfJfGYrGNmoNUKvUtKeUlsVjsCPKlRU8mk/cB+GI0Gt2PiAK/
fSKROJ2IvhWLxVQVuQN4Pkr3GoZxREtLy6u+ax0G4EZmHiyE+Eo0Gp1TMsYJcHPm9EnDnU6nj5FSDi
Ci3mg0OtV/
vXQ6HfXXLUkkEmcQ0RQAYOavxuPxdwC3Xodt2y8T0cxYLFZRnSvv+pMBxIjosmg0+tuS7zMFbgK+qZ
Zl3dHY2Lih9NhyqbRTqdR4Zv5KLBY7EwBuu+22b1mWNdf/
OY3m00ZKyUTUUSgUdC4WTW1h5oZMJqPMIfIpj8OfKG6r0NnZWbHzbKWkUqk9MplMxR706XQ6mkgk+o
RVn3baaZ+ZNGlSzjuf0iGXmVU5bzZLR0dH1aG86XR6i9YNKfediiQSiXIZgrfkGL7hCU/
+a1ftTNjV1TU4mUxer+rr6OioJoJJo9mmOfPMMw+YNGlS6swzz6w015Xmv5RtPrU2EXUBmLUNjKNs8
bMtSWNjY9uWPmepVqASvN1/
n+rK+XzeKfqclKsPQYqKnpVQbT2MkjFuMTZX8yIej7+7Ja9XZgwzyly76lo1DQ0NrVBkPAYAv/
ZLo9kekFJqDct2js4OqKkIy7LqqILikBqNRvNpYtt2AW4knqz1WDRbF70AaSpCCMEAWqFrdmg0mm0I
IjIBDDQMQ89N2zlaYNFURDgczgAYNGnSpErrPGk0Gs1Wx9tMkW3b229ongaAFlg0FZLP58PMvLZQKO
j01xqNZpvBixICEWmBZTtHCyyairAsK0JE8dK8LhqNRlNrmLkgpUwwc27zn9b8N6MFFk1FeB74a7Qn
vkaj2ZYgIqEqG6LZ/
tACi6YivKyugw3DqKaCs0aj0WxVvOgg0iah7R8tsGgqwpsUunTooEaj2ZYwTVMLLP8jaIFFUxGeKai
h1uPQaDQaHwUACWYu1Hogmq2LFlg0FSGEYHLRuxiNRrPN4DgOAxigtb/
```

```
bP9t8an7NtoGU0iaiNmbu3fynNRqN5tPBMAybmcmyLLvWY9FsXbSGRVMRnoZlcK3HodFoNKVIKW24i
eO0wLKdowUWTUUUPfGFEPlaj0Wj0WiKFAqFPDMntQ/
L9o8WWDQV4U0GHbZtZ2s9Fo1GoykSCoUkEfV3HEf7sGznaIFFUxGO49gAYtrpVqPRbEt4cxMJIfTct
J2jBRZNRRiGkYdbqVmrXTUazTZD0dnWNE0tsGznaIFFUxE9PT15AJ2maep6HRqNZpuhu7u7wMzJ119
/XQss2zlaYNFURCQSsQG06FwHGo1mWyIUCtkA+n/ta1/
Tdc62c7TAoqkIKWUB2Ggv1mg0mm0CHR30v4MWWDQVMXXq1Bwzd+jJQaPRbEt0dnZyrceg+XTQAoumU
hhAS6FQ0NmRNRrNNkNDQ8NIIspZlnVgrcei2bpogUVTKQSAQ6FQqNYD0Wg0miKmaRKAXiLSxVm3c7T
AoqmIH/7wh/
2JyJFSHlDrsWg0Gk0RIhIAIKXUpqHtHC2waCqCmQ1mzlmWVVfrsWg0Gk0Rr1pzKxHpLNzbOVpg0VSE
lNLwqjXrWkIajWabwTAMAjCk1uPQbH20wKKpiEgkIgEMqPU4NBqNphSvXIggIr2Z2s7RAoumIrw6HU
II0VvrsWg0Gk0RKaUNoJ2Zu2o9Fs3WRQssmoro6elxmLkVQLLWY9FoNJoinoZliBBCa1i2c7TAoqkI
0zTzRDRCSqknBY1Gsy1RACBs2+6s9UA0WxctsGgqor6+Pg9ASCk7aj0WjUajKSKlzMHV/
GqBZTtHCyyairj55ptzAGwhRLrWY9FoNJoilmXlAQx0HCdT67Foti5aYNFUg1UoFLprPQiNRqMp4jh
ODgBNnTpVCyzbOVpg0VRDynGcnloPQqPRaIqsWrXKBNALt96ZZjtGCyyaijj22GMNANH6+vpaD0Wj0
Wg2MmzYsCYAdXDrnWm2Y7TAoqkIy7KaAHTbtq2LH2o0mm2JRgAdY8eO1ZXkt3O0wKKpiH79+tUDiAC
waj0WjUajKeJVaW4YO3asnpu2c7TAoqkIZo4AyEoptdpVo9FsM0gpQwDytm0btR6LZuuiBRZNRQghB
ICQEEI7tmk0mm0G0zQNAKFIJKLnpu0cLbBoKoKZCwA6HMexaz0WjUajKWLbdpaZM7Zt52o9Fs3WRQs
smorIZDKtAGJEpBPHaTSabQYi6iSililTphRqPRbN1kX7I2jKMnHixEsBXCGEMAFASgmi/
39k7rzzTv38aDSaT53x48ffLIQ41zAMIiIwu9YgIoLjOLj77rv13LQdojUsmrIkk8nbhBBLiQhEBMM
w4LqyAEQ0p8bD02g0/6Nks9mbTdNcIoQAEUEIASEEpJQwDOONWo9Ps3XQAoumLE899VSCiKYxs1PaT
kQdzHxDrcal0Wj+t3n00Uf/A+A1LqpWPIhorZTy+hoNS7OV0QKLZpM4jnM7gP/
4mhfeeeedD9RiPBqNRgMARPQXAIt8zXPvuuuuF2sxHs3WRwssmk1y1113rQDwYlHLIqVMENHvazwsj
UbzP86UKVPmAXi3+H9mXgdAz03bMVpg0WwWKeWtRLQYAIho/
pQpUx6v9Zg0Go0GwC3MvNz798w777zz9VoORrN1+Z8VWFKpVMunda10Ov3tT+taW4O77rprMTO/
KaVst217m/Bd+W+/pxpNLfi05j1mrs9kMvts7evccccdswHMklKucRznD1v7erWEmSOJRGK/
Wo+jltSsWNQdd9yxr5eErMcwjN58Pt9rmmbvscceu3s0Gv2AiLorPVcymTwkFou94G9PJBK/
NgzjGWZeGo1G0yWfb2bm9xOJxOuxWOxHRJQt9qXT6ajjOE48Hu8oPVcmk9nZcZx7TdOc0NTUtLCKsV
0opbwukUj8OR6P/7S0L5VKjTdNc1ZjY+O//MdlMplYc3NzUnXOdDo9Wkr5/Vgsdr2v/
UtSyiWxWCyjOCba0tKSKm1j5rpUKvUbwzCebG5unrmp79HT03NTXV1d0z333PPcpj73cUmn099uaWk
J7I5SqdT5zPzZWCx2VrEtkUicLqW8I5FI3CWEmBeNRm/0nSvwXYGNv/
vP4vH4FdWOL5PJ7OM4zmdisdiDir6yv1UpXV1dg3K53Dmbu/
6sWbMGz5s3r1sIYXR3dxvhcNgUQhjZbNYQQhhCCMNxHFMIYRCR8bWvfe389evXv7Zo0aIlRGQQkQGg
/Ywzzgg8V5raMXny5M8y85FE1C2l7BJCdBNRl5Sye/
fdd99t3rx5b5qm2S2E6DFNs+fUU08tOwd67+5esVjsrdL2RCIxQgjxPWb+ZywW+3tpXzKZ3E1K+Y9E
IvGbeDx+g6/
vJgBZAPtYlnVsY2Njm9d+GICziOjk0jl0cySTyfuJ6OhUKjUhGo3e4+v7FRHdqjpfKpVqKXeddDr9H
Wauj0ajT5e2H3744TOeffbZrrvvvvtt/
zEdHR3xpqamhO88O0opz2LmW+Lx+KpKv9PWoNy8l0wmH2DmGfF4/A4AuOeeeyKtra1/
IaIJy5cvv6Ojo2PGzJkz32FmC4DV2NjYkMlkHABWv3795ubz+bDjOGEpZXi33Xb7bFNT0/4zZ858ip
nDUkqTiPoJIcJeWYMwM4eFEGHv3yEA/
zzrrLNe+VRvRgXULFZ98uTJaQDN5fqJKMvMPQCyzJytq6trBFDIZrNLmdkmIpuZncbGxiFNTU1fyOf
zrZlMZnY+n+8iImfw4MHfiEQiI4QQYOau9evXP93T07MBgD1q1KjD6urqdhVCoFAorF65cuWDvb29q
VgsNnzEiBETpZRJKWVm8eLFU/
L5fG9dXV1k1113vdQ0zQHMnN2wYcNNy5cvny2EcJqamhrHjBlzQVdX16sLFix40TAMx7ZtCQBjxozZ
Z+jQodcVv1M+n/9gwYIFv06n0x1f/OIXj4hGoz5q6VK1detHTp0o+Knxs+fPiwnXfeeXJ3d/
cLs2fP/kvpfYlGow277777zYZhjOru7n5q1qxZNwHAwIEDB33uc5+bLKXsXr9+/
Y0LFy6cVTxm11133WfdQ0zQHMnN2wYcNNy5cvny2EcJqamhrHjBlzQVdX16sLFix40TAMx7ZtCQBjxozZ
Z+jQodcVv1M+n/9gwYIFv06n0x1f/OIXj4hGoz5q6VK1detHTp0o+Knxs+fPiwnXfeeXJ3d/
uGDBkydPTo0RctXbr0aW/
C5GQ0ND02c+85mj5syZ8wgzC2YWcLP3i0gkUrfTTjsdw8y8YMGCJ5hZGIYhmFkMHDhw9MCBA49euHD
h5EKhUICr4RNDhw7de8CAAeNzudz8JUuWPFxHxePwIkLHxePwHzIx8Pr9q5cqVj5qm2Th8+PCJR
GQWAwQ6OjreXbt27TtEJAYMGLBnQ0PDXhs2bHi+u7s7AUAwsyAiGjJkyIHhcHhkNptds2HDhhmO4zA
AYRiGFYlE+jc0NOyayWQ+yuVyGe84qq+vH1ZXVzfCMIwWIrJ6e3uCQyPJvNp
nt6elZ74zIsy4oSkZHP53sAGERkmqYZE0KEmRm2bReklDYR1VX6zlSLZVk3Tpgw4fytdX5NdUyePPl
YAI99nGOZuYuIbAA2gIJlWU2hUKjecZxUNpttZea8EIKbm5s/
a5pmxMtHkk6n0+9JKbNExIMGDdrfNM0mIQSy2ezSRCLxd9u2swMGDPhcS0vLV4spCwB0t7a2PgLAGT
Zs2AQhhOk4TnrNmjUPdXZ2tgFAc3Pz79P79++++++/
u7q6eL1xdtE0rQPHrxvXV3dbuvWrXu+t7CRUQCgBg2bNhTTZhjOru7n5q1qxZNwHAwIEDB33uc5+bLKXsXr9+/
Y0LFy6cVTxm11133WfdQ0zQHMnN2wYcNNy5cvny2EcJqamhrHjBlzQVdX16sLFix40TAMx7ZtCQBjxozZ
Z+jQodcVv1M+n/9gwYIFv06n0x1f/OIXj4hGoz5q6VK1detHTp0o+Knxs+fPiwnXfeeXJ3d/
TYAAQlmXFhBCRXC6LLLYBMEzTbDYMo1+hUOiVUuaZ2fCu1e/
jPCNbGtM075g4ceKkWo+jlJoJLFOmTJkgpfyRN2HXAehnmmZ/27Z1wh/
```

```
Nfx2maYKZbcdx0oZhUDgcjgsh4DhOR09Pz8pQKNTY2Ni4Q2nOCMdx2pPJ5CwpZS+AQjQa3aWlpeVLX
nK+rrVr1z6ezWbbR40adXB9ff3uzNzd2to6NZFILAVQGDZs2K5Dhgw5u3g+IkJ3d/
djS5cufVxKeXFLS8suY8aMuXfMmDE/
qu3d0QDATTfd1BQOhy8CcDSAegANAGK1HZVmW8UwjGKiToeIjOL/
i388wXOtEILq6uqGeAKn7OzsnJnP5zcQUX7IkCH7RyKRQcU8Wtlsdt6qVaumGYZhjhkz5gzLsgYahg
FmTixbtuyadDq9cocddvhMa2vrIQMGDNh32LBhV33xi1+8srZ34v+ppYaFASAUCkV/
+MMfppPJ5DsA+tjnmPlGwzDeklI+4Tv85qlTp1504oknzgSwu5QSUkp4O9eFRDSGmVHaLqVELpd717
Ksfb1zb/yTSCRuam5uPlEI0b/
YBriZXUvG0udPV1fXO0KIpkgksltpe09Pz4K1a9c+P2rUqImmacZLB23bdqatrW36oEGDjhVC9JGik
8nks+vWrXv/M5/5zIRQKDSitC+dTr+4Zs2amaNHjz4+EomM8d0jO5fLrYxEIjv573Fvb+/
8UCg0yjCMhtL21tbWhwcOHHikfwyO43QtXbr0lpEjRx4bDochL8SUAAAgAElEQVRHl/
a1tbVNS6VSC0eNGnVqKBQaVnqNFStWPD106NCvlu6qinR3d7/
vOE5vU1PTV333ItHa2jp96NChJ3uqyD7ft7Gx8WuGYTSUvqAA+vxd+qdQKCyxLGuwEKK+9DOpVOpeZ
s71799/
kv+YZcuWnT1gwIB9m5qaxhcngGJfZ2fn5S0tLecJIforklOdEwqFlhFRwAwJ4CFmPoqINt5bZn4dwJ
eJqF7x+bdisdj+qVTqPGbuY9pi5tVE9DCAX5S2E9GpUsr3Acz0n5OZXyIi54UXXhjX1dWFr3/96xg8
ePAdsVhsm9op/
S8yefLkLwF4j5kXnnXWWZ9NJBLDieh9AAN8Hz0BwJfg+90BnATgbWaeR0RNvr75AHZzHGfjfAegOCe
+KIQ4uHSechynO5VKXRGNRm8otpUeo2qTUiKZTN7d2Nh4sGEYQ4tzKzMjmUxOSyQS83fcccdfAgiVn
iOfzy9vb29/e/
DgwSeXDpiZ7bVr196Ty+W6dthhhzP889SaNWvu7O3tTZaZS9uJSBiGERD4urq6Zjc0NOztv1Zra+tD
Q4YMOdX/+Ww2u2zVqlWPjh49+kxPMwoAIKLe5cuX38DMudGjR19ommZTcX7IZDIPfvTRR4/
vs88+l0Qikb1LhQgiQjqd/l1TU9OBoVBo7+L5vLnj1Ww2+2RjY+NtpfMNEcGyrPHMfK9/
fJvhOQCH+RuJ6FtSytOIaLzvPqyNxWJjUqnUowDG+Q5rA3AFgFtfeeUVpNNp7LvvvhgxYsRfrHYNr
HpqZnAcvvtt3cSUYNlWQOPPPLI3/tvLAAw890ATiSiiK/rCGb+FhH91H/
MJpjBzGOIaLDvGq0AbCIaXuVXmAdg9zJ9KQBR1RgA9AfweV/
7DbFY7BfJZPIRAMf5j4nFYt9MJBJ3EtHEKseo4lm4prj9SxuZuVsI8TVmngTg7DLHLgOwo6L9YbiTr
J+lRHQlM09V9D3NzF/2/x6bIInyu9G3ALSg/
O8RgJknCSE2MPN0Rd8aIpIARigOvVYI8YTjODMUwsK7RLTLJsbpv06PYRhfZ+Y9vGfd359VPPsAcCu
AgwH4hdQFcJ+xc4oTzv77749BgwYBwI9isdhfoKkZt912225CiHkAlk2aNOnzqVTqHQBf9H0sA+BpA
H0WVmbuNQxjdynlVABfq/
SazPw4ER2raF8EYDARNVbxFTJw57ZRm+hXmfkfgLuo9nH4FUIc6zjOy0T0dwC7+cZ3YywWuySZTL5B
RH2Ej48DEf1BSnk8EQ0rbWfmRZFI5Ju5XO4J+DbMXn8PEfXAnbdL27uIaAaAQxWXe5GZ/
0lElyrGcSczn17puJm5cxO/0cNw5wHVWqPEMIwvO45zNIBfKq61CMBQIqp/44030N7ejv322w/
Dhw8HgP39/
lK1oJZRQjkA+OY3v3m1SlgBcC0RHa2YsB9h5kI1wgozzwYQVyyOaSLqqVZY8c6nXBy9XACqB2guM2c
RFFae8YSVm+ATVph5kRDi6EQicdWWEFaY+T0AK+ETVgDAm9S+gfLCCqAWVl6AWlhpY+aTWZ0R9w0Au
5cRVgIOw8y8FuWFgPfhCjMVCysAbgPwdyllwIGWmTcQUTvUwspjQogpUsoXFNqS+QB22MQ4AwghTmT
mkSphBQDKCCuPANgVQWGlnYgeAXAO4KqTS3gzGo1OrnRcmq2DZVlF5/5QMpl8Dj5hhZk7mPlm+IQVA
BBCXOw4zimoQlgB8AwRBaLpPM1drBphxfMnXA2FsMLMvQASUAsrzzLzWPiEFQCXNDc3P0dEz8EnrAC
YHo/
Hz0+lUk9sCWGFme9i5rF+YQVA0jCMg3O53A1QCCsA4GlK+yvalcIKM88CcLNKWAHwoJQyMFcyc493f
/2s2MRv9CjctaRiYYWITrNteweUF1Yai/
Nacf7wtD8/2RaEFaC2AksWAEKhUEDaZOarmHk8gj9Giplv8tTklbKAiNoQfCkA9yULmFI2hadyV75E
zPweEQ1RtG/w+g7ydX0YjUaPTyaTFwP4sa8vbRjGwVLKE8o8/
NWyBMBkAOcq+s6C62T652pOyMyvQb0r6TIM41AAf0RwZ/Ke1xa478z8EXyTHjOvQRkhgJn/
A+AVAEdWMex3TNO8nIieV2hIegB8CGAP1XHhcPh8KeXLCKrwlwPop/
rty8HMPwfQwcxPVTH2vwHoAPAtxfmuZuariv83TTcA0HGcJdFo9FByHTY1NSSXy+UAIBQKDfQLEszc
S0TXqN51Zp7NzEuIqOLoNmZ+CcBoAHFfVwJudKi/fXO8i+BmCwBARIvKnO9tAA1EtKuv/
cFYLHa1Z5b4um/
c70Wj0ZOSyeSDcLUHnwhmfkkIkQHwTUXfYY7jjId6w7UpHoFaWFkohDgTgMqs8xyAw1RzDhElSk3IX
vu/4G6AVDwH1+/zC1WM+XYimk9EKqfvpUSULd1AWpYFAOjp6XkxGo3eVMV1tio1E1gikUgTADiO4+
+6FsCxZSb/
S+A+DJXmEljlLap+W13xgRgdPKQ8zKxUG3q8AcULzczdRDSViH7oa18XDocPTafTJwC42teXZeZxAP
YEsCXU+EkA5wP4k6LvBiKaycyPVnnON4loNBS/
hRDicNu2zyWifUvbvXsOqLUhM4joc77PrwXUmgbPlPcHABdVMeaVoVDoe7ZtPwbFTpGIniCiAxXXWs
TMx2Wz2ekAdvZ1twHoRnWC72TDMN6UUj5T6QHM/
BEzPwtA5YvySyK6uLShOOHMnTv3Ik+lrakxQoic909L0X0ZM1+saAeA3zPzI1VcaoZn0uwzHzFzJ4C
eKsywRe5XaWo8noNi4fR27CsRFK7/
FovFTk6lUncAOMJ3zOpwOHxYKpX6NYATqxyjijlCiAeZ+Wf+DiHEsUQ0mogur/
KcDzNzYIPEzOtM0zzc80Hxa2RmMPOXoNBAEdEH8Glzmfnf/rYS/gFXm3tEmX7lMcx8teM4T/
s7mHk9My+Db04ubnjmzJlzZxXX2erUTGCxbTsFBBxb/8TM3yaizyoOeQjA8UT0mQovkQHwFyI6z9/
```

```
BzP9RSP2b42ki2lvh7AZmfpmZdymjwv8jgAt9n88KIcblcrmxzHyX/wAhxElCCEvhbPyxEEIcx8x/
UEj305j5Jinli2UcQpV4as8mqBf973u+KX4z30oAGSIaqzjfa8y8l6+tk4hSCjUumLkLwHlw723FEN
FR+Xz+Mig0FHDNRAFVPICkaZrjiOg2IuqTCMvTyLSizM5TBTO/
4t3zl4moYfNHAAAS3u47kHaciP4Id4fYR+vDzCkA6Ozs7PQfo6kNhUIhC2CjU38RZv4ZEV2kmlvgbt
L+VMX7OQ/AXACHKPo6UH4hLMftAE4p03cfFA6fABJCiGcRFDqWCCGOSiaTv/
X7cTBzZygUOrBQKPwAQWfjj8NKIjpPSnmbou8iZm4DcH+V53wawIEUTEWQIaIDHce5HkHh7X0AI4ho
qP9kzPw4gK/6mpcSUb8yc8MCIpoMhUmnHJ6G+ngAjyv8d7oA/
JWIDlAct6HSa3ya1ExgcRynT6ItIrqMiD7rXxQAgJn/
CTd+PeB7ocLzFbmImS9T9K3xHCMrhplfBTASChWd19ekWlgBXE9E5/
gbiegHzNzIzAH1HBH91DTNfzFzxbvvTSGEOEZK+RP/
d2bmf4ZCobOI6DkiGlTp+TzpPwM3isHfNwluqOa1vq4EM//
br3HxjnmJiHZQTMjvoIwgIIQ4hYiuq1LIOl5KuRfUJrFbEHR2BjP3CCG+6zjOhVB74n+I6hx9/2VZ1
o8AvIQqHHOJ6HQAAXMdM0+TUu6IoAkr2d7eHnAm1tScHADYtu0AG81A44noXATNjGDXWf2YMnOLipX
eDt9vXgaAVVWcp3j9uwEcU66Pmf0mbgAAEd3k12owc6dhGIdIKU+CK4T1QQhxWD6f3519kXIfB2buZ
ObjpJR3+OcIIrrTNM3pVZpiAeAFZt4FCtOXYRgHwZ1XjvJ1LYBrflOZv+9CUPOfYOYk3LXG//
l1AC6SUt5axZgLQojDmfkGIvqyov+Pfs2/x8p169Y9VMV1PjVq7nSbSqWuA3C4N/
EGdgXMvFoI8SEUC0o5iOgCZv6NYkFr38RL265qZObZRJSHa57x980iojbVQgzgDmY+HL4HnJkvALCC
mf+q0MjcKqV8Mp/
Pv4lNJNWrFG+HMRbBxXZZOBw+rFAo3Ivq7KAriWgWEX1Xca3LDcNYwb6wPE8L8ZrK1ALXJ8NC0Mzyr
MLfp8iJUsofQ+0AXI5r4U7YUxR99zHzd6AQIIjoGM80d4a/
j91Q5a9UMYY2IjrOtu0nqDon7wnMfCWCz9E/
iWgJER3t+3wKQHrw4MFf8b6Dzmu0jXDeeeflAICZJVwz8He8Z1llmv47XG1IYN4pQ4qZryQilZP7Kp
TRrDBzR5n2J+E+3wGHU7ja7j1UGx0iukJKGTDTCiGOcBxnLICbFec70T2UqjVLKzEM42gAv1Zs0l62
LOtS27ZfQBXOqnDnqboyWvlDHcf5Dlw/
wFKWwTUXq8xl9xDRAYr1aTYR7aX4fIdhGKcCuM3v67IpiGgSM3+HFFFinj/
UzxWHJQ3DOMCyrGKx221q/qi50+3MmTOnMfPeRDTB/wF2wzpf96sPN4UnEJzpf5mYuZuZlSp4T/
2lejEXCyHmQO0DswjuTlnlsPU0M+/
of8CJ6E4hxDRmDpgDmHmaaZqXA3iZiAZu6jtWAhH90VN7+u3iKcMwDsrn87+GWm1cjhTcLJ0qs8mtR
PRXx3ECuxYiegLADxTHzGXmZQrb+Fsoo0lj5guY+YBN2NNVvCCEmEJEKvvtk8w8RGWCZObTiWgQlzi
ylo6xmjGwG5J6OLtOzdVEM/2YiI73H+MJ8Q/
Apzpn5m64kRw7NTY2jgEA0zRVZkpNjWDmHAArFotdAuBy1QIFV1OSVanqN8F5KpMhXCfbcsLKmjJmq
BeJqH8Z0/x0ZrZUpl0i+gMz/9C/
qBLRaUQUghuG6+ciIvqoGn+uzXACM49TbHjmmqZ5Qj6ffwrV+ZvN8ebRbyr6TibXH+i3vvYkuwEBgW
PYDTP/LHzmdE/
jo3QyNgzjGMdxrkF15rxbmXk9gOv9HUT0a2YerxJ+DMM42HGc7+28884XAMCwYcMqNnd/
GtRcw7LHHnscTeUdn56DeoEsx+
+8haSPVMuus9mmnDdVpoV2AI+qhCVmXieEuJaIVCanWcycJqLv+NpfsSzrMmZ+RbEzeccwjNNt2362
zCRRFcz8hJTySWa+R9F9pG3bhyO4I9jU+bJE9GcoJHJmfsI0zRs9Pxi/p/
tTUP9+S4noSQr6ucwHMBQK7VJRVUzVhXcvjkQiZ0gpn4XCEU4IkSqjLboCwBrV/
WM3YqPSXS8AwDCMUxzHOb9KIefPAIbAp2Zm5i4hxOVSSr/
ZDUQ0F55wUwxL3GOPPbaJhE+ajeQAoL29fapKi+gtMsuqEVaIaDwzX46g1iCB8tFAK1TaZs/
8noGb4sDP35l5rmrHDjdk96sI+rX9XgjxkeM40xTH3EpEj0opXyojOFXLhQCiCnPUhkgkMs627SkoH
zShYgUzv0FE3y9zrQwrfBDhbmhUGuIXiYj9Y2A3MCQwDwGuSd9xnDPLCLZKmHmWZVl/
UbkcMPONnilPZaY6xLbtUQCuKzrdDh8+/LJUKqUyG9WEmhU/
ZOYcESEej5dzIHqIiCr2FPfUbFH4ws3YjdLJQaFB8SYHLuML8QcA1yjaM0KIc6SU9yq07cuJ6BX4bL
Se38eEfD7/V/jMH8y80LKsI2zbnorqXqZy/IOIrgTwJgC/
gHYiEQ2A+90qhoh+I6W8WPF93yaiC2zbfhPB+/
sWANWkmwRwPTPfXtrIrnNYNxEFws+Z+Qkieg1ANVE13QCOzGazUxD0hVkA4CVmvjp4JO4goufhJmDz
8yGAYX7t2Ga4kJn3g+v4VinPCCHeZ+b7FH3nSymv9gvfzPxa6SJXjBL697//
Xa1joWYr4s1FYDdtQx+8zdMcAOXMoSrOYeaJFAxGSDBzuIxFcAkzD1T0LSGiN6E2FczzTKqBkF1PY2
wpTOPTTdO827btvyvm2OmmaV5RKBTeVpmWPga3AvgI7ia3dGxdRPTdbDb74zKCRzlSAKYQ0e8UfTcb
hjHDtu03FffwaSjSLLCbu0uVTO59ItoJru+f/
5hfOI6zR5XjXmFZ1vhCofC8Yp56CO5mUJWKYpJhGI6U8jHg/
+cPuL6j24yWpWYalrq6ujqgb5RQCfejurC2v8L1jlc5uCagFlY6iKid1HlTfsGKEENm7vWcua5X7Ag
yzHwLgg5lScuyjiKiB+GzR3sC03ds274a1YWpKWHmfxuGMR7uS+P3ybhUCLFISvlAlae9FG611j7fl
5n/FYlEjoebOdfvTzKXmXdWHNPFzOcw8/W+9h4i+icpHMOY+V3TNH/
PzNXk3gERHSeEmACfOc9Tg98AXyi5x9NCiGvLJIZbCte5WuXt3+pv88ZwJ4Bez0xZEcz8nhDixjLCy
i+J6DwKhqW+6N+RFzUsQ4YMqXhnptn6GN4Pw8FIoQ1ENLvMzlwJM/
8Grp+J34SaASBVgjUzr2bmBgomJEsCuANqYWWFEOJ8lcMnM38khJiPoNl3jmEYFxYKhVfgm4uY+V0h
xIRCofAsEY3BJ4SZpxmGMVWlUYDrNPwVVJH+gN2gjctYEbQB4DHTNG9xHOcFCkYLzYBaWFkEdyPkF1
ZWMLMNtT/ebUS0TqXF38S4u4UQxxQKhb/
Ap0HxNPsLieg0xXFXEdHMUpN+UcPS09MzOxqNqp6JmlATgaW7u3vogAEDvgYoX9x7oA6jU5YcZ+ZZQ
```

```
oi7yQ3v9DMPCo9rACCiOVBLjr8ionNVKkohxAkALlDsZopmBFWRqCMLhcLVCKbC7xJCHCyEOA3q3Br
VssowjMNs234QvheAme8RQjzsmW0qrg7s2aQPQzA6ahURHdzb26ty2l0ON2OiKo/O6UR0tf/
ekuvnonrRF4ZCoQm2bU8rowUrxyVE1F8hKGQMw/
iJlFKVCOkdZv6RlPIlBEOEN6B8rpU5CgECzPwKgOehdjIsxwrDMM4s7nJ8TAawL4L3+6/
MHPD5Ke6QFi5c+La/T1MbksnkV+vq6mJA33nPE1beAXC4/
xh2s8gGYOa7hRASgL8+Tw9cU5Aq6mgDgA6/RsO7xuUIRvcBrj/GiVLKu/
3vIDO3EtG9ChPMGsuyTrBtezr5HMw9jfJhnoZaFaxQLW9ZlnWxJ0D4TdJFc74qtLksQogLAfxG4UIw
A8AvbNt+GcEN4Rx2M/r2gZk3eOfzzzkZAB+SIioWrpboYbglDaoZ90mO41ysMD1/
QET3eQKunwe8jdXrpb9vccMzb968bSpDdk0Ellwud61hGBGgz4ubhJuNL2Av80wqgQRlzLzQMIxLHM
dR7UY/QHkHx2fhy7AIbFygj4I6v8hEKeW3VD4PzPxzdnMp+J2YTiI3bPF7/
mOEEEcA+BKrnTqrwpukDpVS/pF8WXjZ9Yy/
0HGcv6KK7JbMfK+UcqRiUskw88Hshsr5TT4JAA4UOwZyHe9+hOCifz8zq0Ink6FQ6OhCofCgyta+iX
E/
TkRvs6J+ERGN97Rjjb5jPgqHw8cAeBJBk10PXO2K6ll6C+qsuAsMw7heSllxaCAzd3oh6Pcg+Du96P
3tD5t8G8BuiucOXV1ddwOAEKJmZl9NgKleRd3SeW8+3N/R/
9uCmReV2WA8LYR4U7UAEdFCqP0TsgDmky85o3fMhXCL3qk4goiuh2/Twq5f25UArvO3m6b5/
Xw+f7fiWm1CiIMKhcL1UAhn1cJuqoRTC4XCMwi+M1cLId6D+05Xc84L2E3P4D/f/EgkchJcYcK/
gVvCrvO+P5Cih4gmSClvVQg/j0K9SfsngF8BqDYtwa+YeR/FWrMEwGVQ55x50bKsCwC8Dt/
3JaLV3t/
b1PxRE4FFCPETIuoGNr64cwHcBYUjqGf7U8alE9FEx3HuV0zY85i5nKrxOXbDWP08LKUcpZJ4mfk3U
koiop8ojrsObsj1SN8xv2XmMaxw2hVCHMPMdax22KoawzCOgnvv/
GaluaZpFnc61aheX4QbwqwqmjYOwCR/H7vZedugDtG82Lvn/
jooTwP4umrBNQzjYG9iq8bBdZ4Q4hpWFDSEGz3wcwRVpauJ6JBcLndXmd3OO2V2gjNY7XybIKIfSSk
frkabZRjGUVLKXyMoGM0H8B6AM33j/
g8zx6B+N2YbhpEGgF122eUTmxo1WwbDME4s7ly9ee85Zv6XakMDN1utKknmP4QQt5YxGb6D8u/
Lc4qdN+AudOdAoZEBcDgzT0AwuRmI6OdQaJSFECc4jnO54p1JW5b1DQCnkSIi9GPQblnWUcz8kGJue
4iZbytj2t0U13ibMH8hxtVEdFg2m30YwfezjZkjpIjsFEKcBDcQpI+2mZlvYmZVMMIKy7JOAjANVdQ
kg+ubshKuoNNnbER0BtwEf33wTO0ne36V/
jm7bf369ed7nzP8x9aSmggsLS0tqUQi8RwAZLPZWQBehjq74TtENFixoGVM0zyamaf41fHeRD5ItQi
ym1F1rGIheRPAapVzEzPfTUSveWozP/cz804Krcbjnv1RFf10FoDl7GY5/MQw85nM/Hn4/
HeYeR0zH+o4zm1QTDib4H1mflJlOyU358d+KsGNiP5N6gin2wEEVNdwtRNRqCu/
HialPB7qLJrlaBNCTPDCI/tESxDR+ex6xvsFpoRlWd/
1vqsqB9Br5Iv28vgbgJ0UO6peIcQJzHwH1GHySohoAjMfiqDDeCvcycjvxL0ebuHOwG6Z3YrR/
ePx+M8AoKmp6bhEIvFqV1dXtenYNVuY5ubm2dlsdjkA5HK5P8J1+FdF3DzNzKpEXws8k2YgTT8zv4v
yeYEeI6KAFpPdiJFvkSK/CBFNIDd1vSrdxAWekOOvE/YLT1uqSgMxLp/
Pf5WZf11mjFVhGMahhULhKgQdSN82TfMnAF5SmWo3wX3MXI/
g2DOhUOhAKeUfEKx71AEgW0YDfIqU8lQENbD3EdFRCo1LhpkP9SKZ/
HmpysLMs4UQ98JnPmI36eXxUsrbEfQhWhgKhY6wbfsBUoSnA3h91KhRUwGtYdlIJpNZDgC2bbdDHS4
7E+5C56+zkAVwuG3bv1FM2KuIyFBJu+wmeYsrpN1/
E9F0qAWm503TvAZAIL8Iuxlu1yg0Df8UQjwPRQ0gIrrMMIzXvbTsFScA2gS/
F0K0M3OfGkHewzrOM8GocqCUYwkR/YaI7lD0ncXM9aROTPUP+CrPekwnN2rqOl/
7YpSpGg23WvQIv118U3jq6WJmyz42c3LLylvkczZj14foIMdxfqDSgsG1VwcEPU9l2wB1ToTTPC1Jx
RMOgKullIbCD6CHiP4ERZ0puBEbKm3QfLjp13cs3ckT0QH5fH4BM1dcnVezdejt7V0BAIZh7Au1z8q
TAPZULGgrABzvOM7DCIYvz6Hy2bufBaCq2DxNCFGvMnET0a+JaA2ri6HeQETf9c+9zHyXEGIIgJMUx
4zz5l7VvFI1Xqjv9xRz7yLLsr5v2/
ZjKmG+HOwWipxNvjIu7AZZHFwoFM71b2bZjT4tl5DvVwA+R76kjuyW5RgDtV/
loUR0EdTh5OXGvdowjIvL+Lx9z3Gc3/mfC3brs323UCj8Eeq8L/
cBOM4wjAYA2HHHHauJUNrq1DIPiwSAurq6gDQOt2bCXChKqXt1cU6joDd9Gq4PRcAkwa6XdgrBRTUh
hLhO9WIy82zLsibYtq2yjy4goicRrOmwCm6hsqmK73SbZVl3OI5TcVr2TcHMTzHzdG+C6wMRHcfM+0
LtGZ9UtAFAUghxFrvpuP3X+q0QYhHUTmDvQB0mN5OZfy+lfNDX3kluErfAxEZusrvlqNJJjoh+KKW8
FL7fl5mfYOYZpEioJYQ4jJm/wGpHtA8B7O5fNDzhdgPUZQkuAHAsqsh+62myXlVN5ER0NTMH/
Aq8zwe0Puw6br5MXkbhosBSjMIjoiuJSNcVqjHCc2IhItVzMp1ch1j/
gpYkoiM9zV2f+c2b2xqhnlPehOtP5teEzBJCfKgS1Jn5HtM0H1MlgfS0wg0ILnRvENHibDb7s/
vuuw8LFiwo7TvFMIwEXMFpS/BLKWV/
BOe2lGma4wqFwh+grma+vsz5PhBC3A6FczwRHTd9+vQT7r///nMLhYK/
ez4UQRuvvfbaU+ecc87OhULBH2U6B0AnqVPkn+CZosrVbArAblmHsx3HmQpf3ioiOp+ITlaY5RKWZX
0bwEQENd7gkrxZxSihhoaG/
ZPJpMoZuybURGDp6uoatPPOO6skccCNMrkd6nToZzDzZ8uoKWdBvctPEtGbfgGHXWdKZcQIMy8KhUK
H5fP5+/zqUs/UchV8iyq7YdKXAZiqGMNj0Wj0onw+/yIqSCl///334z//+U/ZfnbTsl9Obr4Qf9/
PAJB/
fB4roJjYPI3MDxzHuQnBFPBTiehxx3ECE46nBQtMvOwWlzwdwDTFTvFPrA7zfQaudF+Vk5xndhtHQf
v83w3DuI7VoY6HSynryghnH8F18ParUVuJ6G9QqLvhOovHS9XuH374IZ566ilVNfIi/
```

wBwhZQykIEXwA3MfJ5fC+dp9QJmMm+3d3mplqY44XgCy6PRaPQT12jRfDI6OzsHRqPRgLALbPxtV8O
3SWM3S/I4KeUl/gWI3dxFGaij1+Yycx4+fwy4Tph3sFvuwc9z4XD4Yi+Hh18D/
DaAmfD5GTLzR0T0FIBrZs+ejfPPPx9XXOHK2UR0nmmas5599tlXv/Od76B///
4YO3YsVq9erboFm4Vdn795cNcHP0fatn0y1Avxv0md62UZEf1USnkvACxcuBDnnnsuVq9eDWY+A0DD
/ffff95PfvITzJ49u/R8r5YRPJ45+
+yzRz7yyCMTfJ9vZeY3qcRXqXit2bNnXwtAlNk4lUUIcWpf708AACAASURBVC5cnxt/
FNZVcAWYQPQYER1g2/be5Ea0wtf/EkrM4sUNj+M4BcMwqpqTtyY1EVjy+fyUcDg8EujjLV/
8Yc9mRUIvZr5SCJFE0LwAZp5G6lo1gLtwB4Sfp59++rexWOyBeDzeOHjwYOy3336YOHEiXn/
99bTn8HmpQsjpEkKcQ0SBfAREdCG7kTN1vmNejUaj45PJ5JNQC1QBrr76ajz0UNkAkxWWZZ3MzNN6e
npahg0bhlgshrlz5wLA7aZpvs3MgZoczPwvZg6pTkhExzuOc6HClv2iYRhXspsYyr94ziYilemjDcD
34IbL+SeJ3xFRoDCbZ4f92aOPPPvrGMccc02/UqFEYO3YsTj/
9dKxdu7bcfQBc57owgjuTpUT0I8dxnlEITCcbhrEeCsGot7d3sbc7HOUbXwfcHBWq8PPniWg2fA5v7
733HiZOnIjeXmVU6lLDMYT0XQK5sN4AMDBfrOmZ9JULnZEdBb7ckYUJ5xCobAmGo0GkpRpPn3y+fw
My7LqgcC89y4R3QsgkJWYiH7gOM7RCvNHFxHNJXXtmXXe+9lnTjzhhBMKI0eOAbEAwxBa77757bujQo
V35fP5JBNMiLISbldZvDm4jor8w800AsPfee+Oqq67ChRdeCADXW5b12O/fTTG3fbbTc8/
PDDOPvsszFsWFU1GAEAu+yySy4ej0j0+MxWLPx2IxxGIxDBo0qLghOJmIPqNaiOFuDQmmCQzn+htyJo
AYMmSJXj44YexaNGi2wzDWArgoQsvvBC//e1evffexfvhdKvzdswX3b33Xfv4v4vt8b2tr692rV6/
u4/dXvNb7778/H8CD/vNtCma+kplPQVAYfYyI3lUJP0KIccw8AupooXeIaO/SuVII1ASEEWltbH25u/
j/
23jw6iqJ7H39u9cyEVZiJEgV8VRABUVFfUEFQdggIssmOiiC7KIiAiAoCCoJsorLIIqDIokBAFtkXQ
RRFNkXZV4GQmRACSWam637/qB5Mqiu++ju/
9xPPebnneA52T0/3dLqrbt37LEW+NxyTJ5FXLKG+ToUje6RYltWIiEy009kA1ujtBWffEphXvWDmYc
z8kmF7/1KlSrUCgH79+mHBggVo3bo1zpw5I1u2bHnD2LFj+8DgeEpEXAaWU78JdpXgNqj2kAy33AGgR
CoU+NvWK/
244VZxm0Wh0JhGV2bRpEzIyMhAfH48FCxb8alnWONuV2V+pJk3MdIdILNIXheoCoWe8O1m5udt2za5Oe8
jpZirV2OuCCEaENEouMFm05j5Kbj778csy2rdqVOn77p37+4vUaIE3n///
WsrnWHDcl147CCinXAL9V1y2oZZDb+3l2VZO517pCdg57pP06VKoe/fuJtrnSJgxTrsBTOG/x/
YKMXMT27Zd4DpnlXMr3CyFX537bSr792LlC5JjFhBCgIhw9OjRT8hRV70eeR59Y//
IlrDstSyrNzObRNm6Qk22rtYuEX0JM1D8ChHNJIOFhcfjmZw5w/
PjxHOPDb7/9duLMmTNxgwYNKgk047Kfp5MAMOY+VoSExcXh169euGhhx76/
++uutmZmZ6NGjB+rWrYsuXbqA/qYfJzP/qpkGqpVq1ZWULISIsYHuhuwtACZgr7+nBYYPD/
nDWZOMb2DzPw1gDKGdz0DilH5Pgyg/
x07dqyKtcQeeeQR9OzZM6ZrtAlKC0mPwx6Ppz2ApdqvVqAKDEx89f3d33c3acgsHgbgCoUaO
GC+v4H+7FYmehWFPb/oNlWe/lUlFuIoTIyGUhuwtACZgr7+nBYPD/
WznsvxR5xRI6evbs2ewSzykAakgpX4SbNrYaCui1woApWAPFWjEZvH0AoDO57cXHEVGlfPny3Q8ApU
uXxuOPP46XXnoJCxcufCufJ//vzM4p0tUw+nM3Ap0+4B/
+Uz+erT0SDYQaiAQpX85fDsqwWUrsrX4LRh1q9dfj4cffhiVKVkKBgZZWGcBwGeAtDkk08+gsSz/
eFer3eRbdtr4e4zJK17DKqAH8e5DmK+0eqPoF1VP+cWW8DzV6ccuVi5eZ+Uq3cZdkTWR1xyVT6rR4OG6piqleU1/
r/9
i5QFcx7r15V69LYBM7MV5337a9GMoCnAoHAjjGBodmEz80cnULi58mmRbM/
qrVenQqHQHgBo0pVKKlSoVIZ/A9j6wRcBu1ZRWrVqxqxVkV/dvZWDSBDBnnzICNGciF5cuXLlA6V
LL0bv3jkr4h6PPP46XXnoJCxcufCufJ//vzM4p0tUw+nM3Ap0+4B/
AOAs3CrwJ8iouccc+Qp9vnvWsqxfTIs0qPZgYbh1ZcDMz0spLwHw6vvyIMdJuamnoKAMLh8EFmfpw
VjU/npv8ohOjlYDVyrMxZ0fiKkJm6thrAo3p/
D0CSlPIqDL4uRPR0IBA4duB6rVNW7Zs+Ui5cuVi58ewYcMO1ahRo83tt9
9e/vHHH8eSJddwakGPx+1N38DBQ59+
+umBDz30KVoV27drFWjeAYsr4g8rEgevfujflLy6NKlSqYNcvkV3iN+ppI2dDqq1atQuXKXlS8dOX
JkTFZW1kMpSk5VuyhUOjAs88+m79q/1lpypQg/bt22Pfvn65/
ds2dPb4sWLSLLLbcc7WEHULLly6sm+XLlA6V
Ll0bv3jkr4h6PPP4B4UL/zGOjx8/
HjVq1JAzZy3bx585mxv8WECRPQsmVLT19eAlyCy8cEwcvXXlA6V
+OC7bt263V62bFlUqVIFn3yicZFx/11eeXx8/fMv58+fj559/
Nl2165dCR07dkdq/R133kdgCp9nzpZBZERdcC31H4lwlm/KXyyy2YLENvSHEh0MNp9SpGv
C3rJ5FbM7GijDotIOV+1GESD+A+Fd8+L18dIX+0uo+lEwNXfFOtbVnetvTvaVKnsLoQhh8eVMp6TL8qCK
+lZ

x5hbV96qmnMGDAANSqVWtz6dKl55YqVarN888/j2z5/
P5p06ZNBADLsq5p0owfPx7FihVjZ2FQDADS0tIwaNAgVKlShW+66SZv7dq1N+7bt69K7PMJCQkAMH/
mzJmNAoHArSdOnMDHH3+MQCCAoUOHXvF6vc2ee+65a3gz27ZRvnx59OmTg6SE3bt3IxAIYNWqVYCyR
1hGbibTVcuyWkLRpXUGbD/LslY4RA+dOHKClUmvS5/
LaTcOtCwrijz0GzRFnrOEfvzxx5FCCB+Aydl3MvNpR/lzKdwZ4HEi+o3Mgl77oUz/
dMbILgArye3nAACDhRBfvfXWW9vPnDlD7dv/URD5/fff91+6dKnQq6+
+WqdmzZqYNEm1f0eNGnVu8uTJd9asWbPwRx99hPvvvvx+dO3fG6tWrs1jx6Us1b968e82aNTFy5EiMG
TMGGRkZ6NatG2zb/hdOO6Bnz55YvXo1+vTpg0GDBmHt2rWIvWTZ4h1WQnPXHvI9e/
bg3LlzOHr0aN9p06bVlFJi3bp12X/
vr0888US+HTt2lO3YsSPGjBmDrKysGOBtVa9evTYsWLDgtcKFC+PDDz9EYmIivv32W6Snpzc/
fvz4Cy+88EKtgwcP4q233kKAAzJ49+xyAmpcvX8aLL76IIkWKYNKkSahTp87SK1euxGVlQZ
0AgNdeew2nT59Gv379Qt26dfvynnvuKbFp06YcP4iUAuTDUsouW7ZsQZUqVWVf5SqfjIkSOXJ0+ePCT7
36JcuXK4++67v3rrrbdWvfnmmwU3b96Mt9+
+BoPa6Pf7n7csyzNixIjbS5Qog0bNqBx48bo27cv1qxZs/
COO+5om5SUhDp16uCOO+5AUlISBgwY8CWACht0XryvXbt2O6FZ/
78+dPgVJl27tyJbt26IRAIYNy4cSmVK1f26omnU9m7BM1Qk5W/
0hemEj4RbYCBKccKdD0USqMlt1gRFxdXqHDwq7V0/
XI05AAsH79+g5Syhbk9nbZ6PV6RxHRKkNVby2AkjBUN5l5MV9TXRtu2pRJSjRcRKwnw2GwSIWFHXzpCb8nzUsqxRUkp
X6bBXr17o1avX2wDe9vl8e02116698OMz87YULF1LS0tLueeWVV9CrVy8AQGZm5kpkU6YU69KlC8Ve5
IYNG+L06dN44Xjh8+fDhLSrnovvvvuw333/WH9csMNN6B169Y4duxY5TvvvvBM///
wzvv76a0yYMAFPP62KS/
Xq1UOscuBcwyIi2gHNqXjdunUQQmROmt2jQ22fU4f/
+WTJL7/8Mmj   GjBlo1kzJATRt2jQ22fU4f/
78L+XKlcPMmTNBRGjYsCGg1GArTp8p8+vVtKSgpWrlyJMmXKAEDwl19+TOaKEAPGZm5pkpU6YU69KlC8Ve5

8+bNQyAQuNXv9x8LBAKPJiX9sYZLSEjY0rhx4yVfffVV9aVLl+K9997LPratOnLkyOFKlSrd7vF4ro
1T5cuXRygUomPHjvWEslfJHkcA7EhISMiB4du8eTMAoGHDhlv0ZIWZz/366687LMtyzau//
PLLN1AAahNLMr1u3brnCxcujPXr1wNQbaft27fj9ttvT4Iy3NVbgKOEECXhZi4eDgQC7YPB4HITto2
I5v6VZAVQ4wcr4clv/srn/
y8iLxMWGwC8Xm8OdgMR9YXyl3GZIEJNqi59Cue4dTCsSJ3veR8aBiYzM/
MAAPTp0+fepk2b1nryySfx3nvvoVu3bhgxYgS2b98+Nman7vV64fdfO3yRz+erC6iKSbYYuXPnzm0A
cO7cuQQA6N69OxYvXozBgwfj4MGDGxcuXJhDtC0tLQ2G7wEAZGRkpHo8nhdIUV9z/
N5Dhw4NvXDhQtn27dtfW2FUq1YNKSkpePPNNycy87S0tDQvgOzXHbQsqy4RvXvlypVKkUjk2qQKNUD
8SEQLY9d19OhRBAIBxMfHF/T7/
cO6deuGaDSK8+fPQwiBTz755EA4HJ7n8XgBPfjgg4GePXsiJSUFADBw4MCXX3rppfCQkICqlWrhtKlS8f+VluIqNgNN9xQXPtbHDt+/
PjYPn36vH/hwgVMnjwZ58+fR//+/
aNXr169QkRPmFqAzLyGmV1gvKysrCsXL168gGztyez3IhAIvBYIBAZnvxcCCIFoNHrJsqNpNpmu7Hv/
3YVlWHAAIIXKAbB0dpPegiRI6C7H+UkqX1AOAi0R0FG6htFMAXmNml52I1+udGQ6Hl991110vENHdW
7duvVZdAbD/119/PQkAFStWjD3zuPdeVeROT0/PsVq/
6aabIIRoA+Cybdtfmn7v77//7n7v77//7nILb9CgATIyMq5haTZu3Ji9urKSmZexQSMpISHh248//
vjrGEsotmBk5p1ENOHll19udfnyZZQoUBAzNdEoVaxXi3Lli3788WLF9s/
t8XhyyDrs3bv3A+ee5ND1ikajrUQ0F0p1OccOHDgZwCoWrWqnqxcEUK8ev/
99zfSj7ly5crl1NTUVBNJgYzYAYmd3GGxZ24ZTi586dYOY1gUDgmWAw+OnBgwdLVapUCX6/
P1YxQJEiRX4hovxEdPf+/ftznOv+/
6aabIIRoA+Cybdtfmn7v77//7nILb9CgATIyMq5haTZu3Ji9urKSmZexQSMpISHh248//
vjrGEsotmBk5p1ENOHll19udfnyZZQoUBAzNdEoVaxXi3Lli3788WLF9s/
8/
PPE2+rxsnqbMNyPfbi6nEvtQnLq7twNpn8wGCPTVdfLXsfR/
9hL7qQVp4v/sYFsHERXOO8uVJSbnWVVmUeUOTWWYLnf0

```
+uijGDZsGFavXo3169dj1KhRZ0uVKhUsWbJkZbjjq9dff50rVaqELl26oE+fPvjqq6/
w7rvvRkaMGGH4uKqc2bY9DMCtFSsqcPzkyZMxc+bML++9997KWVlZj6anp2PPnj05jjt8+PC3cPs/
gYielVK+8cADDxQ+cuQIVq1ahWXLliEtLe18rVq1noiPj8/fpUuXQPZ7MWDAgIPOc3dfp06dsG/
fPsyYMQMZGRlYtGjRzO3bt5uM7Q4BOElmVebpZLacmOHz+WbZtr2c3HTVEICxUPTr7MekCyHqOgmfi
f56Pf6PIxgM/
ouZ74slKkQUEwRMgkG9G8DnzBwmzUAPUJUSyibznm17V9u2u5LBFNbn89W7dOlSfQDvxsfHo3Llypg
zZw4ef/xxFChQYCAzjyaigrFxo3///vjss892bdq06ckhQ4agbdu2177s/
PnzawBg5MiRIwDcp50LZ8+e3QPgHr2CmD0aNmyIEydOYNasWWjQoEHUAZLPMiRa7wPgggULFk5OTsa
2bduwbds2bNmyJTxw4MCRly9fnp6WlnbLm2+
+iU6dOqF06dLo2rUrhBBnly9fPgnZBB83bdqEfv36HR01atSxefPmffbFF1+ga9eu13B0x48fH+F8r
lAolFMiyxE1nVOtWrU7EhMTMXDgQEyZMgUTJkxYVadOnVeSkpL0+5AC4CkiWlCxYkVrx44d2Lp1K1a
sUN3waDS6FFCtn9i5brjhBlSpUiXjo48+KpqSkhKXHYQM5fXWS0r5maHyP5CV0/
Q7cMc3AOLJbYJ4BUrh1mSauSMQCHQgoqgBO5OnkScJSyAQeDQ9PX1j7P+J6B0p5ThDWfGiEKKnlNLV
i3XAoD649Vm+hmoR6eZTIKIWcXFxRyORyCpHMA3jxo1DkyZNMGTIkMxQKFRi2rRpyD5RZmRkxAQ9cp
TmevfufSIQCAzPly9f+xEjRrRavXo1Jk2ahHr11Fzk9/
sPjhkzZlm+fPmKdejQAQsXLsRnn32G4cOHY9euP1qC06ZNQ5EiRVCzZk2ULl36amJiYvp9991nIWfs
E0IMZ+YF33zzDS5fvpxds2A0M5cB0DZ27rVr1wIAJkyY8HZcXNzaCxcuvDxw4ECf3+9HxYoVwcxpVa
tW7fTpp5+mnjlzJq579+5Yt24dmjZtCo/
HM6ZEiRJ3rVu3Li4SiaBTp0546aWXwMy46aab+jNz+TZt2rTu378/du/
ejc6dO2PSpElZiYmJi+bPn1/lxhtvxOTJkxEMBtG/f3906dLl/
MMPP3xuzZo1JiXFtczsK1CgQNklS5agTZs2+Pbbb9GtWzfMmDEjvU6dOoWWLl2aAyxr27YtpWwTG5R
r1aqFcePGISkp6fIrr7xSq1y5cm22b99O7dq1w9atW3McV758eZcWzN69e5OYuSkR/
fvZZ59Fx44d0aNHD/Tu3Rv9+vV785FHHnnn66+/9mS/F6mpqecTExN/
gmMC99hjj2HcuHH46KOPUKJECQwfPvzeMWPG6AyeZCHEcpi9TkYws2uF7VTvXszKylquD+SsNDSGIV
vVLBaWZTW1bTsfETEz/6MGnP/
VCAQCJ71eb8VwOHxNs4CIJrBZofUHKLl2k0XJt2R26n4HwMMGosIlj8dTLxqNlrRt+5rIYe3atZGZm
YmEhIQVAF5Ettbz9OnTUa5cufMjR4588Lnnnst/
4MABPPPMM7Hzr+vUqdMIAChatKjrOqSU7PP5CiAbONcUlStXRkJCAvbu3QuPx/
M2Kzl5l9Q8M+8H8C4ArFmzBk2aNEGTJk3QtGlT/Tp0yccOXLknmHDhiESiVyjUOfLl+
+JunXrzjl79my5+fP/kLJ56KGHruzevfvA3Llzh48ePRo9e/a8pn1CRM/
07t37qerVq2Pw4MFYsECJwkaj0axIJBJxXNhrAmrMrlWrFt57773MsWPH1rjjjjtuii2cskVTAO8Bu
GfEiBG49dZb0bJlSwwZMgTHjx/fpEwoh3TNgsKIBvI7iZIXv9fn/VUCg0FQalZGZ+xQEU6/
TXkUS0WEq5Y8eOHVfPnz+/r3PnzjUM570eeRBTp06dDqBLvXr1RhUpUqQ7lNFm9jglhGhm2/
YGfQHHzAcBFNZbMKykD3bBUKkhoppEdEpK+R3c8utTWVGHcxj5ORQdZVh97/H7/
dVTU1P7ssGvhpXPzhm4BUCNMWXKFIwYMeLS0aNHl/t8Pj2R3ww1FrrE86DGovtgTv6fh/
IP2pG98t68efPI4cOHf96zZ89detWAiPowcx0ouf4cIYSoY9t2dXL7FO0GMAOafpgT7aDa4t0M+
+ZBtcVNDvczIpFI53vvvRcvv/wyunbtGRlLKl/
VjnMX5UCLabjhPChF9YhrbHJxQX9JUcVnJiTwKVbFt+OOPP+LEiRP7fubIJc5EnkGeiWiKIAUKBA
gTtgzsY72LbdHuZkJQS3vPrvQoiXpZQmqfQP4+Pjx4dCocX6uZwy/
bemiZOZd8OdrABAY2YunEuykgy1Ivg7ycomIvoCWrLCyjvoBUfxUk9WviOixTAnK2sDgUAPAEsMycp
Qhxaug7k2QCUjpmRlimVZm6AlK6xotL1gsGZn5jVCiKWmZAXKcXVNbuAwZm5hSFaWEdF5wzHH8ufP3
ywcDi+AOVl5F8ocTU9WVkOB/FwvNBF1klLWhBtRv8+yrLG5JCtHiagn1D3P0bohohFSSlcrCgp8ey/
ckt6/
M3Oj1NTUvjDbOgwmogFwPxM7iehjKeVqIsrn9XoDN9xwQ9WUlBTXCut65E0wcxQAPB5PK2jJCitwfA
sp5TRDsnKGiPIZ8CLbSPkKmdpK7S3L2i+lXAN3srISQHFDsnIaCvitJyunfD5f/
dTU1Ja5JCs7oSrbfylZOXPmDEaPHn05MTHxRz1ZcWAAk2FIVpx2fwCGZAXAyLi4uBWkRPdywAROnjx
56M4776xgaHGMllLeAUOyQkRPM3NJQ7JyAqoV60pWnEVJSRiSFWZexMz5YEhWAHxKRJ1jViRPPfVU7
Jiutm23NRyzXwgxiIhWGc6TAWXbYRrb3iOijnqyAgBCiCcBvAWH4EBEKFiwYPlLly79Y8Tj8ixhiYE
b4+LiTLiGtwGlhmrYdwnuNtAVy7Ketm17hv6gAlgaCAR6paSkzIRTws8WQSHEPAD9Def5ylBeBTO3s
izrvOPbY7q2Psw8yrDPGMz8ixDiHZOxIxH1ZEWF05lCh4lohAmECWBvIBBoHgqFpsFNd5zPzE8aetx
7LcsaBfNqZoUQYozp9wohejiVGt0E8RcAb9m27ap0ATjGzJMMgwCg9E8qk9up+FtmXm4YKEMejycxI
yNjPBSDTI85zFwRbunzvU4J1ZXsEdEbUsrb4ca6HAdgbE8CuERELaWUnxoSo5EAuusJmFNhugq3d9A
VImpARI+xsop3XR+AztCeCWZO8/
l8nZh5WewaHLyE17Isl+nl9cibICIBAB6PR69uQgjRNhqNtodGbYYCZF+G20X8kNNONPl5vOr3+5dG
IpGv4Aa672bmZGisEVaS7EeIqLK2PY2ZE8Ph8L9zGXP2AZhJudhE6NGlSxf8+9//
```

```
tkuUKPHz1KlTdRO/81BjhwtYCiXA+BMMODQAc/x+/
zvhcHgllCxA9njn1ltvLWNZlg58nQvlS9ZX2w4iel1KecHQarlERH2Z2cRAXEBEB+G0sLRYSUSHici
kibR09erVzatWrYpZs2Zh5syZ8Pv9YObhRHQXaeBqVsq8nVgZ/
7q8iIhoKDPrprBg5hlSyuoweAeRsn7phGzSIKRwVlY0GjUBefMk8kzp9o477qh9/
PhxCJEzZ2LmJV6vd04kEvmR3Mp+mWQwixJCdLBt+x1y00S/CwQC7VJSUobmUkF5H0BupU0Xn56ZX/
F6vRui0ehOmE21nmHm9w1YnNwiBUA/KeXnhopCdygKq/
5wBQG8BGCuvpIHcMLn89ULBoP9iaijtm87M99JmvIhgOPM3F1KuVy/
OKeX3tO27fVEpFe0+jNzW72CA1WKfJ6V3LyuMXJOCNGPmU126ttY+XWU0Y45KIQY7bycOYKImkaj0T
5kBlevByBJExJkBdQeDEVR14+ZCcAmIr11kyyEaCGlXADDACGEaG7b9ig9ESSij5m5FtwD6BEAawGY
BvgWROTP5R6NZuamMDCtiKhHOByeSET3ZduGrKys9KJFi35h+K7rkQdx88031z537pzJhmIQAEFmcb
jfTe+ZZVk9pJSfQ1mRZI/
pgUBglCMelgNnwsyniWgbEbkEzKAAmi76rRDiSSFEgWg0ushw3UedxYdRh8UUjzzyyKFy5cp93r9//
xzPPytc1stQlWZdZHEXEc1nZlcFnZnXxcfHPxMMBlfBXUH/EkCn4cOH63TjtUKIxWyGD8wi5V+3Vd/
njPHjDRWw7wHMyqXqvg3AchhkFpxxqkqpUqXyv/
jii6hVq1ZMLmGm017Tq+5XiaiVlHImzInHe8zc3bBwXwbArz8PToySUt6nzxlEhHA4nBUfH+9iTeVV
5EnCkpKS0uDYsWPtDQnLTx6Pp4sjYW4ShzO5MveQUnYkzXkTwGGv19soNTW1bS6r+dEAXK6mTqtF/
y4A+DAQCHwUDAY3E5FpwmjGzG/CPTkZg5mvCiG6sBJ30ulmb0Ops+q2BFdJUXI/
NByT6vV6EyORSH3D7z0FoCAR6ciwoGVZraLR6Dy4zbGOEVFzVnbmeknwfSK6A0AOtgszZ1qW1dZxd9
XR/hcty2pv2/anhr/tPmbOIiLdLfaMEKK7KVkB0I6ZHwHQU9/
BzD9DIeD1AfEKVMl6uqEkutK0OmLmTI/H0zgajY4hxRTLEUT0tAMC1pk/y1nRl/
VSbhDABCIytdG6er3eY9Fo9DvD7/2QmSsRkUvXgpk/ccq8OSqCUsrkK1euXNY/fz3yJkKh0Jvff/
99aQD6uPcZES2QUu4zJAQ/
EZFOgYcQop1t25MNC4k18fHxXVNSUj6GJgPhjB+fQWFA9FhNRHoFGgA6CCFOO2aN+nubLITo7qjz/
tU40rVr11dNNikA+jLzGHJbThx1FhE6fg5wKsrO79Wvfx8UEPnmmJKvE7sBvCmlXGdYFK+1LGuEbds
79DGClK7XQLjxZieFEP2llF8Zru9HKEzICsO+b4jodgAJd911F+6661oXbgWUFo2r3UNEraDmBxOuZ
B4zV9Wvj5l/IGVaaxorFxNRkIhcVSFmvpyZmZmhb8/LyCtac43Yv7NZT6SwEr7J7Y9hincBlCY3xS/
VsqzEaDRamc0o/JnM/
KyhAvAbVP9RX0WvCAQCvYLB4JdkMIwSQjzFzF3wH5Dx2jE9pJSjyN2TngeF23FhZ0gZ5I2E0jrRf1M
j27aLs4YZYearACIwO/
42tm37XXL3qy95PJ6GUImJnpEvY+bjMPD9SVnRvwoNS+IkCs0cJpieyJyEKsvqDJ5LHo+nmZRyGrTk
jIheJyIPzH37FCHEdFN52rKsZ6Dun55U7oZaXbpeWsuyOkSj0a5E5PLkYebhUsoEAM8bvm8v3DbwYO
ZBzGxSLX3X6/UuiUajq+F+/
uYyc4LhHoGVX1JpaIM1M585derUl8wcZzjX9ciDYOZa7FhQZDMf3uH3+7tKKRfq4xEUAN6VrABoa9v
2QCIqp23fEwgEWgSDwVfJYKYJYCrMycp2ZnYJ2hHRG16v92vbttfCjYEJQb3TH8ENHM4tgkQ0wLZtU
wtrCBG9QpqWCVSC/yIAE3D/jM/
nqx8KhbobfM+y887o4+txAM8AWGhaOEGZKq4mrS0NYDAzN4Ab+JpOShbhU8N8ctCyrJ4waIs5i6rC0
KqlrITh3oS5AtyFmZ+D2bZjpfOu6wuk40KIJJgXdrsc5qIpWbl65syZ+awwN/
+YyCta86Dk5OR5gFppMHOmEKIBET0JM7LaFcy8CMBRaPgTVop/
DQEEWDmY6rECwKOkYQ2Y+SwRCSIqrm3/we/
3t05JSZltWEWDiDo7AE1XC+lPYqCUsje5heHWQTG3TLLK3Z2kyAVCZuZWPp8vlIs8dhRuNhCc6+0Mo
IZpXzQa7Q0NiMbM3zHzfCJ6Tz/
AqerUg4abcVZ19aHaW3rSdAmq7OpaCTJzw2g0OkpPpph5ppTye2Z29bhZgc2GSClNegS9bNtua0g4j
xHRUhhA0qR6wcXJjKX6TAjxE2leLVCAvOkAXD1kAL2J6FVDuXah3+9/
KxKJrIJ79baUiLLIIBLmJIIW3APYRSJqEI1Gr9A/
TEfhfzkCgcDj6enpB7NVV054PJ4moVBoLGm4EahEXsdegRULrZEhgT7p8/
kaOL5RpoR4KtyJdQxvVlZ/
Tph5dtGiRcdFIpHVcGNnMqDGhndhVh43BinsxxTD8z+ZmZvBcbDX4hkocKuOW0wHUD8SiVSFecItaE
g6ggCaOC0fHT5wmogaE9F8vaJMijpcEG6/IQghnmHm9/TvA3DM5/
M1d6jkejX8KBGF4B7LD1iW1UFKudjQchpGRP82LM4BVYX7hbTWODOnQbWRXbAHACeEECP1BW6239X2
6tWrv//Txo88A92ePHlyJwBEIpG5lmU9KaW8GWaKmCm2E9EncFOAYVlWB6/
XG7Jt+2s9g2bmHxychJ4opBFREO4X5kRcXFyjUCj0GpnVUftKKYvAkL3mFsw8iZlr6wMUK4npX2Fmh
bwNoFYuK+x+Pp9vUyQSWaU/
5M41mrZ1hhJ2Mk3E7VhJ5OsVlCMA3gAw23ANi6WUFgwMAcuynmTmp2C2TlgE8+9tTkTdDYPyRo/
HMw2598tfAzCCtNYhK1uHkoZJPwil9WDCMS0mom+YeZLhPNugWjRfaMekARjEzC4WESv2QDu4E5Ltf
r//
2VAo9Cm5W5GbABx0ElVXEFFBQ0KXYVlWQwAD77zzzva4Lhz3j4rk5OQfpJRZzDycmRtGIpGOcKvcJs
NQRQUwxXm2dVZNDBRbmQ16HACWMnMzQwXnpNP20NvBGwOBQM9gMPgF3ABgWJb1BJSJ399hn73gtMx1
AsEyZi5rqlw7Y+47MGA1hBCNPR5PAf0dzHasPvZftSwrkZmH6udiJbT4hJRyLNyV7dVSym9hWIAw88
umyjoz/
+7xeBIjkch0aHMKM59n5qOG85wQQjRxEhx9jPiUiCIweBsBOMHMc5xENkcIIV5n5rGGY0IAerIZrA2
osX4vlN/fdaXb7OfevHnzMKh2kMs/Ipc4QkSvMrOrb8rMr9i2/
V0kEtkAd1n9CBFdNUwKAHAI7jZGGjM3DIfDzQAMNpxrGDMfITPF1RjMvISIEvRKDTOfc1b5JjT2p1A
```

```
DSivDvg8DgcAUBxnveqlNQYplEoS5nTJECBE2VA0uCiG6EdGnhmTgeyJa53yvHk2klHeSGUg4M5eJu
D3Uy6yDhvcLIfrbtr1SH4yc7xsOVZ3TB98VQogfoQkJOqvEz2H25vmBiIaZKlbMfEgI8SIUiC1HEFE
3AKMM92i206vWB/jDQogngsHgh3CLOO2H6mGbGBG5hhCirZSyKoAOHo8nAUD+lJQUo4/
J9ciTEAAux8fHvyGEKGcaP1ipluqxGqoa6aoEWpbVjIgCMGM8dkAtTkzVhjDcidEBZm4aCoWmkAZYB
wAielJKWQfm8Si3GAmgC9yV3u0AMsjMxuzHSkzRJFXQjohO2LbtwnjkFkTU0rbt5rlUKFoC6Egag8c
ZBz4izbfH2TdTCFEempcTgGSv11szGo2+AS0pcdpHO8htv5Hs8XjqSSlHkuMrlO2Y9aw8o0xyE5cAv
JPLHDRASjmA3FormQDaO4u43Fp5pZl5t9/
vLwkAc+bMMT2PeRJ5nrDcfffdN0opV+mDfC4RAtCJmecZJq0PvV7vLABrDX3QEDOfAFBd/
0JWypGu7N6yrGZCiLtgRnZP9Hg8XzGzq8+YWzDzd1D0xNba9qtCiCkwJ0XroFoMJk7/
kkAg0CsUCn2WSxJmuoaZRLRSSukSeWPFkNmsg+Gc62tr2/YkuJOBk0Q0E4ZKFzO3gsrQTfS/
zwC0MWzvSUQ+coNlzznieYvh7qWDmWcQUTVD5ewHZp5sah85CaKpr3va6/
W2Y8Vy0kvXFy3Lamfb9mdw34teULotORJHZl4nhDgCd/
UpaFlWojOoPKsd87uzUjYllbkGEb1ERJedwegaEyUXKvb1yIMgIsHMWSkpKY+YpAycz+hj214hxFio
xYv+2aellBeZ2QT4PMzMReFe5WcAOGvYfo6ZGxDRqzDrqbSTUhaDQUX8T2IulOSA3g4+BuUwbhoHxj
qTukmvZKAQYrVt22vgfgeNwczPk8LOmRYnzxNRGUOF4rij62XCn6wnoouGBVcIQG3bttvAgF8j5VLf
VNt8CUBtx4Vdvxf7iGgGEU3L5acNhFmOfxRUUufyeLIsqyMzv6y3vQxRtESJEl0BIBwO/
2NwcHlGa2ZmQUQoVarUHLjLhMYQQrSWUk6EGzS52u/
3DwwGgxv0Scs5125DewEA9uoZLXBNOCwLgImdMtfj8Xxg2/
a3pv4eK9qsvpo5SkqJ0tQ6GscGnyTn2tZB84lxzvFtfHx885SUlHFwvwDGYOa1TtXgO8N1bySi8axU
cXPsIKKnHIBfDsquk8hMZ4MeARE9TUSHpJTf6N8HVTVoYCjZ9rcs67CU8mv9PKRofB/DXSqN/
a6CcGvOnATQhxQ9UT9mHRG1NWzPtCyrWSQSmay3WpxoJqWcZHjG3gdQ3nAN+4loNpupmI1t264HrYL
i/N7xUMJUfzmYeaIQIsm27Z8om18NAITDYZPO0PXImxBCCNt5Lv/
jIo2Zf4diQrpkB4hoKBFtYyUYqGMeLhBRGhlYZaTYcHob46plWU9IKZvAXNXrDiCNFMvIFKlwC+GtI
aJ4uBeKQQCLkc3nJ1vMB1Acbnd2AJgSCATeDQaDm/
7ChBuLkUKIQ8y8ybBvlBAiaGgrXbQsq7Vt2y4sCYDDUGDoHOBlZr5sWVYdKWXFXMbzr6AlJMx81ePx
1Ldtuyq0ZIoVQ/
INxzvI9WWslK4Hwo2PWcrMt5CBWQagt5SyBhmgBVBM0hzzarZx5B8DvM3zCovP5zNNDKboIKXsAzcT
5ycAbYLB4FJyA9cApSJrSlaOMrMLMMbMIxwZa9NE94XX633ZKUW6VvpQbBc9WUll5hUwJytjyEw1O8
0KDGVKVg55PJ5GwWCwFxkEj3KJn7xebzsoAKcubHbAsqxuAFboPW5n5d/
YUMIEKdlnl7AZ1OC6UUrpat2wUtO9G9q9Y+bhQoj1phaMEKI9lPqii+UE4IAQYh8MAwEzt4GSztbLn
vtNv8c5VztmbmMqUQshWjJzX7hXfauJ6Ccoe4Ls13AByhLAtToSQjzliLm5hOscCf+hpuv7k/jc5/
NNtW17e/YBNjbgrFmzZsPf/
L7r8V8Ky7LyFSpU6GaYx48c4WAr2pLC6+mfn+f1eqdKKdfDLSJ4lYhOw4A/
gapqmGxQ2rJydHc9k1BVjV0wU3MBxbzR37OfoIQRTYnHRzAnK5ugEh9XdQLA8kAg0CMYDM6DJrb4J/
GpEGIGMy/VdzDzYmZO0pMVVkD2ptFo1LQwDjHzFiLqox1zlYgSmbkQDIwgqLaci5ThLAZvhEHhHEA/
p5VsWhRPJGWKqdOXv2PmPWTAW0Ip34ZhgB0w869OJS5HZGRk7AaArKys6wlL8eLFKwM5aM25BhG9zs
oeWwdunsyXL98TTqvDlDXuhYEF46xaiur9PQAL8+fPP4WU+I8ue74GwHPhcHgFDMh4VqqTukJrJhRg
qo/
h87NZiYDpk3cagIlkYOIASLYsq75t21Xw1wHKJ3w+X2IkEpkC96rqHIA2tm0vhBsDM5iZC8Nge8/
Kw8IEABvp9/vnEdEKvS3nrAJvN5xnOv0hJ6/
TArsxc1uYmUzJUDL+LvlpKNDu6+SmfSbD3BMHgCEAChlKwzF2QxW9/83MPzOzy8COFYPhaVaMCL28P
8C27bO56FCMYeZ+hmNyDWZe7/F4hobD4Q2kUcbT09N3A0BGRsY/
ZsD5X48bbrjhnri4ON9f+awQoj0r3xe9dbPe5/O9kpWVtR6GqiMp8L5Jr+cQDIm/
83wHWYms6fGOEGKRlDI3vMhP0FhEUG3s38jgNA3gbWY2CZHtB/A9DOMKM3/
nMDWHwgzSdwUzr7Msq49t21/
BnUxtF0KMdFo0erSAak27Ku8AdpKBqEBErTweT7IpMYJqfblaW0T0nGVZyWzAbgohXgIwEQaRSlb+c
Qlw4+GOCSGmkllzbAERfZVLa2kHlEaX3v7eeOjQoc+c6/nHjB95lrCcPXv2gGVZV//
T55yJPUREL2nb0wA8kZmZOVqfSJw4xcym6k0Q6nfricK3Pp+vT2Zm5hq4M+ttgUCgBRHNI7NS4DEiK
mrIhj+DGUi7mpTksqusSUSjoCoKOcJpwSRC0bX/
qlBTyOPx1MvKyupJbnnnq1Av54dwaz1MZuYfYfAIgmq1mGTwPw3A/
1RWAAAgAElEQVQEAkNCodBCaIMiK62QW+AG3SUJIQYy8ypD5WckKaE7F7iPFXXd6NdERM+RosfrYDg
g99bjZ0KIVWzAukCxgSKGROaiZVl9TSVyIUQHInrH0EOezsxfEZHL5sB5zjvAXeL9s9jj8/
leiEajq/VkBUDSyZMnlwFAXFzcP6YH/b8eqampv0Elzn8apAxK20GjrLMyQOwUDofX6G1aZ//
PMOtBJQNwWTQw8yxmXsfMJquR6UKIMU6b1vXuOOe6X9t2GUrTyATK/
YCZO+sLRWY+C9UKMlVdTnq93obBYLBJLpOxKfYHAoGm0Wj0c3IrBJ9g5q6OyJtetWonhKgMs37Sz3A
L04GZuwkhtkej0TUwU69NCeXrADY4BAKdTv4WMw8xvM+AwjIdg7uinAagj5TStIjdBGCOlNL0910Gl
azoFO+DzmJaOv//jxk/
8tL80Gfb9mnTijZbbBRCLIOhmmBZVgsnUzc52aYDuFXvvTFzBjNnGCbH4wCeCofDX0LTPmDmXX6/
PzEUCo2C5r3h7D8DBS7VX+gVpmycFRD0KsyUwNHMPMhUBiSi1lLK5NxYMobzZDLzE9Fo9EEyiKgJId
qRMtCrrh23yOv1fgggNzn3fxl6mpsDgUCHYDD4ObREgZWZWlG42Qjb/X5/
B9u2FxnwMV8SURZyoYsLId6GoljrMRJACZirP8ZgJan9qm3bJobFCiHEBhieP1IieVOgDXpE1JmVuJ
NezVoTFxc3lJRZmb5yWgalDfR3PH+OA+gYDoeXwa2TsYuZCxQvXrwqAEQikX/MCul/
```

```
PaSUnuTk5FUwCINli9FSylJwA/
QvQDFaFsNsChs0JTFQrvOWoYK51rKs4axApPoKe14gEOjqYGdc+ijZFiF6rIO5pbMQQHV97HXG6o9h
Nou9ZFlWbdu27yOizw37TXHS5/PVCQaDww2t3VSnVfwFaXpbRNSXiLLY3OaG6b4S0Xter/cL27a/
gbvKBP1+OzGViD5wkkDd3mUpET0Bs27WKSgvONd8aVlWZwAfGOaN3US0BMoXT2/
Pz4Rq2d2nbU8TQowGsKRQoUJFnN/xjxk/8hLD4mPmVFKOw0HD/
v2knIVdgEUiekZK2cyUEDhhBBOTcvvVrdnTmPkJAJPgTiIOeDye+qmpqV2gYRScSCWii3CXbH9mZlM
V4iSUu6qrIuQ8QM+R2YeoO4CtTiVCx8gYQwjR3rKsTDZz7XtLKZ+ERqVl5q99Pl+vSCSy3NAuM4az8
ngyGAxOg1tYKUhE+Q0D2wGHzjtRb+WxMoPcykq3xHS+Scz8nGGA/
ZSZj+U24OTyXWegqkyfGZ6L74QQ4x1dBD1ipo85Vk9O67Ic3M6vewA8n5WVtQbuxG0lgNtM1bY/
ue4LTrl9jn4cM/9GRF8QUR2/318PAO677z7Ts3g98iZ8RJQqhJiey/
4FRHSANJkAVjiJ5kQ0xVTlZcX8MTHoMpjZ1vexckTu6iyA9Fb2F4FAoKOzADG51R93JkC9GrjD1AZi
hV0rCEOSJYSYpv9W55hMZm4QjUbjpJSmVospUr1eb4NIJFKPDPg+IURrACbQ/
GgAm0xzTW7BzIuLFi06zNG/0qs4uR7j9/
v7SimTyA3q3wPFejK18q6Soi6bGEHdpZQ94R5XjgD4jpV5rv59k4QQewG4iAdE1M1RYK9VqlSpgc62
6wkLgPxCiAxW1F39ZTpnWVZnxxRQLx8Ok1Lejz8Ra8vlBp+AIQu2LOspAH0NL9oxn89Xm5lrMvN403
ly6Qlfgqru6Kj9dADTyKBJAjVp1YO5ZTE6EAhMdaoOptWTKXp5PJ6ttm2vMFSZxgO4nTQzSFZGh0+F
w+HP8dfVK5OFEI2g8B8mFc18cDs5n86XL199KWVPwzWkAZiZ2/0GkETKb+h2bfsOZl5OBr2E3IIVI+
hJIYRLLwGqevGilHKR4f5NgkpIHtS2z5ZSXoBW1mbm34UQLaC8QXStnw1Q1ScToj+3CAkh6kspx+jH
MfMZy7J6MPOQ7NsLFSqkJ1DXI+8irnDhwvlt2zZNwtuFEDNNrUnLsp52kniTLDtMVVknQoaK8kUArZ
zxVcd5rYyPj28ZDAZHwaDsyswXWIE3dfr+eRiwGk4l5leYQacfO5OtK4QQ7ePi4o4T0cpcFnGuYOZG
UsrCpvtHRE/btv0KuQU7Z/t8vglSyuV/cg/12E5EXUKhUJL+fX8Sm+Lj458KhUIfw/
03TAGQDoPshnPtw6WUJrXa0cxcFm52YioUbd0kh/
GJEOJLdqQPtH2vOIvBBAAQQsQBwN13361rROVZ5BmtmYhKxMfHVyTN6MrJJlvatj3NsDKfC6AIaXiW
/xSs3E5Nwmq9mbk+aT4UrHQ/amZlZZUCMI/
MtLLvc3lYi5g+T0RvsVJZ1L9nJyk8iy7tDAALAoHAoGAwOBeAielkitGBQODDYDC43XD/
lhHRBWiZOjP/5vV660ej0dF/
9TzOhJ8opWwHzR4hFobW1SWv11snMzPzMZiFkGaQW7Qudr5dpCiSeqJwSAgxBn/
DLdaJZ2zbfoCIdC2FICsX6nlwJ9LrnOdVx8fsFUIsY82kkR2qqG3bHxLRw9oxO6BsE/
6yWigzZ3g8nkTbtgeQm+kUBNBSSjk3luTHnrXLly/v/
qvnuB7/3RBC3FqiRIm7De2Cw5Zl9TOJoTFzfyllLyLSJ6Y/DWY+o1cOASWixswTDM/kVr/
f3zIYDMac4vXvuwLlxu6qKBiSIkAJTs7PpVq61DENdS0uiahv0aJF14RCoW9gVvx1hRCipcfjOZqVl
bXbMP4OkVI+aXhnlgcCgd6Ooa1p/DXFMZ/
P1zwcDn8CMxnAFHuZ+cmUlJThMLfLTsNcyYJTIellWAAvgmr5mFplNszJzx4ArzuLUz0+B1A4exstd
h+PHDmy03RteRF5VmEpWLBgLZ/
P56JSkVIbHAJ35WIzKU+Vv2t1HTRM3IACmxZhN8sk6PF4HrMsK44U28X1QrGS0f+rmTWcc/
Qy9BEPQU2KJg+N7YFAoI2DjO9g2G+KTwOBwKCUlJSZcJt07YLqL+vJyu9EVDcSibSAgRGUWxBRSynl
QzD3no1hWVa9aDR6IxQYWY/tyMVHipXPx2W4X+oUy7IGSylNYNk/
i5GWZR0mIldZ3qm0TYS7ynSEiH6BJqjl9HzfyqWc3Ny27UHkVjY+6PwmlzfVn4UQIlFK2QBaKdcp+z
cmxSxzPUsHDhzY9nfOcz3+O/H777/fxMy3eL1ePVmJOZl/BnebZSopEPnfTVZO55KsPMPMLxkm7x/
9fn+jUChUB2axRwA4/TfaH5kAhpiSFQdjVcuQtAHAR36/
f4IJvP8n0bto0aJfZGVlLSUNrMrKN+h2cttybPf7/a0cRV+XcGguEbQsq344HB4DtzJ1bnHU6/
XWFUI0J6Ih+k6nMpXb70wioscNydR2IpoIIDdpfZOg3kWoyvDHcFfyf3IqWXprLgIA4XCYcznP/
3nkScISDAbnhMPhIprFeszjpjHczrO/MXMy5+Kpkls4KwJTX3ctlPjPSG17GhHVEeL/
sXfe8VFU6///PGe2pJC2KUDA0BRUEERFqmJHUBEVsaKoCIJey/
Uq9orlitd6labYuKKIBRRUFFDsIEWpASGEAElIZnbTN7s75/n9sbvczewsknu/
yI2/83698iKcs+fMmdnNzmee8xThi1TNtRtb2oytGRDRM5Ebk9WEWkZh7HwXtgkhzvV6vWPowD3jl3
k8nit1Xb/OutWC8BbHTMRH/RgAzmDm9kQ0/
QCPA4S349IRFn0HyjmhUKgUQFwCrAgDbCwyUYvbNsQXVfRTuJbT9ARffIlYAGCGlDIuKSARXcjMt5H
FR4CZazmcS+cvNmPuklLOsNm6HEtEI8hSkAzhwoQrbNp/j3MRjhB7yNqhadoIIroJFmuN3+9fH1nL/
4yX//
+v6Lqe7vf7lwHhgq9ROOyAf6Fpms8h3tnya2bujQRbBfuhKoHF4PFIodYmySaZebPD4Tirurr6SNin
9wfCfitxSTn3w82wT0D3GxF1SbDN81mkhtEM2OdvseMpj8fzkmEY06wWIw4nlbTLSLuOiM7x+XzjcY
APgxGfmvNM07wZ8WVDElGhadqQYDDYlRPU7UlgmYpu0Wcjfrt4G4cjiT5vxhYWiOgiZh5l85CkA7hf
ShkX8lxZWflmZC3/M98ff/
iWkK7ro0zTHO10OpvkYOFwbZ4MIrJGeFRqmnaTaZp2WWfBzEs0TZuaIK+FHb+5XK4rA4HAtljTIYej
h4ZlZmYWRkyEdllVaxJYa+KyPEZYiLBYiLPiENEQZn6GiKxPxFUOh2OYlLJLog+5Db9kZWWdbxhGD2
ZuEtHCzNUul2tYIBCYbGmvczgcQ51OZ5Xf7//6AI8DhPdNK4nILrR6O+w93K/MyspaGjHxWkP/
aojIjwQhx0S0GjaJoojoDg472FpF5TIieo6Z42r9IPxFdYuU8gsispqaJ3A4109c5mAi+gDhEvfW9l
eklLdRuI5LLI8jbMpuYrGKiKxbAcw2TRNSSgCAlBLMHPcT7a+srLzZ6/
WmduzY8Y3IPGBmmKaJsrKyp9xu94SUlJQRUkqYpgnTNBEKhRojBUZ72FkJFX84D0kpu7vd7iaChYgu
QdihP84iSkQziMg2fT/
+XbbBmiG1noji8ncgnELgAynlz5b2HUlJSacFg8GMBKGvQPim1tGm3QubMPzIk/
```

```
rJNmPWMPOVRPSxzbhfs7KyLjYMYzxs/OES8C+PxzPJMIwrYLHOMvPGpKSkq/1+/
zLLFtF2l8t1ZjAYPNbOjyMRkZw4I2ATfGG39RaxvA4JhUKNFI7UsVKBBN95EetYNeKtal5mvts0zXd
M00yNfm+Ypgmfz/eQaZppaWlpt5um2WSQz+d72efzdevYsWOT7fZQKNRYWlr6T4/
H8xqApOhcUkoYhrGspKSkNHLt/me+P/5wwZKdnT1X1/UemZmZ9zc2NmLv3r3w+/
2f+Xy+QNu2beOKOO3cufOBbdu2Nfbp02duWlpaE8tBKBQqWbNmzZRevXo94nKFczEREaSUgfLy8ts9
Hs8Fbrc71iejYfv27fft3Lmzc9euXf+Wn5//DIAUACgrK7tr/
fr1wZNPPvkDt9sdV5vHNM1iIYRDCNEkOiUYDK6rrKx8qW3bttZshb+tXr36sYyMjJwuXbrsEEJ0jHT
5y8rKbtqwYQO6d+/+aps2bU6I/YIpLy+/
bc2aNS5N0xpOOumkN5OTk6+KzIdgMPhtTU3NBx6P55mYm1p5YWHhpMbGxr49evR4w5rkZ/
fu3fcVFhZmM/PzAwYM8LhcrlMi5/
v45s2b04444ogr27Ztu89CETnO1kAgsCklJWV4tA0AGhoavlm9evWK7t27X5qe/
u8HJGZGbW3tosLCwvd69Ohxj9PpPCLyPkDX9dnbtm1LyczMvKNTp05dhBD7briR851fXV29u0OHDtd
rmuaJtjMzfD7f16mpqcdHv+CllCAi+Hy+b51O51+SkpI6xM4VCoXq9uzZszcUCo3Kz8/3apqWFZ3LN
M2ArutGZmbmL0KI9Gg7M6O+vr44EAjcmJaW1iP2fJkZoVCojohGx74+Ml+Qma8gomSLyAhJKf8K+z/
yJAAHHIkQwwsAsH37dru+O+0aAbgjDwD/U09I/7/i8XjuIaIjhBDn1tfXY+/
evTAM42m32z0qLS2tSc4SZt67adOmBysqKoyBAwf+5HQ6+wL/
9ikIBoPL16xZM79Pnz4fCyEQc0Pes3PnzlvbtWv3iMPhODLy3oOZi9asWfNweXl53UknnfRwenp61G
qrFxUVXbtx48bkYcOGLdE0LSf2OAAQCoV+JKKeloc7NDQ0/
Ms0zbLU1NTbmRnRYwUCgUXLli1bcOyxx/
bNzc0dAaAVAEgpd69bt25SeXl5qxNOOOGtzMzMfZZj0zT1DRs2PGQYRu/
k5OSdvXr1WuV0Ovdt01RVVb0JwJGWlnZ59G+zsbFx3cqVK+fNnz//
zp07dz4ac64wTbNq69atr1RVVZ2dmpo69Ygjjrh D07R2Usr67du3v1VdXX1JQUHB6VlZWU3+puvr61
drmpbhdDq7RB8YmBmGYSyrrKw8o127dsOdTieklPv6vF7vKr/
fX+PxeHKJyBU5vqypqdkVDAZnuFyurJSUlJzY75TIsYJEVO5yuVpHrg+i/
4ZCIY+maadGBUQMWQiHh9vx0H4+fhMBoLi4uEkjEZEQ4p7du3c7hRDQNA1CCEgpq2pra930b//S/
5nvj3jv0D+I+fPnf9bQ0HBGVVXV76e6VSgUiagD0OhyuVKdTqc78oXjra2t3UxE73M4/
PruG264oTnbd4qDxLx584qDwWBudXX1AZvzFYpYHA4HiCi6QxHy+/
07ATQyc8DhcGgAukfcDWQwGCwD0JiSkpLndDpThRAQQsDv92+tq6vbk5ycnJuSktJJCJEMAKZp1nu9
3tXMbHI4g/zTAJ4eP378U4fujP/NIYsSOv/888/+/
vvv261bt66eIIAoEePHhdnZmbeAMBfVVX13tq1a9+iiLQnIsrMzMzu1q3bQw6Ho8POnTvvKi4uLoz
tP/bYY8eYptmwbt269wBASkkAUFBQ0GPXrl0bY9uEECSlpKSkpJTGxsaG2L7U1NS0o48+
+nYpZWDr1q3Tk5KS0iorK3dF+3v16nWj0+lsv3fv3ndKSkrWR4/
fvn37Xq1btx5XUlLybHl5+fboeUkpiYiodevW3UpLS7dEj4+IYExNTc3Ky8vrXVRU9BUAMDPRvx9py
OVyJQshhN/vb4j2A0B2dnYHwzBKYtsOP/zw81NTU09uaGj4ZevWrVFzMkX7o/Naj+F0OpPat29/
XmVl5fKampqK6Ovbt28/KDk5ueuOHTzmhEKhxtj3MD8/v7/T6cwsLi5uEtmQlJSUmpqamq/
r+la79759+/anBgKBUq/Xuz0YDAai7U6nMyk/P/80t9tdsH379ldDoVAwcp6d8/
LyLg0EAju2bdv2NgCkpKRktmvXbqTL5WoHAJWVlR+Wl5f/aj1Wx44dz/P7/
bvKysrWAICmaY6OHTuOSkpKOiIYDJZt27btrVdM0QzHn1CcrK2uYlDJUUlIyvba2thIADjvssNPT09M
HAYBhGJ+UlpauAoBWrVplt2/f/
ipmDm3fvv2VYDDYEHvs1NTU40KhkL5t27bp0fOJkp6ente2bdtLGxoaNu/
cuXNf0UeXy5WUlJSUUV1dXW53/XJzc4+ur68vq6eUxU/
KBAIoF27dhc5HI7MoqKi2UTUGAlbDWmattpuHsUfz8iRIzssW7bs8Nra2gIAME2T+vbte6fX1fb7T6LmY
2KioppW7ZsWS6lpOh3VIcOHbq1a9fuAQDzBzZs33+7z+aqi30WtWrVK6t69+98Mw/
ho69atq4hIEpGUUvKRRx7Za/
PmzT9rmsahUEgSkYz+np2dnazrerWmaUxEMhQKye7du3cpCiY2tDQ8L7P5/tC1/
Xdu3btqhZCUMeOHXO7dOnyjBCiVVFR0c1btmwpjX6/9e/
ff1xKSsqoLVu2XZcXOyNtpumSXl5eWkej+ewwsLCwth2IQR169G6t69+98Mw/
rou9jrH3imi7x+N
pe9hhh122efPmGfX19Q1ERBkZGent27e/atgNM3bNjwMRD+rou9jrH3imi7x+N
99tvy2PaUlJTU9PT0/NLS0m3R7/fo92xSUlJ627ZtT/b7/btKS0vXRduZmVJTU7Py8/
PPMk3T2L59+9Joe0FBwUlZWVnDq6qqPt+xY8cyIiKPx9OldevVzWozRNS2fmYHFx8VQAldHva9M0ye12
LzrssMMu2rt375JgMFgKAMFg0NW+ffsxtqezbV1d3Vpd1+cDQENDA4LBoLtjx44BENA4LBoLtjx44jHQ5H3q5du95kZh
0AnE7nl8Fg8EAEAG/+Iv40WiWEYQw3DsNYMaoKu6wccCvrfwOFiVs3CMAy7/eM/
FF3XL2bmA0r89r+Iz+eL2xf3+XzH2Z2TruuP6roelxzp99B1/
SFmts0YXF1dnWP3GfP5fGd5vd64JFd1dXVtfT6fbe4aXdfHGYaRqH4RvF6vne+T4v8zDMO4o6qqqqqi5
aEED4M6brevdE/f9XVFVV/W5RRjsO5ffe2LFjh40bN87Xm9Xqq+T4v8zDMO4o6qqqqqi5
UmSpxqS3V1dY5hGHHh6jH9dtFFCoVCoVAoRQEkMpCoZBtIjbFnwclWBQKhULRkklBOKmabd
Sf4s+DEiwKhUKhaNEwczkzqySkf3KUZ7VCoVAoAoWiyaprmYOVsI4TrUa1EcXJSFRaFQKBQtlmAwKAGY
oVBI3c/+5Kg3WKFQKBQtFiiIjbFnwclWBQKhULRkklBOKmabd
+7osVLRolWBQKhULRYmFmCcChBMufHyVYFAqFQtFiiRQVrSQi/
```

```
6Fei+LgogSLQqFQKFoskcrIrU3T5EO9FsXBRQkWhUKhULRYIltBpGla6FCvRXFwUYJFoVAoFC0W0zQ
DACqllI2Hei2Kg4sSLAqFQqFosRCRycxthBDK6fZPjhIsCoVCoWjJBImIAAQP9UIUBxclWBQKhULRY
jFNs5GZDdM01ZbQnxwlWBQKhULRYnE4HCEiytE0TW0J/
clRgkWhUCgULZkgAGpoaFBRQn9ylGBRKBQKRYulsbExwMzGqlWrlA/
LnxwlWBQKhULRYtE0LQAg58QTT1T3sz856g1WKBQKRYvF5XIFDvUaFH8MSrAoFAqFosUipexARAGHw
zHgUK9FcXBRgkWhUCgULRZm1gDUCyHaHOq1KA4ujkO9AIVCoVAo/lOISDBzIzOrsOY/
OcrColAoFIoWDRG5ASjB8idHCRaFQqFQtFgitYQ0IvIf6rUoDi5KsCgUCoWixWKaZoiIKgDUHOq1KA
4uSrAoFAqFoiUTBJCvLCx/
fpRgUSgUCkWLRQgRAKABqDrUa1EcXJRgUSgUCkWLJVKl2R8IBHyHei2Kg4sSLAqFQqFosQQCgUYArQ
AowfInRwkWhUKhULRYKioqTAA1r7/+uvJh+ZOjBItCoVAoWiwFBQWtAKQd6nUoDj5KsCgUCoWixRII
BDKYGePGjXMe6rUoDi5KsCgUCoWixeJyudKIKBQIBLRDvRbFwUUJFoVCoVC0WJg5iZkhhFAWlj85Sr
AoFAqFosXicDg0IgrV1NTwoV6L4uCiBItCoVAoWiymaQYAICsrq/
FQr0VxcFGCRaFQKBQtFmauBeCeMWNG8FCvRXFwoUO9AIVCoVAomsM111zzjqZplxARmP+9E0REICLM
mDFD3dv+hCgLi0KhUChaGk8BKCYiCCH2/TAzpJTrD/
XiFAcHJVgUCoVC0aJ47bXXVhPRSms7EVUD+PshWJLiD0AJFoVCoVC0OEzTfIaZ91iaN7/
yyiuzD8mCFAcdJVgUCoVC0eKYNWvWDwDWxDRVm6b51KFaj+LgowSLQqFQKFokoVDoGWauBABmXjNr1
qz3D/
WaFAcPJVgUCoXiIKLrenpzXl9dXZ19sNZixefznf5HHetg8Nprry1l5jWmaXoBPHGo1wMAPp8v648+
pq7r/
Zk56b+co1mf00OBCv1SKBSKGKZOndpb0zQHgPpQKNSgaVqDy+VqGD58+FEej2cdEdUe6Fy6rj9KRKO
JaExWVtZX0Xav1/
ugpmkvpaenV8a+nplTDcP4GcAP2dnZ18b2eb3e4cx8GTPnCiHuyMrKWhM5xmFE9K7D4bg2PT1984Gu
zev13szMzwN42ePx3GjpO5aIijMzM70HOl/M2JOzsrKWW9p6aZq2Kz09Xbe+3jCMDI/HU2XT/
pimaa9nZGRs3d/xrrzyyrOTkpJuf+WVV85s7loPBK/
Xe0rsexfT3ktKeUJ2dvar0Tafz3e8aZrLATxNRLUej2dK7Bhd1y+OtH9qnc/
n852emZm5pJlru1ZKKQC8QESb3G73eampqfv8eqqqqjwZGRnGgcxlGMY7zHwcgIVJSUlPpaamlkb7X
nvttSRN07QOHTp4NmzYUKtpmiaE0IQQmt/v3/c7EWlEpIVCIY2ItAEDBkzw+Xw/
FhYWbo62MfPmCRMm7G3OeUZRgkWhUChimDZt2loi6rWfl/
iZuYGIGpjZn5SU1EoIIRsaGrYzc4CIQsxsJicnp3s8nv7R3CANDQ2FXq93dV5eXr+kpKRORBQMBoNl
ZWVlC0OhUAMzm506dTonOTn5KCEEQqFQaUlJyb/q6uoqs7Ky2hUUFNwghHBGco/4S0tL/
2kYxvbu3bvf5XK5Cpi5Ye/evS/u2LFjpRDCBGD27NnzspKSkk91XS/VNM0MhUISALp169Y7Pz//
megJmaa5fsOGDQ/ouu7t0aPHKTk5Obcxc9327dvvLikpKY6+Ljk52XX88cf/
3ev1LtiwYcMy64Xp37//3UlJSWdVVVVN/
+WXX+ZJKSknJyenW7duLwEIlZeXT92+fftKAEJKSR07duzVtm3bSaWlpU8XFxevl1KSpmmiW7duI9P
T0y+SUlZXVFTMKi4uXhvtE0I4O3XqdP6OHTsWBoNBk4iImYmIhNPpTGrfvv1pRUVFi5lZEBEhvJNAD
ofD3bZt25OISBQXF38V25eent42Nzf3rJ07d34YDAZDkXYtMzPziJycnHP8fn9JWVnZl8FgUBKRcLv
d2W3atBkupUR9ff3WysrKX4QQyXl5eacJIZKZGcyMhoaGnVVVVb8BEC6XKy0tLa03ABEMBo2ampodz
EwARFJSUp7L5WobDAZ9DQ0NFUQkomvQNC1Z07T0UChUJ6U0I+elAXA5HI4UZoZpmvveA1pFUu0AACA
ASURBVKfTuS4QCDQkJye3cblcbUOhUG1dXV0pAI2IHA6HI42ZHaZp+gFoADQhRLKmaanMjFAo9J/
82TQLIjpl3LhxXzd73MFYjEKhULRUpk2bdjYRPQYgmZmTiSjF4XDkhEIhtYWu+D9DCMGmadYJIYTD4
UiJClspZTAQCOhEFHK73VkOhyM1RvTuCgaD1Q6Hw5Gamnq4EEJE+4Bw4jxdDxuxNE3bl0iPmUOhUMg
nhBBut9sTOU6d3+8vJSKkpqZ21jRt31yRMWZtbe36YDDoS0lJaZuRkdFVCAEAjRUVFZ8GAoHKtm3bD
khLSztaSllXXl7+Rk1NTRmAxry8vC7t2rUbF12Dpmmor69fsG7duvkAxqWkpGy98sorRzf3mjn+7y6
/QqFQ/Cl4AcARRNR7/Pjxa3VdX0JEp1lesxDAVACfWNpnzp8//+ahQ4e+D2CYlBJSSkSfuKO/
x7ZLKWGaZiUR5QDYl7lVSonKysqXMjMzLxZC5EXbYv+Nvj72p76+/me/3787MzPz/
Nj22traNXv27FncuXPnaWOR17sok3TrC4vL/
+gdevWIzVNaxXbZxjGZ6WlpT8VFBSckZaWNjC2r7Ky8uPy8vLV+fn5/bKysoZY5qwNhUKVbre7o/
UCNzQ0bHI6nfkOhyMjtn3v3r1zsrOzz3U0LS22XUpZv23bthfy8vJOzMjI2PdeMHOwoqJintfr3dK5
c+er3W53x+jN2+/3/7Jly5Y3OnToMDgrK+v8vG2bthfy8vJOzMjI2PdeMHOwoqJintfr3dK5
bt7xJCpMb2lZeXP5GdnX2Oy+XqaZ3P7ncACAQC3xCR2+12nxjbD4CYuUII0SZWKBCRs6ysbGxmZmb/
5OTke2PnJaL2pmneqGnaHUQkonM5HI7oMW8DsJaZrdYvBzN/
BWBozPFTmXkHEaUAONz6HiFsfbkbQCcAL8W0u5m5LxG9BuDo6FwALmPmYU6n0xcMBn+KOU6UtKysrB
O+/
vrrvnV1dX11XX85Ozv7B5vjJkRZWBQKhSKG6dOnrwfQXUrZ95JLLrkKwI3W1zDz6wBGRb7sY9svJaJ
sNP2C3y/
M3ACAiCjJ0r6XiBoBHNac9TPza0R0TYJuA4DHpv07hG86x1rap3k8ngmGYdyAsEBrsj5N0/
pLKfsB+Fdz1phg3Z8DEER0pqW9weFwDGbmAinlvARjtxLRETZd7wC41G4MET3IzA/
bzPUhER2L8I3aynoAPX7vXGL4FuHQ678c6AAiukVKuYWI4vxcmHk3ETXAXmD8k5mnAfieiKwOtKsBF
ADIOfClYwIR1THzm80YsxxAvs36fgOwtL6+ftzChQuhaRouuOCCBgAXZGdnf36gkysTp0KhUDTFDwB
9+/
a9CTZihYheIaJzrWIFYWvLTjRfrEgbsVJNRDX4D8QKgEsS9O2CjVhh5k0IC5ljLe1feDyeCV6v93zE
i5VqIjrTNM0j8H8gVgD8SkTrrGIFAIQQVzAzm6aZMCFcArFSgQRihZmvl1JOtGn/
```

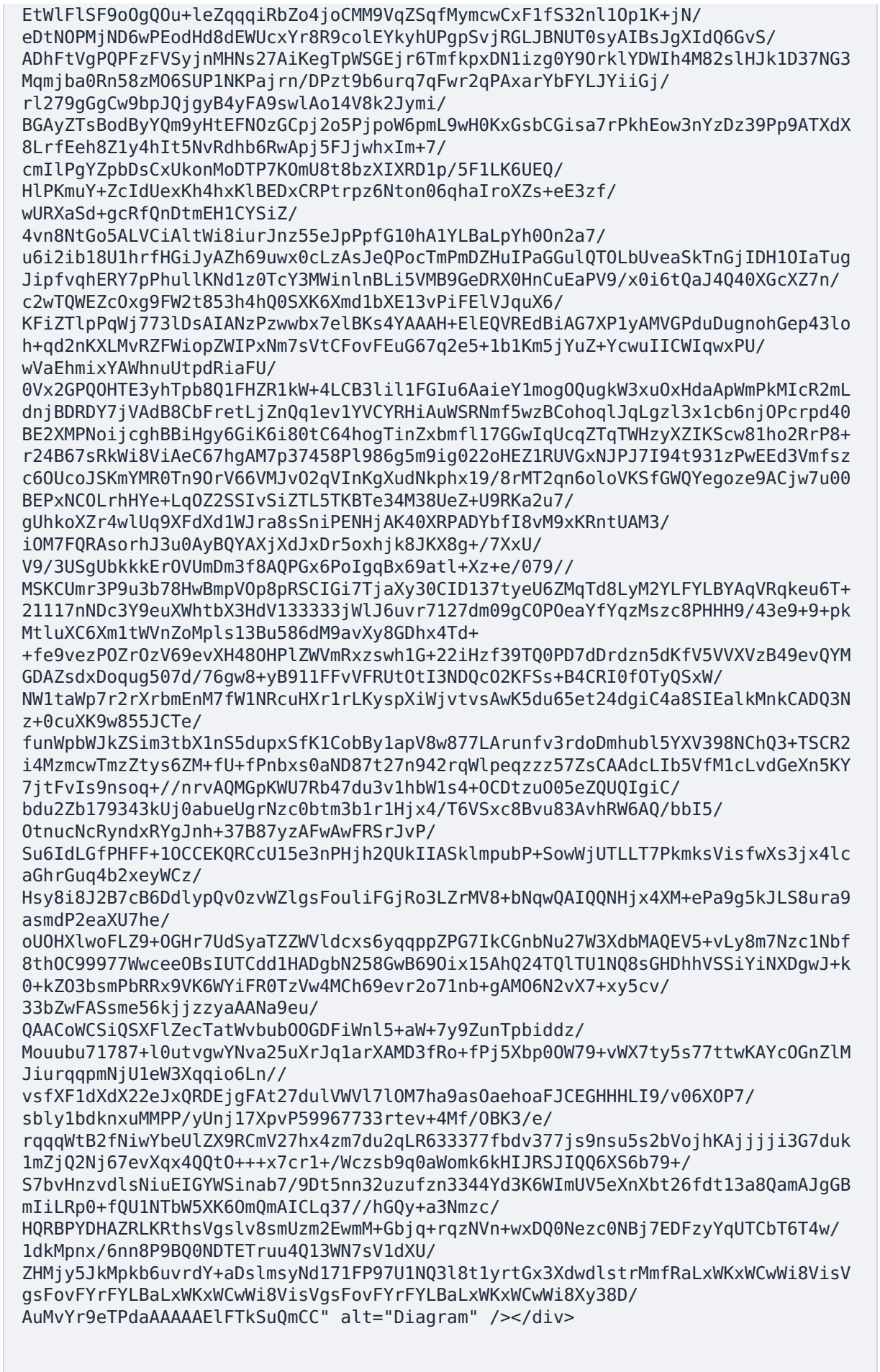
```
gog6wkasMPNiWMRK5P1LxDqEr80BixUAbwohPgXwrk2fDqAE9mLlY2Z+CsDnVrHCzFsA5KIZYoWZnw
OwuzlihZk3M7PLZn1VzPw2gHFOp3NfIxElE9EDBzo/
oASLQqFQWGkEgJSUlLg9dmb+kpnPhOXLn5lrmPkxIlpwoAdh5joAu4go1aZ7D4AuzVk0M78K4GwbIQ
Vm/pmI2tsMqwDwOYDzLK/fCmCkYRgnSSnfsQ4ionOFEE4A/3XeE2beRUTPAfibTd/
tUsqfpZSLrKLud9CZuVWCvglEdDkRtbYc6ycADKC3zZg5RHSW5fV1AEyb1wLADgCTmPnZA10wM//
sdDrvCIVCC21ERz0zLyOifjZDV7vd7vEIi5V2lnG7Ig68zRG+nwghPmTmuc1Y+14A6xKs78moMIkKF
tM0wcxbNE07z+b1CVGCRaFQKGJIT08vAJr6iUT4DmFzdwdrhxDiAQCvohlPsUS00s4ywMyFRHRkc9Y
MYDoRnUBEbW36vgJwlM1x6gE8T0S3Wrp0TdOGEFEHAB9bhQIRjdA0rUxK+VkCsXXARCw145n5GZvul
wG8AuAzhC0EB0pFZJ3J1g4iuh9hv4tTLevYSERbraIkwpsArNtUfiIyiMhOFFUAuIqZZx2oyGLmsuT
k5BGBQOBNu88EEf2LiEbaDN3GzOc3NjbOIaIm73Hk2lbB3iKTiF8APCmljHvf97N2vxBiNhFdbLPuh
wD8NbZN0zQIIUBEZx5oyHUUJVgUCoUihsbGxj3Av51fI6xhZjcRHW19PTPPk1Kebde3H94FcIpN+29
E1K0560V426E9gLhQbGb+EkDnBMLifma+02bMeRzmCwAZlr7rnU7nj6ZpfoHm+UPYQkSXI5zwLdPSt
SiSG2ZeM6+rD0AtALvkey8DqIJliybiF7IIwJU2Y+YgbHFpcq5EtAk2VgtmrotYDV4kojYHumhN087
z+/23EtEQax8zv8DMV9gMMzRNG0pE/wAw2KZ/
F4DuB7oGZi7TNG0cM79v4wOTECHEk8z8V5uu6cw8Ahax6XA42DTNkMfj2Xmgx9h3rOYOUCgUij8zVs
HCzF8wcyURnWDz8l8A1NrdaPbDW8x8rrWRmUvRvKfhqF9FHYBzbLq/
JiI3ws6W1nEPE9EEmxvT5U6nc0vEl6O1pe9ej8fzbiAQ+Aw2Vqb/
gCsjPz0t7WuzsrJG6br+ip1PSyIiFqNdsHeWncvMy5n5BcuYWiHEdNhsRwFYACAFwDGWMT/
CftsImqZdEAqF/
gYb8ZgIIrpaStktwRpeAnCh3TafpmnDQqHQjQBG2Yz7tjlCj5kbhBCXm6b5ts37vr+1P8jMN9nM9wW
Adoh34kYgECgjIra2HwhKsCgUCkVTGgGgsrJyBhE9RETbEtw4KxGOyBjTjLnnMvNpNhaPigTbOftjL
REtAzDOpm8NM28DcJJN30wiGgyLOGLmR7Oysj4OhUJfWPsAzPR4PI8bhvEBbG5C/
wH3ISykrE6xJW63e5hhGBOI6LrmTEhEP8MmgoeZvxBCzCSidyztfgAPSynvsZnuewAbAJxvaV9j3Xq
JOf5VzNw/wdaNLcz8LBFtBGDnUPwWM/ez8z0iovOllP2J6BabOVcCGHSga4hwDTM/
jeb5Tb3EzBch3p9roxDiVwBxojwiznQOJ8xrNkqwKBQKRVP8ALBp06YlkSiQGxK8bimACQc6KTPPA9
DNxjGylpnTEgxLRDERvQD7+jnbEN5KudambyEANyzbUcz8XnZ29gNer/
djxFsPFno8nnGGYbxLRGc0c512zCSi9QAet6yhnpmHBoPBgUQ0JcHYRCwEcLJN+2oietg0zTjnYCJ6
kIjusYnQ2sjMbyCcgySW7QhHWWUgnvuklAG7MOlEMPMSInrONM2Pbbo/
BpBGRMfb9E2QUiYlcOjdAItFKEJVxEnYbh23R0T3cc1Y+wfMnI9461gFgFeZ+XabMUuZ+XmXyxXN1N
tslGBRKBSKpjQCQOfOnQcD+HuC1yyCvSnelkhuj1TEbxVUwSas+XeoYuZJUsp/2vRVENFkAI/
Z9P3CzKsAXGVZ288ej+dqXdffR7yQ+TkrK2ukruvPoRnnux8WEtHLdpFHmqaNAJAhpXyvmXMugM2WG
DNvFUKMY+YPbKJungcwEYC1UGGJEOJuIppuaa9CeOstbiuMmV/
VNG2x1YLzOxQlJydfDWC+1deFmVcAKAQwwuZYjxLRJiKyC3vexswem8+SD4CRwI/
pZYQFztkHunBmXiGEKCKiCyztfgD3A5hsM2wZhZMvZno8nqPxH+aAU4JFoVAoYmDmRgDIzc2Ny9MRY
T6AYc2YchERVQAYajlOPYBgcxwcASBiOfmH1a+BmWuJaJzdkzcz72bmf9rkvdjpdDqH+ny+F4joQkv
fNqfTebZhGBPtth6aCzP/
7Ha7r2fmj2wij64loiIiWtjMaRfBxrLC4aR2l0V8MvIsfe9FtsSs4qNKCHGtlHKGzXHWwN5ysVAIMd
k0zbgkb4mI3NjPb2hoeBHxuW+2EtHrsA/
xfo2I5koprdmVozl2RIJtxV9h79fzKTMbzdzSLBJCzLazoAgh7mTmh2yis75l5j7R/
0Sz8paUlNglMNwvSrAoFApFDGlpaWmAbVgzEM6cavVr2B9fMfNS2PiZEFEZEkTaMLNtRWgiupqZ77d
uK0X6LmPmybBE3EQcS+8F8KLNMc4NBoM3MfNYy3SVmqadHQqFzoxEofxXMPPWpKSk8xsbG99HvFB4T
NO0BaZpfmZd++/
MuQRAV+uYyHldYJrmy0TU1TJsOcIRRFah0CCEuEhKOcXG6fQT2ER0MfPPDodjDDMvgH1Uki1CiMuYe
ZSNhWIvET2IsNXDyidCiIeZebFNKHUlgGrYJ7t7D/
aCbiMRLSai+w503QC8AO61Oi5H5pvMzNfZREb9wMxdY9ccFSx+v7/
ZVRaVYFEoFIoItbW1bfLz8y9I0P0mEmROTcBahPOjPG3TtwZAZ7tBzFxml9+DmW9n5pGwcXpl5lEIi
yK7MNZbpZRP2Fg1RgEYFLlJxs7VoGnaMGYuQDis97+Cmcs1TRvS2Ng4BUB/S/e/
srKyJodCoQVonsPn95En+bioKk3TLor4ppxoWcdmhLdGrHWhQESXmKY5EfHXdhEzn2p9PYAit9t9bi
gUehP2lhdbIlE1SVahEBGV4xCuYwVL348ul+t6Zl5otaBExNnWBBFBL9vlRmHmMiHElAQ+MPvjJrv1
AXibwqUMrNudvwLIs1q4NC3svrJ06VIlWBQKheI/
JRAIPOx0OjOAf1tYmLkG4dT0V9kMqUowVZEQYhIzv2LTtxYJwmKZeU+C/B3/
RDjvh11m0JsiN4y4PiK6lYhust7oiOgWDmeCjXuaJ6KLpZQB0zQ/sltjc2Bmv6Zp5zDzaACXW7q/
8ng8VxqGMRvAgGZMu56ZyxOMudw0zcsQ79OiE9EK2PuFjAXQz2ZL7DsAR9v4flQ5HI6zA4HAg7Bs8/
0OH0kpv4CNCBRCXBmxjlkjbgrdbvcFgUBgLuzF6HeIF4EAMB3AZdZGZq4jotsT+D8lhIiuYeb7rOtD
2IJSjviIoN8AhGAjQkOh0G8A0NjY2Oziy0qwKBQKRQRmvgNhJ0VwuMpxIYDnYB8NVMLh2ilWKpj5St
M0X7e52a1n5kSWhGIAdv4sHwHYTPEZaQFgCsJ1gOJCc4noH8x8GmwKGhLRBiKyS70+gZl/
kVJ+TkTNjVyKQwhxiZTyCGv0TMQh9kKv1/
s0EV10oPNFfHG+sG6nRPr+xsxHW30yIj4j78FGcDLzZCLyI/
76rWdmDUBHmzFDTdMciuZFiG1k5vvIpnRDZJvvesTXKSoDcGZjY+MLsA9Pn0/2+X/
eirzvVodiCCFuZOZnEjjg2kJEDzHzRTbh3L8R0SIKV4iOpZKZi2ATdcTMP+7cufNdAHA4HM2OFFKCR
aFQKCJkZ2dX79mzZxYA+P3+TUT0FoXTuVvZzsxkdTDkcIjyCCKaauMAuZ2Zc+yEQOQpNcW6FcTMq4j
oLYQtLFbeFkLMZeZZNvN9wMwMYLil/
```

QtN02YlsJ48pWnaXABLbfw4mg0R3SalrEC8RaFSCHGWlPJyO+fN/
eAjopdsbpBAOLNsvZ1PBhG9CZvQdA6HLi+CJQcKM5cx8yayqYvDzJcQUQ6HiwMeKLqmaVcT0ceIt1D
cg/
BWShOLEIfT6p8F4G922zoA5jOznVh5l5nbkn0xyElSyjub+d6+HRHlVguKwczTmflR6wBmXk72eYu2
aZo2zOFwSABISkpSFhaFQqH4bzAMYysA+P3+EtiHaBYBKCWbhF6apl1ARPfAkp8iEsXRkGC7x0DYod
FaL2ebEOIOKeUb1gHM/
KUQ4j67ooDMvILCCeX+ZmnfpGna3aZpLrLxkXk3KyvrYdM0P0lws2suLwshPiGiJhEtzOxn5vMQvj5
xIowTVD+OWEnuj2xLWJkrhPga9s6q09kmrT0zf+5wOB6zWV8DEb2XQCTcqWnaNmZuTvgyhBCXmqb5E
uKdYqcSUTnbpLUXQpzPzGcS0c02a18M4CSb8OVlkZDnuFw5RPRMZL7mlDn4mogWw8Z6x8yPk02uHA6
HkFu31oCwwNkmpby9a9euVwNAbm7uATtYR1GCRaFQKGJgZhMA0tPT7QrhVQD4AsBAm3GXSilHIN5/
ogoJ6rpEbsTrKL7YoQFgjJTyTRtxsc7tdl8ppZyPeJGzg4hehCUiCOFIkmullO/Dxg8hKyvrGq/
X+zbs/SGayyKHw/GgaZqLEU60FssYTdOCUsp3Fi1ahC+//
DK2L2EhPCHEnatXr35w9uzZKcFgMLbrGyKaKqWcZx3DzK9FrF3W7Y9fk5OTrwuFQgtt1jcDllpDEWY
y85yIoItLk58ICmd2vcXqAAxgvhDifQ5X2Lau+xIpZesE0VnfRQSlxzJmEzPPYeaHbMbMjVj2DjjpH
4erdU9h5tdtuu8jonttxnyJxD4970QsRvcmJycXAECvXr0W67reHAGlBItCoVDEcvTRR48G4oofRrd
7noBNiDIz/
00IkQfgRpspl9ttLwBA5Ak2rnCdEOIShCspW604xS6X66xAIPAK4mvc1DDzJGaeZnOoq4hoJiwhxcy
8WQhxjtfrfQbNC9dOxK+apo0OhULzEW9RuFfTtBVSyk+ZOfmqq67CqFGjouso5XAF5LgKy5HoqOsmT
56cc8stt2DlypUAgIaGhg29e/
feu2jRorhMscz8PoABNtsfRUlJScCiP8J8JISYB+DyBhcwWZp4spRwMy3ZKJvv
IbsEeUR0ixCiguyT0K1lZjfir2uJEOLnFdwHAdbD4x3A4IWEPu/
ePiO5n5jHR/
0ejhAB0JKInm7EuJVgUCoUimEYL7dq1eokoKlgiWxVXBfZ7rHyIhFtZpv8FADmwj6yjB8DDjVMnEQ2RUk6AxcejuroaJSUldstuQ
2S7p06bLg5ptvtjotGG6H46xAIHAb7Ou0TERY5DSxKESiYO6DjVMnEQ2RUk6AxcejuroaJSUldstuQ
o8ePeDxeODxeNClSxeZn5/vf/
rppz9jZmsEz1uapk2LJFjLFUJg6tSpmDlzJpi5lIgMClsP
ckJxcfFFe/
futfr9LAbQjuKrXhuapg1paGh4BPF5VT6KiEprPpVfAFxqmubcA9l0eeKJJ+DxeHDOOefsEkIEKL48
QgkRjWHmDxDvFDuFmZdJKe38i34DUEbxBTh9AMYzs51Y+Q3AbDu/nv3BzJeapvky4q/
FJxQOCe9kef1WAOl2Yo6IHmDmq2OtUtE8LKZplmqaNqY5a1OCRaFQKCIw8+OIRAnFQkQjI1E61rDTe
ZqmvcXMcRE3zPweM9tmxGXmz4koLvKDme8Ih0OSwh
wxKlzCBGdCps0/oMHD8aLL1p3lewZMmQIPvroI//
RRx99/+GHH5776KOP9nn22SYpPpZlZWVNjGyn7BMRF198MS666KzIXs/ouIBCKirl+/
fpg4cSIcDke1pmkXd+/ePc5nhZl/IiK/
1aLFkdwypmleYBURzPwjh0ZvrLaSkJ8V7AGeKBnhEsHjVt0+ZHtxCs5nE/Fus2nE9EjCIfjN4criWiSjR/
TNwBSEV9c0gBQlcDvaRozHw1LrpyohaWoqOimjIyMhNuAdijBolAoFBGys7N3FRcx7zNTM3O9EOIsh
Pfmrf4dPzidzvsiTqxWv4ZPARxr438SrRXTCfE3mZlEVAObtOxCiEuFKPgWPM/
OFiLegvMfM7WFjxRFCjADQPsF8zSI3Nxcnn3zyyI8//
rh6+fLLnYYNG4ann34aDQ0NYOZnAC4wDON1xE1/
KoTLFsJJAQ5nsf34aDQ0NYOZNAC4wDON1xF+/
KoTLFsSJAQ5nsf3OLopI07SLQ6HQow6Hw3q+m4joV9if76VSynaIrw21A0Dh7t27z7fB
UR0dmNjY3X2FhJbNmzZW9Wr16NAQMGvBcMBpO+/fbbJv0UTk53t9WfhZm/
cDqdt0opP4KTg4XhHyLiK62HGX6Ho+xIxaiFpbCwsGl8hHRKiBzYHm0z8OSbnRvcnbD
6rISAOyeOiPmc0HxKeM/i2wTxPmfMPM4IlrPzPOjbe+++y7OP/985Ofnh/
r06TNu5cqVp0f7fGhoaMHbs2Ip+eqpqDZgeAJLTh33Gz
CqEeAHAyyNHjsSZZ4YjZJ999llkZ2ebUsorbDUsorbcJmixDOtXL9ypUrMXr0aHTu3Bn9+/
fHxIkT3xCTgbo4jUgtZbMCoPTVTzGMgl98JZbUxLc3r42MzBN0PZsW/
Pzc3FkiVLYrsnMPOF69evH3HttdfiyCOPPK9u1fiwAVGF+8G+S3HO2e/.
DTNOOLl6wj8ZTxPJOu8Oj6z3PqcNvf+IBRB/Uq3lBpw/2yj
rrruu4oknnnhgfDAY/qqmpOfKuu+7CgAEDcQMRR+CKK67A559/
r167expKTk8qglqbGxERMnTkSfPn3QunVnrHzyyf968cUXs6Lv+XPPPPYfBgwfjsMM044EDB7a68847
UV1dHbu+dyNC5xrLaVUiHOZul/
fmA7LPA7NO07RHYB+1hcuGxuhn3Pm7F7F9WCEiwKhUIRQRQtRzPmaZnu0RaB0aMPpdpza8CqGFLnhNmLnLnO5XCNDDoDbiM
kuVMIsRz20ORKVRFRh80S6RtO0BwG8GwM8G7OWR4UQ70V8PQ7V8PzIBYNmyZYzFbMqQ8ePXzX
ftutsnJycU5OTk//+1vf2s+/+LvL/z+++7+EyvNPEvRHQJpeuHmAHHh9wfB4drPRJ8mf6ii/X
+fzcjIwAsvbBBLdvNE8WNJYLBjDLqIIV1OYWaB0WPHXFrW1vHvgKdWQEJsCL7ZIIUOvVW
wV0jZI2iO+fcI/KCGz0fOd+b4GeBFIaAaSkuM1OOCwIBLL33Dz/
fu3VuBcMVkAIQKiA4vAmHq++eMQ4iIbhZCX...3bu00Dz1MjHXhIyMsYPhLlYVBHAgWzz/
M7RscMHx42iixcuNAL4EYp5ez6+np88803DGcbn9LNjwORERgNGxawEAjVE9BwRPVBZWYnLLM78c
mzdvxiOPPIKuXbt+984474z77MP9qmHq666Cm+//TZuu+22d9
z1OO+005ObYt68eejjUqR0ee+65FxcsWHBH165duz///

PM47LDDEHt9kSC78fTp0zf17dtXpqamppx22mlYtGgRgH0hxe1qamquu+SSS7Bjxw489thjuPbaa8s
/
+eSTkgsvvHAqgAFjx47Fhx9+iNGjR2PKlCnYsWPHjlAodCkAPPXUU3j22WfRs2dP3HbbbZ8HAoGc0a
NHD4v6WU2bNg2ffPIJBgwY8MXzzz+/+ZRTTkn67LPPEAqFsHLlSjzyyCM49thj9VdffZUuu+wy/
PTTT9B1PfoZ+5KI5lqjkjgcgv4v2DiZI2wZswtfLnY4HCNN00xU0uHtTZs2RbM/
N1uwKBQKhSKGadOmXTh9+nSeNWvWvW47qu7zIMg2N+Qrqu9zMM41NLO+u6Xuv1ev9ibY/
5WWozZpeu6911XS+Jbc/Pz+ezzjprOwAYhvF1bN9pp53GrVu3DhqGcUNkDu7Vqxf/9a9/
ZV3Xaw3DuMd6nBNPPPJH79++/
oba2tvVXX321BwBPmzYt0Tq5Q4cOPHbs2IT9kZ+FmqaVXnLJJf7Y9vHjx7MQorGwsPBSwzDY6XRy27
ZtuaSkJHHrO1xmGUXH66afz6aefvm9c3759Qx6P5P5yfDMIoMw+A333yTAfD333/
PhmG8NWTIkPedTue+1xcVFTEAHjly5Ku6rtcbhsH33nsvA+CffvqJdV2f6/P5ssaMGePt378/
G4bBK1euZAB8zTXXfGCE4Tlz5jAA/vrrr1nX9edatWq1PD8/X8a8R/
uur2EY2+2uxa5dux5NSkqS9957LxuGwS+88AID4MWLFy/Tdf16wzD44YcfZiEEr1+/nnVdL9d1/
TBd118xDIMXL17MAPjVV1+NzjnNMIwdhmHw7t27O0S0tjUeNGsWRz92kjRs3ssvl4vfee48Nw+ALL7y
Q27RpU2UYxsfWtU2ZMoUB8Lp16+LWrev6Bq/Xe7Ku63U/WC3Ul/
TBd118xDIMXL17MAPjVV1+NzjnNMIwdhmHw7t27OS0tjUeNGsWRz92kjRs3ssvl4vfee48Nw+ALL7y
Q27RpU2UYxsfWtU2ZMoUB8Lp16+LWrev6Bq/Xe7Ku63U25/WC3bnquv6DYRgVNu3Vkc/yZ/
v73OzcuXPj9OnTeerUqac0929TWVgUCoWiKSYAdOrUaTRZqiIT0e0Rf4KzrrYOI6E62pKCPwuGKzada
2mo0TRsB4HVr+HIgEGhcvHjxUsMw3kJMtd1QKITly5cjPz//
B0QcKokIvXv3xurVqYXrl3h8XiwYsUKrFq1ansgEPi8R48Ebb888ebY888kj8/e9/
x8yZM1FaWhqtl9Qc1ggbhsbrJycl1Op1uACgpKCGzzz6L6dOn8zHHHPNBbm7uvfqfsEPNGIDU1FQCuQN
hp2K5K9fTq6uo+1dXVHYGwA2uXLl1w5JFHLiKieSeeeKL4dEz1OPPHEi6PhtN999x06d+6Mww8/
fInH4xkjpfykf//+mStXrkQwGIRpmgCAnj17nohIlE6kODd27NjxY1FR0d/
9fv9Jp59+OkXnj17fb775xrYiMoC3Fi9efKHf76eTTgr7UZ9yyikAgKeffnpXNNz466+/
xlFHHYW2bdvWEtHpRHQlX7X7QOAgQMHRrMUH49ICPrPP/
+MmpoatW16iQAAIABJREFUHHfccduJaA6AJ9u0aYNOnTph1apVAIDjjjz9+bVlZWfpf/
vKXc7/66qsmlcYHDRr0rRACEydOxAcffIIC6ujoAYUuhw+EYI6V8x+qDFftsitlsIXCxQzj3j8hxHA
iuirBNtE+nE7nUnR5oM0W0a+6rlf269fvWABN8LDwi+TTHpfmHcBdCJv04+q3RBwT4yoEa
5o2Ukr5oM0W0a+6rlf269fvWABN8oLU1dUhFAphzZo1J0XDiT0eD15//XHzw//XVs3LjRR0Q3/
fLLLzjvvPQrVs3fPjhhzAMY5nD4Vjet2/
ffgB6CSEwZ84cDB06FHPmzCDB06FHPmzMGxxx6LG264SmZAlAghLpZSvq9pmjZZ79mx4PB706tULjz
6e5n3zySRPH15ycHCBcjG+Cjf8oiOii59+UCtHSpUsBAJ9//
jlOPfxXUMiHE81LKt6ysrKeqq6urbeFzcVVR+ncBVGkxqjuroa27dvR29L1Nq16+y
jjjjqq5t13321XX18PzQxffp050OfnBxwOx6UCgZRUkLQ6EQ3nrrLVivr8/ns6vztAxA+ooVK45Q/
HcceFI9HbtWu3Ky0tbvVdDQ80+go8+nw9ZGDGA+5yDvF4vACAjIkqK/
UzU1IS15F133dU5KyvrGLRALHiaGaquMWfPHgBYM27Z27cuNkvrvjHHPyqqVrmUyczvEZrWvHHMy/
u2rXrcfPnz0dQBQEeeeQQRHHPMMXjjjTdrPdIR4Ik79crdNnKeT0GIXoNMnX0fzRCqbj46/h6rzjqH
sq41cycxvYRLAxc33s/
6Nbhnl5eeNt5tkvzc7lr1AoFH9mevocc6GDRsDlcm0ITTqiIE0mw9pnVnVnyXCDIrpfhE1lnztU
wder+o2CZuZaIzjVNcyoR9QbCYc033ngj/H7/+
+3atZt81FHQHQ5In9p59+modwpeRBNtP+RUrZoXv37qNOOOEELF26d3zFj26FJO6dUJZWRlyc3OfMnUt
CQERjPB7PddaJdqGGo3PdOKpz7a0FBwajYvuzs7Z9Gzzz77a0FBwajYvuzs7KUAHLNnz07KihQ
4dOA9A7PT0dQ4YMQfT6GobxxbvPPSnn36K6K6upq5OXlXvaA8CPP/
6I6upqpKeno02bNszpYVCZ99xLT12
fv2a5NjxeDxlRPScpmlXvVVZbjsstWQ1uLBx98ENdeeyeyl1/
eo3v37ikDBw7kEEwIEDIaXE7NmzceuttkqLpl++de//
tX6mfOhsvaOsY3MXENE2Jcpg/qWISYY7odJeKcNUmK/
nO2HPnj3DjAewLJGCu/
biRVmXiKE2Mq2xfCYeQ+Atjbm9smRXBvWyKNQl8t1ZmNjY3Zh6YFhdbefK74HzdeoDdpIaK5yigQ9KnjYbPvBbKhHc3ZDy7ChGNmzQPr
fu/QbjKc1sAqKioqJs2beyuXWvXricXDDxu8cS0OTJgXSAn67NfT85IWiHeWKAHtpqooqa
66r8PpdO7bPolF07SLYrQtGQbs0s0Tbs7fAp9C0vaeNM0zaysBzEJ2tDaWlpEYDtRkKnSfd0ZJxBRMDw
AIYNG4YZM2agffv2xLZM2zfFxbXFz8ChGNGz58+JGtWrWK7dskhF
jLzH+dNWsWBg0ahHnz5kXD9IgEG4YQHDg0f369cOvv/
QHz//fePnnDCCddv27JatzatzaRJK7B06Ed
l8vtPLyso+iAqUMcff+ffFM7wPIHvNmQHfGy+MNQTCCKhskpn/
FCoVWrVph1KhRyk4IHR7/22mnFH/hhGl/
m+9LITA6NGjCIIjycj0gIJyycbIElDyBDlKJqmX
95Tav3y9KsCgUCkWEzMzn1euXDXGXRmARPQARFtdBlkgEyEKbqaoiQsW6jfAvIcTK2XGDpKB/
SClDFKkIN/GjRsZFiXVx7/OtGqJzgDRrlbcUbZFGrtSTA9jWNRu07qyRDCrKfDOZnoIxo/gNHBy5X
dJDv1ktqzaZsFhdGbQvKwXLGetD2hZk4OJ8mXjPcbGnr3IfCk+hmYbj7ByOZkBjbTUKqn0iK8H5iSZ5f/
SADD2DQoEHo2bMnvvzzS5x99tn/
POOMMx5bu3bt9yUlRZWu2bFqPBqDzBFd7HXqpXY1Ma3w3W0e/cNoHmdPbmTkLFyZBEw
aZRTPkfMHeUiVWhBmHXOPuxWa96zKBLwnUH6ZUfRTbmcEEbAgxDj7yZaQDHQ53s3PLFnh7rWe9sd/
EpeqTeaJWvMCvi7JTE1Dg0qhHLaCyNXJTQp2eYpyGNe9LHzVrHq6wUJb9SXdwgGU2FKbQKqMC
UtMqTjG6PU5lqPCc5KhK1VXyiLyCNzy/+nYXD2Epz6n7a5uNGqhs+eRxEnLRfjKU47RPxGBEwCQCSfQ
ELdKqPN3FqVt5o3VvFKLc/
oTZ1KT5f3gjbySu9/h2bDuWfgUIo8kQFc07qS+GXDLzrH55UEI1CbLtZA5v0Im77bw6Zc
RdPyIRSfp2UedGsN0y2aT4OgRHx3BgdkOzbcgNkq0bN8XrJ0yG0mDj6JO05V+RywHs4GZ5Uqm98AI
cP1kZJzSX79+3Kmbe2x6UZfOd8znCQk6vfCACQN/yGZHYFxnq4RZH4jT4rePHgFvFpxRR0+6Cq5
SfdC0Ozt3KsYAPhOs9aRbUTUrXx2BYCOl3A3qXcvqJC54NPG5A3ivuuZl8OhPOgPjwXj5OKWEXC9
ItYs3cuhoe2+PIR2Bm8qAYGPD+2c8A0bO8m8GkuKZFt6LXhpNf0xoY98GzXH2tAKbuqU6Z/
HFNLVtrYvs7WTWWTnFhmq4sTk9Fl8IIZS2oTtRSPWRE6/kGC2ebnzVLbo6NqFaWQXYHmqAl4r

```
1ueeey4eeeQRPP/
8841XXHFFK1gsNVJKycypRHRFWloaWrVqhVWrVmHw4MHo3LnzhW+88UbGhRdeeOvYsWNx4403IhAI4
I033mjUNG33a6+99lcAKC8vR1FRERYsWIBff/11cu/
evf9yxhlnXO12uwEA0et70003bRk+fHj32trattOmTUP0+kYStr1BkarRX375JYQQuP7665GVlTV+4
MCB1xNRm0GDBmHy5MlYsmQJzj///FmXX375C99++
+3q0aNHOydMmACv14s5c+Zg1qxZdf369fv70KFDn5o0aRJKS0vRpk0bzJ49Gx06dHj5H//
4x6Rbb71VmzJlCvLz89GxY0esX78eU6ZM0X/88cdnc3Jy0kaNGoU2bdpg0KBBSE9P3/
Tyyy+3z8zMRJ8+ffCPf/wD3333Hc4991y43e73Pvroo/Pq6+uTo342EXRm/
oWILrK+T8z8IdkUg2TmxR6PZ6JhGF/bbCshkiDvPqvVJeK39ZGUMi6Nv0KhUCiawcyZM0+bPn06f/
fdd35d119PEBli6LreX9f1sgTRED6btu8NwxgYjWix/FxZXV2dEz1Wfn4+A2jyI4TgvXv3smEY/
MEHH3DPnj2DSUlJoa5du/INN9zAhYWFHI0q6dat27zk5GTjsMMO44kTJ/KKFSv41FNP5U8//
ZQrKyvrn3zyyR+HDx/
OmZmZ3Lt3b3788ce5oqJi33rWrVvHZ555JjudTi4oKOAVK1Y8bxjGTdZ15+XlBXNycubqur7F5pzeN
AxjmNPp5Pvvvz8uYio5OXnpySef7LeOa9269W4AvGDBgibt48eP3yCECMW2TZo0iQFwly5dVvh8vuN
1Xa9bu3Ytn3rqqezxeDg/P1/26NFj7TfffLNvzNKlS+Oub05ODi9ZsmTfa1599dWfDj/
8cF+rVq3Yen11XX8+dg2DBw/
mAQMGsNfrvc8wjAWxfSNGjOD09PTA3r172xiGUbRq1So+5ZRTOCMjgzt37sw33XQTr1u37m5d12tKS
kr40ksv5fz8fM7OzuZjjjlm1fLlyz+KzvXQQw9xt27dOC0tjfPy8rbfc889xWVlZWwYBm/
YsIFvvvlm7t69e7BVq1Z1I0eO5G+//XbJ/Hxxx/
nnj17VjocjppTTjmF58yZ0+Taer3emQk+x4sSRBCtY+ZUwzDeSDDuHV3Xa6ztXq/
3QgCYPn169dSpU69v7t9m/IaTQqFQ/H/MjBkzBjPzV263+8Hhw4efDZsKxkKIM03TfNSaAj6CF/
HF4bZomnaZlPIzxFdYvi8rK+sfkSdVaxbUjUT0M+yL170L4BKb9suEEBVSyi9t+qJF/uL8P/
bDXGaeR0TW8gMGwts8rwNoUveImT8H8BCAJTZZgDe43e4zGxsbFwKwRoq8yMxDrI65zPwTgIeI6FPr
4ojoASJ6W0r5A+Kv7d0IO0Q3cSBl5llCiAVSyo+2b9+OCRMmQEoZrR79A4C1ACbEXQngJYQtTE3mI6
JXmDmEeIfsdS6X68xAIPCpzbkCwL2RMYdZ2l9k5iqyrwN0N4CeCDsxx+KNbDfaVXleI4S43jTNpTap
/6cDsHOA/Q7hbcYmTrbMXArgRCHEyEhZACuLAPSB5b1g5ueIaBaAk+bOnTuZiB4aP358s/
xYVJSQQqFQxCClZADo0KHDhbARK8x8vWmaw+zECjPXIT5SqFLTtMtM03wHli9xInrF4/
E85vV651rFCoAKAIvRPLFyN4CNpmnaFdADMz/
bHLHCzD8iHHY919Jez8znAfgnLGIFwK9EdAcRfWzjv1MKYFhjY+MriL+BLwBwik0U0W8Oh+MWIoqLF
GLm1xwOx7SIOLOKlScRvhHvExevv/
46xo8fvwvATCnlHCJCly5dcMIJJ6CiogIA1gH4CPZiZQ4zj0B89MwiDldEbiJWOFzU8bzGxsY3bc4V
Eb+nUYgXKx8R0doEYmU6EblgESuRsPS/
AHjQ5ji7AFwtpZxnFSsRv6y49PkA1kci4qxipZ6IztY07agEYuUzAEcjXqxsFEI8D2AhgJecTmcyAD
ufl/2ifFgUCoUiBmYWRISUlBS7qJ/nNE0rklLOtOmrp/hKyQ0Oh+PcUCj0kjVVPzMv9Xg81+u6/
gosFZ0jadJfI6L/196ZR0lRXX/
8e9+r7hmQbbpNADdC9GCUxYliDNFAjIZNA4obSlxQE9zigj8U9IgKcUtcjjto4hoXwCVxARFUghhIB
hwBA6jghsgyM9U907N1V9W7vz+qhvS8ej0ZTH7nd07O+5zjOVrVr+p19Rzfrfu+93tNjQ5fZeZxujY
gypw8y8x/J0MPI4SNEC8p/c1jfCGEmKGUekW/
FxGdzsw3osgjJprD1wj1P4sQb1mQSyQSx3qeN4uI9KaQ7yOsTBmsHa8TQpwRBEGsu3HkbXOl53nLoF
W1AHgawEj9eNeuXbe/8MIL6eHDhy/
p169fFwD46quvsGDBAwowePTqLMMh5xvAs3mHmI3RfHgDVzPwUET2vza2Jwk7YvyOikYbr/Tn6e9D/
xt5n5jkIF36dN6L7tWvfwMytRHQWMz9sCEiaHMc51ff9PxDRd7RzL1DY/
FLPPm0noi8NvxGklCdLKb1CofCi4e9vCYB+hvu0SinPVUq9iCg4cxynvH///
pcA+K3he5bEBiwWi8VSRGVl5eh169bt9osoYhGAu5RS1aZxhq0PCCEmBUFwuSEbU51Kpca5rjsDgCn
j8QjMnhZVRDSszSitiNccx7nG9/2/
ElFvw7jZRHQWDD4xJcgy80UA5hORXqVzEYAzDAtxvZRyXBAETwI4QDsHIcQ43/
fHU7yR3xcIbdr1YAXM/HOl1P2ITNSKWCuEOEUp9QLi2YvXEVYW6Zmf7Jlnnnnyp59+
+vrs2bPTu3btiqVwqGHHoqQ62yRWRbjV8j
XiWZxPAVwRzV+fQ1VUSRXrNRUJZa8nzXwwOne67/
vTiOhI7XpLouCrv3a8GeHfeazhIxFd4DjO2kKh8Df9byIKVnoS0SH6OCHEpUqpmSj6PYgIuVzuK/
2z/
wobsFgsFktEJpMZsWPHjmsBtAtYmHlDKpU6PZPJxJodloKZpzLz4VGgUMwXyWRyTCaTGY8i87CicU/
AHMRsjoIRPXOxJmrEuJC0zr0AEGkajke871FbJmAvw5jJCJ109W2WOxBuE5xtGDMuCIJbyNy99yyl1
LeIqF235MjfI4A5WBkNYCqAH2mntiaTydGFQuFB0pogMvMaIvoMWsl4dG6i7/
v3TZ8+PT19+vTiU7VRxup5aCXUHHabbjAEZzVEdD4zz9eDRyK6gJm/
B2Ca4TlsRhiQtPvdmTnnOM6ZQRA8Z9CYbBFCPMvM9+sXI6LxzPwLxJ8RAFwC4BhD5c96ImoGoDeQBB
Hdg1BXo3Nrr1695mUymZWIB4/
vEFECgL6lCQDPMvMhiGcQA9d1Nxg+3yE2YLFYLJYIZj6ao4ZyUsq2w1khxAmZTOYKaFsgHfCgECLDz
Hdr188lk8kxvu8Pgnnr4Q0Ao/
QtnUj7ERCRnrn4vKys7IRCofBECQHwXKXUd4jIpMVpMCyOiBbiWYhvs8xj5hoiutMw5hSl1GQy27Jf
C+BLIlphGFeAwTk1msPRRHSqNudGAGMKhcJUAHog+DkRvQhDEEhE5yNcwHVRc4PjOGN9338IWlaImX
cB2KAv+NEcxgGYY8hm3aqUaiSiP+hzAJAlovuYOSY0lVJOCILgLsSfhUtET5r0IkR0OTMPQlx8C2a+
```

```
j4jqoXVMZuaviOgNGIKp6B6/1jNMAOalUqnr6+rqlhDRYG3Mquh7xbo5I9QDvYuohUTRmO2tra0+wg
qtPcKKbi0WiyUilUrdWltb+1vgnxkWZj5BKXUkNAOsDnhNCPEKMz+un4gWpi4lRLErmbkfaZ4WHBrX
ZQzZk6zjOKM8z/
sNwgVU5zkAOcMbNqLrxZzhiGgmM1+AeMbjPWZ+q0SwcoVS6jAiOs9wn4ellC8BeNVwDgBiBnnMPIuZ
C0R0g35OCHGiEOI4xBfcLBHdDUOwAuAOZh4K7RlF+qKRvu9P17NCUVCyyPTsiGgMEV2PuP5knhDiLS
KaZ/qiAGYopW4zXG+yUupcGFyAiejxKHjUmYPQKv8W/QQzLxFCvAwtIGbmJiHE72DO/
DxFRCcbNDCrUqnURNd15xLR8dqYtURUbQpWmLmRQ68h3Tq5xnGc4QAKAPbYh8UGLBaLxVLExo0blwN
ALpd7FMCPEb4JPtXJ4dVSyllBECzQTzDzr4joC6XUYoModjMzJ0waACL6iIgONRw/
yff905j5QsM8XkWolfgfwzwaATQiLmJ9LFrYj9aOfwLgIYqa+GlzuEsp1UREMw1z+JPjODN931+o36
sDniKipQD+aLjXuUqp3sx8r2HcdUopU7DyZ2auRZhd2Q0ztwohTgiC4CQiijVVJKJnDVobENF4AGOh
tVQAsEJKeXep6iwiuoqZZxq23+5g5m9DM+OL5vgEM19tOL6UiOYqpWIZOmb+SAhxrVLqFcM0bjQFTB
yWoPdH3I7/IynlWNd170DYJ6v43MfM/CrM1VQgoncpXuWUcRxnODPXAQiY2QYsFovF8u/
AzAIA1q9fP09KuYOIXiez7bg+bttee+11tu/7Lxu2Wu4sLy9/PQiCtxDXwNQh1EnEtB/
MvBpApeH4RGbeH+asz3KEot0HSkx1O7RS2mgR7IZ4piYjhLiGmWPBCoBXmPkvRPR7w7lqZj7X87xXS
auOKgUzvy2EmAUg5gLMzLOI6CtT9oKZf8XM1xuCwHUIRcMxl+Ioc3IAQo8W/
Xr3QVugI85SSpUhLB0vZjOAS3zff8UgUAaAW5j5fD1zBuA1hEHlHYYxr5gyVsz8iZRyilIqVjIOoBb
AhKj6R5/HDCK6RB8TaX6yCAPzYuqklGOUUlOgib+jKqInDAFJMWP0A0R0su/
7BwZB8HUymeyBb1DWbAMWi8ViaY8AgFQqVR4EwRvoRHYg0kJMaGpqepripa9/llLels/
n30Q8UGhl5i2IV7QAYY+dWBBDYbO5BoSlu/
o8qgBcz8zP6+ciVhgCiGoi+gShJ0i7uQG4jJkfMWQG3mPmhxB6p+hscRxnJBE9UkJXY2I9EU0OgmAR
4s/7GSHES0EQxAIZANdGC3G7Z87MOyIdSSwLIYQ4VQiRj8TNOs8COE8/
SERXCSE+QTzTViulnMTMLxr0LIg+/33Et9jeB3B7id/
pA5i3+DLJZHK8UuqPpFUEMXMLh744dyOug3mQmY8zHP+ciJZA8/PhsL/
SKGY+FmFrhWJqhBC3w7z11hFnSSm3M/
NzRFReXl7eJ51OD8vlcrqou0Os6NZisViKEEIIZsZhhx12BwyVNSU4PQiCmxEvsa0WQkwOguB1GLo2
I1yoTdUVNTCIUREu3ouDIPi74dyHRHRhVLIaq/
yJNCjHaYe3MvMyivriaFzGzDcRkW4C9pGU8sYgCEy6FFdKOdr3/atgNrYzsbWsrGx0Pp9/
xhBMrXAcZ5bnee8aMih3IhRBxzJQAB4tsXV0dhAEGwGsMohLFzHz8QYdx83M/GI0pl1WQAhxlu/
7D5TIIv2FmX3S/
EyYeRsRncfMiwwZjx1EZPo+IKIJnudNh9l5eaJSaopB9PxGNId2+hMOjeYeKKFJmqiU6g3gD9qYRiK
6SSl1p+HZlYSZpyUSiSW+769sy/
xE4yuYOY3wb71T2AyLxWKxtEcAQFlZmSnAiEFEF0TahtHFx6OF6eTI4dZUpbOJNH+M6HiOmWMBB4Bl
iUTiliAIFhrOfeY4zmkc+ojoDQjbqjmO0o41RNsHsWAlErxeqC/
EzLxLSnmZUmoeaeW8zNwihBiplPoxgOsMczRRn0gkRuXz+RuhdXOOtj/O933/
dcN3+iMRCQAnGL7rkybBbrRwLgaw2LBlshzAwfp9OLSTvycas492bopS6irTb4hwm2gFhdVJxWOaHM
eZwMyPGTJxIKI+hmuBmX+FUOQbcz2Ofr8h+hYSM28A8BoRXWEYMwPAzYZbXSKl3MHMMQ0WgJkIzQf3
RHvyQFlZ2dOe5y0HcFDR/dHa2rqzR48em/
bgWjZgsVgslmIOOOCAHwFAIpHozMdvU0qloIkPmblJSjkuKi+NOZ1Gb9LfK3FNaXjz/
shxnCme58V8YJh5u+M4o33f/
32Ja64jogP1DAURPV0iszKXmQfr2zkcerZcGATBEzBU9wghJgJIcWj33imIaLznecchrhmpJaJTfN9
/
BkULXTSPJcy8nJmnGi65wiSWBfBQKpV6sFAoLNS3UwCsZeZYzxwAf0yn01dF2z26GPp+hN4nMa0Gwh
5Lj8DgZ0JEZ0RGgiavGiPMfK+UcguHVv469yM0+ZutHa+TUt4Ig46JiC4HME3PwhHR3VLKJUEQLDT8
/c1GqGXptQfzXuA4zk35fH6Z/vw8z6ttbm6u7ey12rBbQhaLxVLEl19+
+QHQqYBlnhBiTeS22g4iOjMIgulEZNIi1HfwJt1o2PpwKXQsfR6aMymAmkQi8VPf92dBq+6J2ILQDE
3f1nmciC41fP4NAA0wNMMjoouY+U5TZgDApUqpLTBvtZTiTCIqY80QjUOr+ZOZ+XeG7EU1Ed0Hc5l0
HTMPNdz/
1VQqdWldXd1LhkBhK4BeRNTODI2Z30yn02e7rvskAH0b7R0i8gCYAiMw8y0IMxH6qcsADAIwyTSuxL
UWSynvV0pVGU7/
iYiWRuXDOmcHQfCoPgcOS8bP0b8vgIVSytt831+DuCh8LhFNAmD8my3BimQyeanneW8bguinGhsbD0
W8J9O/xGZYLBaLpQilVJKZleM4HfXdWUlEDwdBYCq/
vQrA6WS2ZQc6+B+1IVgBgJOY+U7E9TH1AI7zff88GPQizLwTQCviQc4iaALb6PMbqLSp2DSEb+W6PT
2I6K6ysrKXEW6bmOYfg5mnSSnXmMq/
pZRnA7jUoMf4TEp5MUqXmKd1jQkzr6moqJjouu7vSPMLYeYGhF4g+uL9fiqVmpDJZG6AtgXDYSPBlS
WyOyCim4hohj4PIrqbiL5G2KuoUzDzJ+Xl5ZODIHgF8RL01UR0n1IqJtqNSqFv1QNLCqu5BupBG4e9
pyZ5nrcQcfO8BQg7L5v0VKX4R3l5+cRCofAawq7Sxfy1oqLiIgCKiMr24JoAbMBisVgs7aCwG25tMp
l8iUOH2XYw88dCiMujrQK9NPNhpdQgGHw1viGTAFxEcQv6FinlKIRZlWsNc8wR0XZoQl8OuwoP07cD
mHmnEOJ207ZDJF6diPjiA2Z+oVevXjfl8/lFJTIvJh4gokejrQe9/PsapdQIxDsI1wAY7/
v+4+i8p0tbC4TJMPjRIFz/
9GzCZsdxRmUymZPYbNi2AKX1OXOUUmfp12Tml5j5LWaO9RzqgKyUcnRra+uDFPfg+VQIMY2ZX9b1JF
FgdBziQuTXmNmluBHeZ8lk8kSl1CN6NisSb38b5gq2UnwuhBjX0tLyAmlicmbeKIQ4m4haiIiZ2ZY1
WywWy78DM3chosZCofAmxb0z6oQQE4MgeBaajoOZFzNzGRGZ+gB9k3nMQii01C3oEZme7Y24k2gbG6
```


EtWlFlSF9oOgQOu+leZqqqiRbZo4joCMM9VqZSqfMymcwCxF1fS32nl1Op1K+jN/
eDtNOPMjND6wPEodHd8dEWUcxYr8R9colEYkyhUPgpSvjRGLJBNUT0syAIBsJgXIdQ6GvS/
ADhFtVgPQPFzFVSyjnMHNs27AiKegTpWSGEjr6TmfkpxDN1izg0Y9OrklYDWIh4M82slHJk1D37NG3
Mqmjba0Rn58zMO6SUP1NKPajrn/DPzt9b6urq7qFwr2qPAxarYbFYLJYiiGj/
rl279gGgCw9bpJQjgyB4yFA9swlAo14V8k2Jymi/
BGAyZTsBodByYQm9yHtEFNOzGCpj2o5PjpoW6pmL9wH0KxGsbCGisa7rPkhEow3nYzDz39Pp9ATXdX
8LrfEeh8Z1y4hIt5NvRdhb6RwApj5FJjwhxIm+7/
cmIlPgYZpbDsCxUkonMoDTP7KOmU8t8bzXIXRD1p/5F1LK6UEQ/
HlPKmuY+ZcIdUexKh4hxKlBEDxCRPtrpz6Nton06qhaIroXZs+eE3zf/
wURXaSd+gcRfQnDtmEH1CYSiZ/
4vn8NtGo5ALVCiAltWi8iurJnz55eJpPpfG10hA1YLBaLpYh0On2a7/
u6i2ib18U1hrfHGiJyAZh69uwx0cLzAsJeQPocTmPmDZHuIPaGGulQTOLbUveaSkTnGjIDH1OIaTug
JipfvqhERY7pPhullKNd1z0TcY3MWinlnBLi5VMB9GeDRX0HnCuEaPV9/x0i6tQaJ4Q40XGcXZ7n/
c2wTQWEZcOxg9FW2t853h4hQ0SXK6Xmd1bXE13vPiFElVJquX6/
KFiZTlpPqWj773lDsAIANzPzwwbx7elBKs4YAAAH+ElEQVREdBiAG7XP1yAMVGPduDugnohGep43lo
h+qd2nKXLMvRZFWiopZWIPxNm7sVtCFovFEuG67q2e5+1b1Km5jYuZ+YcwuIICWIqwxPU/
wVaEhmixYAWhnuUtpdRiaFU/
0Vx2GPQOHTE3yhTpb8Q1FHZR1kW+4LCB3lil1FGIu6AaieY1mogOQugkW3xuOxHdaApWmPkMIcR2mL
dnjBDRDY7jVAdB8CbFretLjZnQq1ev1YVCYRHiAuWSRNmf5wzBCohoqlJqLgzl3x1cb6njOPcrpd40
BE2XMPNoijcghBBiHgy6GiK6i80tC64hogTinZxbmfl17GGwIqUcqZTqTWHzyXZIKScw81ho2RrP8+
r24B67sRkWi8ViAeC67hgAM7p37458Pl986g5m9ig022oHEZ1RUVGxNJPJ7I94t931zPwEEd3Vmfsz
c6OUcoJSKmYMR0Tn9OrV66VMJvO2qVInKgXudNkphx19/8rMT2qn6oloVKSfGWQYegoze9ACjw7u00
BEPxNCOLrhHYe+LqOZ2SSIvSiZTL5TKBTe34M38UeZ+U9RKa2u7/
gUhkoXZr4wlUq9XFdXd1WJra8sSniPENHjAK40XRPADYbfI8vM9xKRntUAM3/
iOM7FQRAsorhJ3u0AyBQYAXjXdJxDr5oxhjk8JKX8g+/7XxU/
V9/3USgUbkkkErOVUmDm3f8AQPGx6PoIgqBx69atl+Xz+e/079//
MSKCUmr3P9u3b78HwBmpVOp8pRSCIGi7TjaXy30CID137tyeU6ZMqTd8LyM2YLFYLBYAqVRqkeu6T+
21117nNDc3Y9euXWhtbX3HdV133333jWlJ6uvr7127dm09gCOPOeaYfYqzMszc8PHHH9/43e9+9+pk
MtluXC6Xm1tWVnZoMpls13Bu586dM9avXy8GDhx4Td+
+fe9vezPOZrOzV69evXH48OHPlZWVmRxzswh1G+22iHzf39TQ0PD7dDrdzn5dKfV5VVXVzB49evQYM
GDAZsdxDoqug507d/76gw8+yB911FFvVFRUtOtI3NDQcO2KFSs+B4CRI0fOTyQSxW/
NW1taWp7r2rXrbmEnM7fW1NRcuHXr1rLKyspXiWjvtvsAwK5du65et24dgiC4a8SIEalkMnkCADQ3N
z+0cuXK9w855JCTe/
funWpbWJkZSim3tbX1nS5dupxSfK1CobBy1apV8w877LArunfv3rdoDmhubl5YXV398NChQ3+TSCR2
i4MzmcwTmzZtys6ZM+fU+fPnbxs0aND87t27n942rqWlpeqzzz57ZsCAAdcLIb5VfM1cLvdGeXn5KY
7jtFvIs9nsoq+//nrvAQMGpKWU7Rb47du3v1hbW1s4+OCDtzuO05eZQUQIgiC/
bdu2Zb179343kUj0abueUgrNzc0btm3b1r1Hjx4/T6VSxc8Bvu83AvhRW6AQ/bbI5/
OtnucNcRyndxRYgJnh+37B87yzAFwAwFRSrJvP/
Su6IdLGfPHFF+1OCCEKQRCcU15e3nPHjh2QUkIIASklmpubP+SowWjUTLLT7PkmksVisfwXs3jx4lc
aGhrGuq4b2xeyWCz/
Hsy8i8J2B7cB6DdlypQvOzvWZlgsFouliFGjRo3LZrMV8+bNqwQAIQQNHjx4XM+ePa9g5kJLS8ura9
asmdP2eaXU7he/
oUOHXlwoFLZ9+OGHr7UdSyaTZZWVldcxs6yqqppZPG7IkCGnbNu27W3XdbMAQEV5+vLy8m7Nzc1Nbf
8thOC99977WwceeOBsIUTCdd1HADgbN258GwB69Oix15AhQ24TQlTU1NQ8sGHDhhVSSiYiNXDgwJ+k
0+kZO3bsmPbRRx9VK6WYiFR0TzVw4MCh69evr+4MCh69evr2o71nb+gAMO6N2vX7+xy5cv/
33bZwFASsme56kjjzzyaAANa9eu/
QAACoWCSiQSXFlZecTatWvbWvbubOOGDFiWnl5+aW+7y9ZunTpbiddz/
Mouubu71787+l0utvgwYNva25uXrJq1arXAMD3fRo+fPj5XbpOOW79+vWX7ty5s77ttwKAYcOGnGnZlM
JiurqqpmNjU1eW3Xqqio6Ln//
vsfXF1dXdX22eJxQRDEjgFAt27dulVWVl7lOM7ha9asOaehoaFJCEGHHHHLI9/v06XOP7/
sbly1bdknxuMMPP/yUnj2XpvP59996733/OBK3/e/
rqqqWtB2fNiwYbeUlZX9QRDEjgFAt27dulVWVl7lOM7ha9asOaehoaFJCEGHHHHLI9/v06XOP7/
sbly1bdknxuMMPP/yUnj2XpvP59996733/OBK3/e/
S7bvHnzvdlsNiuEIGYWSinab7/9Dt5nn32uzufzn3344Yd3K6WImUV5eXnXbt26dfdfdt13a8QamAJgGB
mIiLRp0+fQU1NTW5XK6OmQmAICLq37//hGQy+a3Nmzc/
HQRBPYDHAZRLKRthsVgslv8smUzm2EwmM+GbjqrqzNVn+wxDQ0Nezc0NBj7EDFzyYqUTCbT6T4w/
1dkMpnx/6nn8P9BQ0NDTETruu4Q13WN7sV1dXU/
ZHMjy5JkMpkb6uvrdY+aDslmsyNd171FP97U1NQ3l8t1yrtGx3XdwdlstrmfRaLxWKxWCwWCwWCwWi8
gsFovFYrFYLBaLxWKxWCwWi8VisVgsFovFYrFYLBaLxWKxWCwWi8VisVgsFovFYrFYLBaLxWKxWCwWi8
AuMvYr9eTPdaAAAAAElFTkSuQmCC" alt="Diagram" />

```
## Implementing the Zero Trust Mindset: Your First Steps

While a full Zero Trust implementation is a journey, we can outline the
conceptual first steps you'd take to adopt this mindset. This isn't about
writing code yet, but understanding the foundational actions.

1.  **Know Your Architecture and Assets:**
    -   **Action:** Conduct a thorough inventory of all your users, devices
(laptops, mobile phones, IoT), applications, services, and data. Understand
their interdependencies.
    -   **Why it matters:** You cannot protect what you don't know exists.
This initial discovery phase is crucial for defining your "protect surface."

2.  **Identify Your Protect Surface:**
    -   **Action:** Pinpoint your most critical business assets, data, and
applications — the "crown jewels" that, if compromised, would cause the most
damage.
    -   **Why it matters:** Zero Trust implementation is iterative. Starting
with your most valuable assets allows you to demonstrate value quickly and
build momentum.

3.  **Map Transaction Flows:**
    -   **Action:** For each critical asset, understand how users, devices,
and other services legitimately interact with it. What data flows where? Who
needs access to what, and why?
    -   **Why it matters:** This helps you define granular access policies
based on actual need, rather than broad network access.

4.  **Establish Strong Identity as the New Perimeter:**
    -   **Action:** Begin to enforce strong identity verification for all
users and devices. This includes ubiquitous Multi-Factor Authentication (MFA).
    -   **Why it matters:** Identity is the cornerstone of "Verify
Explicitly." Without strong identity, the entire Zero Trust model falters.

These initial steps are about observation, understanding, and shifting your
organization's perspective before diving into specific technological
solutions.

## Real-world Insight: The Drivers for Adoption

Organizations aren't adopting Zero Trust just for theoretical benefits; there
are concrete, compelling drivers that push this transformation:
-   **Regulatory Compliance:** Many industry regulations (e.g., GDPR, HIPAA,
PCI DSS) and government mandates implicitly or explicitly align with Zero
Trust principles. They demand stricter access controls, data protection, and
continuous monitoring, often exceeding baseline standards.
-   **Supply Chain Security:** Protecting against sophisticated attacks
originating from third-party vendors or partners requires explicit
verification of their systems and restricted access, even for trusted
partners.
-   **Digital Transformation:** As businesses rapidly migrate to cloud
services, adopt SaaS applications, and embrace remote or hybrid work models,
Zero Trust provides the necessary security framework for these inherently
distributed and borderless environments. It's the security model built for the
modern enterprise, not the legacy data center.

## Mini-Challenge: Shifting Your Perspective

Imagine you are a security architect for a company that has just moved all its
applications and data to the cloud, and all employees now work remotely.

**Challenge:** How would you explain to your CEO, in simple terms, why relying
```

```
solely on a traditional network firewall (which now only protects your empty
on-premises data center) is no longer sufficient, and why a Zero Trust
approach is absolutely necessary? Focus on the core problem Zero Trust solves.

**Hint:** Think about where your users and data actually reside now, and what
"inside" and "outside" mean in this new context. Consider the implications of
a compromised credential in both models.

## Common Pitfalls & Troubleshooting

While Zero Trust is a powerful paradigm, its implementation can be challenging
and fraught with common mistakes. These often arise from misunderstanding the
fundamental shift required.

1.  **Treating Zero Trust as a Product:**
    -   **Pitfall:** Believing that purchasing a single "Zero Trust solution"
or vendor appliance will magically solve all security problems.
    -   **Troubleshooting:** Recognize that Zero Trust is a comprehensive
strategy requiring changes across people, processes, and technology. It's an
ongoing journey, not a one-time purchase. Focus on integrating existing tools
and phasing in new capabilities.

2.  **Lack of Comprehensive Asset Inventory:**
    -   **Pitfall:** Attempting to implement Zero Trust without a deep,
current understanding of all users, devices, applications, and data within the
organization.
    -   **Troubleshooting:** Prioritize a robust asset discovery and
management program. You can't apply "least privilege" or "verify explicitly"
effectively if you don't know what you're trying to protect or who is
accessing it.

3.  **Ignoring Identity Management Modernization:**
    -   **Pitfall:** Neglecting to modernize or properly configure Identity
and Access Management (IAM) systems, especially around strong authentication
(MFA).
    -   **Troubleshooting:** Strong, centrally managed identity is the
cornerstone of "Verify Explicitly." Invest in robust IAM solutions and enforce
MFA across *all* accounts. This is often the highest impact initial step.

4.  **Insufficient Executive Buy-in and Organizational Resistance:**
    -   **Pitfall:** Without strong leadership support, Zero Trust initiatives
can stall due to budget constraints, a lack of cross-departmental cooperation,
or user resistance to new security measures.
    -   **Troubleshooting:** Clearly articulate the business value and risk
reduction to leadership. Engage stakeholders early and often. Communicate
changes transparently to users, explaining the "why" behind new processes.
Start with high-impact, low-friction areas to build early wins.

## Summary: A New Era of Security

In this chapter, we've explored the foundational ideas behind Zero Trust
Security. We've seen how the traditional "castle-and-moat" model crumbles
under the weight of modern threats and distributed environments. We then
introduced Zero Trust as the imperative solution, built on three core
principles: **Verify Explicitly, Use Least Privileged Access, and Assume
Breach.**

**Key Takeaways:**
-   Traditional perimeter-based security is no longer adequate for modern
threats and distributed IT environments.
-   Zero Trust is a security strategy and philosophy, not a specific product
or single technology.
```

```
-   Its core principle is "Never trust, always verify" for every access
request.
-   The three pillars are Verify Explicitly, Use Least Privileged Access, and
Assume Breach.
-   Implementing Zero Trust requires a comprehensive understanding of your
organizational assets, a shift in mindset, and a commitment to a holistic
security transformation.
-   Initial steps involve knowing your assets, defining your protect surface,
mapping transaction flows, and strengthening identity management.

This shift in mindset is crucial for building resilient, future-proof security
architectures. In the next chapter, we'll dive deeper into the first
principle: "Verify Explicitly" and begin to explore the components that make
it possible.

## References

-   Zero Trust adoption framework overview | Microsoft Learn: https://
learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-
overview
-   What is Zero Trust? | Microsoft Learn: https://learn.microsoft.com/en-us/
security/zero-trust/zero-trust-overview
-   GitHub - ukncsc/zero-trust-architecture: Principles to help you design and
deploy a zero trust architecture: https://github.com/ukncsc/zero-trust-
architecture
-   zero-trust-overview.md - security-docs - GitHub: https://github.com/
MicrosoftDocs/security/blob/main/security-docs/zero-trust/zero-trust-
overview.md

This page is AI-assisted and reviewed. It references official documentation
and recognized resources where relevant.
```

CHAPTER 02

Deciphering Zero Trust: Core Principles and Philosophy

Introduction: Shifting from Trust to Verification

Welcome back! In our previous chapter, we set the stage for understanding the critical need for modern security strategies. Now, we're diving deep into the heart of one of the most transformative approaches in cybersecurity today: Zero Trust. This chapter isn't about specific tools or technologies yet; it's about understanding the fundamental philosophy that underpins Zero Trust.

Think of it as learning the "why" before the "how." By grasping the core principles, you'll be equipped to apply Zero Trust thinking to any environment, regardless of the specific products or services you use. This philosophical understanding is what truly differentiates a successful Zero Trust implementation from a mere collection of security tools.

The Paradigm Shift: From Implicit Trust to Explicit Verification

For decades, cybersecurity operated on a "castle-and-moat" model. Once you were inside the network perimeter, you were generally trusted. This implicit trust was a fundamental flaw, especially as organizations moved to cloud services, remote work became common, and threats grew more sophisticated. Attackers who breached the perimeter could often move freely, or "laterally," within the network.

Zero Trust flips this model on its head. It operates on a simple, yet radical, premise: **"Never trust, always verify."** This means no user, device, application, or network segment is inherently trusted, whether it's inside or outside the traditional network perimeter. Every access request must be explicitly authenticated and authorized based on all available data points.

Why the "Assume Breach" Mindset is Essential

The core of Zero Trust isn't just about verifying; it's also about assuming that a breach will happen. This "assume breach" mindset forces us to design security with resilience and containment in mind, rather than solely focusing on

prevention. If an attacker does get in, how quickly can we detect them? How much damage can they do? How can we limit their movement? These are the questions Zero Trust helps us answer.

The Pillars of Zero Trust: Core Principles

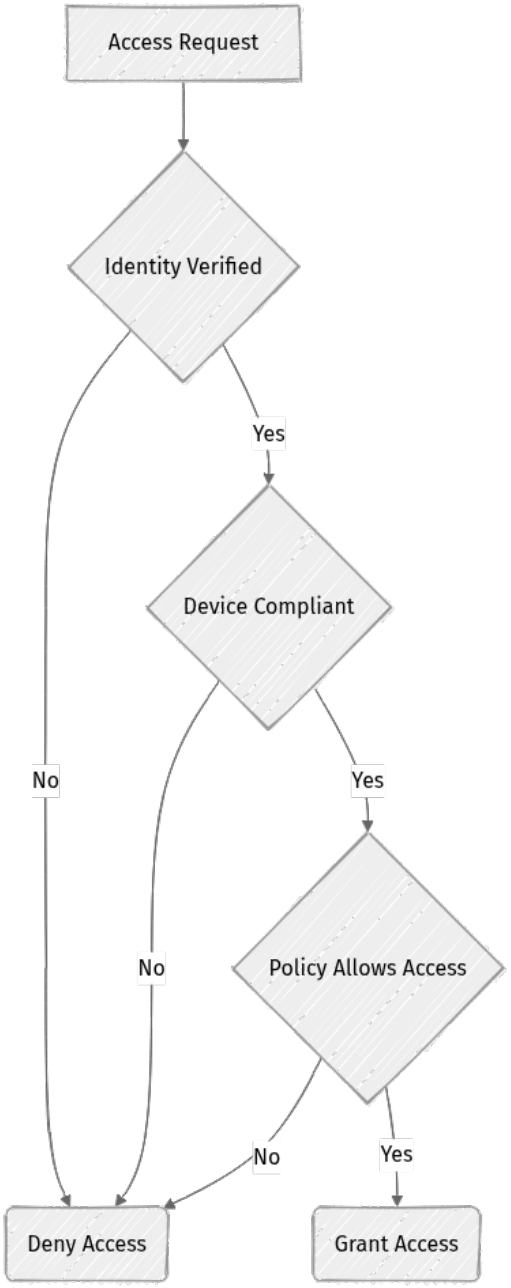
Zero Trust is built upon three foundational principles. These aren't steps in a sequence but rather intertwined concepts that must be applied holistically.

1. Verify Explicitly

This is arguably the most recognizable principle of Zero Trust. It means that every access attempt—whether by a user, device, or application—must be authenticated and authorized. No exceptions.

- **What it means:** Don't assume anything is safe just because of where it's coming from. Every identity and every device trying to access a resource must prove who and what it is, and confirm its health.
- **Why it's crucial:** This principle eliminates the implicit trust that attackers exploit. If an attacker compromises a user account or a device, they can't simply move on to the next resource without re-verification.
- **How it works:**
    - **Strong Identity Verification:** Multi-factor authentication (MFA) is non-negotiable. It's the baseline for verifying user identities.
    - **Device Health and Compliance:** Is the device updated? Does it have antivirus running? Is it encrypted? Devices must meet security policies before being granted access.
    - **Contextual Access Policies:** Access decisions aren't just about "who" but also "what," "where," "when," and "how." For example, a user might only be allowed to access sensitive data from a compliant device, during business hours, from a known location.

Here's a simplified view of the "Verify Explicitly" decision flow:



2. Use Least Privileged Access

Once access is granted, it should be the bare minimum required for the task at hand, and only for the necessary duration. This principle is about minimizing the "blast radius" if an account or device is compromised.

- **What it means:** Users and systems should only have access to the resources they absolutely need to perform their duties, and for the shortest possible time. No more, no less.
- **Why it's crucial:** If an attacker compromises an account with excessive privileges, they gain control over many systems. Least privilege access limits what an attacker can do, even if they successfully breach an identity.

- **How it works:**
    - **Just-in-Time (JIT) Access:** Granting elevated privileges only when they are needed and for a limited time (e.g., 30 minutes to perform a specific administrative task).
    - **Role-Based Access Control (RBAC) / Attribute-Based Access Control (ABAC):** Defining granular roles and permissions based on job functions or attributes, ensuring users can only access what their role requires.
    - **Micro-segmentation:** Dividing networks into small, isolated segments. This prevents lateral movement by an attacker, even if they compromise a single segment. Each segment has its own strict access controls.

3. Assume Breach

This principle is about designing your security architecture with the expectation that attackers will eventually bypass your defenses. It shifts the focus from purely preventing intrusions to also rapidly detecting, containing, and remediating them.

- **What it means:** Plan for the worst. Assume that an adversary might already be inside your network or will get in at some point.
- **Why it's crucial:** No security system is impenetrable. By assuming breach, you build in resilience and prepare for incident response, reducing the impact and duration of an attack. It moves you from a reactive stance to a proactive one.
- **How it works:**
    - **Continuous Monitoring:** Actively monitoring all network traffic, user behavior, and system logs for anomalous activity that could indicate a breach.
    - **Segment Everything:** Applying micro-segmentation not just to networks but also to applications, data, and workloads. This isolates potential compromises.
    - **Automated Response:** Implementing automated playbooks to respond to detected threats, such as isolating compromised devices or revoking access.
    - **End-to-End Encryption:** Encrypting all communications, even within the internal network, ensures that data remains protected even if traffic is intercepted.

Zero Trust: A Philosophy, Not a Product

📌 **Key Idea:** Zero Trust is a strategic approach and a set of guiding principles, not a single piece of software or hardware you can buy.

Many vendors offer "Zero Trust solutions," but these are usually components that help implement Zero Trust, not the complete strategy itself. True Zero Trust requires a holistic shift in an organization's security posture, processes, and culture. It demands:

- **Organizational Commitment:** Leadership buy-in and a willingness to evolve security practices.
- **Iterative Implementation:** It's a journey, not a destination. You implement Zero Trust gradually, focusing on critical assets first, and continuously refining your policies.
- **Integration:** Zero Trust principles must be integrated across identity, devices, applications, data, and infrastructure.

Mini-Challenge: Applying the Principles

Imagine you are a security architect for a company that uses cloud-based document storage (like SharePoint or Google Drive) and a mix of company-issued and personal devices (BYOD) for employees.

Challenge: How would you apply the three core Zero Trust principles (Verify Explicitly, Least Privileged Access, Assume Breach) to secure access to these cloud documents? Give one concrete example for each principle.

Hint: Think about what an attacker might try to do and how each principle would stop or limit their actions.

Common Misconceptions & Pitfalls

Implementing Zero Trust isn't without its challenges. Here are a few common pitfalls to watch out for:

- **Treating it as a "Set and Forget" Solution:** Zero Trust requires continuous monitoring, policy refinement, and adaptation to new threats and business needs. It's an ongoing process.
- **Focusing Only on Network Segmentation:** While critical, micro-segmentation is just one piece of the puzzle. Identity, device, application, and data security are equally important.

- **Ignoring User Experience:** Overly restrictive policies can frustrate users and lead to workarounds, creating new security risks. Balancing security with usability is key.
- **Lack of Organizational Buy-in:** Without support from leadership and collaboration across IT, security, and even business units, Zero Trust initiatives often falter. It's a cultural shift as much as a technical one.

Summary: The Foundation for Modern Security

This chapter has laid the philosophical groundwork for understanding Zero Trust Security. We've covered:

- The critical shift from perimeter-based security to an "assume breach" mindset.
- The three core principles: **Verify Explicitly**, **Use Least Privileged Access**, and **Assume Breach**.
- Why Zero Trust is a strategic philosophy, not a single product, requiring holistic organizational commitment.

Understanding these principles is paramount before diving into the technical implementations. They are the lens through which all future security decisions will be made. In the next chapter, we'll begin to explore the practical components and strategic approach to implementing Zero Trust within an organization, building on this foundational knowledge.

References

- What is Zero Trust? | Microsoft Learn
- Zero Trust adoption framework overview | Microsoft Learn
- GitHub - ukncsc/zero-trust-architecture: Principles to help you design and deploy a zero trust architecture

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 03

Identity is the New Perimeter: Strengthening Authentication and Authorization

In the digital world, the traditional "castle-and-moat" security model is obsolete. Gone are the days when we could simply build a strong wall around our network and assume everything inside was safe. With cloud computing, mobile devices, and remote work, our resources are everywhere, and the old network perimeter has dissolved.

So, if the network isn't the perimeter, what is? In a Zero Trust world, the answer is clear: **identity**. Every user, every device, every application, and every service must explicitly prove who and what it is, and what it's authorized to do, before gaining access to any resource. This chapter dives deep into how we establish and enforce this new identity-centric perimeter, focusing on robust authentication and granular authorization.

To get the most out of this chapter, you should already be familiar with the core principles of Zero Trust, particularly "Verify Explicitly" and "Use Least Privileged Access," which we covered in previous discussions. We're now going to put those principles into practice for the most critical component: who gets in and what they can do.

The Shift: From Network Perimeter to Identity Perimeter

For decades, cybersecurity focused on protecting the network edge. Firewalls guarded the entry points, and once inside, access was often implicitly trusted. This approach worked when all company data and users were primarily within the physical office.

Why the Traditional Perimeter Failed

The rise of cloud services, SaaS applications, personal devices, and remote work shattered this model. Data now lives in data centers, public clouds, and SaaS platforms. Users access resources from anywhere, on any device. The idea of a single, defensible network boundary became a myth.

📌 `Key Idea:` In Zero Trust, we treat every access request as if it originates from an untrusted network, regardless of its actual location. Trust is never assumed; it must always be earned.

This means that instead of relying on where a request comes from, we rely on who or what is making the request. This fundamental shift places identity at the forefront of our security strategy.

Strong Authentication: The First Line of Defense

Authentication is the process of verifying who a user or what a device claims to be. In Zero Trust, this isn't a one-time login; it's a continuous, context-aware process.

Multi-Factor Authentication (MFA)

MFA is non-negotiable in a Zero Trust environment. It requires users to provide two or more distinct pieces of evidence to verify their identity.

What is MFA?

Instead of just a password (something you know), MFA adds another layer, such as:

- **Something you have:** A physical token, a smartphone with an authenticator app, a smart card, or a FIDO2 security key.
- **Something you are:** A biometric scan like a fingerprint or facial recognition.

Why is MFA Crucial for Zero Trust?

Passwords alone are vulnerable. They can be guessed, stolen, phished, or reused. MFA significantly raises the bar for attackers. Even if a password is compromised, the attacker still needs the second factor to gain access.

⚡ `Quick Note:` Modern MFA solutions, especially those leveraging FIDO2 standards (like Passkeys), are highly resistant to phishing attacks, making them a cornerstone of strong identity verification. As of 2026-05-28, FIDO2 is the recommended standard for strong, phishing-resistant authentication.

How MFA Works (Simplified)

When a user tries to log in:

1. They enter their username and password.

2. The authentication system then prompts for a second factor (e.g., a code from their authenticator app, a push notification approval, or a biometric scan).
3. Only after both factors are successfully verified is access granted.

Single Sign-On (SSO)

Managing multiple usernames and passwords for different applications is a headache for users and a security risk. SSO solves this by allowing users to log in once to a central identity provider (IdP) and then access multiple connected applications without re-authenticating.

What is SSO?

SSO provides a unified authentication experience. Instead of remembering credentials for Slack, Salesforce, Confluence, and dozens of other tools, a user logs into a central system (e.g., Okta, Azure AD, Ping Identity). This central system then asserts the user's identity to other applications.

Why is SSO Important for Zero Trust?

1. **Improved User Experience:** Reduces password fatigue, leading to less password reuse and fewer support tickets.
2. **Centralized Control:** All authentication events are routed through and logged by a single, trusted IdP. This makes monitoring, auditing, and enforcing policies much easier.
3. **Enhanced Security:** Allows organizations to enforce strong MFA policies across all integrated applications from a single point.
4. **Simplified Provisioning/Deprovisioning:** When an employee joins or leaves, their access can be managed efficiently through the central IdP.

How SSO Works (Briefly)

SSO typically relies on industry standards like SAML 2.0 (Security Assertion Markup Language) or OpenID Connect (OIDC).

1. A user attempts to access an application (Service Provider, SP).
2. The SP redirects the user's browser to the Identity Provider (IdP).
3. The IdP authenticates the user (e.g., with username/password + MFA).
4. Upon successful authentication, the IdP sends a signed assertion (SAML) or ID token (OIDC) back to the SP, confirming the user's identity.
5. The SP trusts this assertion and grants access to the user.

Granular Authorization: Least Privilege in Action

Authentication verifies who you are. Authorization determines what you are allowed to do. In Zero Trust, authorization must be as granular as possible, adhering strictly to the principle of least privilege.

Principle of Least Privilege (PoLP)

What is PoLP?

PoLP dictates that every user, device, and application should be granted only the minimum necessary permissions to perform its specific task, and for the shortest possible duration. No more, no less.

Why is PoLP Crucial for Zero Trust?

🧠 `Important:` PoLP is a core tenet of "Assume Breach." If an attacker compromises an identity with least privilege, their ability to move laterally and access critical data is severely limited. It drastically reduces the "blast radius" of a potential breach.

For instance, a marketing intern doesn't need administrative access to the production database. They might only need read access to a specific marketing campaign dashboard.

Attribute-Based Access Control (ABAC)

While Role-Based Access Control (RBAC) assigns permissions based on predefined roles (e.g., "Admin," "Editor," "Viewer"), ABAC takes authorization to the next level by making dynamic access decisions based on a rich set of attributes.

What is ABAC?

ABAC uses attributes associated with the user, the resource being accessed, the environment, and the action being requested to determine access.

Examples of Attributes:

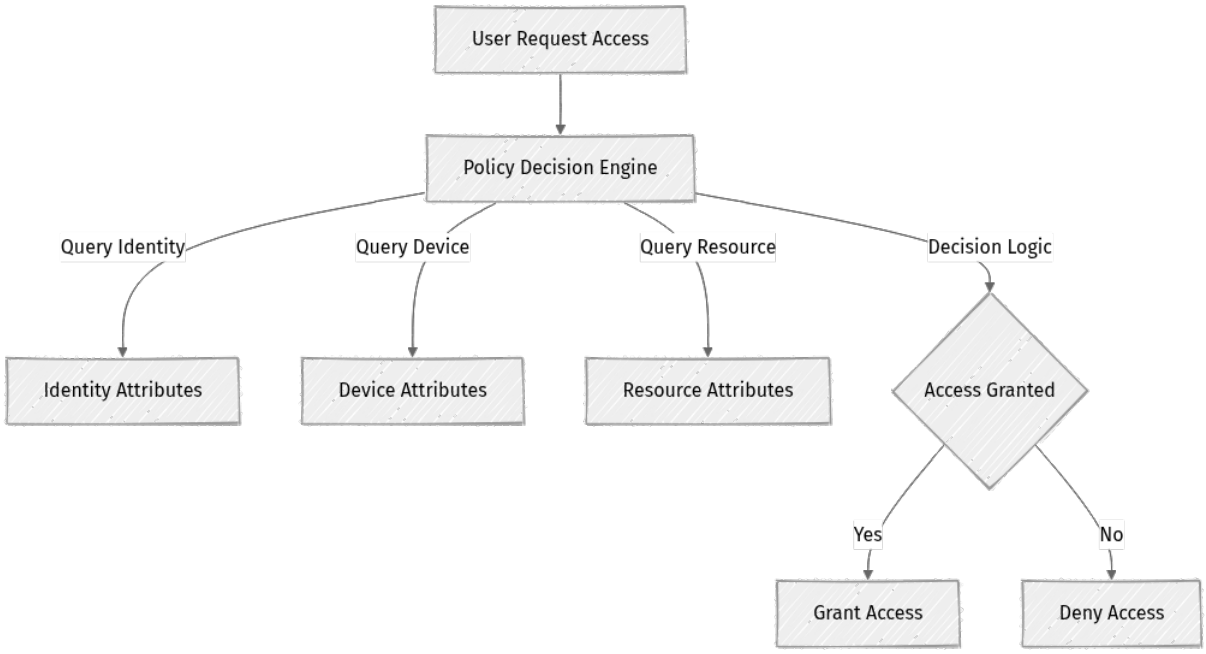
- **User Attributes:** Role, department, security clearance, location, manager.
- **Resource Attributes:** Sensitivity level (e.g., "Confidential," "Public"), owner, creation date, type.
- **Environmental Attributes:** Time of day, IP address, device health (e.g., patched, encrypted), network location.
- **Action Attributes:** Read, write, delete, execute.

Why is ABAC Powerful?

ABAC provides far greater flexibility and scalability than traditional RBAC, especially in complex, dynamic environments. Instead of creating hundreds of static roles, you define policies that evaluate attributes in real-time.

For example, a policy might state: "A user with the `Finance` role can `read` `Confidential` documents only if they are accessing from a `corporate device` and within `business hours`."

This dynamic evaluation ensures that access is always context-aware and aligned with current security posture.



The ABAC Policy Decision Engine evaluates various attributes to make a dynamic access decision.

Just-in-Time (JIT) and Just-Enough-Access (JEA)

These concepts extend PoLP by making access not only minimal but also temporary.

What are JIT and JEA?

- **Just-in-Time (JIT) Access:** Grants permissions only for a limited, short duration (e.g., 30 minutes, 1 hour) when they are explicitly requested and approved.
- **Just-Enough-Access (JEA):** Ensures that the elevated permissions granted are precisely what's needed for the specific task at hand, and no more.

Why are JIT and JEA Essential for Critical Resources?

⚡ `Real-world insight:` JIT/JEA are invaluable for administrative access to highly sensitive systems (e.g., production servers, critical databases, cloud infrastructure). Instead of persistent admin rights, users request temporary elevation, which is then automatically revoked. This dramatically reduces the window of opportunity for attackers to exploit elevated privileges.

Step-by-Step Implementation: Modernizing Identity with Zero Trust

Implementing Zero Trust identity management is an iterative journey. Here's a structured approach, focusing on general best practices rather than specific vendor code.

Phase 1: Understand Your Current Identity Landscape

Before you can secure identities, you need to understand them thoroughly.

Step 1: Discover All Identity Sources

Start by identifying every system that manages user identities in your organization.

- List every system that authenticates users: Active Directory (AD), LDAP, Azure AD, Okta, Google Identity, custom databases, SaaS app-specific identity stores.
- Identify all users, service accounts, and their current group memberships and permissions. Don't forget those forgotten accounts!

Step 2: Map Existing Access Flows

For your most critical applications and data, understand who accesses what, when, and how.

- Document the current access paths for your most sensitive resources.
- Identify any "shadow IT" applications that might have their own unmanaged identity stores. These are significant blind spots.

⚠️ `What can go wrong:` An incomplete inventory creates blind spots, leaving unmanaged identities as potential backdoors for attackers. Take your time with this foundational step.

Phase 2: Implement Strong Authentication Mechanisms

This phase focuses on centralizing and strengthening how users prove who they are.

Step 1: Roll Out Multi-Factor Authentication (MFA)

This is your highest priority for immediate security uplift.

- **Choose an Identity Provider (IdP):** If you don't have a modern, cloud-native IdP (like Azure AD, Okta, Ping Identity, Duo), now is the time to invest. It's your central hub for identity.
- **Configure MFA Policies:** Within your chosen IdP, enable MFA for all users. Prioritize administrative accounts, then gradually roll out to all employees.
- **Enroll Users:** Guide users through the enrollment process for their second factor (e.g., authenticator app, hardware key, FIDO2 device).
- **Phased Rollout:** Start with a pilot group, gather feedback, and then expand. User adoption is critical!

⚡ `Pro tip:` Provide clear documentation and training for users. Emphasize why MFA is important for their security, not just the company's.

Step 2: Centralize Authentication with Single Sign-On (SSO)

Aim to route all application access through your central IdP to simplify and secure logins.

- **Integrate Applications:** Systematically integrate all your SaaS and custom applications with your central IdP using standards like SAML 2.0 or OpenID Connect (OIDC).
- **Migrate Legacy Authentication:** For older applications, plan a migration strategy from legacy authentication methods to modern SSO. This might involve proxies or application modernization.
- **Automate Provisioning:** Use SCIM (System for Cross-domain Identity Management) to automatically provision and deprovision user accounts in integrated applications from your central IdP. This ensures consistent access and timely revocation.

Phase 3: Enforce Granular Authorization

Once users are strongly authenticated, control what they can access with precision.

Step 1: Refine Access with Least Privilege Roles

Review and refine your access controls to strictly follow the Principle of Least Privilege (PoLP).

- **Audit Existing Permissions:** Use the inventory from Phase 1 to identify all existing permissions. You'll likely find many that are overly permissive or no longer needed.
- **Create Tightly Scoped Roles:** For each application and data set, define roles with the absolute minimum permissions required. Think about what a user needs to do their job, not what they might need.
- **Remove Default Global Permissions:** Eliminate "everyone" or "all authenticated users" access to sensitive resources. Explicitly grant access instead.
- **Regular Review:** Schedule regular audits of user and service account permissions. Access requirements change, and so should permissions.

Step 2: Adopt Attribute-Based Access Control (ABAC)

Move beyond static roles where possible, especially for sensitive data, to enable dynamic decision-making.

- **Identify Key Attributes:** Determine which user, device, resource, and environmental attributes are relevant for making access decisions in your environment (e.g., user department, device compliance status, data classification, time of day, network location).
- **Define ABAC Policies:** Translate your security requirements into attribute-based policies within your IdP or a dedicated Policy Decision Point (PDP).
- **Pilot and Test:** Implement ABAC for a small, non-critical resource first, thoroughly test, and then expand. This allows you to fine-tune policies without impacting critical operations.

Step 3: Enable Just-in-Time (JIT) and Just-Enough-Access (JEA)

For highly privileged access, make it temporary and precisely scoped.

- **Identify Privileged Accounts:** Pinpoint all accounts with administrative access to critical infrastructure (cloud consoles, production servers, network devices, sensitive applications).
- **Implement a Privileged Access Management (PAM) Solution:** Use a PAM tool (e.g., CyberArk, Delinea, Azure PIM) to manage, monitor, and gate access to these accounts.

- **Configure JIT/JEA Workflows:** Set up workflows where users must request elevated access, provide a justification, and have it approved. The access is then granted for a limited time and automatically revoked. This significantly reduces the attack surface.

Phase 4: Monitor and Continuously Improve

Zero Trust is a continuous journey, not a one-time project. Your identity and access controls need constant vigilance.

Step 1: Establish Robust Monitoring and Logging

Ensure you have visibility into every access attempt and decision.

- **Log Everything:** Ensure all authentication attempts, authorization decisions, and access events are logged and sent to a Security Information and Event Management (SIEM) system.
- **Anomaly Detection:** Use your SIEM or other security tools to detect unusual login patterns, unauthorized access attempts, or sudden changes in permissions. These could indicate a breach in progress.

Step 2: Conduct Regular Audits and Refinements

Your environment changes, and so should your security policies.

- **Continuous Review:** Continuously review your identity and access policies, user permissions, and MFA adoption rates.
- **Adjust as Needed:** Adjust policies and configurations as your environment, business needs, and threat landscape evolve.

Mini-Challenge: Designing an ABAC Policy

Let's put your understanding of ABAC to the test.

Challenge: You need to design an ABAC policy for accessing your company's `Highly Confidential Customer Data` database. Outline the attributes you would consider and how they would combine to grant or deny access.

Hint: Think about different types of users (e.g., role, department), the devices they use (e.g., corporate vs. personal, compliant vs. non-compliant), the sensitivity of the data, and even the context of the access request (e.g., network location, time of day).

What to Observe/Learn: How many dynamic factors can you identify that would make access decisions more secure than just a simple role? How would this policy adapt if a user changed roles or a device became non-compliant?

Common Pitfalls & Troubleshooting

Implementing Zero Trust identity can present challenges. Being aware of these common pitfalls can help you navigate them effectively.

⚠️ `What can go wrong:`

- **MFA Fatigue or Bypass:** Users might become annoyed by frequent MFA prompts, leading to attempts to bypass it or falling victim to phishing attacks that trick them into approving MFA requests.
    - **Solution:** Implement context-aware MFA (e.g., only prompt if location changes, device is unknown). Adopt phishing-resistant MFA like FIDO2/Passkeys. Educate users on the importance of not approving unsolicited MFA requests.
- **Too Permissive Policies:** Due to fear of breaking business operations or legacy system constraints, organizations might initially create overly broad access policies. This undermines the "least privilege" principle.
    - **Solution:** Start with "deny all" and explicitly grant only what's needed. Use JIT/JEA for sensitive resources. Conduct regular, thorough access reviews to identify and revoke excessive permissions.
- **Shadow IT Identities and Accounts:** Unsanctioned applications or services might create their own identity stores that are not integrated with your central IdP, leading to unmanaged and unsecure accounts.
    - **Solution:** Implement discovery tools to identify all applications and data sources. Establish clear policies for application integration with the central IdP. Conduct regular audits for unmanaged accounts.
- **Poor User Experience:** Overly complex authentication flows or too many prompts can frustrate users, leading to workarounds that compromise security.
    - **Solution:** Balance security with usability. Streamline SSO for common applications. Provide clear communication and training. Leverage intelligent, risk-based access policies that reduce prompts when risk is low.

Summary

This chapter has highlighted why identity is the new perimeter in a Zero Trust world, a fundamental shift from traditional network-centric security.

Here are the key takeaways:

- **Identity as the Perimeter:** With the dissolution of network boundaries, every user, device, and service must explicitly verify its identity and authorization.
- **Multi-Factor Authentication (MFA):** Essential for strong identity verification, significantly reducing the risk of credential compromise.
- **Single Sign-On (SSO):** Centralizes identity management, improves user experience, and simplifies security policy enforcement across applications.
- **Principle of Least Privilege (PoLP):** Granting only the minimum necessary access for a specific task and duration is crucial to limit the impact of a breach.
- **Attribute-Based Access Control (ABAC):** Enables dynamic, granular authorization decisions based on a rich set of user, device, resource, and environmental attributes.
- **Just-in-Time (JIT) and Just-Enough-Access (JEA):** Critical for securing privileged accounts by granting temporary, time-bound access.
- **Continuous Monitoring:** Identity and access management in Zero Trust is an ongoing process requiring constant assessment, logging, and refinement.

Understanding and implementing these identity-centric security measures are foundational to a successful Zero Trust strategy. In our next chapter, we'll shift our focus from who is accessing resources to what they are accessing them with: **device security and compliance**.

References

- Zero Trust adoption framework overview | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview
- What is Zero Trust? | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
- Principles to help you design and deploy a zero trust architecture | NCSC GitHub: https://github.com/ukncsc/zero-trust-architecture
- Zero Trust Identity and Access Management Best Practices | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-identity-access-management
- Attribute-Based Access Control (ABAC) | NIST: https://csrc.nist.gov/glossary/term/attribute-based_access_control

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 04

Securing Every Device: Endpoints, Workloads, and IoT

Securing Every Device: Endpoints, Workloads, and IoT

Welcome back! In our previous chapters, we laid the groundwork for Zero Trust, understanding its core principles and how it transforms identity and access management for users. We established that "never trust, always verify" applies to human identities. But what about the other vital components in our digital ecosystem? What about the laptops, servers, containers, and countless IoT devices that connect to our networks every day?

This chapter dives deep into securing every device under the Zero Trust umbrella. You'll learn how Zero Trust principles apply to endpoints (like your laptop or smartphone), workloads (servers, virtual machines, containers), and even the often-overlooked Internet of Things (IoT) devices. By the end, you'll understand why treating every device as a potential threat, and explicitly verifying its identity and health, is non-negotiable in modern cybersecurity. This proactive approach is essential for preventing lateral movement and containing breaches in a world without a traditional network perimeter.

The Device as a First-Class Identity in Zero Trust

In a Zero Trust world, a device is no longer just a piece of hardware that passively connects to the network. It's an **identity** that needs to be authenticated, authorized, and continuously monitored, just like a user. The traditional network perimeter has dissolved, and attackers frequently target devices as entry points to gain initial access or move deeper into a system. Therefore, securing devices is paramount to preventing lateral movement and containing breaches.

Why does a device need an identity? Because its access to resources must be controlled and conditional. Every device, regardless of its type, must meet specific security criteria before being granted access to organizational resources. This involves verifying not only who is using the device (user identity), but also what the device is, where it is connecting from, and critically, how healthy it is.

📌 **Key Idea:** In Zero Trust, devices are treated as identities that require explicit, continuous verification and validation, just like users. Their security posture directly impacts their access privileges.

Endpoints: Securing Your Digital Frontline

Endpoints are the most common entry points into an organization's network. Laptops, desktops, smartphones, and tablets are used daily by employees to access sensitive data and applications. Securing these devices is a foundational element of any Zero Trust strategy.

What is Device Identity and How is it Established?

Every endpoint must possess a clear, verifiable identity. This typically involves registering the device with the organization's identity provider (IdP) or a dedicated device management system. This registration process often provisions a unique device ID and a digital certificate that the device uses to authenticate itself to the network and applications.

Why is this important? Without a unique identity, your system can't differentiate between a legitimate corporate laptop and an unauthorized, potentially malicious device attempting to connect.

Continuous Device Health and Posture Assessment

Beyond basic identity, Zero Trust demands that we continuously verify the health or posture of an endpoint. What does "health" mean here? It refers to the current security state of the device, including factors like:

- **Operating System Version:** Is it running a supported OS version and up-to-date with the latest security patches?
- **Antivirus/Anti-Malware Status:** Is a security agent installed, running, and updated with current definitions?
- **Local Firewall Status:** Is the device's local firewall enabled and configured correctly to block unauthorized connections?
- **Encryption Status:** Is the hard drive encrypted to protect data at rest?
- **Compliance with Policies:** Does the device meet organizational security policies (e.g., no unauthorized software, strong password protection, specific browser configurations)?

This assessment isn't a one-time check at login; it's continuous. If a device's posture degrades (e.g., antivirus stops running, a critical patch is missing, or it's jailbroken), its access privileges should be automatically adjusted or revoked in real-time. This dynamic adaptation is crucial for maintaining security.

Endpoint Detection and Response (EDR) for Vigilance

EDR solutions are critical for continuous monitoring and rapid response on endpoints. They collect rich telemetry data from devices (such as process activity, network connections, file changes, and registry modifications) and use advanced analytics and threat intelligence to detect suspicious or malicious behavior. When a threat is identified, EDR can automatically:

- Isolate the compromised device from the network.
- Terminate malicious processes.
- Alert security teams for investigation.
- Initiate automated remediation actions.

⚡ **Real-world insight:** Many organizations leverage a combination of Mobile Device Management (MDM) for smartphones and tablets, and Endpoint Management Solutions (EMS) for laptops and desktops. These tools integrate seamlessly with Identity Providers to enforce device policies, report posture, and apply conditional access rules. For example, a user might only be able to access sensitive cloud applications from a corporate laptop that is fully patched and has EDR running.

Workloads: The Secure Engine of Your Applications

Workloads refer to the compute resources that run your applications and services. This includes virtual machines (VMs), containers, serverless functions, and even physical servers. Securing workloads in a Zero Trust model focuses on limiting their attack surface and ensuring they only communicate and access what is absolutely necessary for their function.

Establishing Workload Identity

Just like users and endpoints, every workload needs a robust identity to participate in a Zero Trust ecosystem. Common methods include:

- **Managed Identities (Cloud Providers):** Cloud providers like Azure, AWS, and GCP offer managed identities for their resources. These allow workloads (e.g., a VM, a function app) to authenticate securely to other cloud services (like databases or storage accounts) without needing hardcoded credentials, which are a major security risk.
- **Service Accounts (Kubernetes):** In container orchestration platforms like Kubernetes, service accounts provide an identity for pods to interact with the Kubernetes API and other services within the cluster.

- **Certificates:** X.509 certificates can be used to establish trust and identity between services, especially in hybrid or on-premises environments, enabling secure mutual TLS (mTLS) communication.

Micro-segmentation: Containing the Blast Radius

Micro-segmentation is a cornerstone of Zero Trust for workloads. It involves dividing networks into small, isolated segments, often down to individual workloads or application components. This means that if one workload is compromised, the attacker's ability to move laterally to other workloads or segments is severely restricted.

Imagine a traditional network as a large open office building where, once inside, an attacker can move freely. Micro-segmentation is like giving every desk, every meeting room, and every server rack its own locked door, requiring separate, explicit authentication and authorization for each. This drastically reduces the "blast radius" of a breach.

Runtime Protection and API Security for Applications

Workloads often expose APIs or run critical applications. Securing these involves several layers:

- **API Gateways:** These act as a single entry point for all API calls, enforcing authentication, authorization, rate limiting, and input validation before requests reach backend services.
- **Web Application Firewalls (WAFs):** WAFs protect web applications from common web-based attacks such as SQL injection, cross-site scripting (XSS), and other OWASP Top 10 vulnerabilities.
- **Runtime Application Self-Protection (RASP):** RASP solutions integrate directly into the application runtime environment, providing continuous monitoring and protection from within the application itself. They can detect and block attacks in real-time by analyzing application behavior.

IoT and OT Devices: Unique Challenges, Critical Security Needs

The Internet of Things (IoT) and Operational Technology (OT) devices present unique challenges for Zero Trust. These can range from smart sensors and cameras to industrial control systems (ICS) and building management systems (BMS). They often have limited processing power, infrequent or difficult-to-apply updates, long lifecycles, and may use proprietary or legacy protocols.

Device Profiling and Anomaly Detection

Due to their unique nature and limited capabilities, a key step for IoT/OT security is to profile these devices. This means understanding and baseline their normal behavior: what protocols they use, what resources they access, what data they send, and their typical communication patterns. Any deviation from this established baseline can be flagged as anomalous and potentially malicious, triggering alerts or automated mitigation.

Strict Network Segmentation for Isolation

Strict network segmentation is even more critical for IoT/OT devices. These devices should be isolated from corporate IT networks and often from each other. Firewalls and access control lists (ACLs) should explicitly define what each device can communicate with, following the principle of least privilege. For example, a temperature sensor in a warehouse should only be allowed to send data to its specific collection point, not to HR systems or other critical infrastructure.

Secure Onboarding and Lifecycle Management

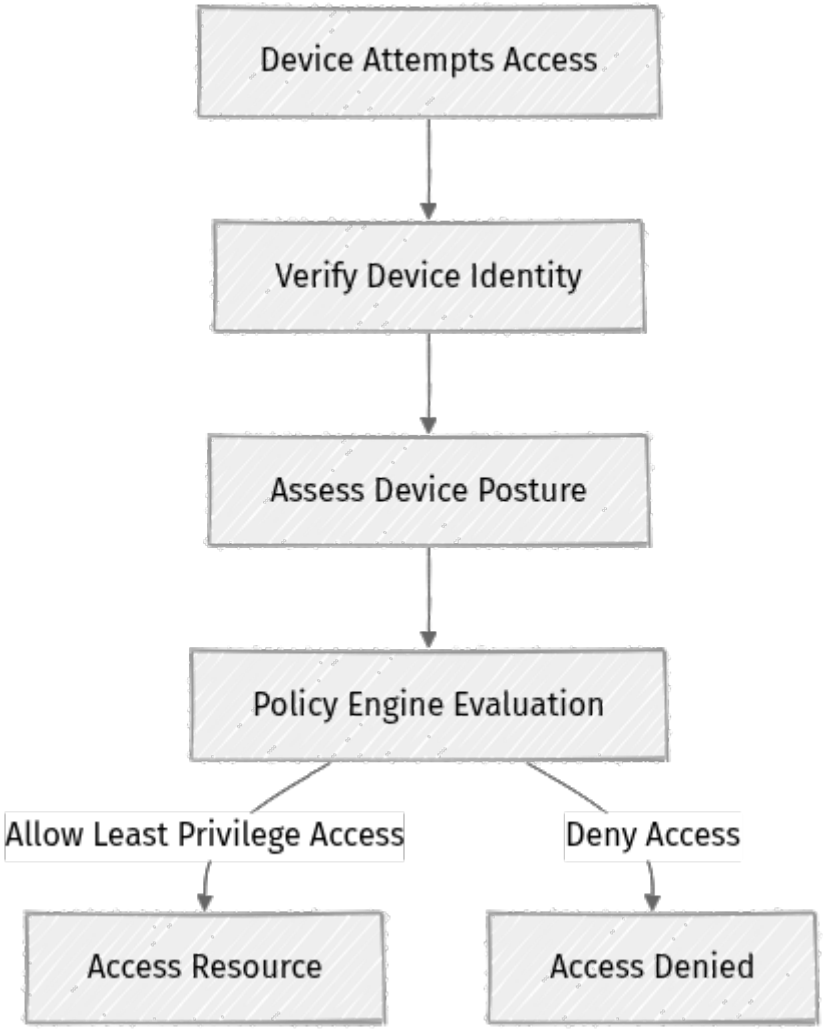
Many IoT devices are traditionally "fire and forget," but Zero Trust demands a more rigorous approach. This includes:

- **Secure Onboarding:** Ensuring devices are provisioned with unique identities (e.g., using hardware-based identities like Trusted Platform Modules (TPMs) or secure elements) and issued certificates during initial setup.
- **Secure Updates:** Implementing mechanisms for secure, signed firmware updates throughout the device's lifecycle.
- **Secure Decommissioning:** Having a plan to securely wipe or decommission devices at the end of their operational life.

🧠 **Important:** Many IoT/OT devices cannot run traditional security agents or handle complex authentication protocols. Zero Trust for these devices often relies more heavily on network-level controls, behavioral analytics, secure gateways that act as proxies, and robust device profiling to enforce trust policies.

The Device Trust Flow: A Visual Journey

Let's visualize how a device earns trust and access in a Zero Trust environment. This continuous process evaluates multiple factors before granting access.



1. **Device Attempts Access:** An endpoint, workload, or IoT device initiates a request to access a specific resource (e.g., a file server, a database, an API).
2. **Verify Device Identity:** The system first checks if the device is known and authenticated. This might involve validating a device certificate, a managed identity token, or a service account.
3. **Assess Device Posture:** Next, the system evaluates the device's current security health against predefined policies. Is it patched? Is its antivirus running? Is it encrypted?
4. **Policy Engine Evaluation:** A central policy engine takes all available context into account: the device's identity, its current posture, the user's identity (if applicable), the sensitivity of the requested resource, the device's location, and other environmental factors.
5. **Access Granted/Denied:** Based on the comprehensive policy evaluation, access is either granted (with the absolute minimum necessary privileges) or denied. This decision is dynamic and can change if the device's posture changes during an active session.

Step-by-Step Approach: Implementing Zero Trust for Devices

Implementing Zero Trust for devices is a comprehensive and continuous journey that requires careful planning, iterative execution, and cross-functional collaboration. Here’s a conceptual guide to get started. Remember, this isn't a one-time project but an ongoing evolution of your security posture.

Step 1: Inventory and Classify All Devices

You cannot secure what you don't know exists. The first critical step is to gain complete visibility into your device landscape.

- **Action:** Conduct a thorough discovery process. Use network scanning tools, asset management systems, cloud inventory services, and even manual audits to identify all endpoints, servers, containers, virtual machines, and IoT/OT devices connected to your networks or accessing your resources.
- **Action:** Classify each device by its type, owner, purpose, criticality, and the sensitivity of the data or systems it accesses. Prioritize devices handling sensitive data or critical operations.
- **Why it matters:** An unknown or unclassified device is an unmanaged risk. Comprehensive inventory and classification enable you to prioritize security efforts and apply appropriate policies.

Step 2: Establish Robust Device Identity and Registration

Every device must have a unique, verifiable identity that your Zero Trust system can recognize and trust.

- **Action for Endpoints:** Implement a Mobile Device Management (MDM) or Endpoint Management Solution (EMS) to register, enroll, and manage corporate-owned devices. For Bring Your Own Device (BYOD) scenarios, explore Mobile Application Management (MAM) or secure virtual desktop infrastructure (VDI) solutions.
- **Action for Workloads:** Configure managed identities for cloud workloads within your cloud provider's console (e.g., Azure Managed Identities, AWS IAM Roles for EC2). For on-premises servers and microservices, implement a robust certificate management system (e.g., using a Public Key Infrastructure or PKI).
- **Action for IoT/OT:** Implement secure device onboarding processes. This often involves leveraging hardware-based identities (like TPMs or secure elements) and automated certificate issuance, ensuring each device has a unique cryptographic identity.

- **Why it matters:** Device identity is the foundation for "Verify Explicitly." Without it, your security systems lack the context to make informed access decisions.

Step 3: Implement Continuous Device Posture and Health Checks

Beyond identity, you need to continuously assess the current security state of your devices.

- **Action for Endpoints:** Configure your MDM/EMS to enforce security baselines (e.g., minimum OS patch level, active antivirus, disk encryption) and integrate these posture checks with a Conditional Access policy engine (e.g., Microsoft Entra Conditional Access).
- **Action for Workloads:** Implement automated vulnerability scanning, configuration management tools (e.g., Ansible, Puppet), and Cloud Workload Protection Platforms (CWPP) for continuous monitoring and runtime protection of containers and virtual machines.
- **Action for IoT/OT:** Deploy Network Access Control (NAC) solutions and specialized IoT security platforms that can profile devices, monitor their behavior, and detect policy violations or anomalies based on their unique characteristics.
- **Why it matters:** An authenticated device that is compromised due to poor posture is still a major risk. Continuous posture checks ensure devices meet security standards before and during access.

Step 4: Enforce Least Privilege Access for Devices

Grant devices only the minimum access required to perform their specific function, for the shortest possible duration.

- **Action:** Define granular network segmentation policies. Use next-generation firewalls, network access control lists (ACLs), and cloud network security groups (NSGs) to limit device-to-device and workload-to-workload communication based on explicit allow-lists.
- **Action:** Implement application-specific access policies. For example, configure a web server to only communicate with its designated database and specific API gateways, not other internal systems or the internet directly.
- **Action:** Utilize attribute-based access control (ABAC) or policy-based access control (PBAC) where access decisions are dynamic and consider multiple attributes, including device identity, its current posture, the user's context, and the sensitivity of the resource.

- **Why it matters:** Limiting access drastically reduces the potential "blast radius" if a device or workload is compromised, preventing lateral movement of attackers.

Step 5: Monitor, Analyze, and Respond Continuously

Zero Trust is an ongoing process of vigilance, monitoring, and adaptation. Your security posture must evolve with the threat landscape and your organizational needs.

- **Action:** Deploy Endpoint Detection and Response (EDR) solutions on endpoints and Cloud Workload Protection Platforms (CWPP) for workloads to provide deep visibility into activities and detect advanced threats.
- **Action:** Implement Security Information and Event Management (SIEM) or Security Orchestration, Automation, and Response (SOAR) systems. These aggregate logs and security alerts from all device types, enabling centralized analysis and automated responses to detected threats.
- **Action:** Regularly review access policies and device posture requirements. Adjust them as your environment, applications, and threat intelligence evolve. Conduct periodic penetration testing and red team exercises to validate your device security controls.
- **Why it matters:** Threats are constantly evolving. Continuous monitoring helps detect new attack techniques, identify vulnerabilities, and ensures your Zero Trust policies remain effective and adaptive.

Mini-Challenge: Securing a New Smart Sensor

Imagine your organization is deploying new smart temperature sensors in a remote warehouse. These sensors collect data and send it to a central cloud application for analysis. They have limited processing power, cannot run a full operating system, and cannot host traditional security agents like antivirus or EDR.

Challenge: Outline the key Zero Trust steps you would take to secure these new smart sensors, focusing on identity, access, and monitoring, given their unique constraints.

Hint: Think about how you would establish identity without an agent, how you would control access at the network level, and what kind of "monitoring" makes sense for a low-power device.

What to observe/learn: This exercise helps you apply the principles of Zero Trust to a constrained, real-world scenario, emphasizing that Zero Trust isn't a one-size-fits-all product but a strategic approach that adapts to device capabilities.

Common Pitfalls & Troubleshooting

Implementing Zero Trust for devices can be complex, often encountering challenges with legacy systems, visibility gaps, and policy enforcement. Here are some common pitfalls and how to address them:

- **Ignoring Legacy Devices and Technical Debt:** Many organizations have older systems (e.g., legacy Windows servers, specialized industrial control systems, older IoT devices) that cannot run modern security agents or support contemporary authentication protocols. Neglecting these creates significant blind spots and potential backdoors.
    - **Troubleshooting:** Isolate these devices with strict network segmentation (e.g., dedicated VLANs, firewalls). Use proxy-based authentication or secure gateways where possible to mediate their access. Implement robust network-level anomaly detection and continuously monitor their traffic for unusual behavior. Plan for modernization or replacement.
- **Lack of Comprehensive Device Inventory and Asset Management:** If you don't have an accurate, up-to-date inventory of all devices on your network, you cannot secure them effectively. Shadow IT (unauthorized devices) is a major risk.
    - **Troubleshooting:** Implement robust, automated asset discovery tools that continuously scan your networks (both wired and wireless) and cloud environments. Enforce strict device onboarding processes for all new devices and integrate them with your identity and management systems. Conduct regular audits and reconciliation.
- **Over-reliance on Network-Level Controls Alone:** While network segmentation and firewalls are crucial, especially for IoT/OT, for endpoints and modern workloads, they must be complemented by identity-based access, continuous posture checks, and application-level security.
    - **Troubleshooting:** Adopt a layered approach. Don't just segment; verify explicitly at every access attempt. Ensure that identity context (user, device, workload identity) drives access decisions, not just network location. Implement application-aware security controls.

- **Inconsistent Policy Enforcement Across Environments:** Security policies might be well-defined but not consistently applied across all device types, operating systems, or environments (on-premises, hybrid cloud, multi-cloud). This leads to security gaps.
    - **Troubleshooting:** Use a centralized policy engine (e.g., a Conditional Access system, a cloud security posture management platform) that integrates with your identity provider and various device management solutions. This ensures uniformity and consistent enforcement of Zero Trust policies across your diverse device ecosystem.

Summary

Securing every device—endpoints, workloads, and IoT—is a critical pillar of Zero Trust Security. This chapter has highlighted the importance of treating devices as first-class identities requiring explicit verification. Here are the key takeaways:

- **Devices as Identities:** Every device must have a unique, verifiable identity and be treated as a principal that requires authentication and authorization, just like a user.
- **Verify Explicitly & Continuously:** This means not only knowing what a device is but also continuously assessing its health, posture, and behavior against predefined security policies.
- **Least Privilege Access:** Grant devices only the minimum access required for their specific function and for the shortest possible duration, limiting potential lateral movement in case of a compromise.
- **Micro-segmentation:** Crucial for containing threats by isolating devices and workloads into small, manageable segments, reducing the "blast radius" of a breach.
- **Specialized IoT/OT Approaches:** These devices have unique constraints and often require specialized Zero Trust strategies, relying more heavily on network controls, device profiling, behavioral analytics, and secure gateways.
- **Continuous Monitoring & Response:** Zero Trust for devices is an ongoing process of vigilance, leveraging Endpoint Detection and Response (EDR), Cloud Workload Protection Platforms (CWPP), and Security Information and Event Management (SIEM)/Security Orchestration, Automation, and Response (SOAR) to detect and respond to threats dynamically.

In the next chapter, we'll shift our focus from securing the access to devices and identities to the data itself, exploring how Zero Trust principles help us protect our most valuable assets wherever they reside.

References

- Zero Trust adoption framework overview | Microsoft Learn
- What is Zero Trust? | Microsoft Learn
- GitHub - ukncsc/zero-trust-architecture: Principles to help you design and deploy a zero trust architecture
- NIST SP 800-207: Zero Trust Architecture (General reference for Zero Trust principles, checked 2026-05-28)

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 05

Micro-segmentation Mastery: Network Security Beyond the Perimeter

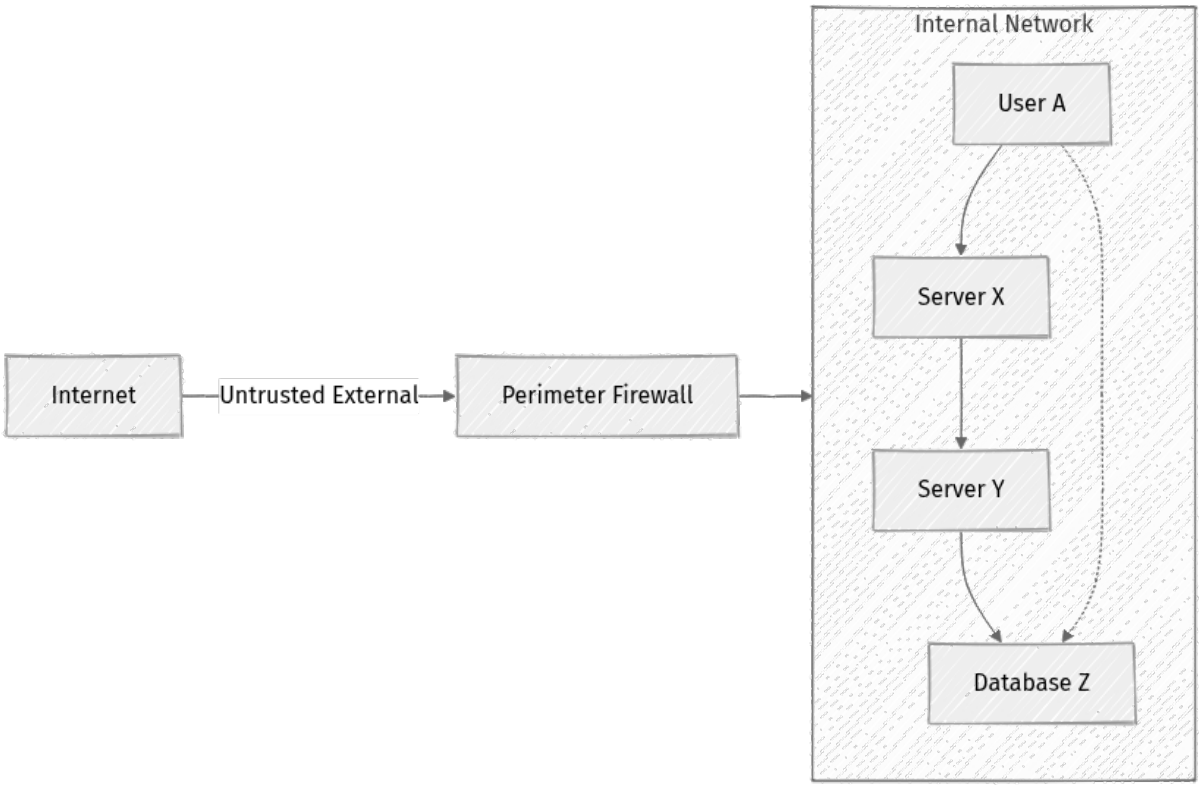
Welcome back, future Zero Trust architect! In previous chapters, we laid the groundwork for Zero Trust, understanding its core principles like "never trust, always verify" and "assume breach." Now, we're going to dive deep into a powerful technique that brings these principles to life at the network level: **Micro-segmentation**.

This chapter will equip you with a solid understanding of what micro-segmentation is, why it's critical in modern security, and how to start implementing it. We'll move beyond the outdated idea of a hard outer shell and a soft, trusting interior, and instead build a network where every component is treated as its own protected island.

By the end of this chapter, you'll be able to articulate the benefits of micro-segmentation, understand its core components, and even design basic micro-segmentation policies for a common application architecture. Ready to shrink your attack surface? Let's begin!

The Problem with Traditional Perimeters

For decades, network security focused on building a strong "castle-and-moat" defense. A robust perimeter firewall stood between the untrusted internet and the trusted internal network. Once inside, users and systems often had relatively free rein, implying an inherent trust in anything originating from within the "safe" zone.



This model works until it doesn't. What happens when an attacker breaches the perimeter? ⚠️ `What can go wrong:` Once an attacker bypasses the perimeter, they can move freely across the "trusted" internal network. This is known as **lateral movement**, and it's how small incidents escalate into major data breaches. The blast radius of a single compromise becomes the entire internal network.

What is Micro-segmentation?

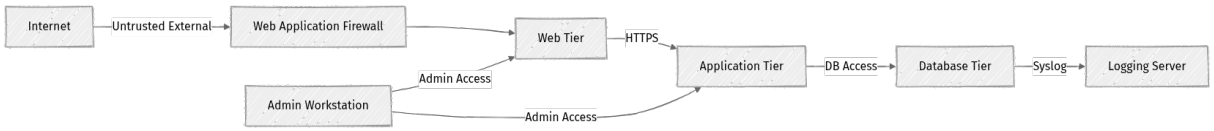
Micro-segmentation is a network security technique that divides data centers and cloud environments into distinct, isolated security segments down to the individual workload level. Instead of one large internal network, you create many small, highly controlled zones. Each zone has its own strict security policies defining exactly what can communicate with it, and under what conditions.

Think of it like this: instead of a single, massive office building with one main entrance, imagine a building where every single office, meeting room, and even individual desk cubicle has its own locked door. To move from one room to another, you need explicit permission, even if you're already inside the building.

📌 `Key Idea:` Micro-segmentation applies the Zero Trust principle of "least privileged access" directly to network communication.

How Micro-segmentation Changes the Game

With micro-segmentation, every workload (a server, a virtual machine, a container, a serverless function) becomes its own security perimeter. Communication between any two workloads, even if they're on the same physical network segment, requires explicit authorization.



In this diagram, notice how communication is restricted:

- The `Internet` can only talk to the `WAF`.
- The `WAF` can only talk to the `Web Tier`.
- The `Web Tier` can only talk to the `App Tier` (on specific ports/protocols like HTTPS).
- The `App Tier` can only talk to the `DB Tier` (for database access).
- The `DB Tier` can only send logs to the `Log Server`.
- `Admin Workstations` have specific, limited access for management.

If an attacker compromises the `Web Tier`, they cannot immediately jump to the `DB Tier` because there's no direct, open communication path. Their lateral movement is severely restricted, limiting the "blast radius" of the breach.

Core Components for Micro-segmentation

Implementing micro-segmentation relies on several key elements:

1. **Policy Enforcement Points (PEPs):** These are the components that actually apply your security rules.
    - **Host-based Firewalls:** Like `iptables` on Linux or Windows Firewall. These protect individual servers.
    - **Network Security Groups (NSGs) / Security Groups (SGs):** In cloud environments (Azure, AWS, GCP), these virtual firewalls control traffic to/from virtual machines or network interfaces.
    - **Virtual Firewalls:** Software-defined firewalls deployed within your network fabric, often managed centrally.
    - **Service Mesh:** For containerized applications, a service mesh (like Istio or Linkerd) can enforce policies between services at the application layer.

2. **Identity and Context:** Modern micro-segmentation moves beyond simple IP addresses. Policies can be based on:
    - **Workload Identity:** Tags, labels, service accounts, or cryptographic identities associated with a specific application or service.
    - **User Identity:** Who is trying to access the resource?
    - **Device Posture:** Is the device healthy, patched, and compliant?
    - **Application Context:** What application is trying to communicate, and for what purpose?
3. **Visibility and Analytics:** You can't secure what you can't see. Tools that provide deep insight into network traffic flows are crucial for defining and validating micro-segmentation policies.

Step-by-Step Implementation: Securing a 3-Tier Application in the Cloud

Let's walk through a conceptual example of micro-segmenting a common 3-tier web application (Web, Application, Database) using cloud-native security groups, a very common approach. We'll use a simplified model, but the principles apply broadly.

`⚡ Real-world insight:` Cloud Security Groups (like AWS Security Groups or Azure Network Security Groups) are often the first and most accessible way to implement micro-segmentation in cloud environments. These are virtual firewalls that control traffic at the network interface level for resources such as virtual machines.

Scenario: A Simple E-commerce Application

Our application has:

- **Web Tier:** Public-facing web servers (e.g., Nginx, Apache)
- **Application Tier:** Backend logic servers (e.g., Node.js, Java Spring Boot)
- **Database Tier:** Database servers (e.g., PostgreSQL, MySQL)

Step 1: Inventory and Mapping

Before writing any rules, understand your current architecture. This initial mapping is critical for defining effective policies.

- **Identify all workloads:** List every server, container, or service that needs protection.

- **Map communication flows:** Document what talks to what, on what ports, and using what protocols.
    - Internet needs to reach Web Tier (HTTPS 443).
    - Web Tier needs to reach App Tier (e.g., HTTP 8080).
    - App Tier needs to reach DB Tier (e.g., PostgreSQL 5432).
    - Administrators need SSH/RDP access to all tiers (e.g., SSH 22, RDP 3389) from specific management subnets.

Step 2: Define Security Zones (Groups)

In cloud environments, we often define security groups to act as logical boundaries. Each group will represent a "tier" of our application. We'll associate our compute instances with these groups.

- `SecurityGroup-WebTier`
- `SecurityGroup-AppTier`
- `SecurityGroup-DBTier`
- `SecurityGroup-AdminAccess` (for management hosts, though often admin access is granted to other groups from an admin IP range)

Step 3: Create Least Privilege Policies

Now, we'll define inbound rules for each security group. Remember, outbound rules are often more permissive by default, but it's best practice to restrict those too if possible. For simplicity, we'll focus on inbound rules here, along with necessary outbound rules for inter-tier communication.

Policy for `SecurityGroup-WebTier`: This group should only accept HTTPS traffic from the internet and SSH/RDP from our admin network.

```
{
  "name": "SecurityGroup-WebTier",
  "inbound_rules": [
    {
      "protocol": "TCP",
      "port": 443,
      "source": "0.0.0.0/0", // Allow from anywhere on the internet
      "description": "Allow HTTPS from internet"
    },
    {
      "protocol": "TCP",
      "port": 22, // Or 3389 for RDP
      "source": "192.168.1.0/24", // Example: Your admin network CIDR
      "description": "Allow SSH from Admin Network"
    }
  ],
  "outbound_rules": [
```

```
    {
      "protocol": "TCP",
      "port": 8080,
      "destination": "SecurityGroup-AppTier", // Allow to App Tier
      "description": "Allow HTTP to Application Tier"
    }
  ]
}
```

- **Explanation:**
  - The first rule allows web browsers (any IP address, `0.0.0.0/0`) to connect to our web servers on port 443 (HTTPS).
  - The second rule allows administrators from a specific `192.168.1.0/24` network to SSH into the web servers. This is crucial for management without exposing SSH to the entire internet.
  - The outbound rule explicitly permits the web tier to initiate connections to the application tier on port 8080.

Policy for `SecurityGroup-AppTier`: This group should only accept traffic from the `WebTier` and SSH/RDP from our admin network.

```
{
  "name": "SecurityGroup-AppTier",
  "inbound_rules": [
    {
      "protocol": "TCP",
      "port": 8080,
      "source": "SecurityGroup-WebTier", // Allow only from Web Tier Security
Group
      "description": "Allow HTTP from Web Tier"
    },
    {
      "protocol": "TCP",
      "port": 22, // Or 3389 for RDP
      "source": "192.168.1.0/24", // Example: Your admin network CIDR
      "description": "Allow SSH from Admin Network"
    }
  ],
  "outbound_rules": [
    {
      "protocol": "TCP",
      "port": 5432,
      "destination": "SecurityGroup-DBTier", // Allow to DB Tier
      "description": "Allow PostgreSQL to Database Tier"
    }
```

```
  ]
}
```

- **Explanation:**
  - The first rule is crucial: it only allows connections on port 8080 if they originate from instances associated with `SecurityGroup-WebTier`. This prevents any other internal system from directly hitting your application servers.
  - The second rule maintains admin access, again from a specific network.
  - The outbound rule allows the application tier to connect to the database tier on port 5432 (PostgreSQL).

Policy for `SecurityGroup-DBTier`: This group should only accept traffic from the `AppTier` and SSH/RDP from our admin network.

```
{
  "name": "SecurityGroup-DBTier",
  "inbound_rules": [
    {
      "protocol": "TCP",
      "port": 5432,
      "source": "SecurityGroup-AppTier", // Allow only from App Tier Security
Group
      "description": "Allow PostgreSQL from Application Tier"
    },
    {
      "protocol": "TCP",
      "port": 22, // Or 3389 for RDP
      "source": "192.168.1.0/24", // Example: Your admin network CIDR
      "description": "Allow SSH from Admin Network"
    }
  ],
  "outbound_rules": [
    // For a database, outbound rules are often minimal or restricted to
monitoring/backup
    // No specific outbound rule needed for this simple scenario, assuming no
external connections.
  ]
}
```

- **Explanation:**
  - The database is the most sensitive component. This policy ensures only the application tier can connect to it on the database port. No other system, not even the web tier, can directly access the database.
  - Admin access is retained, as always.

🧠 `Important:` In a real-world scenario, you would also apply these security groups to the actual compute instances (VMs, containers) for each tier. The cloud provider's network fabric then enforces these rules.

Mini-Challenge: Expanding Your Micro-segmentation

You've done a great job segmenting the core application. Now, let's add a common component.

Challenge: Your team decides to add a dedicated **Logging Server** to centralize all application and system logs. This server needs to receive logs from the `Web Tier` and `App Tier` on UDP port `514` (syslog). Administrators also need SSH access to the logging server from the admin network.

1. **Define a new security group** for the Logging Server.
2. **Write the inbound rules** for this new security group to meet the requirements.
3. **Update the outbound rules** for the `Web Tier` and `App Tier` security groups to allow them to send logs to the new Logging Server.

Hint: Think about which security groups need to send traffic, and which needs to receive it. Remember to always define the least privilege necessary.

What to observe/learn: How to integrate new components into an existing micro-segmented architecture and maintain the principle of least privilege.

💡 **CLICK FOR SOLUTION (AFTER YOU'VE TRIED IT!)**

1. New Security Group for Logging Server (`SecurityGroup-LogServer`):

```
{
  "name": "SecurityGroup-LogServer",
  "inbound_rules": [
    {
      "protocol": "UDP",
      "port": 514,
      "source": "SecurityGroup-WebTier", // Allow from Web Tier
      "description": "Allow Syslog from Web Tier"
    },
    {
      "protocol": "UDP",
      "port": 514,
      "source": "SecurityGroup-AppTier", // Allow from App Tier
      "description": "Allow Syslog from Application Tier"
    },
    {
      "protocol": "TCP",
      "port": 22,
      "source": "192.168.1.0/24", // Allow SSH from Admin Network
      "description": "Allow SSH from Admin Network"
    }
  ],
  "outbound_rules": [
    // Typically, a logging server might send logs to an analytics
platform,
    // but for this challenge, we'll keep it simple and assume no specific
outbound.
  ]
}
```

2. Update Outbound Rules for `Web Tier` and `App Tier`:

Update for `SecurityGroup-WebTier` (add this to its `outbound_rules` array):```json { "protocol": "UDP", "port": 514, "destination": "SecurityGroup-LogServer", "description": "Allow Syslog to Logging Server" }

```
**Update for `SecurityGroup-AppTier` (add this to its `outbound_rules`
array):**```json
    {
      "protocol": "UDP",
      "port": 514,
      "destination": "SecurityGroup-LogServer",
      "description": "Allow Syslog to Logging Server"
    }
```

Common Pitfalls & Troubleshooting

Micro-segmentation is powerful, but it's easy to stumble if not implemented carefully. Here are some common challenges and how to address them:

1. **Overly Permissive Policies:** The most common mistake. Accidentally allowing `0.0.0.0/0` (any source) on a critical port or protocol defeats the purpose of segmentation.
    - **Troubleshooting:** Regularly audit your policies. Use automated tools to scan for overly broad rules. Double-check every "allow" rule during reviews.
2. **Policy Sprawl and Complexity:** As your environment grows, managing hundreds or thousands of granular rules across various systems can become overwhelming and lead to misconfigurations.
    - **Troubleshooting:** Use tagging, automation (Infrastructure as Code), and centralized policy management tools (like a security orchestration platform or cloud-native policy engines). Group workloads logically and apply policies to groups rather than individual instances.
3. **Ignoring Non-IP Traffic:** While security groups are IP-based, modern micro-segmentation often involves application-layer policies, especially with service meshes in containerized environments like Kubernetes. Relying solely on IP-based rules might miss crucial intra-service communication.
    - **Troubleshooting:** Understand the full stack of your applications. For containerized applications, explore service mesh solutions that provide application-layer policy enforcement.
4. **Lack of Visibility:** It's hard to define policies if you don't know what's communicating. Blindly blocking traffic can lead to outages.
    - **Troubleshooting:** Implement robust network flow logging (e.g., VPC Flow Logs in AWS, NSG Flow Logs in Azure, or network monitoring tools on-premise). Analyze these logs to understand actual traffic patterns before implementing strict rules. Many tools offer a "monitor mode" to simulate policy enforcement without actually blocking traffic.

5. **Operational Overhead:** Manual policy updates are error-prone and slow, especially in dynamic environments.
    - **Troubleshooting:** Automate policy deployment using tools like Terraform, CloudFormation, or Ansible. Integrate policy changes into your CI/CD pipelines to treat security policies as code, enabling faster, more reliable updates and version control.

Summary

Micro-segmentation is a cornerstone of Zero Trust Security, fundamentally transforming how we protect our networks.

Here's what we covered:

- **Beyond the Perimeter:** We moved past the outdated "castle-and-moat" model to understand why granular network control is essential in modern threat landscapes.
- **Definition:** Micro-segmentation divides networks into small, isolated security zones, often down to individual workloads, each with its own strict access policies.
- **Why it Matters:** It drastically reduces the blast radius of a breach, prevents lateral movement of attackers, and enforces the principle of least privilege at the network layer.
- **Key Components:** Policy enforcement points (security groups, host firewalls, service mesh), workload and user identity, contextual information, and robust visibility are crucial for effective implementation.
- **Practical Application:** We walked through a conceptual example of micro-segmenting a 3-tier application in a cloud environment using security groups, demonstrating how to define least-privilege policies.

Micro-segmentation is not a one-time project; it's an iterative journey. Start small, gain visibility into your network flows, define strict policies based on actual needs, and automate where possible to manage complexity.

Next, we'll explore another vital pillar of Zero Trust: **Identity and Access Management (IAM) in a Zero Trust World**, where we'll focus on explicitly verifying every user and workload identity before granting access.

References

- Zero Trust adoption framework overview | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview
- What is Zero Trust? | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
- Principles to help you design and deploy a zero trust architecture | NCSC GitHub: https://github.com/ukncsc/zero-trust-architecture
- zero-trust-overview.md - security-docs - GitHub: https://github.com/MicrosoftDocs/security/blob/main/security-docs/zero-trust/zero-trust-overview.md

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 06

Data-Centric Security: Protecting Information at Rest and in Transit

Introduction

In the intricate landscape of modern cybersecurity, data stands as the ultimate asset and, consequently, the ultimate target. While securing user identities and devices (topics we thoroughly explored in previous chapters) establishes robust entry points, these are merely the gates to your digital kingdom. The true objective of most sophisticated cyberattacks is to gain access to, compromise, or exfiltrate sensitive information. This reality brings **Data-Centric Security** to the forefront of any effective defense strategy, shifting our focus to protecting the data itself, wherever it may reside.

This chapter will guide you through the critical principles of data-centric security within a Zero Trust framework. We'll uncover why direct data protection, independent of its location or access method, is not just a best practice but a fundamental requirement in today's dynamic threat environment. You'll delve into essential techniques such as data classification, robust encryption for data at rest and in transit, granular access controls, and proactive Data Loss Prevention (DLP) strategies.

By the end of this journey, you'll possess a clear understanding of how to apply Zero Trust principles directly to your organization's most valuable asset: its data. This ensures your information remains secure, whether it's stored peacefully in a database or actively traversing your networks.

The Zero Trust Imperative for Data

The foundational Zero Trust principle, "Never Trust, Always Verify," extends with paramount importance to your organization's data. This means that even if a user's identity is authenticated and their device is deemed compliant, access to specific data must still be explicitly verified and granted based on the strictest interpretation of the least privilege principle. Data-centric security fundamentally reorients the security paradigm from defending perimeters to intrinsically securing the data itself.

What is Data-Centric Security?

Data-centric security is a strategic approach that prioritizes the continuous protection of data throughout its entire lifecycle—from its initial creation to its eventual deletion. This protection remains constant regardless of where the data is located (on-premises servers, cloud storage, user endpoints) or its current state (at rest, in transit, or actively in use). Rather than relying solely on network boundaries as primary defenses, data-centric security embeds security mechanisms directly into the data itself.

📌 **Key Idea:** Data-centric security ensures the data is inherently protected, not just the network, application, or device that contains or processes it.

Why Data-Centric Security Matters in Zero Trust

1. **Assume Breach as a Foundation:** Zero Trust builds its entire philosophy on the premise that breaches are not a matter of if, but when. Should an attacker manage to bypass other security layers (like identity or device controls), data-centric security acts as the critical last line of defense. By encrypting data and applying strict access controls directly to it, stolen data becomes unusable without the correct decryption keys or authorized access rights.
2. **Enforcing Least Privilege:** Access to data is granted only when it is absolutely necessary for a specific task, for the shortest possible duration, and with the minimum required permissions. This approach actively prevents over-privileged users or compromised accounts from accessing sensitive information that is not essential for their current operational needs.
3. **Verify Explicitly at Every Interaction:** Every single attempt to access data, even from within what was once considered a "trusted" internal network, must be rigorously authenticated and authorized. This decision is based on a comprehensive context, considering who is requesting access, what data they are trying to reach, when they are doing it, from where, and how.

Core Concepts of Data-Centric Protection

Implementing a robust data-centric security strategy requires a solid grasp of several interconnected concepts and the technologies that support them.

Data Classification: Knowing Your Crown Jewels

You cannot effectively protect what you do not understand or value. Data classification is the foundational process of categorizing information based on its sensitivity, business value, and any applicable regulatory or compliance requirements. This initial step is often the most critical because it dictates the entire subsequent security posture.

How it Works:

- **Define Categories:** Organizations must establish clear, unambiguous data categories. Common examples include "Public," "Internal Use Only," "Confidential," "Highly Confidential," and categories for regulated data like "Personal Identifiable Information (PII)" or "Protected Health Information (PHI)."
- **Tag Data:** Once categories are defined, these classifications must be applied to actual data. This involves tagging individual files, specific columns in databases, objects in cloud storage buckets, and even within application data structures. Tagging can be performed manually by data owners or, more practically at scale, through automated discovery and classification tools.
- **Inform Policies:** The classification directly informs and dictates the security controls that must be applied. For instance, "Highly Confidential" data will inherently require much stricter access controls, mandatory encryption, and more aggressive Data Loss Prevention (DLP) policies compared to data classified as "Public."

🧠 **Important:** Incorrectly classifying data carries significant risks. Over-classification can lead to unnecessary operational overhead and user frustration, while under-classification can expose highly sensitive information to unauthorized access, potentially resulting in severe breaches and regulatory penalties.

Encryption: The Unbreakable Lock

Encryption is the bedrock of data protection in a Zero Trust environment. It transforms data into an unreadable, scrambled format, rendering it unintelligible and useless to anyone who does not possess the correct decryption key.

Encryption at Rest

This crucial layer of protection secures data when it is stored on any persistent medium, such as hard drives, databases, cloud storage buckets, or backup tapes. Even if an adversary manages to bypass other controls and gain access to the physical storage, the data remains encrypted and therefore protected.

- **Disk Encryption:** Encrypts entire storage volumes or hard drives. Examples include Microsoft BitLocker for Windows or LUKS (Linux Unified Key Setup) for Linux systems.
- **Database Encryption:** Protects specific tables, columns, or the entire database content. Technologies like Transparent Data Encryption (TDE) offered by various database vendors encrypt data files at the storage level, making it transparent to applications.
- **Cloud Storage Encryption:** Leading cloud providers (e.g., AWS S3, Azure Storage, Google Cloud Storage) offer robust server-side encryption options, often enabled by default, for objects stored in their services.

Encryption in Transit

This protects data as it travels across networks, safeguarding it against eavesdropping, interception, or tampering during communication.

- **TLS (Transport Layer Security):** The modern and secure successor to SSL, TLS encrypts communication channels between web browsers and servers (HTTPS), between applications and APIs, and across many other network services. **TLS 1.3** is the latest stable version (as of 2026-05-28), providing significant security enhancements, improved performance, and reduced handshake latency compared to its predecessors. Organizations should prioritize its adoption and deprecate older, less secure versions (1.0, 1.1, and even 1.2 where feasible).
- **VPNs (Virtual Private Networks):** VPNs establish encrypted tunnels for network traffic, crucial for securing remote access for employees or creating secure site-to-site connections between different organizational networks.
- **End-to-End Encryption:** This advanced form of encryption ensures that data is encrypted at the sender's device and remains encrypted until it reaches the recipient's device, with only the legitimate endpoints having the ability to access the unencrypted information.

⚡ **Quick Note:** Strong cryptographic algorithms like **AES-256 (Advanced Encryption Standard with a 256-bit key)** are the industry standard and highly recommended for securing both data at rest and data in transit due to their proven resilience against modern attacks.

Granular Access Policies: Beyond "Yes" or "No"

In a Zero Trust model, data access is never a simple binary choice of "allow" or "deny." Instead, it revolves around highly granular, context-aware policies that define how, when, and under what precise conditions access is permitted.

- **Attribute-Based Access Control (ABAC):** Moving beyond traditional Role-Based Access Control (RBAC), ABAC leverages a rich set of attributes to make real-time access decisions. These attributes can include characteristics of the user (e.g., department, security clearance, job function), the device they are using (e.g., compliant, managed, patched status), the environment (e.g., network location, time of day), and the data itself (e.g., classification, owner, sensitivity).
- **Conditional Access:** These policies enforce specific conditions that must be met before access is granted. For example, accessing highly sensitive data might require multi-factor authentication (MFA), a device that passes all compliance checks, and connection from a trusted network location. If any condition is not met, access is denied or restricted.

Data Loss Prevention (DLP): Stopping the Leaks

Data Loss Prevention (DLP) solutions are designed as a critical safeguard to prevent sensitive data from leaving the organization's control, whether through accidental exposure or malicious intent.

How DLP Works:

1. **Identification:** DLP systems continuously scan data (at rest, in transit, and in use) to identify sensitive patterns. This can involve recognizing credit card numbers, PII, intellectual property, or specific keywords, often leveraging predefined rules and integrating with your data classification tags.
2. **Monitoring:** DLP actively observes data movement across a wide array of communication channels, including email, cloud storage services, user endpoints (laptops, desktops), web uploads, and even physical media like USB drives.
3. **Enforcement:** When sensitive data movement violates a defined policy, DLP can take various enforcement actions: blocking the transfer, quarantining the data, automatically encrypting the data before it leaves, or generating immediate alerts for security teams.

⚡ **Real-world insight:** Many modern DLP solutions are deeply integrated with cloud platforms (e.g., Microsoft Purview DLP, Google Cloud DLP) to provide seamless protection for data residing within SaaS applications, cloud storage, and other cloud services, reflecting the shift to hybrid and multi-cloud environments.

Step-by-Step Implementation: Building Data-Centric Security

Implementing data-centric security is an iterative journey that must be tightly integrated with your broader Zero Trust strategy. It's not a one-time project but an ongoing process of discovery, protection, and refinement.

Step 1: Discover and Classify Your Data Landscape

You can't protect what you don't know you have. This initial phase is about gaining a comprehensive understanding of your data.

1. **Inventory Data Sources:** Begin by meticulously identifying every location where your organization's data is stored. This includes traditional databases, network file shares, cloud storage buckets, SaaS application data, user endpoints, and even backup systems.
2. **Define a Clear Classification Scheme:** Develop a practical, easy-to-understand data classification policy. This policy should clearly define what constitutes "Public," "Internal," "Confidential," and "Highly Confidential" data, along with any specific categories for regulated data like PII or PHI.
    - Challenge: Consider a common scenario: how would you classify an employee's personal contact information (e.g., home address, phone number) versus a publicly available product marketing description? Think about the impact if each were accidentally exposed.
3. **Implement Data Discovery Tools:** Deploy automated tools capable of scanning your identified data repositories. These tools use pattern matching, machine learning, and keyword analysis to identify sensitive information and apply initial classification tags.
    - Example: A discovery tool might use regular expressions to find potential credit card numbers, look for keywords like "confidential agreement," or analyze existing metadata to suggest classifications.

4. **Review and Refine Classifications:** Automated tools provide a great starting point, but manual review and input from data owners (e.g., department heads, legal counsel) are crucial. This ensures classifications are accurate, relevant, and align with business needs and compliance obligations.

Step 2: Enforce Encryption Everywhere

Make encryption a default, always-on protection mechanism for all sensitive data, regardless of whether it's stored or in transit.

1. **Encrypt Data at Rest:**
    - **Databases:** Ensure all databases that store sensitive or classified information are configured to utilize their native encryption features, such as column-level encryption for specific sensitive fields or Transparent Data Encryption (TDE) for entire database files.
    - **Cloud Storage:** Verify that all cloud storage buckets (e.g., AWS S3, Azure Blob Storage) have server-side encryption enabled by default. This often involves selecting the appropriate encryption key management option (e.g., platform-managed keys, customer-managed keys).
    - **Endpoints and Servers:** Implement full-disk encryption for all corporate-managed endpoints (laptops, desktops) and servers. This protects data even if the device is lost or stolen.

2. **Encrypt Data in Transit:**
    - **Mandate TLS 1.3:** Configure all public-facing web servers, internal APIs, and application-to-application communication to exclusively use HTTPS with strong TLS 1.3 ciphers. Actively deprecate and disable older, vulnerable TLS versions (1.0, 1.1) and work towards phasing out TLS 1.2 where possible, as TLS 1.3 offers superior security and performance as of 2026-05-28.
    - **Secure Internal Network Traffic:** Do not assume that traffic within your internal data centers or cloud Virtual Private Clouds (VPCs) is inherently secure. Implement encryption for inter-service communication using methods like mTLS (mutual TLS) for service mesh architectures or secure VPN tunnels between network segments.
    - **Secure Remote Access:** Ensure that all remote access to corporate resources, whether via traditional VPNs or modern Secure Access Service Edge (SASE) solutions, enforces robust encryption for all transmitted data.

Step 3: Define and Implement Granular Access Policies

Shift away from broad, permissive access to fine-grained, context-aware controls that truly embody the principle of least privilege.

1. **Map Data to Identities and Roles:** Understand precisely which identities (human users, service accounts, applications) legitimately require access to which classified data. This mapping should be based on job function and business need.
2. **Develop Context-Aware Conditional Access Policies:**
    - Scenario Example: Consider a highly sensitive document, perhaps titled "Highly Confidential - Q4 Financials." A Zero Trust policy might dictate that this document can only be accessed by specific members of the finance team, from a corporate-managed and compliant device, only when connected to the corporate network (or a verified VPN), and only after successfully completing multi-factor authentication.
    - Implementation: Configure your Identity Provider (IdP) and access control systems (e.g., Cloud Identity and Access Management, network access control solutions) to enforce these intricate, multi-attribute conditions.

```
// Conceptual Policy Rule for "Highly Confidential" financial data
IF (Data.Classification == "Highly Confidential")
AND (Data.Category == "Financials")
```

```
    AND (User.Group == "Finance_Analysts" OR User.Group == "Finance_Managers")
    AND (Device.ComplianceStatus == "Compliant")
    AND (Network.Location == "Corporate_Internal" OR Network.Type ==
"Corporate_VPN")
    AND (User.MFA_Satisfied == TRUE)
    THEN ALLOW ACCESS (Read-Only)
    ELSE DENY ACCESS
```

1. **Regularly Review and Audit Policies:** Data access requirements are dynamic. Periodically audit your access policies to ensure they remain aligned with current business requirements, compliance mandates, and the enduring principle of least privilege. Remove any stale or overly permissive rules.

Step 4: Deploy and Tune Data Loss Prevention (DLP)

DLP solutions serve as an essential safety net, proactively detecting and preventing both accidental and malicious attempts to exfiltrate sensitive data from your control.

1. **Select a Suitable DLP Solution:** Choose a DLP solution that integrates seamlessly with your existing IT infrastructure, including cloud services, email platforms, and endpoint security systems. Modern solutions often offer unified management across these domains.
2. **Configure Granular DLP Rules:**
    - Begin by configuring rules to detect common sensitive data types, such as PII, credit card numbers, and intellectual property patterns.
    - Crucially, integrate your DLP rules with your data classification tags. For instance, a rule might automatically block emails containing documents tagged as "Highly Confidential" if they are destined for external domains, or automatically encrypt them.
    - Example: A DLP rule might block any attempt to copy a file tagged "Confidential - Customer Data" to a personal cloud storage service or a USB drive.
3. **Monitor and Alert on Violations:** Configure your DLP system to generate immediate alerts for any policy violations. These alerts should be integrated into your Security Information and Event Management (SIEM) system for centralized monitoring and rapid incident response.

4. **Iterative Tuning for Accuracy:** DLP solutions, especially during initial deployment, can sometimes generate false positives. Start by deploying rules in a "monitor-only" mode to understand their impact. Continuously review incidents, adjust rules based on observed data flows and user feedback, and conduct user education campaigns to minimize disruption while maximizing protection effectiveness.

Step 5: Continuous Monitoring and Auditing

Zero Trust demands constant vigilance across all security domains, and data access is no exception. This continuous oversight is vital for detecting anomalies and responding swiftly.

1. **Log All Data Access:** Ensure comprehensive logging of every data access attempt, modification, and transfer across all your systems, including databases, file shares, cloud storage, and applications. These logs are your forensic trail.
2. **Monitor for Anomalies:** Leverage Security Information and Event Management (SIEM) systems and User and Entity Behavior Analytics (UEBA) tools to monitor for unusual data access patterns. This could include a user attempting to access an unusually large volume of data, accessing data outside their typical working hours, or from an unfamiliar location.
3. **Regular Audits:** Conduct periodic, independent audits of data access logs and the effectiveness of your data access policies. Verify that policies are being enforced as intended, that no unauthorized access has occurred, and that audit trails are complete and tamper-proof.
4. **Robust Incident Response:** Develop and regularly test a clear incident response plan specifically tailored for data breaches or policy violations. This plan should detail steps for immediate containment, eradication of the threat, recovery of affected data, and thorough post-incident analysis to prevent recurrence.

Mini-Challenge: Design a Data Access Policy

Let's put these concepts into practice. Imagine your organization operates a critical database containing highly sensitive employee Personal Identifiable Information (PII), which has been classified as "Confidential

- PII".

Challenge: Design a conceptual Zero Trust access policy for this "Confidential

- PII" database. Your policy should explicitly consider the following attributes:
- **Who** needs access (specific roles or groups)?
- **What** level of access (e.g., read-only, read/write, delete)?
- **When** can they access it (e.g., specific time windows, days of the week)?
- **Where** can they access it from (e.g., specific network locations, device types)?
- **How** must they authenticate (e.g., standard login, strong MFA, biometric)?

Write down a few distinct conceptual rules for at least two different roles within your organization that might interact with this data.

Hint: Think about the different needs and responsibilities of an HR specialist versus an IT support engineer. Should their access conditions be identical?

💡 **CLICK FOR A POSSIBLE APPROACH (DON'T PEEK UNTIL YOU'VE TRIED!)**

Here's a possible approach, demonstrating granular control:

Data: `Employee_PII_Database` (Classification: "Confidential

- PII")

Role 1: HR Specialist - **Access Level:** Read/Write (to manage and update employee records). - **Conditions:** - **Who:** User must be a member of the `HR_Specialist` Active Directory group. - **Device:** Must be a corporate-managed, fully compliant endpoint (e.g., regularly patched, running required antivirus, device health attested). - **Time:** Access permitted only during standard business hours (e.g., Monday-Friday, 8 AM - 6 PM local time). - **Location:** Access allowed only from an approved corporate network segment (e.g., office IP range) or via an authenticated, compliant corporate VPN connection. - **Authentication:** Requires strong Multi-Factor Authentication (MFA), such as a FIDO2 security key or a biometric prompt.

Role 2: IT Support Engineer (for database maintenance/ troubleshooting) - **Access Level:** Read-only (strictly for diagnostic queries), with no direct PII modification privileges. - **Conditions:** - **Who:** User must be a member of the `IT_DB_Support` Active Directory group. **Device:** Must be a corporate-managed, hardened administrative workstation, fully compliant. - **Time:** Access requires a just-in-time (JIT) approval workflow, granting access for a limited duration (e.g., 1 hour) only when an approved change ticket is linked. - **Location:** Access permitted only from a secure, segregated network segment dedicated to IT operations. - **Authentication:** Requires strong MFA, and all access attempts are recorded with session logging and auditing.

What to observe/learn: Real-world data access policies become incredibly granular, leveraging multiple attributes simultaneously. The "least privilege" principle is paramount, ensuring that even legitimate access is precisely constrained by factors like time, location, device posture, and specific approvals. This complexity is necessary to truly secure sensitive data in a Zero Trust model.

Common Pitfalls & Troubleshooting

Implementing a data-centric security strategy within a Zero Trust framework can be complex. Here are some common challenges and how to address them effectively:

- **Pitfall 1: Over- or Under-Classification of Data**
    - **Problem:** Classifying every piece of data as "Highly Confidential" creates excessive overhead, slows down legitimate business processes, and leads to user frustration. Conversely, under-classifying truly sensitive data as "Public" exposes it to devastating breaches and compliance failures.
    - **Troubleshooting:**
        - **Invest in Robust Tools:** Utilize advanced data discovery and classification tools that leverage machine learning and pattern recognition for initial automated tagging.
        - **Engage Data Owners:** Actively involve data owners (the departments or individuals responsible for the data) in defining and refining classification policies. Their business context is invaluable.
        - **Iterative Refinement:** Treat classification as an ongoing process. Regularly review and adjust your classification scheme based on evolving business needs, new data types, and changes in regulatory requirements.

- **Pitfall 2: Inadequate Encryption Key Management**
    - **Problem:** The strength and security of your encrypted data are directly tied to the security of its encryption keys. Losing keys means permanent data loss, while compromised keys render your encryption useless. Weak key management is a critical vulnerability.
    - **Troubleshooting:**
        - **Utilize HSMs/KMS:** Employ Hardware Security Modules (HSMs) or cloud-based Key Management Services (KMS) for secure generation, storage, and management of encryption keys. These services are designed to protect keys from unauthorized access and tampering.
        - **Implement Strict Controls:** Enforce rigorous access controls and rotation policies for all encryption keys. Keys should be rotated regularly, and access to them should be granted on a least-privilege, just-in-time basis.
- **Pitfall 3: "Set It and Forget It" Mentality with Policies**
    - **Problem:** Data classification, access policies, and DLP rules are not static configurations. New data types emerge, business processes change, and regulatory landscapes evolve. A stagnant security posture will quickly become ineffective.
    - **Troubleshooting:**
        - **Establish Review Cycles:** Institute regular, scheduled review cycles for all data security policies and configurations. Assign clear ownership for these reviews.
        - **Automate Where Possible:** Automate as much of the data discovery, classification, and policy enforcement process as feasible to reduce manual effort and ensure consistency.
        - **Continuous Monitoring:** Rely on continuous monitoring and auditing to detect when policies become misaligned or ineffective, prompting necessary updates.

- **Pitfall 4: DLP False Positives or Negatives**
    - **Problem:** Overly aggressive DLP rules can block legitimate business operations, causing user frustration and hindering productivity. Conversely, rules that are too lax will fail to catch actual data exfiltration attempts.
    - **Troubleshooting:**
        - **Start in Monitor-Only Mode:** Begin by deploying DLP rules in a "monitor-only" or "audit" mode. This allows you to understand their impact and identify false positives without immediately blocking legitimate traffic.
        - **Iterative Tuning:** Continuously review DLP incidents, adjust rules based on observed data flows and user feedback, and refine your policies.
        - **User Education:** Educate users on what constitutes sensitive data, why DLP is in place, and how to handle sensitive information appropriately to reduce accidental violations.

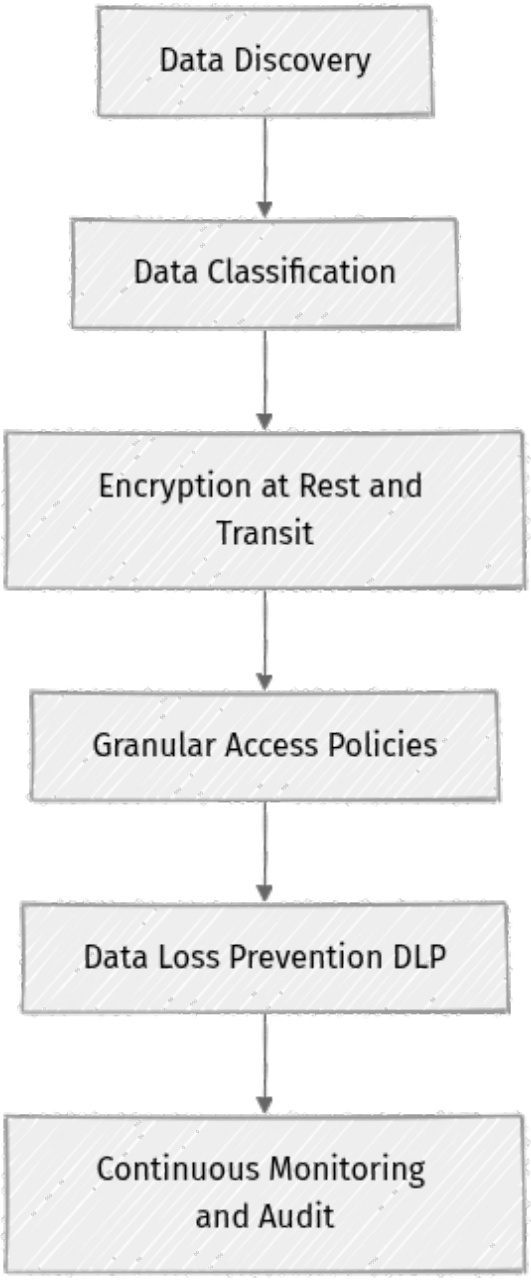
Summary

Data-centric security is not merely a component but a fundamental pillar of any successful Zero Trust architecture. By shifting focus from perimeter defenses to the intrinsic protection of your data, you establish a resilient defense that remains effective regardless of where the data resides or how it is accessed.

Here are the key takeaways from this chapter:

- **Data as the Ultimate Target:** In a Zero Trust world, data is recognized as the ultimate asset to protect, demanding direct and continuous security measures.
- **Classification is the Foundation:** Accurate data classification is the critical first step, enabling you to apply appropriate and proportionate security controls.
- **Encryption is Non-Negotiable:** Implement robust encryption for all sensitive data, both when it is stored (at rest) and when it is being transmitted across networks (in transit), utilizing modern standards like TLS 1.3 and strong algorithms like AES-256.

- **Granular Access is Paramount:** Move beyond simple "allow/deny" decisions. Implement context-aware access policies (such as Attribute-Based Access Control) to enforce the principle of least privilege for every data interaction.
- **DLP as a Safety Net:** Deploy Data Loss Prevention (DLP) solutions to proactively identify and prevent sensitive information from leaving your organizational control.
- **Continuous Vigilance:** Maintain constant logging, monitoring, and auditing of all data access activities to quickly detect and respond to anomalies and potential breaches.



Understanding and meticulously implementing data-centric security is absolutely crucial for any organization embarking on a Zero Trust journey. In the next chapter, we'll shift our focus to **Application Security: Securing Workloads and APIs**, ensuring that the software interacting with your data is just as secure and adheres to Zero Trust principles.

References

- Zero Trust adoption framework overview | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview
- What is Zero Trust? | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
- Principles to help you design and deploy a zero trust architecture | NCSC GitHub: https://github.com/ukncsc/zero-trust-architecture
- TLS 1.3 Specification | IETF RFC 8446: https://www.rfc-editor.org/rfc/rfc8446
- Advanced Encryption Standard (AES) | NIST FIPS 197: https://csrc.nist.gov/pubs/fips/197/final

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 07

Application and Workload Security: From Development to Deployment

Introduction

Welcome back! In our journey through Zero Trust, we've explored how to verify identities and secure network access. Now, it's time to turn our attention to the very heart of most modern organizations: applications and their underlying workloads. These are the engines that drive business, making them prime targets for attackers.

Securing applications and the services they rely on—often called "workloads"—is a critical, yet complex, undertaking. Traditional security models often assumed that once an application was inside the network perimeter, it was inherently trustworthy. Zero Trust shatters this assumption, demanding that we apply "never trust, always verify" to every line of code, every API call, and every interaction between application components.

In this chapter, we'll dive deep into how Zero Trust principles transform application and workload security. We'll cover everything from baking security into the development process to protecting workloads in dynamic cloud environments. A solid grasp of core Zero Trust concepts, especially identity and network segmentation, from previous chapters will be very helpful here.

Core Concepts: Securing the Digital Engine Room

Applications are no longer monolithic blocks; they are often distributed systems comprising many microservices, APIs, and data stores. Securing them requires a holistic approach that spans the entire lifecycle, from the first line of code to ongoing operations.

Zero Trust for Applications: The "Never Trust, Always Verify" Codebase

At its core, applying Zero Trust to applications means scrutinizing every request, every data flow, and every access attempt within and to your applications. This isn't just about protecting the perimeter; it's about protecting the internal logic and data of the application itself.

Why does this matter so much? Modern applications are complex. They might interact with dozens of other services, databases, and external APIs. Each interaction is a potential point of compromise. By verifying explicitly at every step, even within the application's internal workings, we drastically reduce the attack surface and limit the damage an attacker can do if they gain a foothold.

Secure by Design: Shifting Left with Zero Trust

The most effective way to secure applications is to build security in from the very beginning, rather than trying to bolt it on at the end. This concept, often called "shifting left," integrates security practices into every phase of the Software Development Lifecycle (SDLC).

What does "shifting left" look like with Zero Trust?

- **Threat Modeling:** Before writing code, identify potential threats and vulnerabilities. How might an attacker exploit this feature? What data needs extra protection?
- **Secure Coding Practices:** Developers write code with security in mind, avoiding common pitfalls like SQL injection or cross-site scripting (XSS).
- **Automated Security Testing:** Integrate static application security testing (SAST) and dynamic application security testing (DAST) into your CI/CD pipelines to catch vulnerabilities early.
- **Supply Chain Security:** Verify the integrity of third-party libraries and components used in your application.
- **Configuration Management:** Ensure secure defaults and configurations for all application components.

By adopting a DevSecOps mindset, where security is a shared responsibility across development, operations, and security teams, organizations can proactively address risks.

Workload Identities and Access Management

Just as human users need identities to access resources, applications and services (workloads) also need identities. A workload identity is a digital identity used by a software workload (like a microservice, container, or serverless function) to authenticate to other services and resources.

Why are workload identities critical for Zero Trust? Workload identities enable explicit verification for automated processes. Instead of relying on shared secrets or broad network access, each workload is granted a unique identity with precisely defined permissions.

- **Managed Identities:** Cloud providers offer "managed identities" (e.g., Azure Managed Identities, AWS IAM Roles for EC2/Lambda) which eliminate the need for developers to manage credentials directly. The cloud platform handles the lifecycle of these identities, making them highly secure.
- **Service Accounts:** In container orchestration platforms like Kubernetes, service accounts provide an identity for pods to interact with the Kubernetes API and other services.

📌 **Key Idea:** Every automated process, every application component, should have its own unique, verifiable identity.

Micro-segmentation for Application Workloads

We discussed network micro-segmentation in a previous chapter. For applications, this means extending that concept to isolate individual application components or microservices. Instead of a flat network where any service can talk to any other, micro-segmentation ensures that:

- A frontend web service can only talk to its designated backend API.
- A database service can only accept connections from its authorized application tier.
- An analytics service can only read from specific data stores.

How does this improve security? If an attacker compromises one microservice, micro-segmentation prevents them from easily moving laterally to other, unrelated services. It significantly limits the "blast radius" of a breach.

Common tools for micro-segmentation in application contexts include:

- **Network Policies:** In Kubernetes, `NetworkPolicy` objects define how groups of pods are allowed to communicate with each other and other network endpoints.

- **Service Meshes:** Technologies like Istio or Linkerd can enforce fine-grained access policies between services at the application layer (Layer 7), adding capabilities like mutual TLS (mTLS) for encrypted and authenticated communication.
- **Cloud Native Firewalls/Security Groups:** Cloud providers offer granular firewall rules (e.g., AWS Security Groups, Azure Network Security Groups) to control traffic between virtual machines or container instances.

API Security: The New Perimeter

In a world of microservices and cloud-native applications, APIs have become the primary interface for communication. They are, in essence, the new perimeter. Securing APIs is paramount for Zero Trust.

Zero Trust principles applied to APIs include:

- **Explicit Verification:** Every API request must be authenticated and authorized. This often involves tokens (like JWTs) that prove the caller's identity and permissions.
- **Least Privilege:** An API endpoint should only grant the minimum necessary permissions to perform its function.
- **Assume Breach:** APIs must be designed with robust input validation, rate limiting, and monitoring to detect and mitigate attacks even if authentication is bypassed.
- **End-to-End Encryption:** All API communication should use TLS/SSL.

Step-by-Step Implementation: Securing a Microservice Interaction

Let's walk through a simplified scenario: securing a backend microservice that needs to read data from a database. We'll use conceptual examples that map to common cloud patterns.

Scenario: A "Product Catalog" Microservice

Imagine you have a `ProductCatalog` microservice that fetches product details from a `ProductsDB`. Another `OrderProcessing` microservice needs to add new orders to an `OrdersDB`. Both microservices run in a containerized environment (like Kubernetes) and need to interact with cloud-managed databases.

Step 1: Define Workload Identities and Permissions

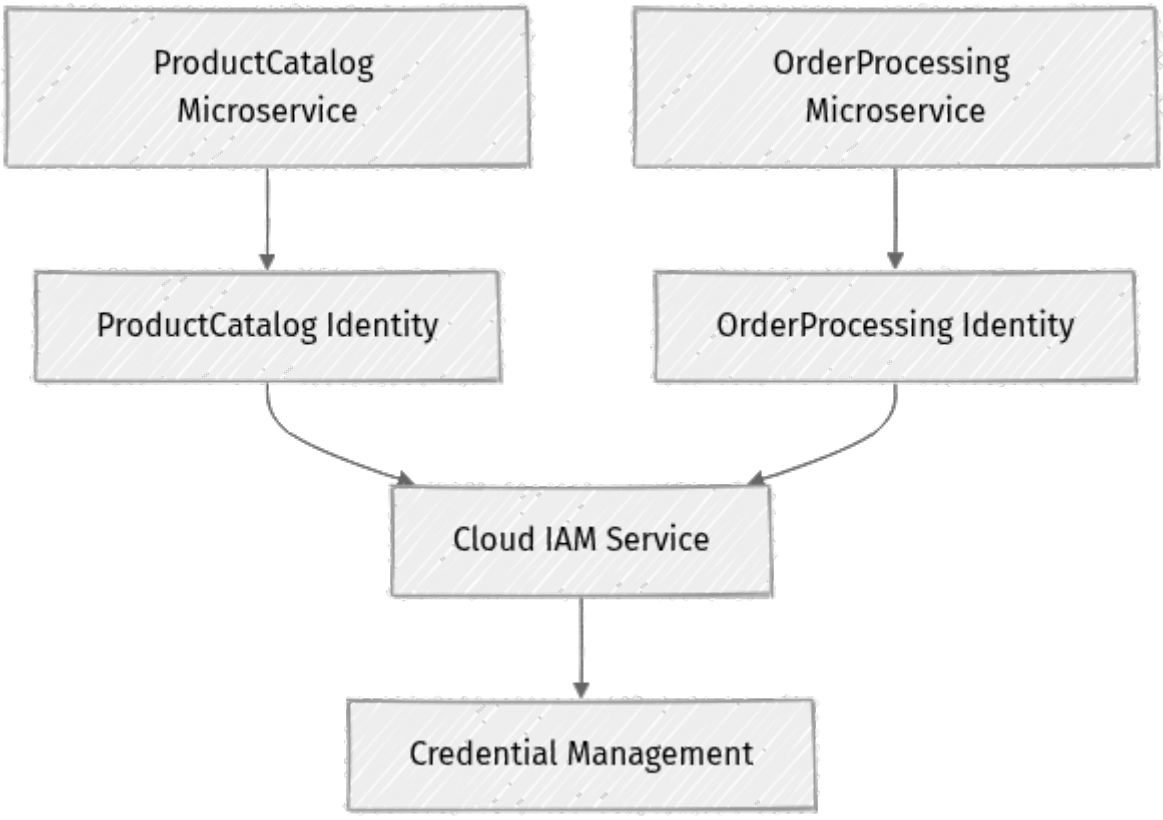
First, each microservice needs its own identity. We'll use a cloud-agnostic concept of a "managed identity" for simplicity, representing what cloud providers offer.

```
# Conceptual YAML for a Workload Identity Definition
# This would typically be managed via your cloud provider's IAM system (e.g.,
Azure AD, AWS IAM)
# or Kubernetes Service Accounts.

# Identity for the ProductCatalog Microservice
identity: product-catalog-service-id
description: "Identity for the Product Catalog microservice to access product
data."

# Identity for the OrderProcessing Microservice
identity: order-processing-service-id
description: "Identity for the Order Processing microservice to manage orders.
"
```

Explanation: We've conceptually defined two unique identities. In a real cloud environment, you would create these using the provider's Identity and Access Management (IAM) service. For Kubernetes, you'd define `ServiceAccount` resources.



Step 2: Implement Least Privilege Access

Now, we'll assign specific permissions to each workload identity.

ProductCatalog Microservice needs:

- `read` access to `ProductsDB`.
- No access to `OrdersDB`.

OrderProcessing Microservice needs:

- `read`, `write`, `delete` access to `OrdersDB`.
- No access to `ProductsDB`.

Here's a conceptual policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:Scan",
        "dynamodb:Query"
      ],
      "Resource": "arn:aws:dynamodb:region:account-id:table/ProductsDB",
      "Principal": {
        "Federated": "arn:aws:iam::account-id:oidc-provider/my-oidc-provider",
        "StringEquals": {
          "oidc.eks.region.amazonaws.com/id/EXAMPLED:sub": "system:serviceacco
unt:default:product-catalog-service-id"
        }
      }
    }
  ]
}
```

Explanation: This is an example of an AWS IAM policy (as of 2026-05-28, using OIDC for Kubernetes service accounts) that grants read-only access to `ProductsDB`.

- `"Action"`: Specifies the allowed database operations (read actions for DynamoDB).
- `"Resource"`: Defines exactly which database table the actions apply to.
- `"Principal"`: This is crucial for workload identity. It specifies who is allowed to assume this role. Here, it's a Kubernetes service account (`product-catalog-service-id`) federated via OIDC.

For the `OrderProcessing` microservice, you'd create a similar policy but grant `PutItem`, `UpdateItem`, `DeleteItem` actions on the `OrdersDB` resource.

Step 3: Apply Micro-segmentation

Even with strong identity and access management, we want to restrict network communication. Let's use a Kubernetes `NetworkPolicy` to ensure the `ProductCatalog` service can only talk to the `ProductsDB` endpoint (assuming `ProductsDB` has a service endpoint within the cluster or a specific egress IP).

First, ensure your `ProductCatalog` pod has a label, e.g., `app: product-catalog`.

```
# network-policy-product-catalog.yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-product-catalog-to-productsdb
  namespace: default
spec:
  podSelector:
    matchLabels:
      app: product-catalog # This policy applies to pods with this label
  policyTypes:
    - Egress # We are controlling outbound traffic
  egress:
    - to:
        - ipBlock:
            cidr: 10.0.0.1/32 # Replace with the actual IP of your ProductsDB
endpoint
      ports:
        - protocol: TCP
          port: 5432 # Or the specific port for your database (e.g., 3306 for
MySQL, 5432 for PostgreSQL)
```

Explanation: This `NetworkPolicy` specifies that pods labeled `app: product-catalog` are only allowed to make outbound connections (`egress`) to the specific IP address (`10.0.0.1/32`) and port (`5432`) of the `ProductsDB`. All other outbound traffic from these pods would be blocked by default (assuming a network policy controller is active in your Kubernetes cluster).

Step 4: Secure API Endpoints

If `ProductCatalog` exposed an API, we'd secure it with an API Gateway.

```
# Conceptual API Gateway Configuration
# This would be configured in an API Gateway service (e.g., AWS API Gateway,
Azure API Management, NGINX Plus)

apiGateway:
  routes:
    /products:
      methods: [GET]
      target: http://product-catalog-service:8080/products
      authentication:
        type: JWT # Require a JSON Web Token
```

```
        issuer: https://your-identity-provider.com/
        audience: your-api-audience
      authorization:
        policy: allow-read-products # Policy to check scopes/claims in the JWT
      rateLimit:
        requestsPerSecond: 100
```

Explanation: This conceptual configuration shows an API Gateway protecting the `/products` endpoint.

- It routes `GET` requests to the `ProductCatalog` microservice.
- Crucially, it requires a **JWT** for authentication, validating its `issuer` and `audience`.
- It then applies an `authorization policy` to check if the user/client has the necessary permissions (e.g., a `read:products` scope in the JWT).
- `rateLimit` helps prevent abuse and denial-of-service attacks.

Mini-Challenge: Design a Least-Privilege Policy

Let's put your Zero Trust thinking to the test.

Challenge: Imagine a new microservice, `InventoryUpdater`, whose sole purpose is to decrement stock counts in the `ProductsDB` when an order is placed. It should only be able to update stock quantities and nothing else.

Write a **conceptual IAM policy statement** (similar to the JSON example in Step 2) that grants the `InventoryUpdater` workload identity the absolute minimum permissions required. Assume the `ProductsDB` table has a `stock_quantity` attribute.

Hint:

- What specific database action is needed to decrement a value? (e.g., `UpdateItem` for DynamoDB, `UPDATE` for SQL).
- Can you constrain the action to only modify the `stock_quantity` attribute and nothing else? (Some databases/IAM systems allow this at a fine-grained level).

What to Observe/Learn: This challenge highlights the difficulty of achieving true least privilege in complex systems. You'll observe how critical it is to understand both the application's exact needs and the capabilities of your IAM system to enforce granular controls.

Common Pitfalls & Troubleshooting

Implementing Zero Trust for applications and workloads is a journey. Here are some common missteps:

1. **Over-privileged Workload Identities:** Granting workloads more permissions than they truly need (e.g., `*` permissions). This is the most common and dangerous pitfall, directly violating the least privilege principle.
    - **Troubleshooting:** Regularly audit IAM policies. Use tools to analyze actual access patterns and compare them against granted permissions to identify and revoke excessive access.
2. **Lack of Granular Network Policies:** Failing to implement micro-segmentation, allowing wide-open network communication between application components. This negates the "assume breach" principle.
    - **Troubleshooting:** Use network flow logs and monitoring tools to visualize communication paths. Implement network policies incrementally, starting with critical services, and test thoroughly.
3. **Ignoring API Security:** Treating internal APIs as inherently trusted. Attackers often pivot to internal APIs once they gain initial access.
    - **Troubleshooting:** Implement API Gateways with strong authentication, authorization, and rate limiting for all APIs, both external and internal. Conduct regular API penetration testing.
4. **Failure to Integrate Security into CI/CD (DevSecOps):** Leaving security testing and policy enforcement to the end of the development cycle. This makes vulnerabilities expensive and difficult to fix.
    - **Troubleshooting:** Embed SAST/DAST tools, dependency scanners, and policy-as-code checks directly into your CI/CD pipelines. Automate security gates.

Summary

In this chapter, we've explored the critical role of Zero Trust in securing applications and workloads. This isn't just about protecting the network perimeter; it's about embedding security into every layer of your application's architecture and lifecycle.

Here are the key takeaways:

- **Zero Trust for applications** means explicit verification for every internal and external interaction, assuming no inherent trust.
- **Shifting left** integrates security into the entire SDLC, from threat modeling to automated testing, promoting a DevSecOps culture.
- **Workload identities** provide unique, verifiable identities for automated processes and application components, enabling least privilege access.
- **Micro-segmentation** isolates individual application services, limiting lateral movement and reducing the blast radius of a breach.
- **API security** is paramount, as APIs are the new perimeter, requiring strong authentication, authorization, and protective measures.

By applying these principles, you move beyond reactive security to build applications that are inherently more resilient and trustworthy. Up next, we'll delve into data security, exploring how Zero Trust protects your most valuable asset, regardless of where it resides.

References

- Zero Trust adoption framework overview | Microsoft Learn
- What is Zero Trust? | Microsoft Learn
- GitHub - ukncsc/zero-trust-architecture: Principles to help you design and deploy a zero trust architecture
- Kubernetes Network Policies
- AWS IAM Policies and Permissions

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 08

Designing Your Zero Trust Architecture: A Phased Implementation Strategy

Introduction

Welcome back! In our previous chapters, we laid the theoretical groundwork for Zero Trust Security, exploring its core principles like "verify explicitly," "least privileged access," and "assume breach." Now, it's time to translate that theory into a practical, actionable plan. Designing a Zero Trust architecture can seem daunting, but it doesn't have to be.

This chapter will guide you through building a robust Zero Trust architecture using a phased, iterative implementation strategy. We'll explore how to break down the monumental task into manageable steps, focusing on key areas like identity, devices, networks, and data. Our goal isn't to achieve perfection overnight, but to build momentum and progressively enhance your security posture.

By the end of this chapter, you'll understand how to approach Zero Trust as a strategic journey, identify critical starting points, and begin sketching out a roadmap for your organization. You'll move beyond understanding what Zero Trust is, to confidently planning how to implement it effectively.

The Zero Trust Journey: A Phased Approach

Implementing Zero Trust isn't a one-time project; it's a continuous journey of improvement and adaptation. Think of it as evolving your security posture, one strategic phase at a time, rather than a single, massive overhaul. This phased approach helps manage complexity, minimizes disruption, and allows you to demonstrate value incrementally.

The core idea is to apply Zero Trust principles across all aspects of your digital estate. This includes identities, devices, applications, data, and infrastructure.

`📌 Key Idea:` Zero Trust is an iterative process. Start small, gain wins, and expand.

Phase 1: Foundation and Discovery

Before you can secure everything, you need to understand what "everything" even means in your environment. This initial phase is all about gaining visibility and defining your scope.

1. Inventory and Assessment

You can't protect what you don't know you have. This step involves a comprehensive inventory of your existing architecture.

- **Users and Identities:** Who are your users? What roles do they have? Are there service accounts?
- **Devices:** What devices access your resources? Laptops, mobile phones, IoT devices, servers? Are they corporate-owned or personal?
- **Applications and Services:** What applications do your users access? Where do they live (on-premises, cloud, SaaS)?
- **Data:** Where is your sensitive data stored? How is it classified? Who needs access to it?

`⚡ Real-world insight:` Many organizations discover forgotten "shadow IT" or outdated systems during this phase, highlighting critical blind spots. The NCSC (UK's National Cyber Security Centre) emphasizes "knowing your architecture" as a foundational principle.

2. Identify Critical Assets

Not all assets are created equal. Prioritize the crown jewels – the critical business assets and processes that, if compromised, would cause the most significant damage. These will be your initial focus areas for enhanced Zero Trust controls.

3. Establish a Policy Engine (Conceptual)

While you won't deploy a full policy engine on day one, you should start thinking about how access decisions will be made. A Zero Trust policy engine conceptually evaluates every access request against multiple attributes: user identity, device health, location, application sensitivity, and more.

Phase 2: Strengthening Identity as the Perimeter

In a Zero Trust world, identity becomes the new perimeter. This phase focuses on ensuring that every user and service accessing resources is explicitly verified and authorized.

1. Multi-Factor Authentication (MFA) Everywhere

This is arguably the most impactful "quick win" in your Zero Trust journey. MFA adds a crucial layer of security beyond just a password, making it significantly harder for attackers to compromise accounts.

🧠 `Important:` Deploy MFA for all users and all access scenarios, especially for administrative accounts. This should be a non-negotiable step.

2. Implement Conditional Access Policies

Conditional Access allows you to define policies that grant or deny access based on real-time conditions. This moves beyond simple user/password checks to a dynamic, context-aware decision.

- **Who:** The user or group trying to access.
- **What:** The application or resource they are trying to access.
- **Where:** Their network location (e.g., corporate network, unknown IP).
- **How:** The device they are using (e.g., corporate laptop, personal mobile).
- **Risk:** Real-time risk assessment from identity protection services.

3. Identity Governance and Administration

Ensure you have robust processes for managing identities throughout their lifecycle: provisioning, de-provisioning, role changes, and privileged access management (PAM) for highly sensitive accounts.

Phase 3: Securing Endpoints and Workloads

Once identities are strong, the next focus is on the devices and applications (workloads) that identities use to access resources.

1. Device Health and Compliance

Verify that every device attempting to access resources meets your security standards. This includes checking for:

- Up-to-date operating systems and patches.
- Antivirus/anti-malware solutions.
- Disk encryption.
- Compliance with corporate policies.

2. Endpoint Detection and Response (EDR)

EDR solutions provide deep visibility into device activity, helping to detect and respond to threats on endpoints in real time. This is crucial for the "assume breach" principle.

3. Workload Segmentation

Divide your applications and services into smaller, isolated segments. This limits the blast radius of a breach, preventing an attacker from easily moving laterally from one compromised application to others.

Phase 4: Enhancing Network and Data Security

While identity is the new perimeter, network and data security remain vital components of a comprehensive Zero Trust strategy.

1. Network Micro-segmentation

Extend the segmentation concept to your network infrastructure. Instead of broad network zones, create granular, policy-driven segments for individual applications, services, or even specific functions within an application. This drastically reduces lateral movement opportunities.

Diagram unavailable in this PDF export.

This diagram illustrates how a Policy Engine, after verifying identity and device compliance, grants access to a specific application segment, which then has limited, explicit access to its required data stores. Critically, it does not automatically grant access to other application segments.

2. End-to-End Encryption

Ensure data is encrypted not just at rest, but also in transit across all networks, both internal and external. This protects data from interception and tampering.

3. Data Classification and Protection

Classify your data based on sensitivity (e.g., public, internal, confidential, highly restricted). Implement data loss prevention (DLP) policies to prevent sensitive data from leaving your control.

Phase 5: Automation, Monitoring, and Continuous Improvement

Zero Trust is not a static state. This final phase focuses on making your security posture adaptive, responsive, and constantly improving.

1. SIEM and SOAR Integration

Integrate your security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platforms. This allows for centralized logging, threat detection, automated responses, and streamlined incident management.

2. Threat Intelligence Integration

Feed up-to-date threat intelligence into your policy engine and security tools to proactively block known malicious IPs, domains, and attack patterns.

3. Regular Audits and Policy Refinement

Continuously review and audit your Zero Trust policies, access logs, and system configurations. As your environment evolves, your policies must evolve too. Perform regular penetration testing and red team exercises to find weaknesses.

⚠️ `What can go wrong:` Neglecting this phase means your Zero Trust architecture becomes brittle and outdated, failing to protect against new threats.

Step-by-Step Implementation: Prioritizing Your First Steps

Now that we've outlined the phases, let's talk about where to actually begin. Overwhelm is a common pitfall. The key is to start with high-impact, manageable steps that build confidence and demonstrate tangible security improvements.

Step 1: Secure Administrative Identities with MFA

This is often the single most effective initial step. Administrative accounts have the keys to your kingdom. Protecting them with MFA immediately raises the bar for attackers.

Action Plan:

1. **Identify All Admin Accounts:** List every user account with elevated privileges across all systems (domain admins, cloud console admins, application admins, database admins, etc.). Don't forget service accounts that might have admin-like permissions.
2. **Enable MFA for Admin Accounts:** Implement MFA for these accounts first. Choose a strong MFA method (e.g., authenticator apps, FIDO2 security keys) over weaker ones (SMS).
3. **Monitor Usage:** Track MFA adoption and any attempts to bypass it.

This step doesn't require complex code, but rather a focused configuration effort within your identity provider (e.g., Azure AD, Okta, Google Workspace Identity).

Step 2: Map Critical Business Applications and Data

Once admin accounts are safer, turn your attention to your most valuable assets.

Action Plan:

1. **List Your Top 3-5 Critical Applications:** These are the apps that, if compromised, would halt business operations or lead to significant data loss.
2. **Map Data Flows for Each App:** For each critical application, draw out (literally, on a whiteboard or using a tool) how data flows into, out of, and within the application. Identify where sensitive data resides.
3. **Identify Users and Devices Accessing These Apps:** Who needs access? What devices do they use? This will inform your first conditional access policies.

This mapping exercise is a conceptual planning step. It helps you visualize your environment and identify logical points for policy enforcement.

Step 3: Draft Your First Conditional Access Policy (Conceptual)

Let's imagine you've identified your critical HR application. You want to ensure only authorized users, from compliant devices, can access it.

Conceptual Policy Draft:

```
Policy Name: High-Security HR App Access

Target Users:
  - Include: HR Department Users Group
  - Exclude: Break Glass Accounts (for emergencies, with extreme logging)

Target Applications:
  - Include: "HR Management System" application

Conditions:
  - User Risk: Medium or High (Block access)
  - Sign-in Risk: Medium or High (Require password change, then MFA)
  - Device State: Compliant (Require device to be marked as compliant by MDM/
MAM)
  - Location: Any location (but if outside corporate network, require MFA)

Access Controls:
  - Grant Access:
    - Require Multi-Factor Authentication
    - Require device to be marked as compliant
    - Require an approved client application (e.g., corporate browser,
specific mobile app)
```

This isn't executable code, but a structured way to think about and document your policy. You would then translate this into your chosen Identity and Access Management (IAM) platform's policy language (e.g., Microsoft Entra ID Conditional Access, Okta Adaptive MFA policies).

Mini-Challenge: Designing a Policy for Sensitive Data

Let's put your policy-thinking hat on!

Challenge: Imagine your organization has a "Highly Confidential Customer Data" share on a cloud storage service (e.g., SharePoint, Google Drive). Draft a conceptual Zero Trust Conditional Access policy to protect this data.

Consider these factors:

- **Who** should access it? (e.g., specific team, specific roles)
- **What** devices should they use? (e.g., corporate laptops only, no personal devices)
- **Where** can they access it from? (e.g., only from trusted networks, or from anywhere if device is compliant)
- **When** might access be suspicious? (e.g., unusual sign-in locations, impossible travel)
- **How** can you enforce stronger verification? (e.g., MFA, device compliance, approved apps)

Hint: Start with a default "deny" mindset. Then, explicitly define the conditions under which access is granted. Think about the most critical attributes for this specific data.

What to Observe/Learn: This exercise helps you practice translating abstract security principles into concrete access rules, reinforcing the "verify explicitly" and "least privileged access" tenets.

Common Pitfalls & Troubleshooting

Implementing Zero Trust is a journey, and like any journey, there can be bumps in the road. Being aware of common pitfalls can help you navigate them more smoothly.

Pitfall 1: Trying to Do Everything at Once

Problem: Attempting to implement all Zero Trust principles across your entire organization simultaneously. This leads to overwhelming complexity, resource exhaustion, and often, project failure.

Solution: Embrace the phased approach discussed in this chapter. Start with high-impact, manageable wins (like MFA for admins), demonstrate success, and then expand iteratively. Prioritize based on risk and business criticality.

Pitfall 2: Neglecting User Experience

Problem: Implementing stringent security controls without considering the impact on legitimate users. This can lead to frustration, productivity loss, and users finding workarounds that undermine security.

Solution: Involve users and business stakeholders early. Communicate the "why" behind changes. Design policies that are as seamless as possible for legitimate users while still providing strong security. Leverage modern, user-friendly MFA methods. Provide clear documentation and support.

Pitfall 3: Lack of Visibility and Monitoring

Problem: Implementing Zero Trust controls but lacking the tools to monitor their effectiveness, detect anomalies, or respond to incidents. Without proper logging and analytics, you're essentially flying blind.

Solution: Integrate robust logging and monitoring solutions (SIEM, EDR, cloud security posture management tools) from the outset. Ensure your policy engine logs all access decisions. Regularly review logs for suspicious activity, policy violations, and opportunities to refine your policies. Remember, "assume breach" means you must be ready to detect and respond.

Summary

In this chapter, we've explored the strategic framework for designing and implementing your Zero Trust architecture. We've learned that:

- Zero Trust is a **phased journey**, not a single destination, requiring continuous iteration and improvement.
- The implementation begins with a **discovery phase** to inventory assets and identify critical resources.
- **Identity** is the new perimeter, making MFA and conditional access policies foundational.
- Securing **endpoints and workloads** through compliance checks and segmentation is crucial.
- **Network micro-segmentation** and **end-to-end encryption** enhance protection for data in transit and at rest.

- **Automation, monitoring, and continuous refinement** are essential for an adaptive security posture.
- Starting with **high-impact, low-complexity steps** like securing admin MFA is key to building momentum.
- Avoiding common pitfalls like **over-scoping, neglecting user experience, and lacking visibility** will smooth your implementation journey.

You've taken a significant step from understanding Zero Trust concepts to planning its practical application. In the next chapter, we'll dive deeper into specific technologies and configurations that enable these Zero Trust principles, helping you build out the technical components of your architecture.

References

- Zero Trust adoption framework overview | Microsoft Learn
- What is Zero Trust? | Microsoft Learn
- GitHub - ukncsc/zero-trust-architecture: Principles to help you design and deploy a zero trust architecture
- zero-trust-overview.md - security-docs - GitHub (Microsoft Docs)

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 09

Monitoring, Automation, and Threat Intelligence in Zero Trust

Introduction to Dynamic Zero Trust Defense

Welcome to Chapter 9! So far, we've built a solid foundation for understanding Zero Trust principles, from verifying identities and securing devices to segmenting networks and protecting applications. But here's a crucial question: once you've implemented these controls, how do you ensure they remain effective against an ever-evolving threat landscape?

The answer lies in the dynamic interplay of **continuous monitoring**, **intelligent automation**, and **proactive threat intelligence**. Zero Trust isn't a "set it and forget it" solution; it's a living, breathing security strategy that constantly adapts. In this chapter, we'll dive into how these three pillars work together to provide the real-time visibility and response capabilities essential for a truly resilient Zero Trust architecture. You'll learn what to monitor, how automation can be your force multiplier, and why staying ahead of threats with intelligence is non-negotiable.

Ready to make your Zero Trust framework truly dynamic? Let's get started!

The Pillars of Dynamic Zero Trust

Implementing Zero Trust means assuming that a breach is inevitable and that no entity, inside or outside your network, should be trusted by default. This "assume breach" mindset requires constant vigilance and the ability to react instantly. This is where monitoring, automation, and threat intelligence become indispensable. They form a powerful feedback loop that allows your security posture to evolve with the threats it faces.

Continuous Verification through Monitoring

Monitoring is the eyes and ears of your Zero Trust environment. It provides the essential visibility needed to verify every access attempt and resource interaction, just as the "Verify Explicitly" principle demands. Without robust monitoring, you're essentially flying blind, unable to detect anomalies or policy violations in real-time.

📌 **Key Idea:** Monitoring gives you the data to make informed, real-time access decisions.

What should you monitor? Practically everything relevant to your security posture:

- **Identity Activity:** This includes successful and failed login attempts, changes in user roles, access to sensitive data, and unusual geographic login patterns. Are users accessing resources they normally don't? Are there too many failed login attempts for an account?
- **Device Health and Posture:** Beyond just "is it managed?", monitoring should track device compliance with security policies (e.g., up-to-date antivirus, OS patches, encryption status). Any deviation could indicate compromise.
- **Network Traffic and Flow:** While Zero Trust reduces implicit trust on the network, monitoring traffic within micro-segments is still vital to detect lateral movement or data exfiltration attempts. Look for unusual data volumes or communication patterns between segments.
- **Application Behavior:** Monitor how applications are accessed, what data they're processing, and any unusual API calls. This helps identify compromised applications or insider threats.
- **Data Access and Movement:** Track who accesses sensitive data, when, and from where. Look for large data transfers, attempts to access restricted data, or data being moved to unauthorized locations.

Why is continuous monitoring critical? Zero Trust policies are conditional. They depend on the current state of identities, devices, and the environment. Continuous monitoring provides this real-time state information. For instance, if a device suddenly fails a health check, continuous monitoring allows your access policies to instantly revoke or downgrade its access, rather than waiting for a manual intervention.

Automation: The Engine of Real-time Response

Monitoring provides the data, but human analysts can't keep up with the sheer volume of security events. This is where automation steps in as the indispensable engine of Zero Trust, enabling rapid, consistent, and scalable responses.

🧠 **Important:** Automation transforms monitoring insights into actionable, real-time security enforcement.

Automation in Zero Trust isn't just about scripting; it's about orchestrating security actions based on predefined policies and detected anomalies. Think of it as your security system's reflexes.

How automation supercharges Zero Trust:

- **Dynamic Policy Adjustment:** Based on real-time monitoring data, automation can dynamically adjust access policies. If a user's risk score increases due to suspicious activity, automation can trigger a step-up authentication challenge or temporarily restrict access to sensitive resources.
- **Automated Remediation:** When a threat is detected, automation can initiate immediate containment or remediation actions. This might include:
    - Isolating a compromised device from the network.
    - Revoking access tokens for a suspicious user.
    - Blocking malicious IP addresses at the firewall.
    - Forcing a password reset for a compromised account.
- **Orchestrated Incident Response:** Automation can streamline the initial phases of incident response, gathering forensic data, notifying relevant teams, and applying initial containment measures, saving precious time during a breach.

Consider this: A user logs in from an unusual location. Without automation, an alert might be generated, but it could take minutes or hours for a human to investigate and respond. With automation, a predefined playbook could instantly challenge the user with MFA, block the login, or temporarily suspend the account, significantly reducing exposure.

Threat Intelligence: The Brain Guiding Your Defenses

If monitoring is the eyes and automation is the reflexes, then **threat intelligence (TI)** is the brain of your Zero Trust security, providing context and foresight to your defenses. TI isn't just a list of bad IPs; it's analyzed information about current and emerging threats, adversary tactics, techniques, and procedures (TTPs).

⚡ **Real-world insight:** Threat intelligence helps your Zero Trust policies become predictive, not just reactive.

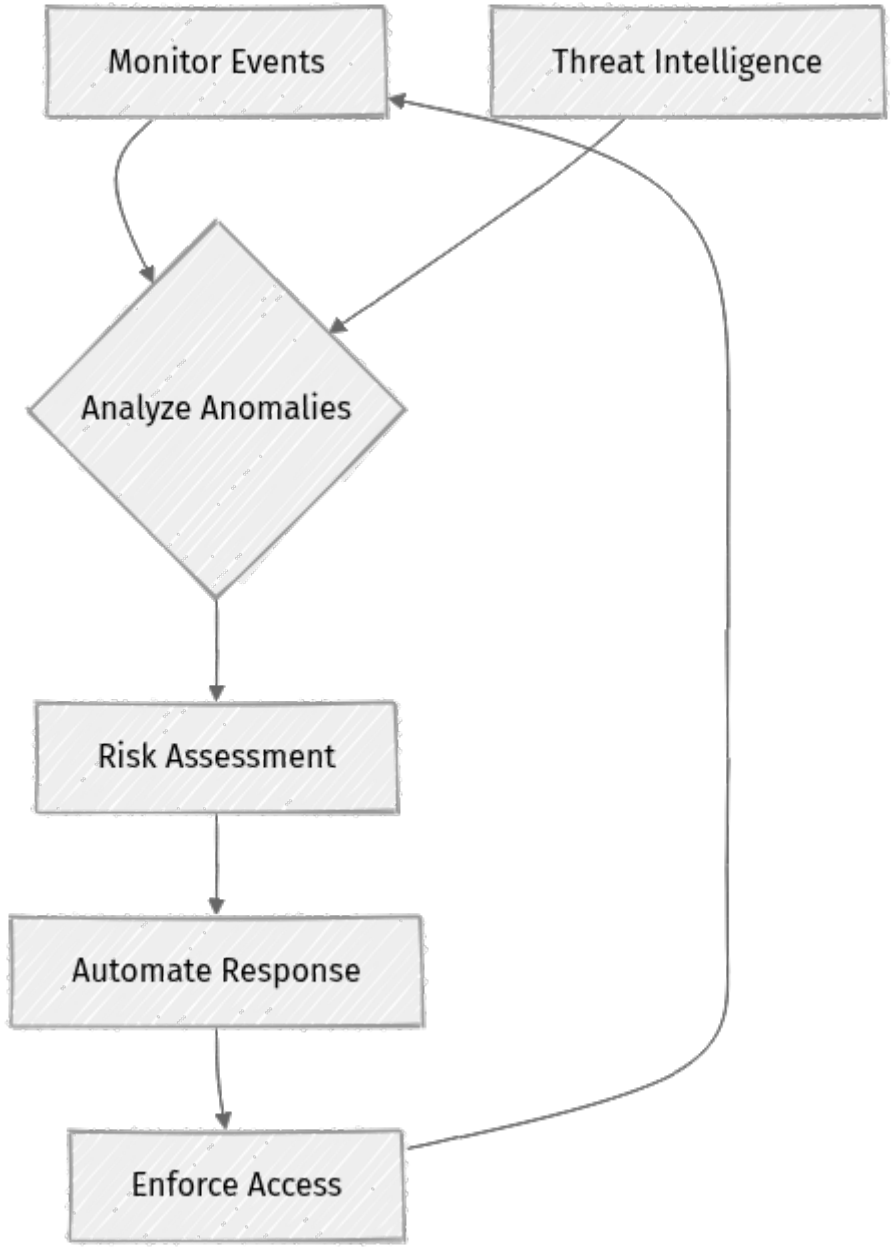
How Threat Intelligence enhances Zero Trust:

- **Proactive Blocking:** Integrating TI feeds (e.g., known malicious IP addresses, phishing domains, malware hashes) into your firewalls, web application firewalls (WAFs), and endpoint detection and response (EDR) solutions allows you to proactively block access attempts from known bad actors.
- **Contextual Risk Scoring:** TI can enrich the context around an access request. If a user tries to access a resource from an IP address identified in a recent ransomware campaign, your Zero Trust policy can assign a higher risk score and enforce stricter controls.
- **Detecting Emerging Threats:** By staying updated with the latest TTPs, your monitoring systems can be tuned to detect subtle indicators of compromise (IOCs) that might otherwise go unnoticed.
- **Informing Policy Decisions:** Threat intelligence helps security teams understand the most relevant threats to their organization, allowing them to prioritize and fine-tune Zero Trust policies to defend against those specific risks.

Combining internal monitoring data with external threat intelligence creates a powerful defense mechanism. You're not just looking for "something weird"; you're looking for "something weird that matches a known attack pattern."

The Continuous Zero Trust Feedback Loop

These three components don't work in isolation. They form a continuous feedback loop that is fundamental to the dynamic nature of Zero Trust.



- **Monitor Events (A):** Collect data from all sources (identities, devices, networks, applications, data).
- **Analyze (B):** Process this data, looking for anomalies, deviations from baselines, and policy violations. Threat intelligence (C) provides crucial context here, helping to identify known threats.
- **Dynamic Policy Engine (D):** Based on the analysis and risk assessment, the Zero Trust policy engine determines the appropriate access decision.
- **Automate Response (E):** If a threat or policy violation is detected, automated playbooks trigger immediate actions.
- **Enforce Access Policy (F):** The updated policy is enforced, modifying access rights as needed.

- **Loop back to Monitor (A):** The system continues to monitor, capturing the effects of the enforcement and watching for new events.

This loop ensures that your Zero Trust posture is always adapting, learning, and responding to the latest information and threats, embodying the principle of continuous verification.

Practical Steps for Integration

Integrating monitoring, automation, and threat intelligence into your Zero Trust strategy involves leveraging existing security tools and, in many cases, introducing new capabilities like Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms.

Step 1: Centralized Logging and SIEM Integration

The first practical step is to ensure all your relevant security events are collected in a central location. This means consolidating logs from:

- Identity Providers (e.g., Azure Active Directory, Okta)
- Endpoint Detection and Response (EDR) solutions
- Firewalls and network devices
- Cloud Access Security Brokers (CASB)
- Web Application Firewalls (WAFs)
- Application logs

Why it matters: A SIEM (Security Information and Event Management) system acts as the central hub for this data. It aggregates, correlates, and analyzes logs from various sources, helping to identify patterns and anomalies that individual logs might miss.

Conceptual Example: Configuring Log Forwarding

Imagine you have an identity provider and a firewall. You'd configure them to send their logs to your SIEM.

1. **Identity Provider (e.g., Azure AD):** Enable diagnostic settings to stream audit logs, sign-in logs, and non-interactive sign-in logs to a Log Analytics Workspace or Event Hub, which your SIEM can then ingest.
2. **Network Firewall:** Configure syslog forwarding to send traffic logs, intrusion detection alerts, and blocked connection events to your SIEM.

This isn't code you'd write, but configuration you'd perform within the management consoles of these services. The output might look like this:

```
# Conceptual example of a firewall syslog configuration
log-server <SIEM_IP_ADDRESS> port 514 protocol udp
log-facility local7
log-severity informational
```

Step 2: Defining Automation Playbooks

Once your logs are centralized, you can start defining automation rules or "playbooks" within your SIEM or a dedicated SOAR (Security Orchestration, Automation and Response) platform. These playbooks outline specific actions to take when certain conditions are met.

Scenario: Automated Response to a High-Risk Login

Let's say your SIEM detects a login from a new, suspicious IP address that's also flagged by your threat intelligence feed.

Automation Playbook Logic:

1. **Trigger:** SIEM alert for "Login from new/suspicious IP" and "High-risk user activity."
2. **Conditions:**
    - IP address matches a known malicious IP from threat intelligence.
    - User's risk score is above a threshold (e.g., 70 out of 100).
    - Login location is geographically unusual for the user.
3. **Actions (in order of execution):**
    - **Action 1 (Immediate):** Force a step-up Multi-Factor Authentication (MFA) challenge for the user.
    - **Action 2 (If MFA fails or not possible):** Temporarily block the user's account for 15 minutes.
    - **Action 3:** Send an alert to the security operations center (SOC) team with full context.
    - **Action 4:** Create an incident ticket in the ticketing system.

This playbook would be configured using a graphical interface or YAML/JSON definitions within your SOAR or conditional access policy engine.

```yaml
# Conceptual YAML for an automated response playbook (simplified)
name: "High-Risk Login Response"
trigger:
```

```
  type: "SIEM_Alert"
  alert_name: "SuspiciousLoginAttempt"
conditions:
  - field: "ip_reputation"
    operator: "equals"
    value: "malicious"
  - field: "user_risk_score"
    operator: "greater_than"
    value: 70
actions:
  - type: "IdentityProvider"
    action: "ForceMFA"
    target: "{{alert.username}}"
  - type: "IdentityProvider"
    action: "BlockUserAccount"
    target: "{{alert.username}}"
    duration: "15m"
    if_previous_fails: true # Only if ForceMFA fails
  - type: "Notification"
    action: "SendEmail"
    recipient: "soc@example.com"
    subject: "High-Risk Login Alert: {{alert.username}}"
  - type: "TicketingSystem"
    action: "CreateIncident"
    severity: "High"
    title: "Suspicious Login for {{alert.username}}"
```

This YAML is a simplified representation of how such a playbook might be defined. Real-world SOAR platforms offer extensive integrations and more complex logic.

Step 3: Integrating Threat Intelligence Feeds

Your SIEM/SOAR and other security tools (like firewalls or EDR) need to be configured to ingest and utilize threat intelligence feeds.

Process:

1. **Choose TI Sources:** Select reputable threat intelligence providers (e.g., commercial feeds, open-source feeds like AbuseIPDB, or government-sponsored feeds).
2. **Configure Ingestion:** Your SIEM/SOAR platform will have connectors or APIs to ingest these feeds automatically. This often involves scheduling regular updates.
3. **Apply to Policies:**
    - **Firewalls:** Configure your firewalls to block traffic from IP addresses listed in known malicious IP feeds.
    - **Identity Providers:** Use TI to enhance risk scoring for login attempts.
    - **EDR/XDR:** Use TI to identify known malware hashes or command-and-control (C2) domains.

```
# Conceptual command for adding a threat intelligence feed to a security
platform
# (This would be done via a GUI or API in a real product)
security-platform-cli ti add \
    --name "Malicious_IP_Feed" \
    --source "https://threatintel.example.com/bad_ips.csv" \
    --format "csv" \
    --update-frequency "hourly" \
    --action-on-match "block_traffic"
```

This command represents the intent of integrating a threat intelligence feed, which would typically be managed through a vendor-specific console or API.

Mini-Challenge: Designing an Automated Data Exfiltration Response

You've learned about the components. Now, let's put them to work.

Challenge: Design a conceptual automated response playbook for a scenario where an employee's device is detected attempting to upload a large amount of sensitive data to an unauthorized cloud storage service (e.g., a personal Dropbox account, not approved by your organization).

Your task:

1. Identify the **trigger(s)** for this event.
2. List potential **conditions** that would confirm this is a high-risk event (and not a false positive).
3. Outline the **automated actions** (at least three) your Zero Trust system should take, in order of priority, to contain the threat and minimize data loss.

Hint: Think about what data sources would detect this, what makes it "unauthorized," and how you'd prevent further data movement while alerting the right people.

Common Pitfalls & Troubleshooting

Even with the best intentions, implementing monitoring, automation, and threat intelligence can hit roadblocks.

1. **Alert Fatigue:**
    - **Pitfall:** Over-alerting, where too many non-critical alerts desensitize security teams, leading to missed critical incidents.
    - **Troubleshooting:** Prioritize alerts based on actual risk and impact. Tune detection rules to reduce false positives. Implement alert suppression for known benign activities. Use automation to handle low-severity events without human intervention.
2. **Over-Automation (The "Runaway Script"):**
    - **Pitfall:** Automating responses without thorough testing can lead to unintended consequences, such as blocking legitimate users, isolating critical systems, or disrupting business operations.
    - **Troubleshooting:** Implement a phased approach for automation (e.g., "alert only" -> "suggest action" -> "partial automation" -> "full automation"). Test playbooks rigorously in a sandbox environment. Include human approval steps for high-impact automated actions until confidence is built. Implement circuit breakers or kill switches for automated processes.
3. **Stale or Irrelevant Threat Intelligence:**
    - **Pitfall:** Using outdated threat feeds or feeds that aren't relevant to your industry or specific threat landscape. This can lead to ineffective blocking or, conversely, blocking legitimate traffic.
    - **Troubleshooting:** Regularly review and update your TI sources. Integrate multiple, diverse feeds. Prioritize feeds that are highly relevant to your organization's specific risks and assets. Supplement external feeds with internal intelligence derived from your own security incidents.

4. **Lack of Integration:**
    - **Pitfall:** Security tools operating in silos, unable to share data or trigger actions across platforms.
    - **Troubleshooting:** Invest in platforms (SIEM/SOAR) that facilitate broad integration. Prioritize tools with robust APIs and pre-built connectors. Work towards a unified security fabric where different components can communicate and act cohesively.

Summary

In this chapter, we've explored the dynamic core of Zero Trust security: continuous monitoring, intelligent automation, and proactive threat intelligence.

Here are the key takeaways:

- **Monitoring is Essential:** It provides the real-time visibility needed to verify every access attempt and resource interaction, making your Zero Trust policies adaptive.
- **Automation is Your Force Multiplier:** It enables rapid, consistent, and scalable responses to detected threats, dynamically adjusting policies and containing breaches faster than human intervention.
- **Threat Intelligence Provides Context and Foresight:** By integrating external and internal threat data, your Zero Trust defenses become more proactive, capable of blocking known bad actors and identifying emerging attack patterns.
- **A Continuous Feedback Loop:** These three components work together in a synergistic loop, ensuring your security posture is constantly learning, adapting, and responding to the evolving threat landscape.
- **Practical Steps Involve Integration:** Centralized logging via SIEMs, defining clear automation playbooks in SOAR platforms, and integrating diverse threat intelligence feeds are crucial implementation steps.

By mastering these elements, you move beyond a static security perimeter to a truly dynamic, resilient, and adaptive Zero Trust environment. In the next chapter, we'll shift our focus to the crucial aspects of **Governance, Compliance, and Continuous Improvement** – ensuring your Zero Trust journey is sustainable and meets regulatory requirements.

References

- Zero Trust adoption framework overview | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview
- What is Zero Trust? | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
- GitHub - ukncsc/zero-trust-architecture: Principles to help you design and deploy a zero trust architecture: https://github.com/ukncsc/zero-trust-architecture
- NIST Special Publication 800-207: Zero Trust Architecture: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 10

Zero Trust in the Cloud: Adapting Principles for IaaS, PaaS, and SaaS

Introduction: Securing Beyond the Traditional Perimeter

Welcome back! In our journey through Zero Trust, we've established its core principles: **Verify Explicitly, Use Least Privileged Access, and Assume Breach**. These principles fundamentally challenge traditional perimeter-based security, where everything inside the network was trusted. But what happens when there is no clear network perimeter?

That's the reality of cloud computing. Organizations are rapidly adopting Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models, moving critical applications and data out of on-premises data centers. This shift dissolves the traditional network boundary, making the "trust but verify" model not just inadequate, but dangerous.

In this chapter, we'll dive into why Zero Trust isn't just a good idea for the cloud—it's **essential**. We'll explore how to adapt the foundational Zero Trust principles to the unique characteristics and shared responsibility models of IaaS, PaaS, and SaaS. By the end, you'll understand how to apply a consistent security philosophy across your diverse cloud footprint, ensuring your digital assets remain protected, no matter where they reside.

To get the most out of this chapter, you should have a solid grasp of the core Zero Trust concepts covered in previous sections and a basic understanding of cloud service models (IaaS, PaaS, SaaS).

Core Concepts: The Cloud's Impact on Zero Trust

The cloud fundamentally changes the security landscape. Let's explore the key shifts and how they directly influence the application of Zero Trust.

The Vanishing Perimeter

Remember the castle-and-moat analogy for traditional security? A strong perimeter, everything inside is safe. In the cloud, that moat often evaporates. Your users are accessing resources from anywhere, on any device. Your applications are distributed across multiple cloud providers, regions, and even hybrid environments.

This dynamic, borderless environment means:

- **No Implicit Trust:** Every access request, regardless of origin, must be treated as untrusted.
- **Identity is the New Perimeter:** User and workload identities become the primary control plane for access.
- **Micro-segmentation is Crucial:** Networks must be segmented down to individual workloads or even functions, limiting lateral movement if a breach occurs.

Understanding the Shared Responsibility Model

A critical aspect of cloud security is the **shared responsibility model**. Cloud providers (like AWS, Azure, GCP) are responsible for the security of the cloud, while you, the customer, are responsible for the security in the cloud. This distinction is vital for applying Zero Trust effectively.

Here's a quick breakdown:

Responsibility	Cloud Provider (e.g., AWS, Azure)	Customer (You!)
IaaS	Physical security, host infrastructure, virtualization layer	Operating systems, network configuration, applications, data, identity management
PaaS	Runtime environment, OS, underlying infrastructure	Applications, data, identity and access management, API security
SaaS	Application, runtime, OS, infrastructure, network	Data (often), identity and access management, configuration, user behavior

🧠 Important: The more managed the service (from IaaS to PaaS to SaaS), the more responsibility shifts to the cloud provider. However, your responsibility for **data, identity, and configuration** always remains significant. Zero Trust helps you fulfill your part of this shared model.

Adapting the Zero Trust Pillars to Cloud Contexts

The three core Zero Trust principles—Verify Explicitly, Use Least Privileged Access, and Assume Breach—remain the bedrock, but their implementation details evolve in the cloud.

1. Verify Explicitly

In the cloud, "Verify Explicitly" means scrutinizing every access request with an even higher degree of paranoia.

- **Identity-Centric Access:** Every human and non-human identity (service accounts, managed identities, application IDs) must be strongly authenticated. Multi-Factor Authentication (MFA) is non-negotiable for all identities.
- **Device Posture:** Verify the health and compliance of devices accessing cloud resources. Is the device managed? Up-to-date? Free of malware?
- **Contextual Policies:** Access decisions must consider not just who and what, but where (location, IP address), when (time of day), and how (application, sensitivity of data).

2. Use Least Privileged Access

Applying least privilege in the cloud is about precision.

- **Granular Permissions:** Instead of broad roles, assign the absolute minimum permissions required for a specific task. Cloud IAM policies allow for highly granular control over resources.
- **Just-In-Time (JIT) Access:** Grant elevated permissions only when needed, for a limited duration, and automatically revoke them afterward. This minimizes the window of opportunity for attackers.
- **Attribute-Based Access Control (ABAC):** Use attributes (e.g., project, department, data sensitivity) to define access policies, making them more dynamic and scalable than role-based access control (RBAC) alone.

3. Assume Breach

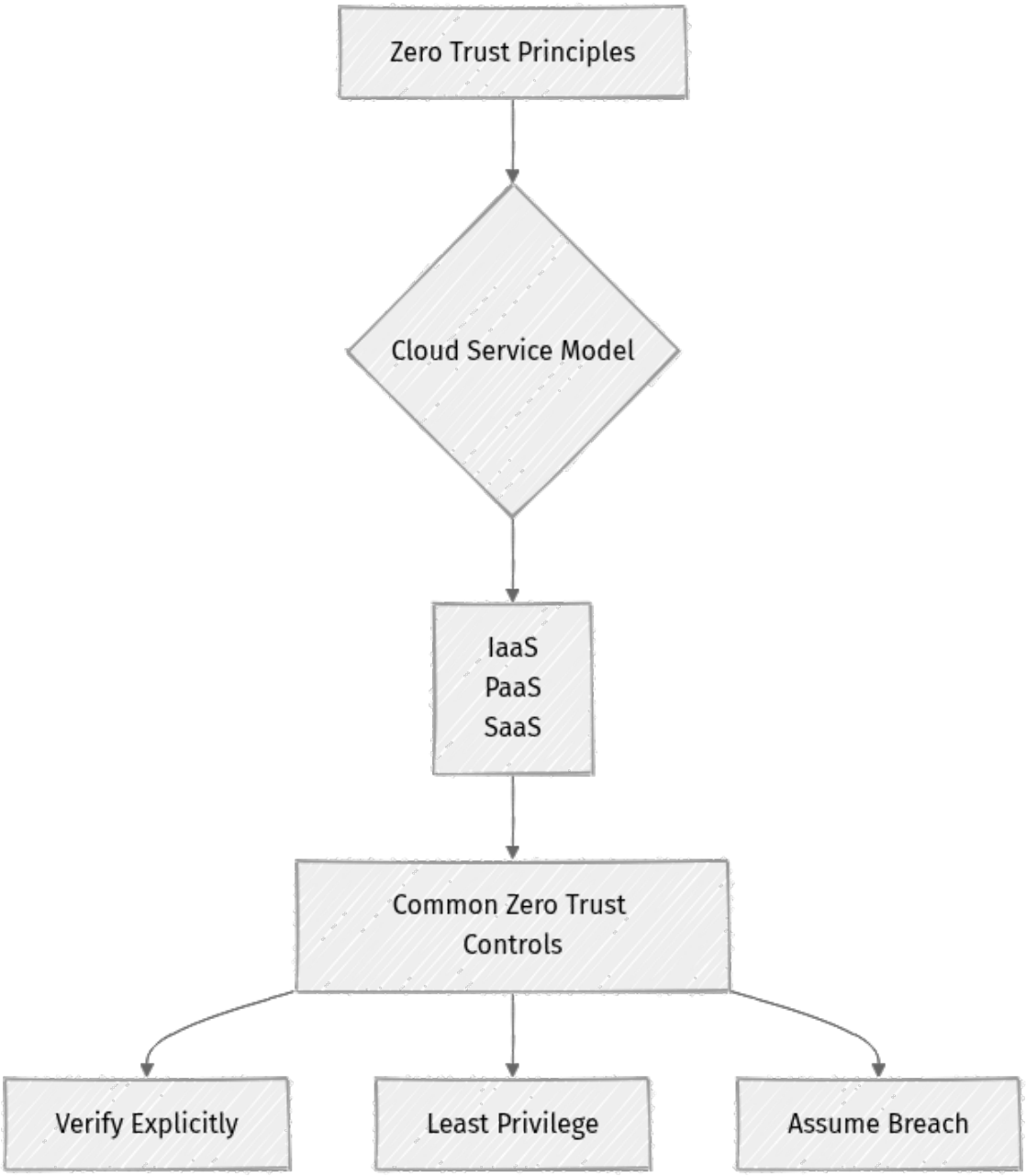
With the understanding that breaches are inevitable, cloud environments demand proactive containment and rapid response.

- **Micro-segmentation:** This is key. In the cloud, micro-segmentation goes beyond traditional network segments. Think cloud-native security groups, network ACLs, private endpoints, and service meshes that isolate workloads from each other, even within the same virtual network.

- **End-to-End Encryption:** Encrypt data at rest (storage, databases) and in transit (network traffic, API calls) by default. This protects data even if an attacker gains access to infrastructure.
- **Continuous Monitoring and Logging:** Robust logging and security information and event management (SIEM) solutions are crucial for detecting anomalies, identifying threats, and providing forensic data for incident response.

Zero Trust Across Cloud Service Models

Let's look at how these principles manifest differently across IaaS, PaaS, and SaaS.



IaaS (Infrastructure as a Service)

With IaaS, you manage virtual machines, networks, and storage, giving you significant control but also significant responsibility.

- **Verify Explicitly:**
    - Implement strong IAM for accessing VMs (e.g., SSH keys, Bastion hosts, JIT access).
    - Use host-based firewalls and endpoint detection and response (EDR) on VMs.
    - Integrate VM identities with your central identity provider.
- **Least Privileged Access:**
    - Strictly define network security groups (NSGs) or security lists to allow only necessary traffic between VMs and to/from the internet.
    - Use cloud IAM roles to grant minimal permissions for managing VMs, storage, and networks.
    - Separate administrative networks from application networks.
- **Assume Breach:**
    - Automate OS patching and configuration management.
    - Encrypt all storage volumes and network traffic between VMs.
    - Implement intrusion detection/prevention systems (IDS/IPS) at the network layer.
    - Monitor VM logs for suspicious activity.

PaaS (Platform as a Service)

PaaS abstracts away much of the infrastructure, letting you focus on your application code. Your responsibility shifts to securing the application itself and how it interacts with the managed platform services.

- **Verify Explicitly:**
    - Use managed identities or service principals for applications to authenticate to other PaaS services (e.g., a web app accessing a managed database).
    - Secure API endpoints with strong authentication (API keys, OAuth, mutual TLS).
    - Enforce conditional access for developers accessing PaaS management portals.

- **Least Privileged Access:**
    - Grant your application's managed identity only the specific permissions needed for the database, storage, or other services it consumes.
    - Configure platform-specific access controls (e.g., database user permissions, storage bucket policies) with fine granularity.
    - Restrict network access to PaaS services using private endpoints or service endpoints.
- **Assume Breach:**
    - Enable platform-native security features like vulnerability scanning for web apps or database threat detection.
    - Encrypt data stored in managed databases and storage accounts.
    - Continuously monitor PaaS service logs for anomalous behavior.

SaaS (Software as a Service)

SaaS gives you the least control over the underlying infrastructure and application, as you're primarily consuming a service. Your Zero Trust focus shifts heavily to identity, data governance, and monitoring user behavior within the application.

- **Verify Explicitly:**
    - Integrate SaaS applications with your corporate Single Sign-On (SSO) solution, enforcing MFA for all users.
    - Implement Conditional Access policies based on user, device, location, and application risk.
    - Leverage Cloud Access Security Brokers (CASBs) to add an enforcement layer for SaaS usage.
- **Least Privileged Access:**
    - Assign users the minimum necessary roles and permissions within the SaaS application itself.
    - Regularly review and audit user access to critical SaaS data.
    - Restrict data sharing capabilities within the SaaS application where possible.

- **Assume Breach:**
    - Monitor user activity within SaaS applications for unusual patterns (e.g., large downloads, access from new locations).
    - Configure data loss prevention (DLP) policies within the SaaS application or via a CASB.
    - Regularly review the SaaS vendor's security posture and compliance certifications.

Step-by-Step Implementation: Securing a Hybrid Cloud Application

Let's walk through a conceptual implementation of Zero Trust for a common scenario: a web application running on IaaS VMs, connected to a PaaS database, with users authenticated via a corporate SaaS identity provider.

Our goal isn't to write specific cloud provider code, but to understand the sequence of actions and principles applied at each layer.

Scenario: Modernizing a Legacy Application

Imagine a company is migrating an internal web application.

- **Frontend/Backend:** Hosted on Virtual Machines (IaaS) in a private cloud network.
- **Database:** Migrated to a managed database service (PaaS) like Azure SQL Database, AWS RDS, or Google Cloud SQL.
- **Identity:** Users authenticate via an enterprise identity provider (SaaS) like Okta, Azure Active Directory (now Microsoft Entra ID as of 2026-05-28), or Google Workspace Identity.

Step 1: Centralize Identity and Access Management (IAM)

The first step in any Zero Trust journey, especially in the cloud, is to unify identity.

- **Action:** Integrate your IaaS and PaaS services with your enterprise SaaS identity provider. This means configuring your cloud platform (e.g., AWS IAM, Azure AD, GCP IAM) to trust your central IdP.
- **Why it matters:** This establishes a single source of truth for all human and non-human identities, enabling consistent authentication and authorization policies across your entire cloud footprint.

- **Zero Trust Principle: Verify Explicitly** is strengthened by having a robust, centralized identity verification process.

⚡ Real-world insight: Most cloud providers offer native integration with popular IdPs using standards like SAML 2.0 or OpenID Connect. This allows users to log in once (SSO) and access multiple cloud resources.

Step 2: Implement Network Micro-segmentation for IaaS

Now, let's secure the IaaS layer where our web application runs.

- **Action:** Define granular network security groups (NSGs in Azure, Security Groups in AWS, Firewall Rules in GCP) for your virtual machines.
    - Create a security group for web servers, allowing inbound traffic only on ports 80/443 from your load balancer.
    - Create another security group for application servers, allowing inbound traffic only from the web server security group on specific application ports.
    - Create a security group for management (e.g., SSH/RDP bastion hosts), allowing access only from specific administrative IPs.
- **Why it matters:** This isolates workloads, preventing an attacker who compromises one VM from easily moving laterally to others.
- **Zero Trust Principle:** This is a direct application of **Assume Breach** (limiting blast radius) and **Least Privileged Access** (network permissions).

Step 3: Secure Application and API Access for PaaS

Our application needs to talk to the managed database.

- **Action:**
    1. Create a **managed identity** (e.g., Azure Managed Identity, AWS IAM role for EC2, GCP Service Account for Compute Engine) for your IaaS web application VMs.
    2. Grant this managed identity **least privilege access** to your PaaS database. This means allowing only necessary database operations (e.g., read/write to specific tables) and restricting administrative access.
    3. Configure your PaaS database to **only accept connections** from the private IP addresses of your IaaS application VMs or via a private endpoint.

- **Why it matters:** This eliminates the need for hardcoded database credentials on your VMs, making access more secure and auditable. Restricting network access ensures only authorized services can connect.
- **Zero Trust Principle: Verify Explicitly** (the application's identity is verified) and **Least Privileged Access** (minimal permissions and restricted network path).

Step 4: Data Protection Everywhere

Data is king, and it needs protection regardless of its location.

- **Action:**
    1. Enable **encryption at rest** for all IaaS storage (VM disks) and PaaS databases. Most cloud providers offer this by default or as an easy option.
    2. Ensure **encryption in transit** for all communication (e.g., enforce HTTPS for web traffic, SSL/TLS for database connections).
    3. Implement **data classification** and apply Data Loss Prevention (DLP) policies, especially for sensitive data flowing through or stored in your cloud environment.
- **Why it matters:** Even if an attacker bypasses other controls, encrypted data remains protected. DLP helps prevent accidental or malicious exfiltration.
- **Zero Trust Principle:** A core part of **Assume Breach**, ensuring data confidentiality even if other layers fail.

Step 5: Continuous Monitoring and Threat Detection

Zero Trust is an ongoing process, not a one-time setup.

- **Action:**
    1. Integrate cloud-native logging (e.g., CloudWatch Logs, Azure Monitor, Cloud Logging) from your IaaS VMs, PaaS database, and SaaS identity provider into a centralized Security Information and Event Management (SIEM) system.
    2. Configure alerts for unusual activity (e.g., failed logins, changes to security configurations, large data transfers).
    3. Regularly review security posture management tools (e.g., Cloud Security Posture Management - CSPM) provided by your cloud vendor or third-party solutions.

- **Why it matters:** Constant vigilance helps detect breaches early, understand attack patterns, and refine your Zero Trust policies.
- **Zero Trust Principle:** The ultimate expression of **Assume Breach**, enabling rapid response and continuous improvement.

Mini-Challenge: Zero Trust for a Remote Worker

Imagine your company uses:

- A **SaaS** CRM (e.g., Salesforce).
- A **PaaS** analytics platform (e.g., Databricks, Azure Synapse).
- **IaaS** VMs for custom backend services (e.g., a legacy application server).

A remote employee, "Alice," needs to access all three. Describe how you would apply the 'Verify Explicitly' principle to Alice's access requests for each of these service models, considering the shared responsibility model for each.

Hint: Think about where the identity verification occurs and what contextual factors you can leverage at each level.

What to observe/learn: This challenge reinforces the idea that "Verify Explicitly" adapts based on your level of control and the specific characteristics of IaaS, PaaS, and SaaS. You'll see how different tools and approaches come into play for a consistent Zero Trust posture.

Common Pitfalls & Troubleshooting

Implementing Zero Trust in the cloud can be complex. Here are some common challenges and how to address them:

- **Over-reliance on Cloud Provider Defaults:** Many cloud services come with default security settings that are often too permissive or not aligned with Zero Trust.
    - **Troubleshooting:** Always review and customize security configurations (IAM policies, network rules, encryption settings) to enforce least privilege. Don't assume defaults are secure enough.

- **Identity Sprawl:** Having multiple, disconnected identity stores across various cloud accounts, subscriptions, or SaaS applications.
    - **Troubleshooting:** Prioritize centralizing identity management with a single enterprise identity provider. Use federation (SAML/OIDC) to connect all your cloud services to this central IdP.
- **Neglecting Cloud-Native Tools:** Trying to force traditional on-premises security tools into a cloud environment where they may not be effective or efficient.
    - **Troubleshooting:** Embrace cloud-native security services (e.g., cloud firewalls, managed WAFs, security posture management, native SIEM integrations). These are designed to work seamlessly with the cloud's dynamic nature.
- **Lack of Automation:** Manually configuring security policies across a dynamic cloud environment leads to inconsistencies, errors, and security gaps.
    - **Troubleshooting:** Adopt Infrastructure as Code (IaC) for defining security policies (e.g., Terraform, CloudFormation, Azure Bicep). Automate policy enforcement and security checks in your CI/CD pipelines.

Summary

Zero Trust in the cloud is not just a recommendation; it's a necessity for modern cybersecurity. By understanding the nuances of IaaS, PaaS, and SaaS, you can effectively adapt the core Zero Trust principles to secure your entire digital estate.

Here are the key takeaways from this chapter:

- The cloud dissolves the traditional network perimeter, making **identity the new perimeter**.
- The **shared responsibility model** dictates your security obligations across IaaS, PaaS, and SaaS.
- **Verify Explicitly** means strong, contextual authentication for all identities and devices.
- **Least Privileged Access** requires granular permissions, JIT access, and ABAC across cloud resources.
- **Assume Breach** necessitates robust micro-segmentation, end-to-end encryption, and continuous monitoring.

- Implementation involves centralizing identity, segmenting networks, securing application access, protecting data, and continuous monitoring.
- Avoid common pitfalls like relying on defaults, identity sprawl, ignoring cloud-native tools, and manual configurations.

Remember, Zero Trust is an iterative journey. As your cloud footprint evolves, so too will your Zero Trust implementation.

In the next chapter, we'll delve into the crucial role of **Automation and Orchestration in Zero Trust**, exploring how to scale your security efforts and respond dynamically to threats.

References

- What is Zero Trust? | Microsoft Learn
- Zero Trust adoption framework overview | Microsoft Learn
- Principles to help you design and deploy a zero trust architecture | NCSC GitHub
- Shared responsibility in the cloud - Azure Security
- AWS Shared Responsibility Model

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 11

Building the Zero Trust Culture: Governance, Compliance, and Organizational Buy-in

Introduction: Beyond the Tech — The Human Element of Zero Trust

Welcome back! In our journey through Zero Trust, we've explored its core principles, dived into identity and access management, secured networks, devices, and applications, and even looked at data protection and automation. We've built a strong technical foundation, but here's a crucial insight: Zero Trust isn't just a technical implementation. It's a profound shift in an organization's security philosophy.

This chapter shifts our focus from the "what" and "how" of technology to the equally vital "who" and "why" of organizational change. We'll uncover why fostering a Zero Trust culture, establishing robust governance, ensuring regulatory compliance, and securing widespread organizational buy-in are not merely good practices, but absolute necessities for successful and sustainable Zero Trust adoption. Without these elements, even the most sophisticated technical controls can falter.

By the end of this chapter, you'll understand how to weave Zero Trust into the fabric of your organization, making it a natural part of operations rather than an imposed burden.

Zero Trust as a Cultural Shift

Implementing Zero Trust means challenging decades of ingrained security assumptions. It moves from a model where everything inside the network was implicitly trusted to one where nothing is trusted by default. This change impacts everyone, from executives making strategic decisions to developers writing code and end-users accessing resources.

The "Never Trust, Always Verify" Mindset

At its heart, Zero Trust demands a new way of thinking. Instead of assuming good intent based on location or network segment, every access request, every user, every device, and every application must be explicitly verified. This fundamental shift requires:

- **Increased Vigilance:** Everyone becomes a part of the security posture, understanding that their actions have implications.
- **Proactive Security:** Moving from reacting to breaches to actively preventing and containing them.
- **Collaboration:** Security teams, IT operations, development, and even business units must work together to define and enforce policies.

📌 **Key Idea:** Zero Trust is a journey of continuous verification, not a destination product. Its success hinges on embedding this philosophy into daily operations.

Impact on User Behavior and IT Operations

Consider the implications:

- **Users:** May encounter more frequent authentication prompts (e.g., MFA), stricter access controls, and new guidelines for handling sensitive data. Clear communication is essential to turn potential frustration into understanding.
- **IT Operations:** Must adapt to managing devices and identities in a "hostile" environment, where every connection needs validation. This often means new tools, processes, and skill sets.
- **Developers:** Need to build applications with Zero Trust principles in mind from the outset, integrating identity and authorization checks directly into their code.

Governance Frameworks for Zero Trust

Effective governance provides the structure and authority needed to implement and maintain Zero Trust principles across the organization. It defines who is responsible for what, how decisions are made, and how policies are enforced.

Defining Policies, Roles, and Responsibilities

A robust Zero Trust governance framework typically includes:

1. **Strategic Vision:** A clear, documented statement outlining the organization's commitment to Zero Trust and its alignment with business goals.
2. **Policy Development:** Crafting specific, actionable policies that translate Zero Trust principles into rules. Examples include:
    - All remote access must use MFA.
    - Access to sensitive data must be time-bound and approved by data owners.
    - Devices must meet minimum security posture requirements before accessing corporate resources.
3. **Roles and Responsibilities Matrix:** Clearly assigning ownership for different aspects of Zero Trust (e.g., CISO for strategy, IT operations for implementation, application owners for policy definition).
4. **Risk Management Integration:** Incorporating Zero Trust into the overall enterprise risk management framework, identifying and mitigating risks associated with access.

Establishing a Zero Trust Steering Committee

For larger organizations, a dedicated Zero Trust steering committee is invaluable. This cross-functional group typically includes representatives from:

- **Executive Leadership:** For strategic direction and resource allocation.
- **Security Teams:** For technical expertise and policy enforcement.
- **IT Operations:** For infrastructure and system management.
- **Application Development:** For integrating security into software lifecycles.
- **Legal/Compliance:** For regulatory alignment.
- **Business Units:** To ensure policies support business needs without undue friction.

This committee ensures that Zero Trust initiatives are aligned with business objectives, properly funded, and consistently implemented.

Policy-as-Code (Conceptual)

While this chapter focuses on governance, it's worth noting the concept of **Policy-as-Code**. This approach treats security policies like software code, allowing them to be version-controlled, tested, and automated. It ensures consistency and reduces manual errors. While the policy definitions themselves are part of governance, the implementation often leverages automation tools.

Ensuring Regulatory Compliance

Modern regulatory landscapes are complex and ever-evolving. Zero Trust isn't just a security best practice; it's a powerful enabler for meeting and exceeding compliance requirements.

How Zero Trust Aligns with Major Regulations

Many regulations and standards, such as GDPR, HIPAA, PCI DSS, NIST, and ISO 27001, emphasize principles that are inherently supported by Zero Trust:

- **Least Privilege:** Granting minimum necessary access is a core requirement for many data privacy and security regulations.
- **Strong Authentication:** MFA is a common control required or strongly recommended by most standards.
- **Data Segmentation:** Micro-segmentation helps isolate sensitive data, reducing the scope of compliance audits and containing breaches.
- **Continuous Monitoring:** Zero Trust's emphasis on continuous verification naturally leads to better auditing and monitoring capabilities, critical for demonstrating compliance.
- **Data Encryption:** End-to-end encryption, a Zero Trust best practice, is often mandated for data in transit and at rest.

⚡ **Real-world insight:** Implementing Zero Trust can simplify compliance audits. By demonstrating robust access controls, continuous monitoring, and data protection, organizations can more easily prove adherence to various regulatory mandates.

Proactive Compliance Through Explicit Verification

Zero Trust shifts compliance from a reactive, audit-driven process to a proactive, continuous one. Instead of merely checking boxes for an audit, organizations are continuously verifying security posture, thereby inherently meeting many compliance requirements.

For example, a Zero Trust policy requiring a device to be patched and free of known vulnerabilities before accessing sensitive data directly supports compliance mandates for secure configurations and vulnerability management.

Strategies for Organizational Buy-in

Even the best technical strategy will fail without widespread support. Gaining organizational buy-in is paramount for Zero Trust success.

Leadership Sponsorship (Top-Down)

Zero Trust must be championed from the top. Executive leaders need to:

- **Articulate the Vision:** Clearly communicate why Zero Trust is essential for the business, linking it to risk reduction, competitive advantage, and customer trust.
- **Allocate Resources:** Provide the necessary budget, personnel, and time for the transformation.
- **Lead by Example:** Adhere to Zero Trust policies themselves, demonstrating commitment.

Without executive sponsorship, Zero Trust can be perceived as "just another IT project" and struggle to gain traction.

Communication and Training (Bottom-Up)

Effective communication and comprehensive training are crucial for securing buy-in from all levels:

- **Tailored Messaging:** Different groups need different information.
    - **Executives:** Focus on business value, risk reduction, and compliance.
    - **IT Staff:** Focus on technical implementation, new tools, and process changes.
    - **End-Users:** Focus on "what's in it for them" (e.g., enhanced security, protecting company data) and clear instructions on new procedures.
- **Ongoing Education:** Zero Trust principles should be integrated into ongoing security awareness training.
- **Feedback Channels:** Provide avenues for users to ask questions, report issues, and provide feedback, making them feel heard and part of the solution.

Demonstrating Value

Show, don't just tell. Demonstrating the tangible benefits of Zero Trust helps build confidence and support:

- **Quantify Risk Reduction:** Present metrics on reduced incident rates, faster detection, or fewer successful phishing attempts.
- **Highlight Efficiency Gains:** Show how automation and streamlined access processes can improve productivity for IT and users (e.g., faster onboarding, self-service password resets).
- **Show Compliance Improvements:** Demonstrate how Zero Trust directly helps meet regulatory requirements and strengthens audit posture.

Step-by-Step Implementation: Weaving Zero Trust into Your Organization

Now, let's outline a process for integrating Zero Trust governance, compliance, and culture.

Step 1: Assess Current State & Identify Gaps

Before implementing new policies, understand your starting point.

1. **Review Existing Policies:** Examine current security policies related to access, data handling, device management, and incident response. Identify areas that contradict or are insufficient for Zero Trust.
2. **Conduct Cultural Assessment:** Gauge employee understanding of security, their comfort with new technologies, and potential resistance points. Surveys, interviews, and workshops can help.
3. **Align with Business Objectives:** Work with business leaders to understand critical assets, processes, and strategic goals. Zero Trust must support these, not hinder them.

Step 2: Define Zero Trust Principles and Policies

Translate the philosophy into actionable rules.

1. **Articulate Core Principles:** Based on your organization's context, define what "never trust, always verify" means for you.
    - Example Principle: "All access requests, regardless of origin, must be authenticated and authorized based on identity, device posture, and resource attributes."

2. **Draft Specific Policies:** Create clear, concise policies.
    - Example Policy (Plain Language): "To access financial systems, all users must use Multi-Factor Authentication (MFA) and their device must pass a security health check (e.g., up-to-date antivirus, no critical vulnerabilities) at the time of access. Access is limited to necessary roles only and is automatically revoked after 8 hours of inactivity."
    - Example Policy (Conceptual Pseudo-code):

```
POLICY AccessFinancialSystem:
  IF User.Identity.Authenticated_Via_MFA AND
     Device.Posture.Is_Compliant AND
     User.Role IN ["Finance_Manager", "Auditor"] AND
     Access.Time_Since_Last_Activity < 8_hours
  THEN GRANT_ACCESS
  ELSE DENY_ACCESS
```

```
These policies form the basis for your technical controls.
```

Step 3: Establish a Governance Structure

Formalize who makes decisions and who enforces them.

1. **Form a Zero Trust Steering Committee:** As discussed, create a cross-functional team with executive sponsorship. Define their mandate, meeting cadence, and decision-making authority.
2. **Define Ownership:** Clearly assign responsibility for different Zero Trust pillars (Identity, Device, Network, App, Data) to specific teams or individuals.
3. **Establish Review Processes:** Set up regular reviews of policies, technical implementations, and incident responses to ensure continuous improvement.

Step 4: Develop a Communication & Training Plan

Prepare your organization for the change.

1. **Identify Stakeholders:** Categorize your audience (executives, IT, developers, general employees).

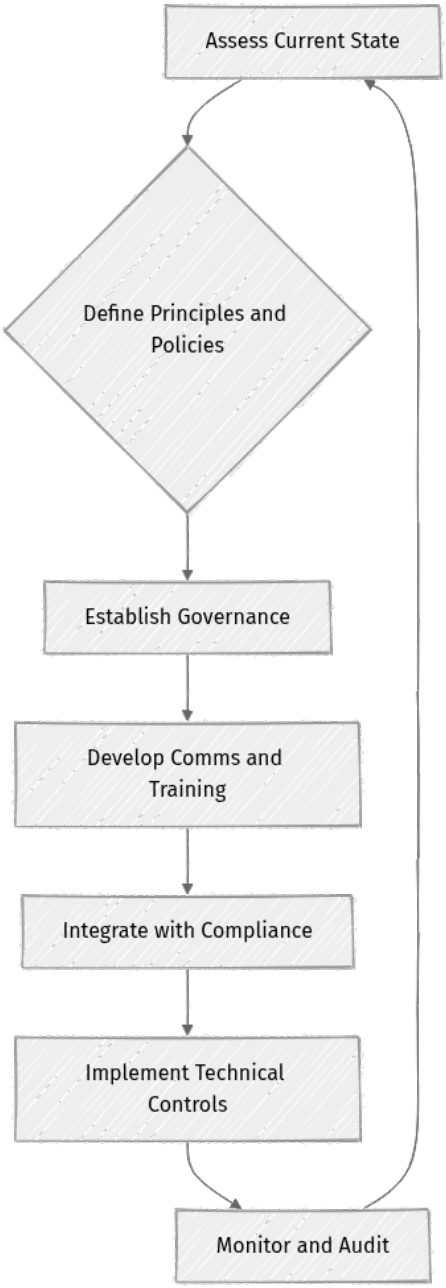
2. **Craft Tailored Messages:**
    - **Executives:** "Zero Trust reduces our attack surface, protects customer data, and ensures regulatory compliance."
    - **End-Users:** "Enhanced security protects your data and the company. We'll show you how new processes are simple and secure."
3. **Select Communication Channels:** Use town halls, email campaigns, intranet articles, and dedicated training sessions.
4. **Create Training Modules:** Develop practical, role-based training. For end-users, focus on how to use new tools (e.g., MFA apps, secure remote access), not just what Zero Trust is.

Step 5: Integrate with Compliance Frameworks

Ensure your efforts contribute to meeting regulatory mandates.

1. **Map Controls to Requirements:** Create a matrix that maps your Zero Trust policies and technical controls to specific clauses in relevant compliance frameworks (e.g., NIST SP 800-207, GDPR Article 32).
2. **Automate Reporting:** Where possible, leverage your Zero Trust tooling to generate reports that demonstrate compliance (e.g., MFA usage rates, non-compliant device counts).
3. **Regular Audits:** Conduct internal and external audits to verify that Zero Trust implementation effectively meets compliance obligations.

Here's a simplified view of the iterative process:



Mini-Challenge: Crafting a User-Friendly Policy Announcement

Let's put some of these communication strategies into practice.

Challenge: Imagine your organization is rolling out a new mandatory Multi-Factor Authentication (MFA) policy for accessing all internal applications, effective next month. Draft a short, engaging, and informative announcement email (3-5 paragraphs) to be sent to all employees.

Hint: Focus on why this change is happening (security benefits), what users need to do, when it takes effect, and where they can get help. Anticipate common questions or concerns.

What to observe/learn: This exercise helps you practice communicating complex security changes in a way that minimizes resistance and maximizes adoption, a critical skill for any Zero Trust leader.

Common Pitfalls & Troubleshooting

Even with the best intentions, organizational and cultural aspects of Zero Trust can encounter roadblocks.

1. **Lack of Executive Sponsorship:**
    - **Pitfall:** Zero Trust is viewed as an "IT problem" without strategic backing, leading to underfunding and resistance from other departments.
    - **Troubleshooting:** Continuously articulate the business value of Zero Trust (risk reduction, compliance, competitive advantage) to senior leadership. Secure a direct executive champion.
2. **Insufficient User Training & Communication:**
    - **Pitfall:** Employees feel new security measures are inconvenient or unclear, leading to workarounds or non-compliance.
    - **Troubleshooting:** Invest heavily in clear, consistent, and empathetic communication. Provide ample, accessible training and support channels. Explain the "why" behind changes.
3. **Ignoring Compliance Implications:**
    - **Pitfall:** Implementing Zero Trust without mapping it to regulatory requirements, potentially missing opportunities to simplify audits or even failing to meet specific mandates.
    - **Troubleshooting:** Involve legal and compliance teams early. Create a clear mapping of Zero Trust controls to regulatory requirements. Use Zero Trust to proactively demonstrate compliance.

4. **Treating Zero Trust as a Product:**
    - **Pitfall:** Believing that purchasing a specific tool or suite automatically makes an organization "Zero Trust," without changing underlying processes, policies, or culture.
    - **Troubleshooting:** Emphasize that Zero Trust is a strategy and a journey. Tools are enablers, but the philosophical shift, governance, and cultural adoption are paramount. Focus on incremental, principle-driven implementation.

Summary: The Foundation of Sustainable Security

In this chapter, we've explored the essential, often overlooked, human and organizational dimensions of Zero Trust Security. We've learned that:

- **Zero Trust is a Cultural Shift:** It demands a fundamental change in mindset from implicit trust to continuous verification, impacting all organizational stakeholders.
- **Robust Governance is Key:** Defining clear policies, roles, and responsibilities through frameworks and steering committees provides the structure for effective implementation.
- **Compliance is a Natural Byproduct:** Zero Trust principles inherently align with and often exceed the requirements of major regulatory frameworks, enabling proactive compliance.
- **Organizational Buy-in is Non-Negotiable:** Securing leadership sponsorship, fostering effective communication, and demonstrating tangible value are critical for widespread adoption and sustained success.

Implementing Zero Trust is a continuous journey, not a one-time project. By focusing on culture, governance, and compliance alongside technical controls, you build a resilient, adaptable, and truly secure organization.

Next up, in Chapter 12, we'll look at the future of Zero Trust, exploring advanced topics, scaling strategies, and emerging trends to keep your organization ahead of the curve.

References

- Zero Trust adoption framework overview | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview
- What is Zero Trust? | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
- GitHub - ukncsc/zero-trust-architecture: Principles to help you design and deploy a zero trust architecture: https://github.com/ukncsc/zero-trust-architecture
- zero-trust-overview.md - security-docs - GitHub: https://github.com/MicrosoftDocs/security/blob/main/security-docs/zero-trust/zero-trust-overview.md

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.

CHAPTER 12

Continuous Improvement and the Future of Zero Trust

Introduction to Evolving Zero Trust

Welcome to the final chapter of our Zero Trust Security guide! If you've been following along, you've likely realized that Zero Trust isn't a one-time project; it's a dynamic, ongoing journey of adaptation and improvement. The digital landscape, with its constantly evolving threats and technologies, demands that our security posture remains equally agile.

In this chapter, we'll shift our focus from initial Zero Trust deployment to the critical aspects of continuous maintenance, iterative refinement, and future-proofing your security strategy. We'll explore how continuous monitoring, automation, and threat intelligence become your organization's eyes and hands in maintaining a robust Zero Trust framework. We'll also cast our gaze forward, examining the emerging trends that will shape the evolution of Zero Trust.

By the end of this chapter, you will understand:

- Why Zero Trust inherently requires a continuous improvement mindset.
- The essential mechanisms for monitoring, auditing, and enforcing Zero Trust policies in real-time.
- How automation and integrated threat intelligence significantly enhance your security posture.
- Key future trends that are influencing and will define Zero Trust security models.

This chapter builds upon your solid understanding of core Zero Trust principles, including explicit verification, least privileged access, and assuming breach, as covered in previous sections. Now, let's learn how to keep your Zero Trust architecture resilient, effective, and forward-looking.

The Iterative Nature of Zero Trust

Implementing Zero Trust is akin to building and maintaining a highly secure, constantly evolving fortress. You don't just build it once and walk away; you continuously patrol its walls, upgrade its defenses, and adapt to new siege tactics. In the digital realm, this continuous improvement is not merely a best practice but a necessity for Zero Trust's long-term effectiveness.

Why Zero Trust is a Journey, Not a Destination

The "assume breach" principle lies at the heart of Zero Trust, acknowledging that no defense is impenetrable. This acceptance of potential compromise drives the need for constant vigilance and improvement.

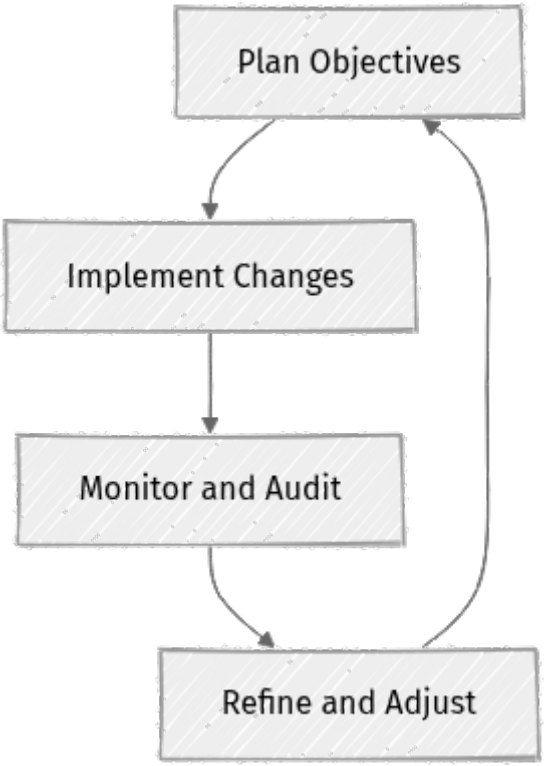
Here’s why Zero Trust must be an ongoing process:

- **Evolving Threat Landscape:** New vulnerabilities, sophisticated attack vectors, and persistent adversaries emerge daily. Your security controls must evolve to counter them effectively.
- **Changing Business Needs:** Organizations grow, adopt new cloud services, onboard new applications, and change operational models. Zero Trust policies must adapt to support these changes without compromising security.
- **Technological Advancements:** New security tools, identity solutions, and automation capabilities become available. Integrating these can significantly enhance your Zero Trust posture.
- **Human Factor:** Users change roles, devices are lost, and human error can introduce vulnerabilities. Policies need regular review to reflect these realities and maintain their relevance.

📌 **Key Idea:** Zero Trust is a strategic philosophy that adapts to change, rather than a static configuration. Its effectiveness stems from its ability to continuously evolve.

The Zero Trust Improvement Cycle

A robust Zero Trust strategy integrates a continuous improvement loop, often aligned with the Plan-Do-Check-Act (PDCA) cycle. This structured approach ensures that security posture is consistently evaluated and refined.



1. **Plan Objectives:** Define clear security goals, assess current risks, identify critical assets, and design or update Zero Trust policies. This includes reviewing your current architecture, identifying gaps, and prioritizing improvements based on business objectives and threat intelligence.
2. **Implement Changes:** Deploy the planned modifications. This could involve configuring new security controls, updating identity provider settings, implementing new network segmentation, or rolling out revised access policies.
3. **Monitor and Audit:** Continuously observe the effectiveness of the implemented changes. Collect telemetry, analyze logs, perform regular security audits, and conduct penetration testing to identify weaknesses, policy misconfigurations, or emerging threats.
4. **Refine and Adjust:** Based on the insights from the "Monitor and Audit" phase, refine and adjust policies and controls. This might mean tightening access, reconfiguring tools, or rolling back ineffective changes. This feedback then directly informs the next "Plan" phase, restarting the cycle.

Step-by-Step: Implementing a Dynamic Zero Trust Policy Review

Let's walk through a conceptual example of how to implement and continuously improve a dynamic Zero Trust policy. This isn't about writing application code, but rather about configuring and managing security controls as an iterative process.

Imagine we want to enforce a policy: "Access to sensitive financial data is only allowed from corporate-managed devices that are compliant and located within approved geographic regions."

Step 1: Define the Initial Policy (Conceptual Configuration)

We'll start with a basic policy that blocks access if the device isn't compliant. This would typically be configured in a Conditional Access policy engine (e.g., Microsoft Entra ID Conditional Access, as of 2026-05-28).

Where to configure: In your Identity Provider's Conditional Access policies or a dedicated Policy Enforcement Point (PEP) management console.

```
# Policy Name: Access to Sensitive Financial Data
conditions:
  users:
    include: [ "Finance_Group" ]
  applications:
    include: [ "Financial_App" ]
  devices:
    # Initial condition: Device must be marked as "compliant" by MDM
    device_state: "compliant"
actions:
  grant:
    access: "block" # Default to block if not compliant
  sessions:
    enforce_mfa: "always" # Always require MFA for this app
```

Explanation:

- `conditions.users`: Specifies that this policy applies to users in the `Finance_Group`.
- `conditions.applications`: Targets access to the `Financial_App`.
- `conditions.devices.device_state`: This is our first Zero Trust check. It requires the device to be marked as `compliant` by an endpoint management solution (like Microsoft Intune or similar MDM).
- `actions.grant.access`: If the conditions are met, access is granted. If `device_state` is not `compliant`, the `block` action would implicitly apply here, or we'd have a separate policy to block non-compliant devices.

- `actions.sessions.enforce_mfa`: Even if compliant, all access to this app always requires Multi-Factor Authentication (MFA), reinforcing explicit verification.

Step 2: Enhance with Location-Based Restrictions

Now, let's refine the policy to include a geographical constraint. We only want access from approved regions.

Where to configure: Update the same Conditional Access policy.

```
# Policy Name: Access to Sensitive Financial Data
conditions:
  users:
    include: [ "Finance_Group" ]
  applications:
    include: [ "Financial_App" ]
  devices:
    device_state: "compliant"
  # New condition: Device must be from an approved geographic region
  locations:
    include: [ "Approved_Corporate_Regions" ] # A named location set (e.g.,
specific countries/IP ranges)
actions:
  grant:
    access: "block" # Default to block if not compliant or not from approved
region
  sessions:
    enforce_mfa: "always"
```

Explanation:

- `conditions.locations`: We've added a new condition. `Approved_Corporate_Regions` would be a pre-defined list of IP ranges or countries that your organization deems safe for sensitive access. If a compliant device tries to access the app from outside these regions, access will be blocked.

Step 3: Configure Monitoring and Alerting (Conceptual SIEM Rule)

To continuously check our policy's effectiveness and detect violations, we need to monitor the logs generated by our Conditional Access policy.

Where to configure: In your SIEM platform (e.g., Microsoft Sentinel, Splunk, Elastic SIEM).

```
# Kusto Query Language (KQL) example for Microsoft Sentinel
# This query looks for blocked access attempts to "Financial_App"
# specifically due to location or device compliance issues.
```

```
SecurityEvent
| where TimeGenerated > ago(1h)
| where EventID == "ConditionalAccessPolicyApplied" // Specific event for CA
policies
| extend PolicyDetails = parse_json(EventData)
| where PolicyDetails.ApplicationDisplayName == "Financial_App"
| where PolicyDetails.Result == "Blocked"
| where PolicyDetails.FailureReason has_any ("DeviceNotCompliant", "LocationNo
tApproved")
| project TimeGenerated, PolicyDetails.UserPrincipalName, PolicyDetails.Device
Name, PolicyDetails.Location, PolicyDetails.FailureReason
| order by TimeGenerated desc
```

Explanation:

- This is a simplified KQL query (common in cloud SIEMs) that filters security events.
- It specifically looks for events where a Conditional Access policy was applied, targeting our `Financial_App`.
- It then filters for `Result == "Blocked"` and identifies `FailureReason` related to device compliance or location.
- This monitoring is crucial for the "Check" phase of our PDCA cycle. It tells us if and why users are being blocked, allowing us to identify legitimate issues or potential policy misconfigurations.

Step 4: Automate Remediation/Response (Conceptual SOAR Playbook)

If a critical policy violation occurs (e.g., multiple attempts to access sensitive data from a non-compliant device in a suspicious location), we want an automated response.

Where to configure: In your SOAR platform (e.g., Microsoft Sentinel Playbooks, Palo Alto Networks Cortex XSOAR).

```
{
  "playbook_name": "Block_Suspicious_Financial_Access",
  "trigger": {
    "type": "SIEM_Alert",
    "alert_name": "HighSeverity_FinancialApp_BlockedAccess"
  },
  "steps": [
    {
      "name": "Isolate_Device",
      "action": "MDM_IsolateDevice",
      "parameters": {
        "device_id": "{{trigger.alert.device_id}}"
      },
      "condition": "{{IsHighRiskUser(trigger.alert.user_id)}}"
    },
    {
```

```
      "name": "Force_Password_Reset",
      "action": "IDP_ForcePasswordReset",
      "parameters": {
        "user_id": "{{trigger.alert.user_id}}"
      },
      "condition": "{{IsHighRiskUser(trigger.alert.user_id)}}"
    },
    {
      "name": "Notify_Security_Team",
      "action": "Send_Email",
      "parameters": {
        "to": "security_ops@example.com",
        "subject": "URGENT: Suspicious Financial App Access Blocked",
        "body": "User {{trigger.alert.user_id}} attempted access from
{{trigger.alert.device_id}} ({{trigger.alert.location}}) and was blocked due
to {{trigger.alert.failure_reason}}. Automated actions taken."
      }
    }
  ]
}
```

Explanation:

- This JSON snippet represents a conceptual SOAR playbook.
- `trigger`: The playbook starts when a high-severity alert from the SIEM (like the one we defined in Step 3) is generated.
- `steps`:
    - `Isolate_Device`: If the user is identified as high-risk, the device is automatically isolated by the MDM.
    - `Force_Password_Reset`: For high-risk users, a password reset is forced in the Identity Provider (IDP).
    - `Notify_Security_Team`: An email is sent to the security operations team with all relevant details.
- This demonstrates the "Act" phase, where automated responses contain threats rapidly, reducing the window of opportunity for attackers.

Step 5: Review and Refine the Policy

After running this policy and monitoring for a period, you might observe:

- **False Positives:** Legitimate users traveling to unlisted regions are blocked, causing business disruption.
- **New Threats:** A new type of non-compliant device is bypassing the MDM check.
- **Performance Impact:** The policy is too granular and slowing down access.

Where to refine: Back in your Conditional Access policy engine and SIEM.

Based on these observations (the "Check" phase), you would "Act" by:

- **Updating Approved Regions:** Add new legitimate business travel regions to `Approved_Corporate_Regions`.
- **Enhancing Device Posture:** Integrate an Endpoint Detection and Response (EDR) solution to provide more granular device health signals beyond simple MDM compliance.
- **Adjusting Policy Scope:** Perhaps create a less strict policy for view-only access to financial data, while keeping the strict one for write access.

This iterative loop of defining, implementing, monitoring, and refining is the essence of continuous improvement in Zero Trust.

Continuous Monitoring and Enforcement

For Zero Trust to be effective, it requires constant awareness of your environment. This means monitoring every access request, every device posture, and every user behavior to detect anomalies and enforce dynamic policies.

The Eyes and Ears of Zero Trust

Continuous monitoring provides the telemetry necessary to detect anomalous behavior, enforce dynamic policies, and respond swiftly to threats.

Key areas for continuous monitoring include:

- **Identity and Access:** Track who is accessing what, from where, and when. Look for unusual login patterns, access attempts to sensitive resources, or privilege escalation.
- **Device Posture:** Continuously verify if the device is compliant with security policies (e.g., up-to-date patches, antivirus running, encrypted). Any deviation should trigger a re-evaluation of access.
- **Network Traffic:** Monitor internal and external traffic for suspicious flows, lateral movement attempts, or data exfiltration.
- **Application Behavior:** Observe how applications are being used, looking for deviations from normal operation or attempts to exploit vulnerabilities.
- **Data Access:** Track who is accessing sensitive data, how often, and if that access aligns with their role and task.

Centralized Logging and SIEM/SOAR

To make sense of the vast amount of data generated by continuous monitoring, a centralized logging solution is essential. Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms are critical tools here.

- **SIEM:** Aggregates logs and security events from all security controls, applications, and infrastructure components. It correlates events to identify potential threats and provides dashboards for security analysts, acting as your central nervous system for security intelligence.
- **SOAR:** Automates incident response workflows. When a SIEM detects a threat, SOAR can automatically trigger actions like isolating a compromised device, blocking an IP address, or initiating an alert to a security team, drastically reducing response times.

⚡ **Real-world insight:** Many organizations (as of 2026-05-28) leverage cloud-native SIEMs like Microsoft Sentinel or Splunk for on-premises/hybrid environments. These tools are crucial for correlating events across diverse Zero Trust components, providing a comprehensive, real-time view of your security posture.

Automating Policy Enforcement and Remediation

Manual security responses are simply too slow for modern, rapidly evolving threats. Automation is a cornerstone of an effective, continuously improving Zero Trust architecture. It allows policies to adapt in real-time, enforcing security with speed and precision.

Dynamic Policies and Automated Responses

Zero Trust policies should not be static. They must be dynamic, adapting in real-time based on changing context, risk scores, and threat intelligence.

Examples of automation in Zero Trust:

- **Conditional Access:** If a user tries to access sensitive data from an unmanaged device or an unusual location, conditional access policies (e.g., in Microsoft Entra ID, formerly Azure Active Directory as of 2026-05-28) can automatically prompt for MFA, block access, or force a password reset.

- **Device Compliance:** An Endpoint Detection and Response (EDR) solution detects malware on a device. Automated policies can immediately quarantine the device, revoke its access to corporate resources, and trigger remediation steps.
- **Micro-segmentation:** If a vulnerability is detected in a specific application, automated tools can instantly adjust micro-segmentation policies to isolate that application, preventing lateral movement.
- **Threat Hunting:** SOAR playbooks can automatically query threat intelligence feeds when a suspicious IP address or file hash is observed, enriching incident data for faster analysis.

🧠 **Important:** Automation must be carefully designed and thoroughly tested. Poorly configured automation can lead to legitimate users being locked out of critical systems or, worse, inadvertently create new security bypasses. Start with simple, well-understood automations and iterate as confidence grows.

Integrating Threat Intelligence

External threat intelligence provides crucial context that allows your Zero Trust policies to be more proactive and effective. It transforms your security from purely reactive to intelligently predictive.

Enhancing Zero Trust with Global Insights

Threat intelligence feeds provide up-to-date information about new vulnerabilities, active attack campaigns, malicious IP addresses, phishing domains, and other indicators of compromise (IoCs). Integrating this into your Zero Trust strategy allows for:

- **Proactive Blocking:** Automatically block access from known malicious IP ranges or prevent downloads of files with known bad hashes at your network edge or endpoint.
- **Risk Scoring:** Dynamically adjust user and device risk scores based on their interaction with known threat indicators, leading to more granular access decisions.
- **Faster Detection:** Improve the accuracy of your SIEM alerts by correlating internal events with external threat data, reducing false positives and highlighting true threats.

⚡ **Quick Note:** Threat intelligence can come from various sources, including commercial vendors, open-source projects, and government agencies. Ensure the feeds are relevant to your organization's threat profile and integrate them carefully to avoid overwhelming your systems with irrelevant data. Prioritize high-fidelity, actionable intelligence.

Emerging Trends and the Future of Zero Trust

The core principles of Zero Trust are enduring, but the technologies and methods for implementing them are constantly evolving. Staying abreast of these trends is crucial for future-proofing your Zero Trust architecture.

The Road Ahead for Zero Trust

Several key trends are shaping the future of Zero Trust:

- **AI and Machine Learning for Anomaly Detection:** AI/ML algorithms are becoming increasingly sophisticated at identifying subtle anomalies in user behavior, device patterns, and network traffic that human analysts might miss. This moves Zero Trust from purely rule-based to intelligence-driven, enabling more predictive security.
- **Identity-First Security:** As traditional network perimeters dissolve, identity becomes the primary control plane. Future Zero Trust implementations will further emphasize strong identity verification and continuous authentication, potentially moving beyond traditional MFA to continuous behavioral biometrics and adaptive access based on real-time risk.
- **Quantum-Resistant Cryptography (Post-Quantum Cryptography - PQC):** While still in research and standardization (as of 2026-05-28), the advent of quantum computing poses a long-term threat to current cryptographic standards. Future Zero Trust architectures will need to incorporate PQC to ensure long-term data confidentiality and integrity against quantum attacks.
- **Zero Trust Network Access (ZTNA) Evolution:** ZTNA has become a critical component for secure remote access in Zero Trust. Expect ZTNA solutions to become more integrated, offering deeper inspection capabilities, broader application support, and seamless integration with other security services like CASB (Cloud Access Security Broker) and SWG (Secure Web Gateway) into comprehensive SASE (Secure Access Service Edge) frameworks.

- **Data-Centric Zero Trust:** Beyond network and identity, a greater focus will be placed on protecting the data itself, regardless of where it resides. This involves advanced data classification, end-to-end encryption, and granular access controls directly tied to data sensitivity and classification labels.
- **Automated Policy Generation and Optimization:** AI-driven tools may soon assist in generating optimal Zero Trust policies, continuously evaluating their effectiveness, and suggesting refinements to balance security and usability across complex environments.

Zero Trust is not merely a set of technologies; it's a strategic philosophy that will continue to adapt and thrive as the cybersecurity landscape evolves. Its enduring relevance lies in its adaptive nature.

Mini-Challenge: Zero Trust Metrics

It's time to put your strategic thinking to the test!

Challenge: Imagine you are leading the continuous improvement efforts for Zero Trust in a medium-sized enterprise. Propose three key metrics or Key Performance Indicators (KPIs) you would track to measure the ongoing effectiveness and improvement of your Zero Trust identity and access management (IAM) initiative. For each metric, briefly explain why it's important and what insight it provides.

Hint: Think about what Zero Trust IAM aims to prevent (e.g., unauthorized access, credential compromise) and what it aims to achieve (e.g., efficient, secure access). Consider both security effectiveness and user experience.

What to observe/learn: This exercise helps you connect the theoretical benefits of Zero Trust with concrete, measurable outcomes, which is crucial for demonstrating value, securing resources, and guiding future improvements within an organization.

Common Pitfalls & Troubleshooting in Continuous Improvement

Even with the best intentions, maintaining and continuously improving a Zero Trust architecture can encounter significant challenges. Recognizing these pitfalls and knowing how to troubleshoot them is crucial.

- **Stagnant Policies:**
    - **Pitfall:** Zero Trust policies are defined at the outset but are rarely reviewed or updated. As the environment changes (new applications, users, threats), these policies become outdated, leading to security gaps or unnecessary friction for legitimate users.
    - ⚠️ **What can go wrong:** Outdated policies can create shadow IT, allow unauthorized access, or block critical business functions.
    - **Troubleshooting:** Establish a clear, recurring schedule for policy review (e.g., quarterly or bi-annually) with assigned ownership for specific policy sets. Integrate policy updates into your existing change management processes. Leverage automation and policy validation tools to identify rule redundancies, conflicts, or unused policies.
- **Alert Fatigue and Unactionable Data:**
    - **Pitfall:** Over-monitoring leads to a deluge of alerts from various systems, many of which are false positives or low priority. Security teams become overwhelmed, potentially missing critical threats amidst the noise.
    - ⚠️ **What can go wrong:** Critical security incidents can be missed, leading to delayed response and increased breach impact.
    - **Troubleshooting:** Refine SIEM rules and SOAR playbooks to focus on high-fidelity alerts and critical events. Tune detection thresholds and integrate threat intelligence to filter out known benign activity. Implement a structured alert triage process and leverage SOAR automation to filter, enrich, and automatically respond to common, low-risk alerts. Prioritize "signal over noise."

- **Lack of Organizational Buy-in for Ongoing Efforts:**
  - **Pitfall:** Initial Zero Trust implementation gets executive support and funding, but sustained resources, budget, and cross-departmental collaboration wane over time, hindering continuous improvement efforts.
  - ⚠️ **What can go wrong:** Zero Trust initiatives stall, leading to incomplete protection and a fragmented security posture.
  - **Troubleshooting:** Regularly communicate the value and ROI of Zero Trust to all stakeholders, highlighting averted breaches, compliance achievements, and improved operational efficiency. Emphasize the iterative nature of Zero Trust from the very beginning. Foster a culture of shared security responsibility across IT, development, and business units through training and clear communication.
- **Over-reliance on a Single Vendor Solution:**
  - **Pitfall:** While integrated solutions can be efficient, relying solely on one vendor for all Zero Trust components can lead to vendor lock-in, limit flexibility, and create single points of failure if that vendor has a vulnerability or outage.
  - ⚠️ **What can go wrong:** Limited ability to adapt to new threats, higher costs, or single points of failure that impact your entire security posture.
  - **Troubleshooting:** Adopt a multi-vendor strategy where appropriate, focusing on interoperability and open standards (e.g., using SAML/OIDC for identity across different services). Prioritize solutions that offer robust APIs for integration with your existing security ecosystem. Regularly assess vendor roadmaps to ensure alignment with your long-term Zero Trust vision.

Summary

Congratulations on completing our Zero Trust Security learning guide! You've journeyed from understanding the fundamental shift in security thinking to strategizing its continuous evolution in a dynamic threat landscape.

Here are the key takeaways from this final chapter:

- **Zero Trust is a Journey:** It's an iterative process requiring constant adaptation and improvement, not a one-time deployment. The "assume breach" mentality necessitates continuous vigilance.

- **Continuous Improvement Cycle:** The Plan-Do-Check-Act (PDCA) model provides a robust framework for systematically refining Zero Trust policies and controls.
- **Monitoring is Paramount:** Centralized logging, SIEM (Security Information and Event Management), and SOAR (Security Orchestration, Automation, and Response) are essential for real-time visibility, threat detection, and understanding policy effectiveness.
- **Automation is Key:** Dynamic policies and automated responses enable rapid threat containment, remediation, and policy enforcement, drastically reducing the window of opportunity for attackers.
- **Threat Intelligence Enhances Proactivity:** Integrating external threat data allows for more intelligent, predictive, and proactive security measures, improving detection accuracy and blocking known threats.
- **Future-Proofing:** Emerging trends like AI/ML for anomaly detection, identity-first security, quantum-resistant cryptography, and the evolution of ZTNA/SASE will continue to shape and enhance Zero Trust architectures.

The world of cybersecurity is dynamic, and your Zero Trust architecture must be equally agile. By embracing continuous improvement, leveraging automation and threat intelligence, and staying informed about future trends, you can build and maintain a security posture that truly protects your organization in the face of evolving and sophisticated threats.

References

- Zero Trust adoption framework overview | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview
- What is Zero Trust? | Microsoft Learn: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
- Principles to help you design and deploy a zero trust architecture | NCSC GitHub: https://github.com/ukncsc/zero-trust-architecture
- NIST Special Publication 800-207, Zero Trust Architecture: https://csrc.nist.gov/publications/detail/sp/800-207/final
- Microsoft Entra Conditional Access documentation: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview
- Microsoft Sentinel documentation: https://learn.microsoft.com/en-us/azure/sentinel/overview

This page is AI-assisted and reviewed. It references official documentation and recognized resources where relevant.