
ZERO TRUST INNOVATORS

Password

SVP Cybersecurity Strategy and Group Fellow

John Kindervag

ZERO TRUST INNOVATORS

NSTAC Zero Trust Briefing
September 8, 2020

John Kindervag
ON2IT

Sec. 3. Modernizing Federal Government Cybersecurity.

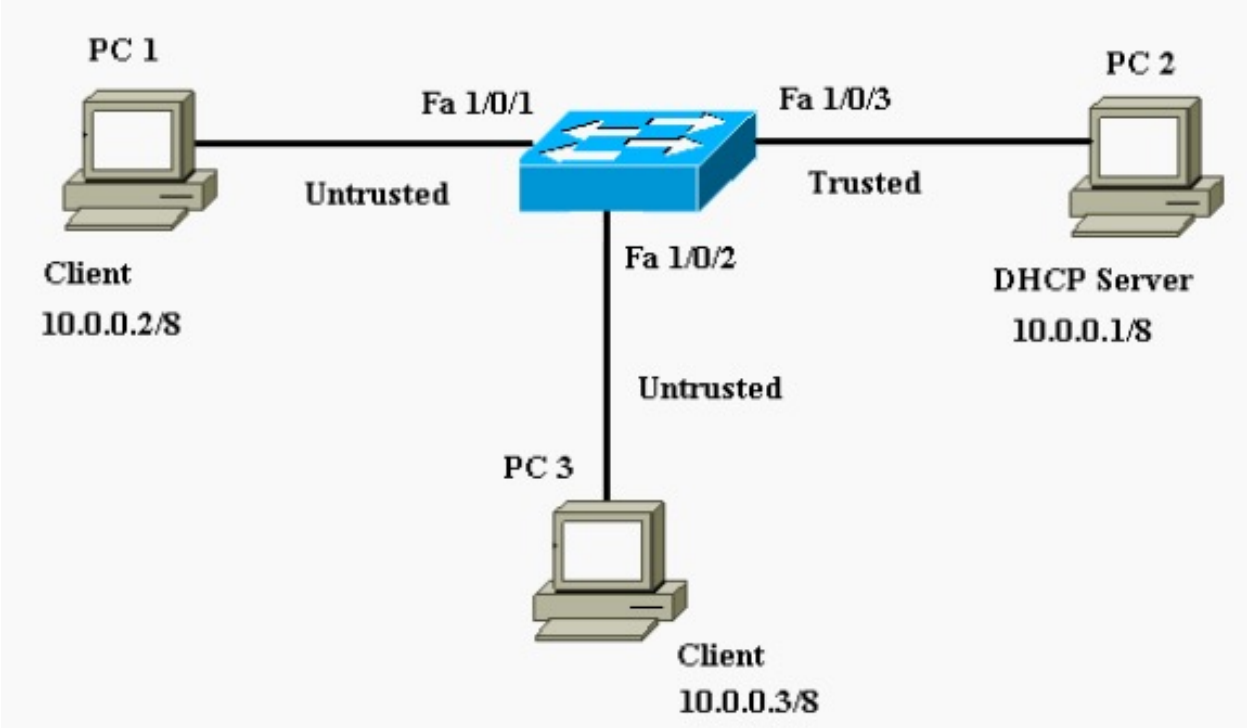
(a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

requires the Federal Government to partner with the private sector. The

Some History

- The Turn of the Century:
  The Trust Model and the Adaptive Security Algorithm

The Trust Model and the Adaptive Security Algorithm



PIX Firewall Adaptive Security

The Adaptive Security feature applies to the dynamic translation slots and static translation slots created with the static and mailhost commands. The Adaptive Security algorithm is a very stateful approach to security. Every inbound packet is checked against the Adaptive Security algorithm and against connection state information in memory. This stateful approach to security is regarded in the industry as being far more secure than a stateless packet screening approach.

Adaptive Security follows these rules:

- Allow any TCP connections that originate from the inside network.

Some History

- The Turn of the Century:
  The Trust Model and the Adaptive Security Algorithm
- June 2008 – Joined Forrester Research

Some History

- The Turn of the Century:
  The Trust Model and the Adaptive Security Algorithm
- June 2008 – Joined Forrester Research
- Fall 2008 – First Zero Trust Presentation at a Country Club in Montreal. Four additional presentations followed at Country Clubs along the East Coast of the US

Some History

- The Turn of the Century:
  The Trust Model and the Adaptive Security Algorithm
- June 2008 – Joined Forrester Research
- Fall 2008 – First Zero Trust Presentation at a Country Club in Montreal. Four additional presentations followed at Country Clubs along the East Coast of the US
- Two Years of Zero Trust Research

Some History

- The Turn of the Century:
  The Trust Model and the Adaptive Security Algorithm
- June 2008 – Joined Forrester Research
- Fall 2008 – First Zero Trust Presentation at a Country Club in Montreal. Four additional presentations followed at Country Clubs along the East Coast of the US
- Two Years of Zero Trust Research
- 2010 – First Zero Trust Report Published:
  “No More Chewy Centers”

No More Chewy Centers

For Security & Risk Professionals

September 14, 2010 | Updated: September 17, 2010

No More Chewy Centers: Introducing The Zero Trust Model Of Information Security

by John Kindervag
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For a generation of information security professionals, this was the motto we grew up with. It was a motto based on trust and the assumption that malicious individuals wouldn't get past the "hard crunchy outside." In today's new threat landscape, this is no longer an effective way of enforcing security. Once an attacker gets past the shell, he has access to all the resources in our network. We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily pierce our current security protections. To confront these new threats, information security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. To help security professionals do this effectively, Forrester has developed a new model for information security, called Zero Trust. This report, the first in a series, will introduce the necessity and key concepts of the Zero Trust Model.

https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

Authentic Zero Trust

- It is a strategy designed to stop data breaches and other cyber-attacks.
- It leverages design principles proven to work over more than a decade
- It uses the standard 5-step methodology for implementing a Zero Trust architecture
- It provides demonstrable, positive security outcomes for companies who adopt Zero Trust

Some Zero Trust Misconceptions

- Zero Trust means making a system trusted

- Zero Trust is about identity

- There are Zero Trust products

- Zero Trust is complicated

ZERO TRUST INNOVATORS

Zero Trust is Strategic
Zero Trust is Implementable

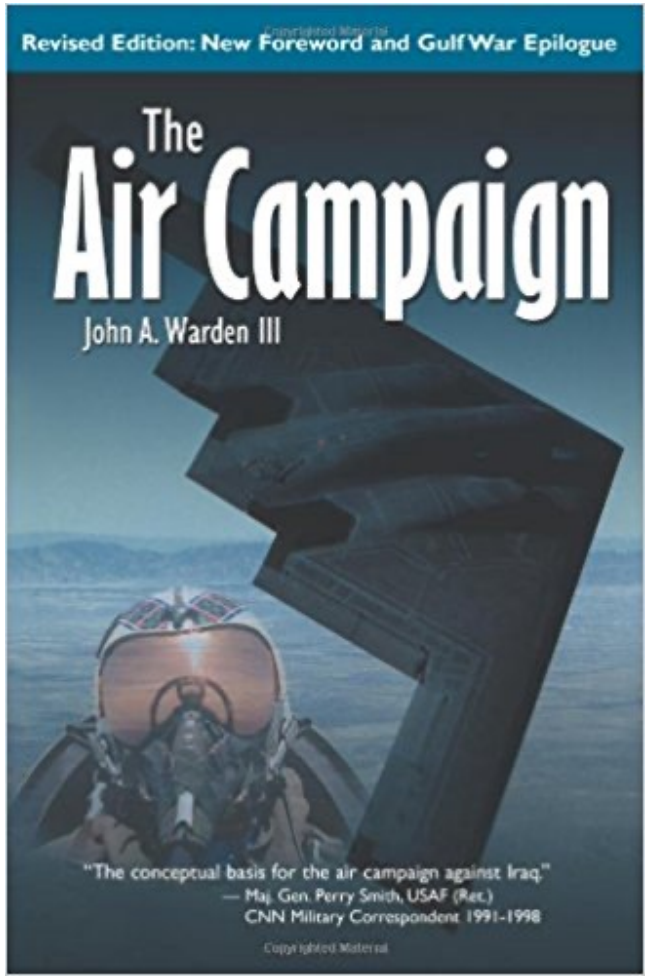
Zero Trust is Strategic

Zero Trust is Implementable

ZERO TRUST INNOVATORS

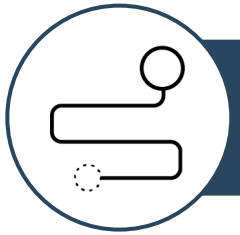
Strategic Engagement

John Warden

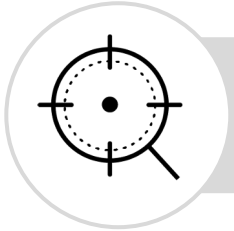


The Four Levels of Strategic Engagement

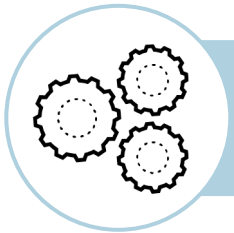
Grand Strategy — The Ultimate Goal



Strategy — The Big Idea



Tactics — The Things You Use



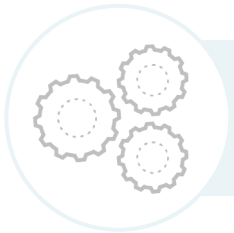
Operations — The Way You Use Them

The Four Levels of Cyber War

Grand Strategy | Stop Data Breaches

Strategy | Zero Trust

Tactics | Tools & Techniques



Operations | Platform & Policies

ZERO TRUST INNOVATORS

Cyber Security Grand Strategy: Prevent Data Breaches

The Washington Post
Democracy Dies in Darkness

Federal Insider

Hacks of OPM databases compromised 22.1 million people, federal authorities say

By Ellen Nakashima July 9, 2015

ZERO TRUST INNOVATORS

Committee on Oversight and Government Reform

U.S. House of Representatives

114th Co[illegible]

The OPM Data Breach: How the
National Security for M

Majority St[illegible]

Hon. Jason Chaf
Committee on Oversight a

Hon. Mark Mead
Subcommittee on Gov

Hon. Will Hurd, Chairman
Subcommittee on Information Technology

September 7, 2016

www.oversight.house.gov

Recommendation 2 – Reprioritize Federal Information Security Efforts Toward a Zero Trust Model

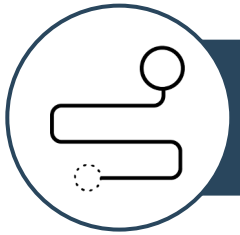
OMB should provide guidance to agencies to promote a zero trust IT security model. The OPM data breaches discovered in 2014 and 2015 illustrate the challenge of securing large, and therefore high-value, data repositories when defenses are geared toward perimeter defenses. In both cases the attackers compromised user credentials to gain initial network access, utilized tactics to elevate their privileges, and once inside the perimeter, were able to move throughout OPM's network, and ultimately accessed the "crown jewel" data held by OPM. The agency was unable to visualize and log network traffic which led to gaps in knowledge regarding how much data was actually exfiltrated by attackers.

To combat the advanced persistent threats seeking to compromise or exploit federal government IT networks, agencies should move toward a "zero trust" model of information security and IT

[55] Gov't Accountability Office, GAO-11-634, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management* (Oct. 2011) (stating the average CIO's tenure is two years).

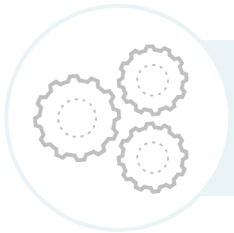
The Four Levels of Cyber War

Grand Strategy — Stop Data Breaches



Strategy — Zero Trust

Tactics — Tools & Techniques



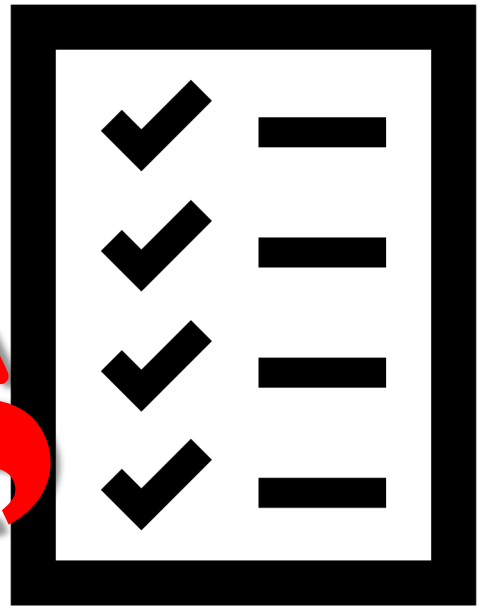
Operations — Platform & Policies

Not a Strategy

3-1 | Expense in depth isn't a strategy

Source: https://www.forrester.com/Forresters+TargetedAttack+Hierarchy+Of+Needs+Assess+Your+Core+Capabilities/fulltext/-/E-RES107121

TACTICS



TRUST

is a dangerous

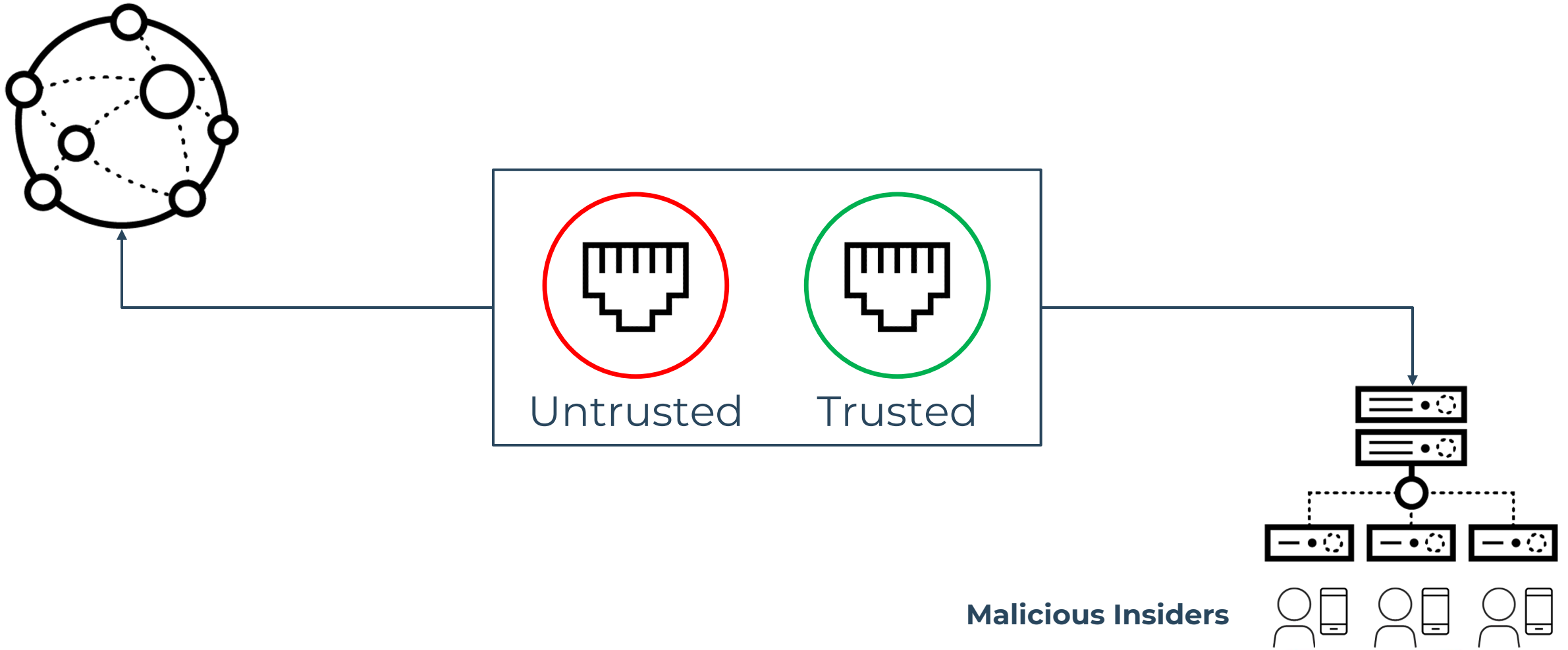
VULNERABILITY

that is

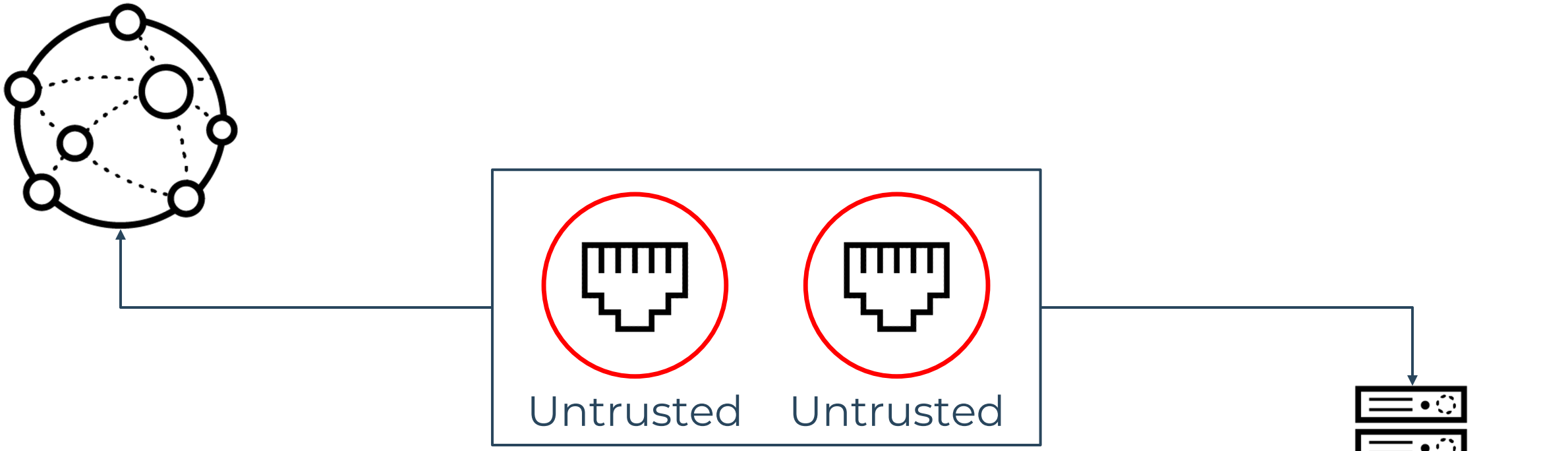
EXPLOITED

by **MALICIOUS** actors

Which One Goes to the Internet?



Zero Trust



People are NOT Packets!

ZERO TRUST INNOVATORS

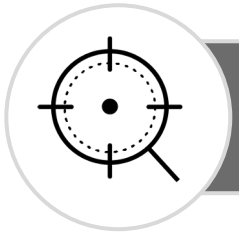
Zero Trust is Strategic

Zero Trust is Implementable

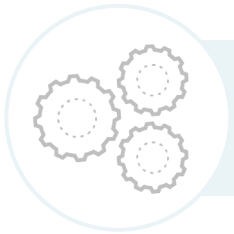
The Four Levels of Cyber War

Grand Strategy | Stop Data Breaches

Strategy | Zero Trust



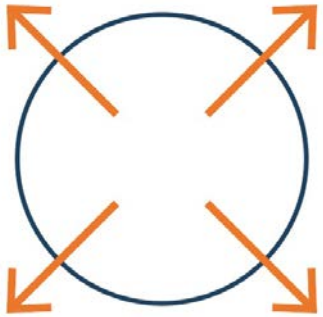
Tactics | Tools & Techniques



Operations | Platform & Policies

Zero Trust Design Concepts

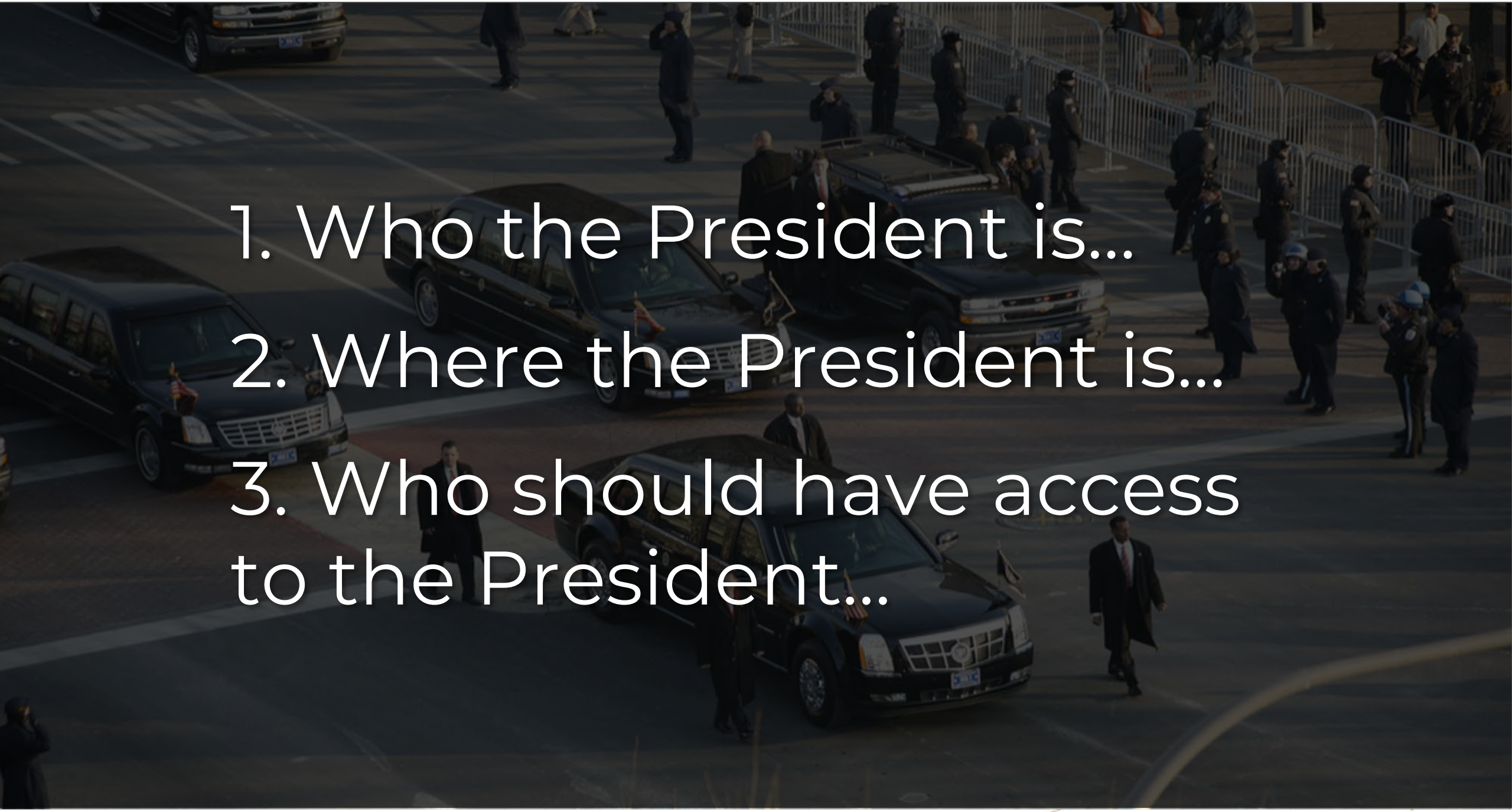
Focus on
business outcomes

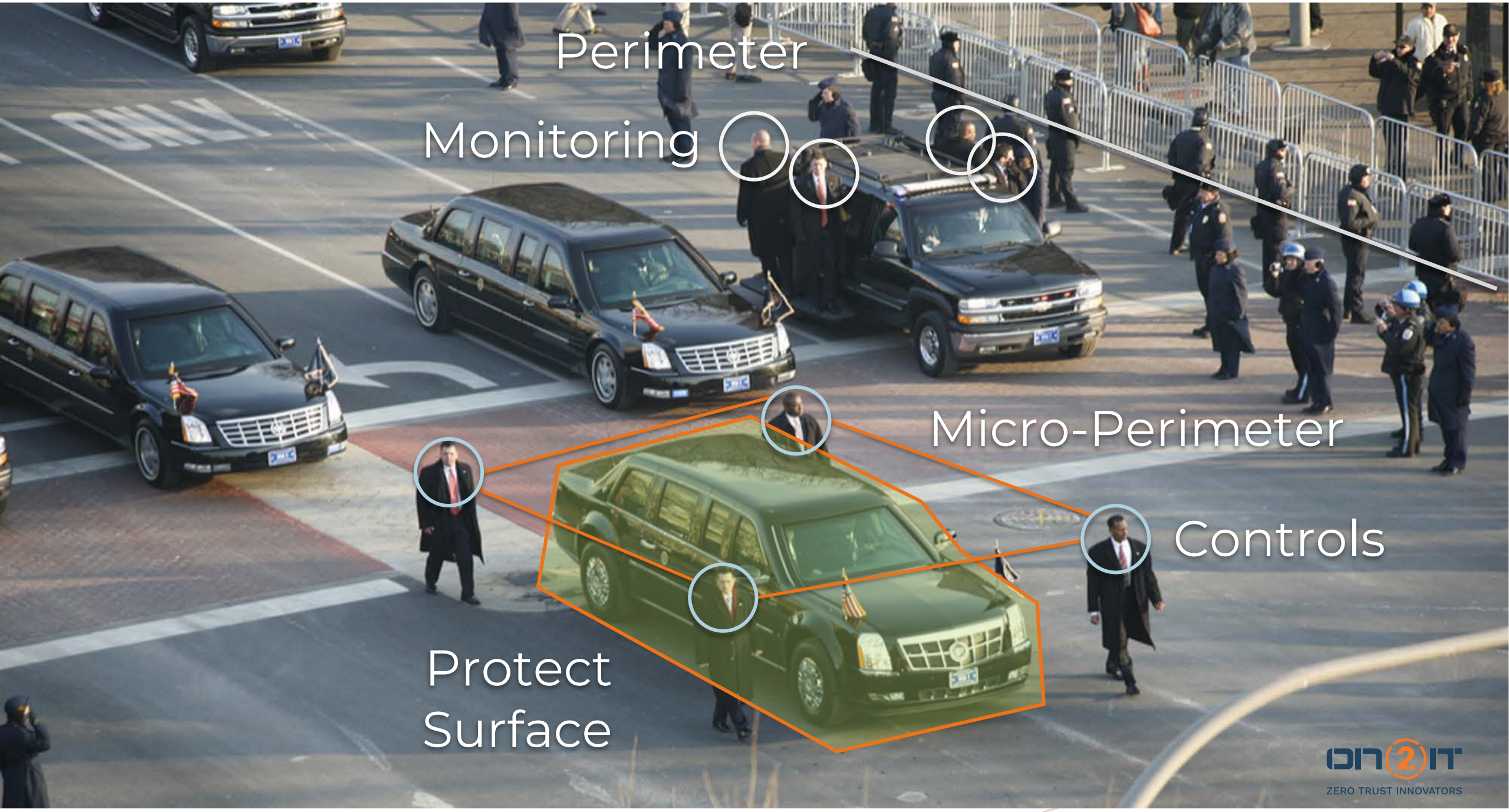


Design from
the inside out

Determine who/what
needs access

Inspect and log
all traffic


1. Who the President is...
2. Where the President is...
3. Who should have access to the President...


Perimeter
Monitoring
Micro-Perimeter
Controls
Protect
Surface
ZERO TRUST INNOVATORS


ZERO TRUST

Start Your Zero Trust Journey with the First Step

- Flørli stairs in Lysefjorden, Norway

The 5-Step Methodology for Deploying Zero Trust Guides Your Journey

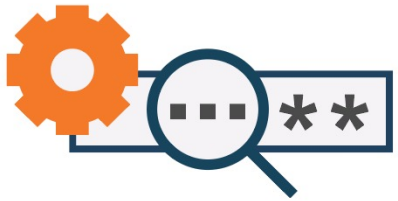
DAAS

Data Application Assets Services

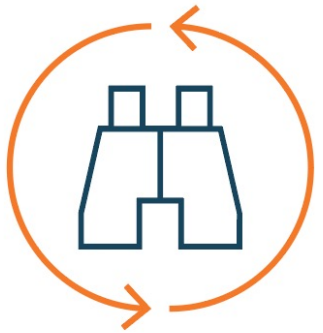
Define the protect surface

Map the transaction flows

Build a Zero Trust architecture



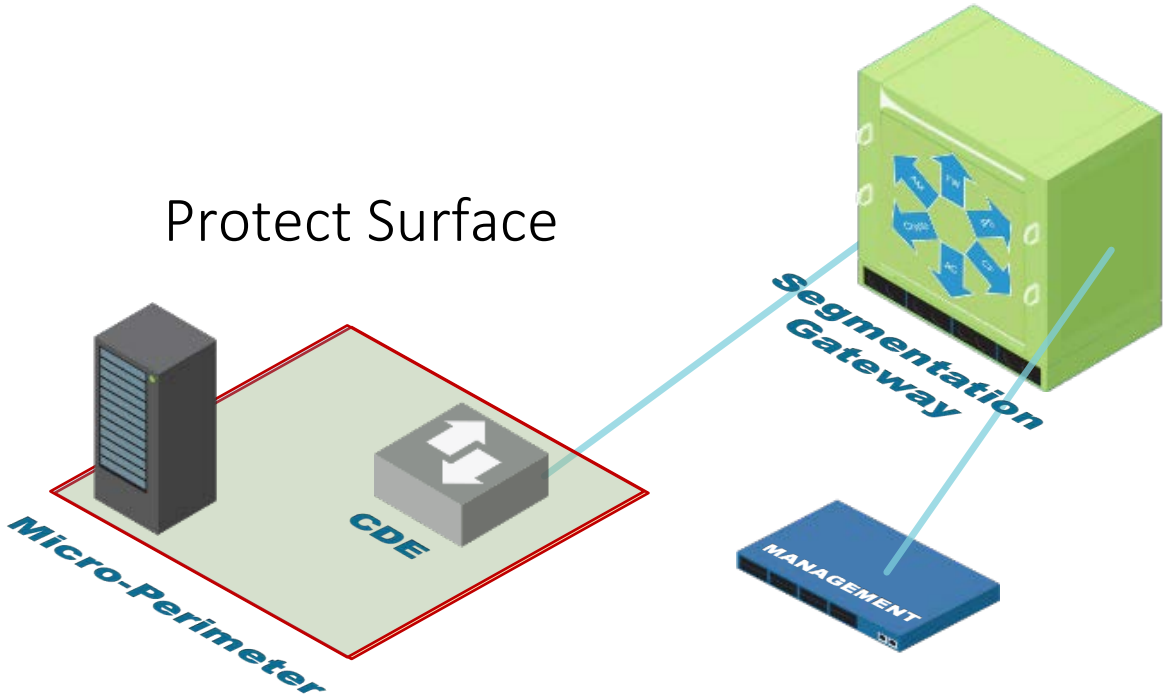
Create Zero Trust policy



Monitor and maintain

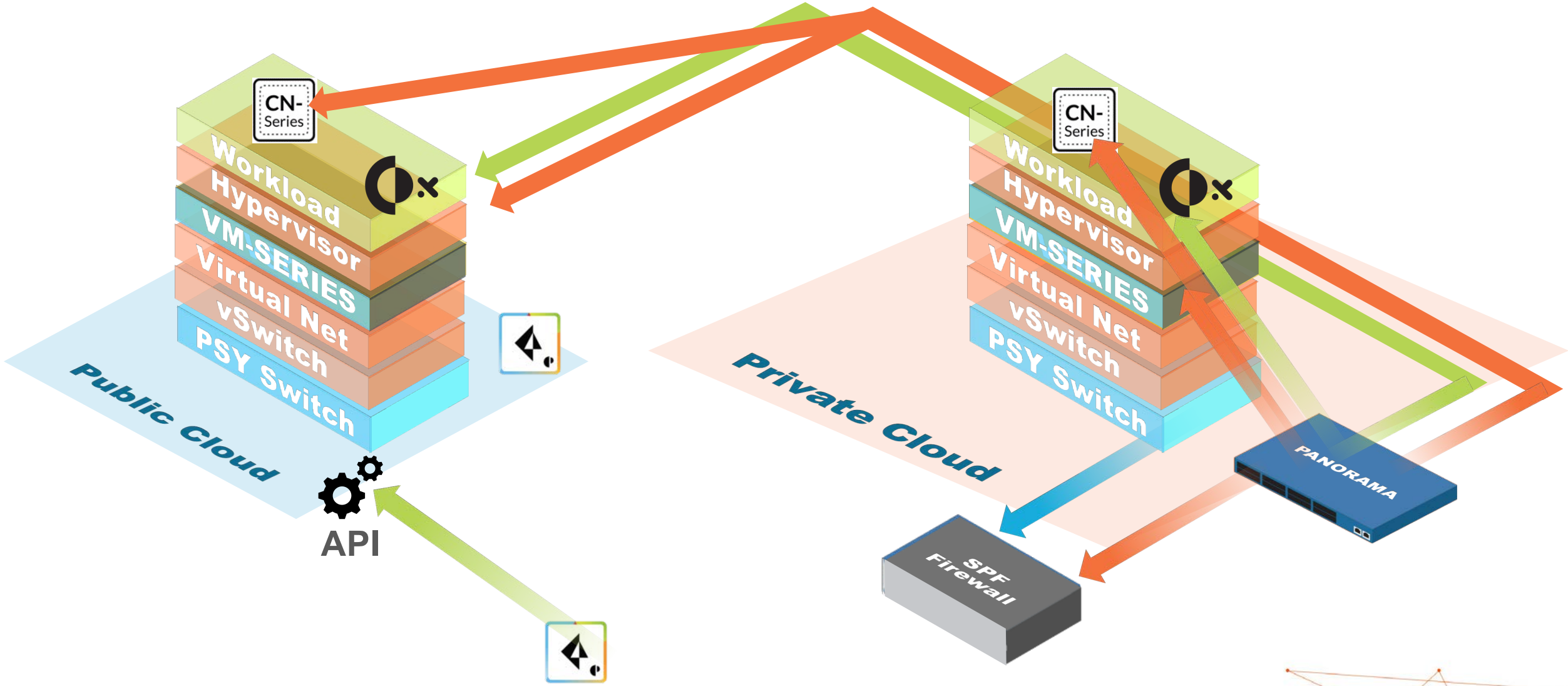
ZERO TRUST INNOVATORS

Zero Trust Defines Network Segmentation



1. Why are you segmenting?
2. How are you enforcing segmentation at Layer 2-7?

Extend Zero Trust to Public and Private Clouds



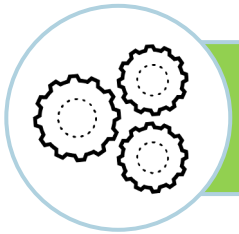
ZERO TRUST INNOVATORS

The Four Levels of Cyber War

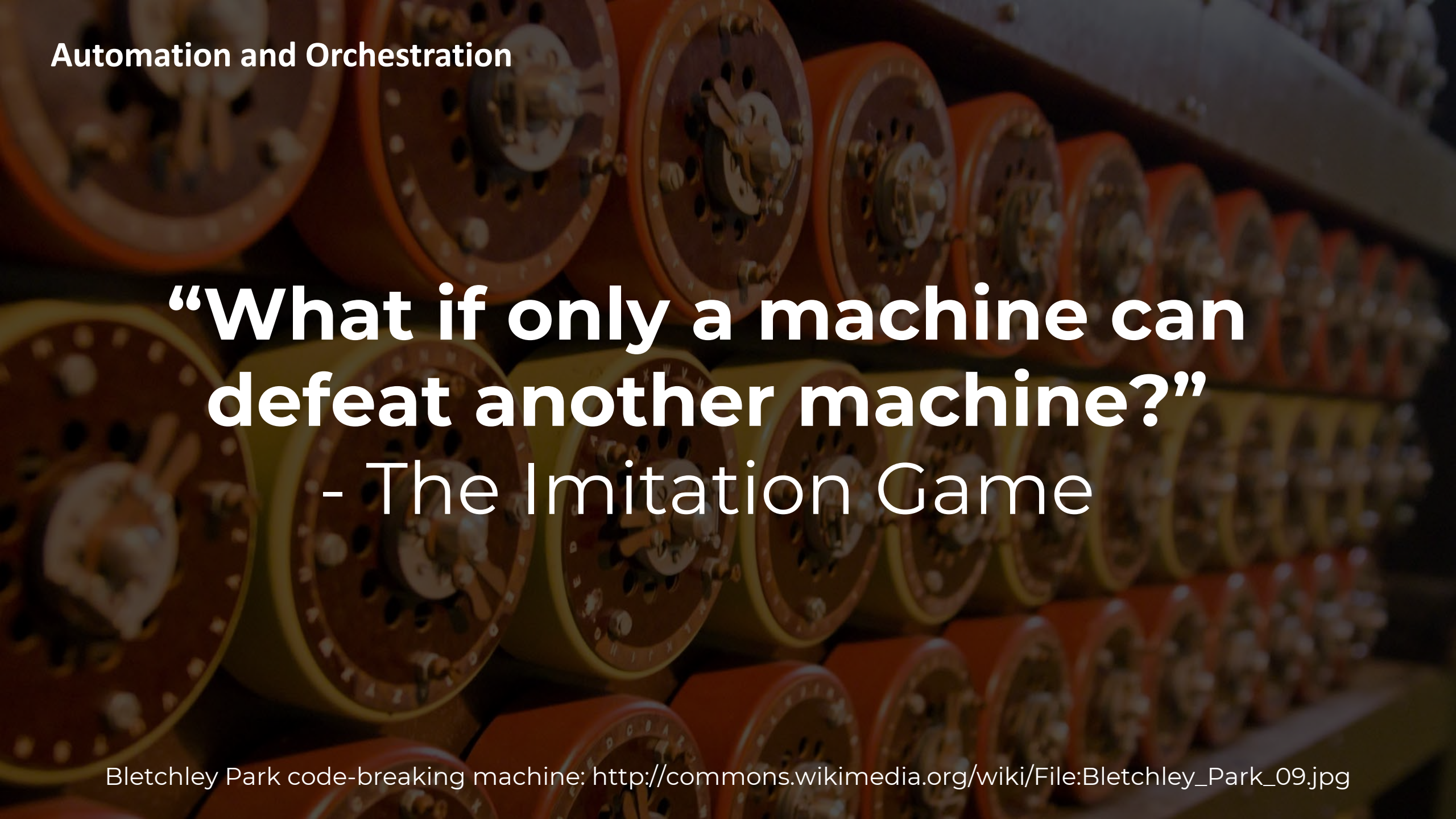
Grand Strategy — Stop Data Breaches

Strategy — Zero Trust

Tactics — Tools & Techniques



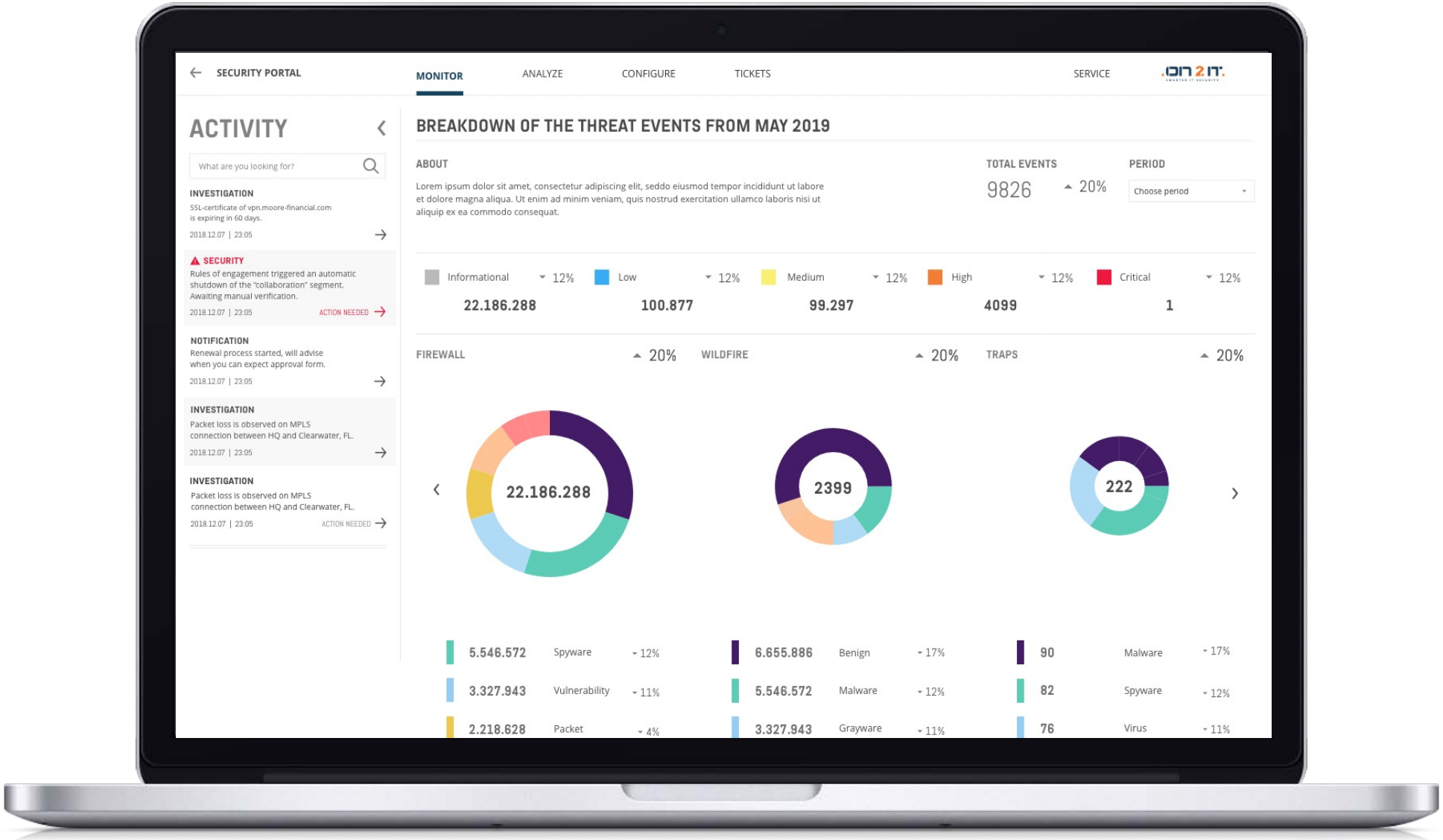
Operations — Platform & Policies



“What if only a machine can defeat another machine?”

- The Imitation Game

Bletchley Park code-breaking machine: http://commons.wikimedia.org/wiki/File:Bletchley_Park_09.jpg



on2it.net/auxo-demo/

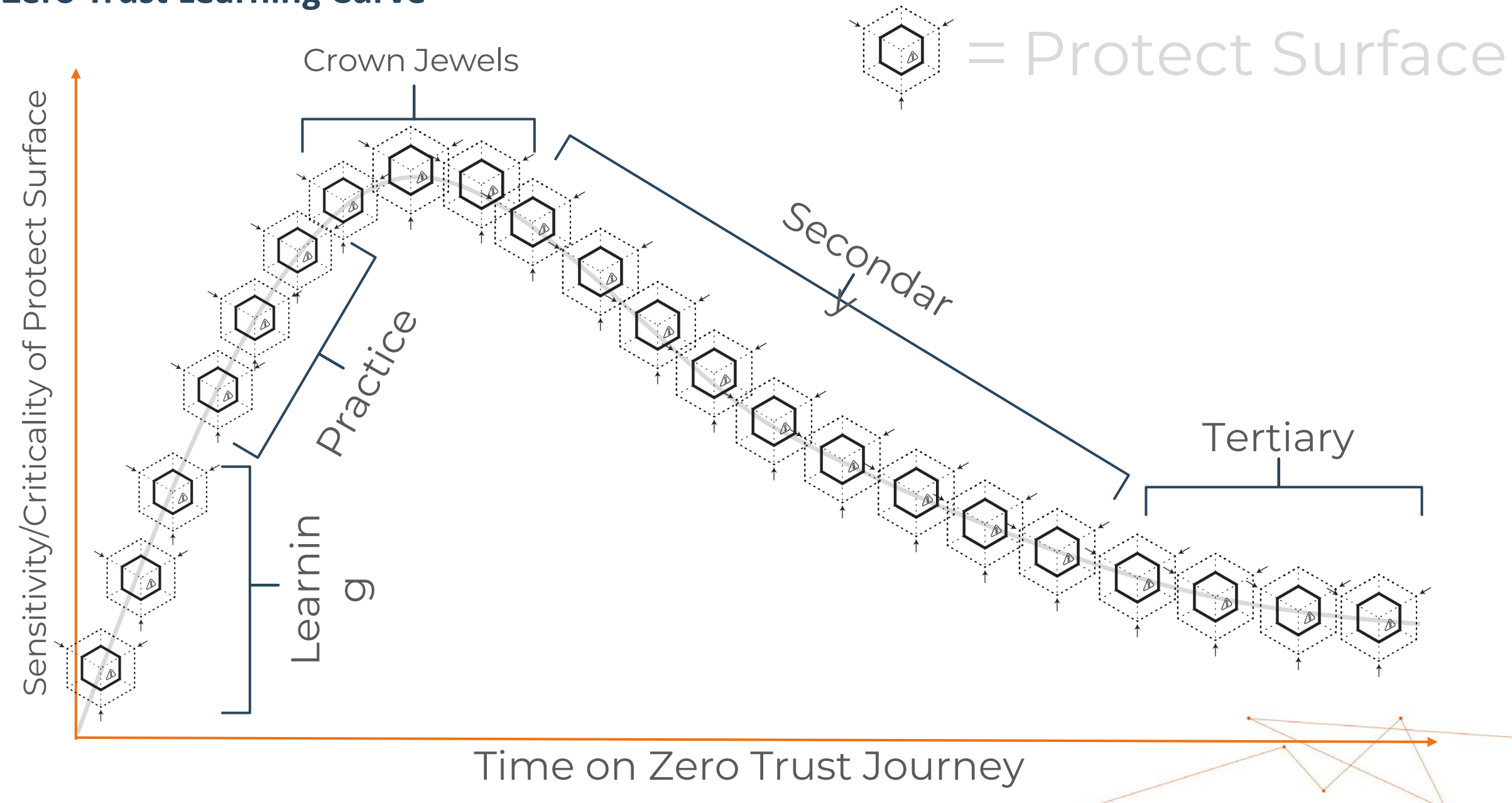
The Kipling Method of Zero Trust Rule Writing

Who	What	When	Where	Why	How
User ID	**Application ID**	Time Limitations	**Device ID**	Classification	**Content ID**
Auth type			System Object	Data ID	Threat Protection
			Workload		SSL Decryption
			Geolocation		URL Filtering
					Wildfire

Cloud:
IF Who (UID) = Sales, What (AID) = Salesforce, When (TOD) = Working Hours, Where (LOC) = US, Why (CLASS) = Toxic, How (CID) = SFDC_CID, THEN Allow.

On Prem:
IF Who (UID) = Epic_Users, What (AID) = Epic, When (TOD) = Any, Where (LOC) = Epic_Srvr, Why (CLASS) = Toxic, How (CID) = Epic_CID, THEN Allow.

Zero Trust Learning Curve



Zero Trust Maturity Model

Protect Surface _____

DAAS Element _____

	Initial	Repeatable	Defined	Managed	Optimized
 1. Define your Protect Surface	1	2	3	4	5
 2. Map the Transaction Flows	1	2	3	4	5
 3. Architect a Zero Trust Environment	1	2	3	4	5
 4. Create Zero Trust Policy	1	2	3	4	5
 5. Monitor and Maintain the Network	1	2	3	4	5

Total Score _____

STAY IN CONTACT

John Kindervag

+31 88-2266200

info@on2it.net

Twitter.com/kindervag

ON2IT.net

ON2IT

ZERO TRUST INNOVATORS

STAY IN CONTACT

Yuri Bobbert

+31 88-2266200

yuri.bobbert@on2it.net

linkedin.com/in/yuribobbert

ON2IT.net

ON2IT

ZERO TRUST INNOVATORS


ZERO TRUST INNOVATORS