ZERO TRUST INNOVATORS

Authentic Zero Trust

John Kindervag

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

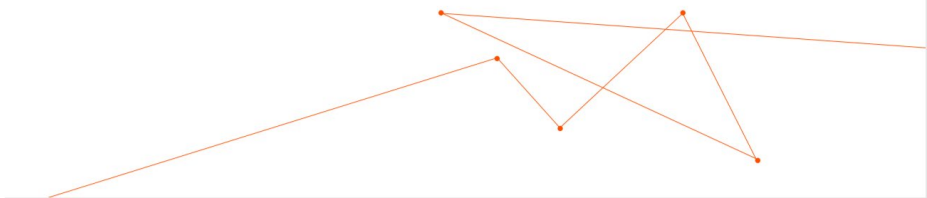
Sec. 3. Modernizing Federal Government Cybersecurity.

(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

Authentic Zero Trust

- It is a strategy designed to prevent data breaches and stop other cyber-attacks from being successful.
- 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

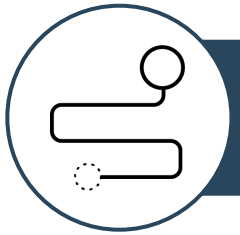
- Zero Trust is about identity

- There are Zero Trust products

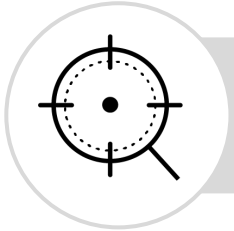
- Zero Trust is complicated

The Four Levels of Strategic Engagement

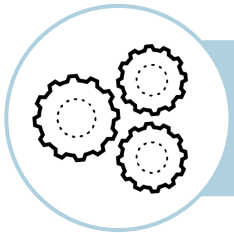
Grand Strategy — The Ultimate Goal



Strategy — The Big Idea



Tactics — The Things You Use



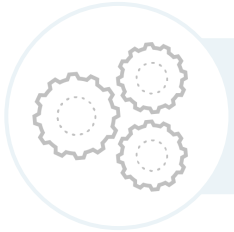
Operations — The Way You Use Them

The Four Levels of Cyber War

Grand Strategy | Stop Data Breaches

Strategy | Zero Trust

Tactics | Tools & Techniques



Operations | Platform & Policies

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 C

The OPM Data Breach: How th
National Security for M

Majority St

Hon. Jason Cha
Committee on Oversight

Hon. Mark Mea
Subcommittee on Gov

Hon. Will Hu
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.

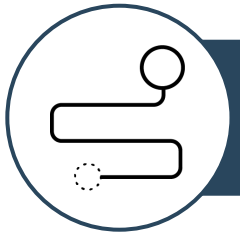
To combat the advanced persistent threats seeking to compromise or exploit federal government IT networks, agencies should move toward a "zero trust" model of information security and IT

[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).

20

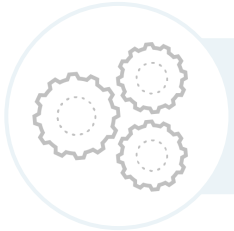
The Four Levels of Cyber War

Grand Strategy | Stop Data Breaches



Strategy | Zero Trust

Tactics | Tools & Techniques



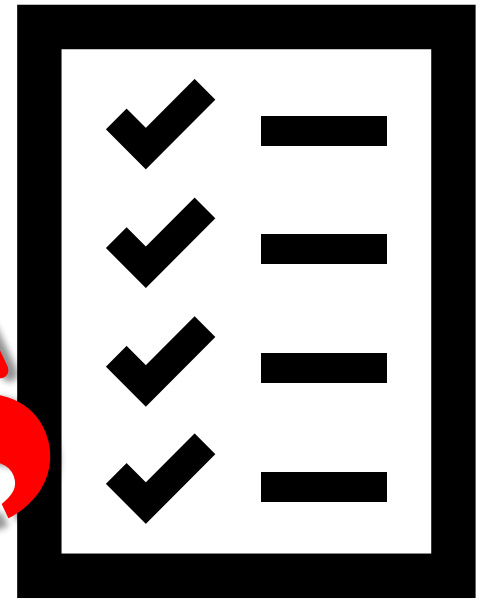
Operations | Platform & Policies

Not a Strategy

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

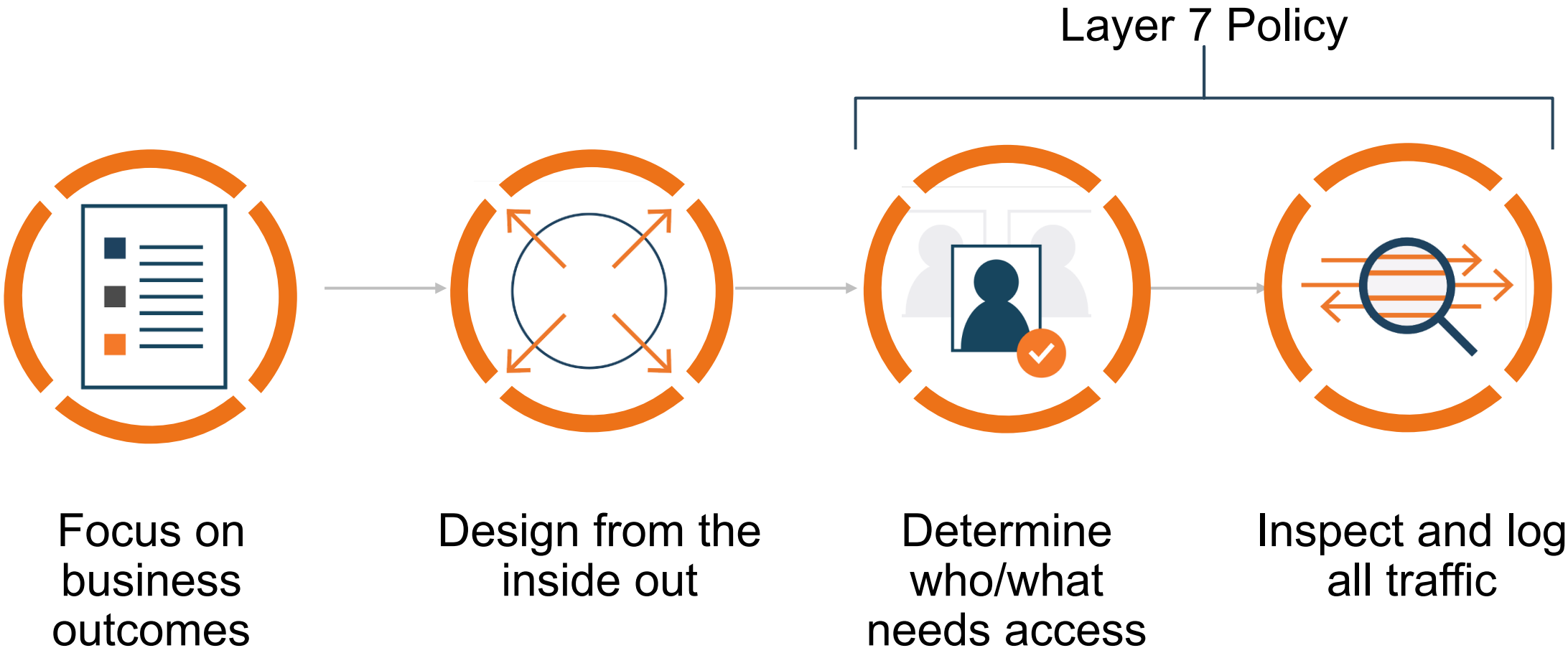
Source: https://www.forrester.com/Forresters+TargetedAttack+Hierarchy+Of+Needs+Assess+Your+Core+Capabilities/fulltext/-/E-RES107121

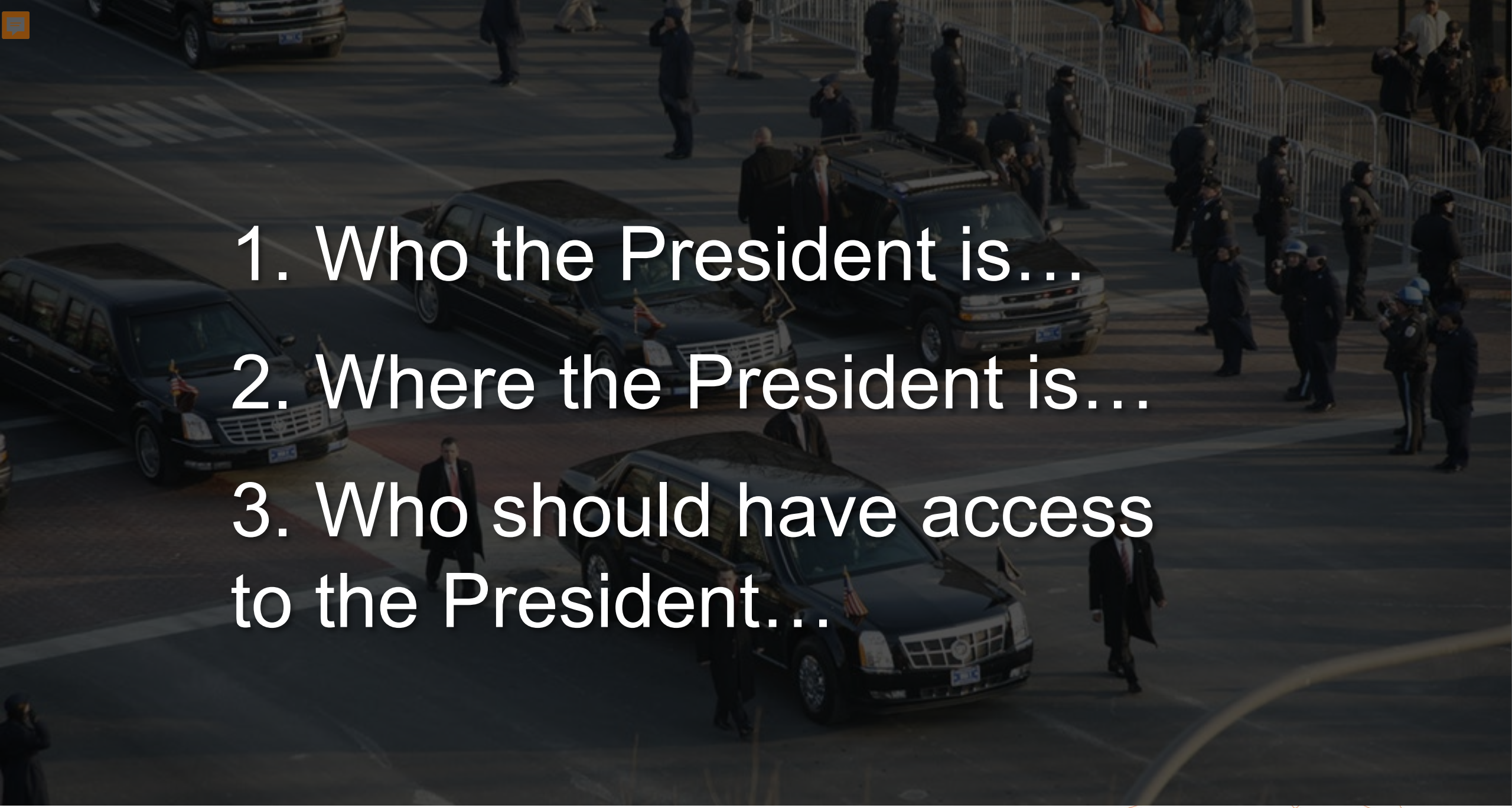
TACTICS

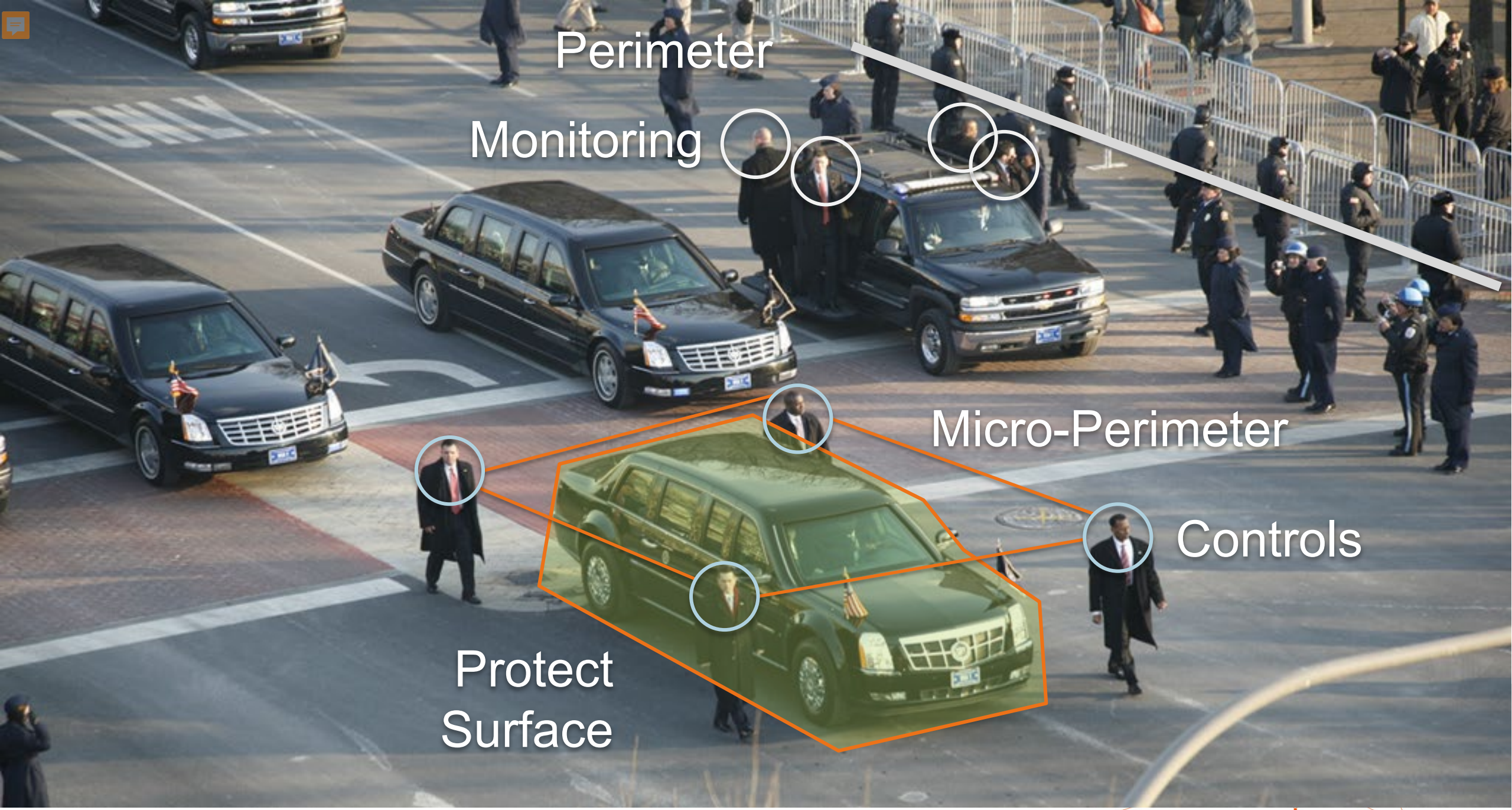



TRUST
is a dangerous
VULNERABILITY
that is
EXPLOITED
by MALICIOUS actors

Zero Trust Design Concepts




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

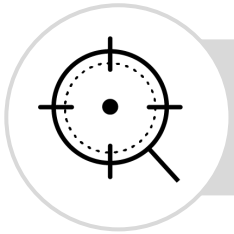

Perimeter
Monitoring
Micro-Perimeter
Controls
Protect
Surface


ZERO TRUST

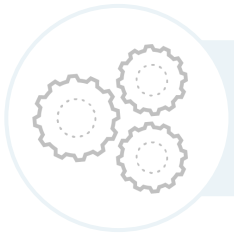
The Four Levels of Cyber War

Grand Strategy — Stop Data Breaches

Strategy — Zero Trust



Tactics — Tools & Techniques



Operations — Platform & Policies

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

Define the protect surface

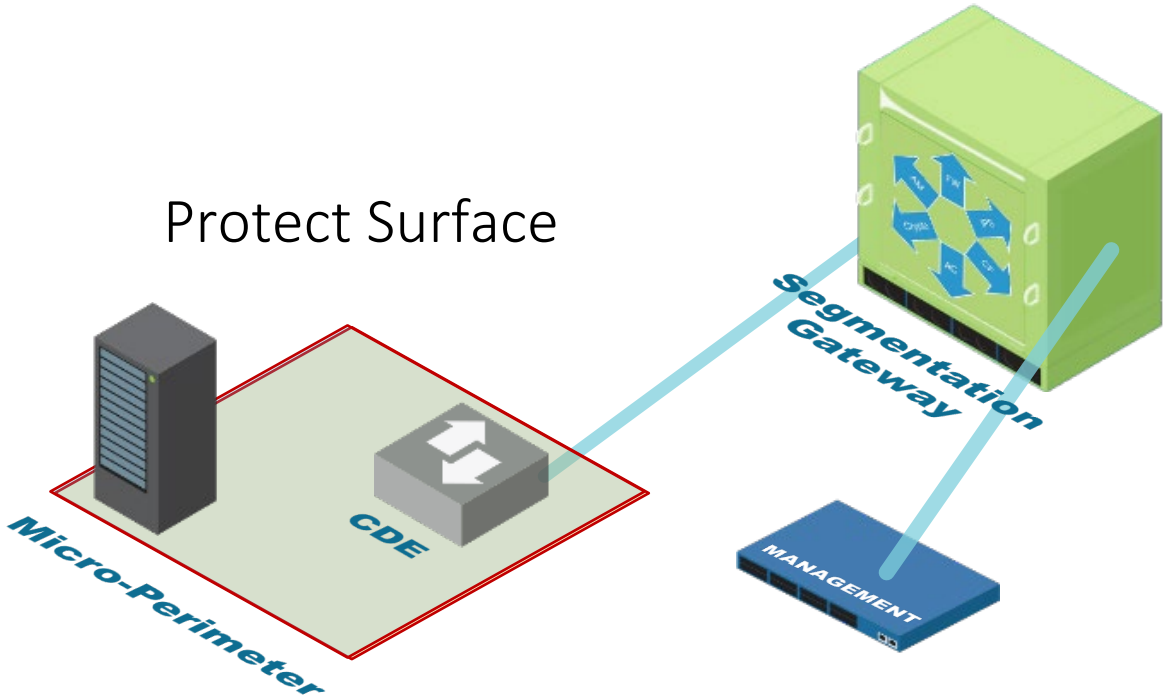
Map the transaction flows

Architect a Zero Trust Environment

Create Zero Trust policy

Monitor and maintain

Zero Trust Defines Network Segmentation



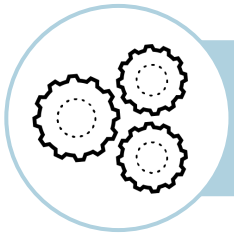
1. Why are you segmenting?
2. How are you enforcing segmentation at Layer 2-7?

The Four Levels of Cyber War

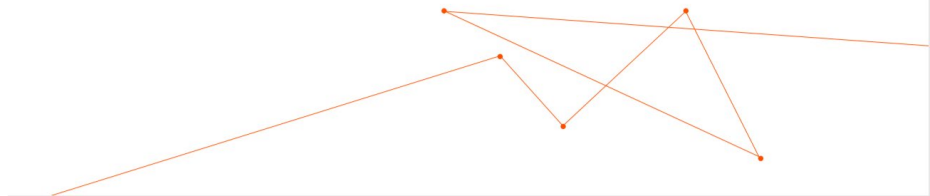
Grand Strategy — Stop Data Breaches

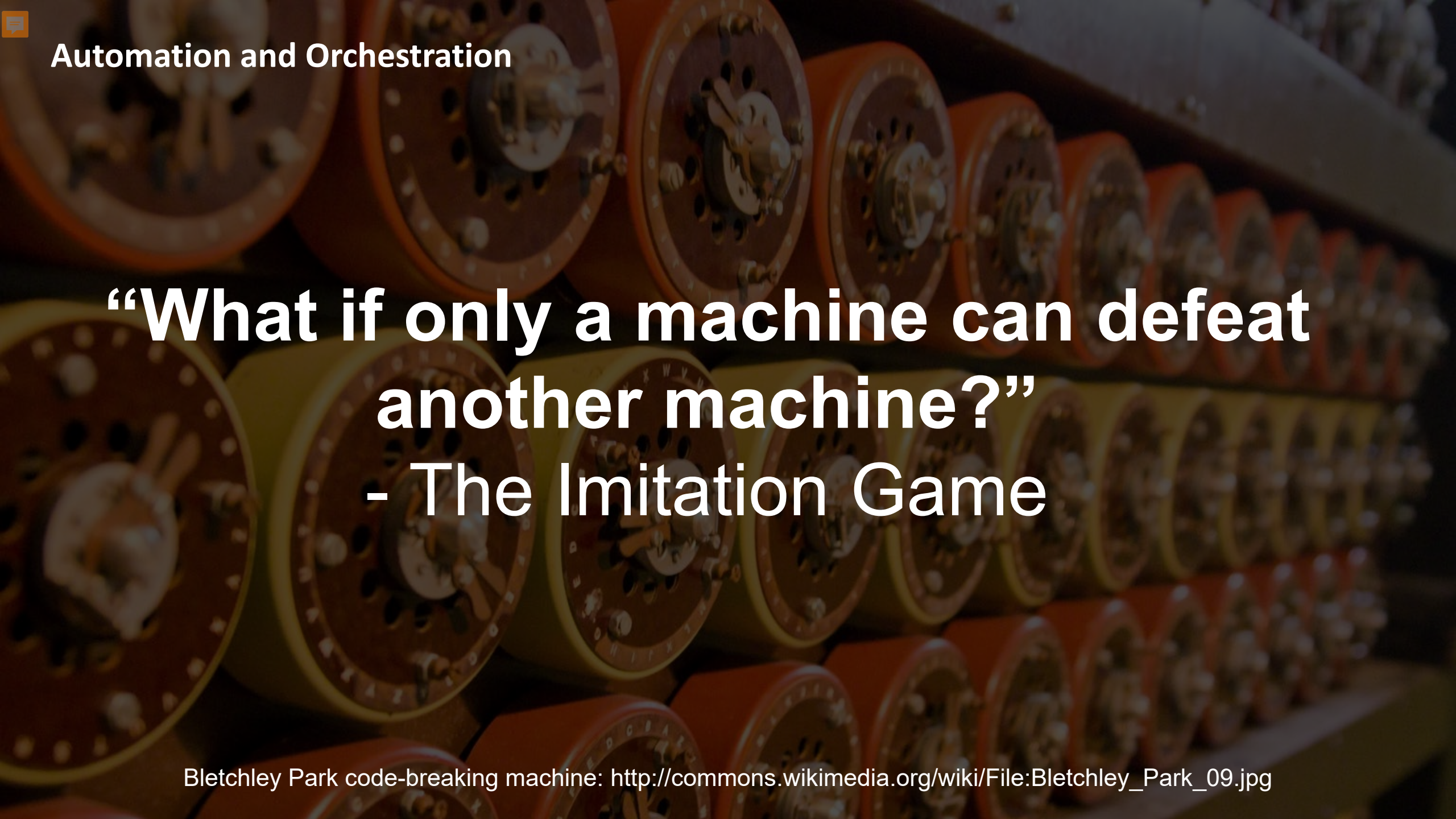
Strategy — Zero Trust

Tactics — Tools & Techniques



Operations — Platform & Policies

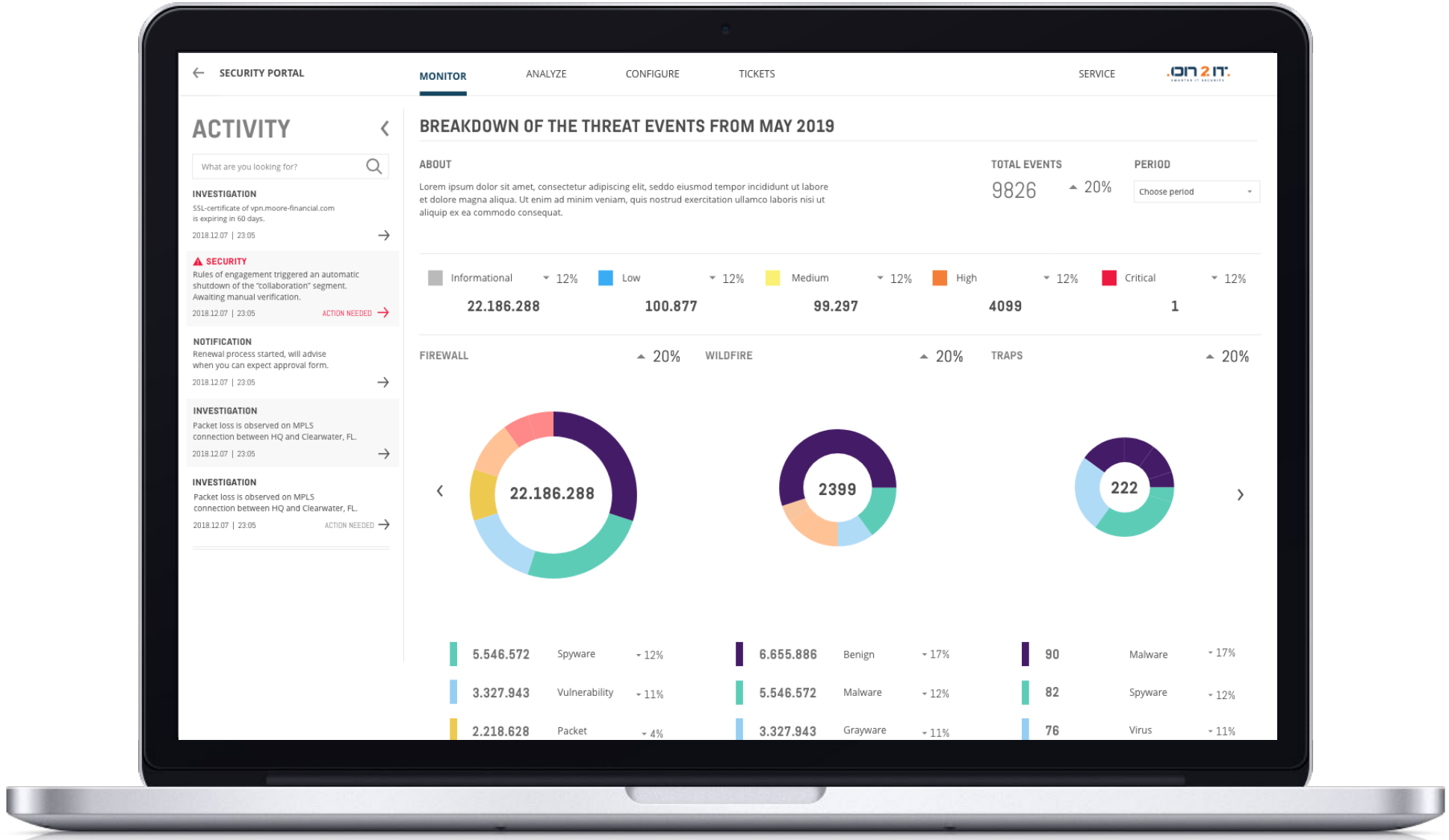




“What if only a machine can defeat another machine?”

- The Imitation Game

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

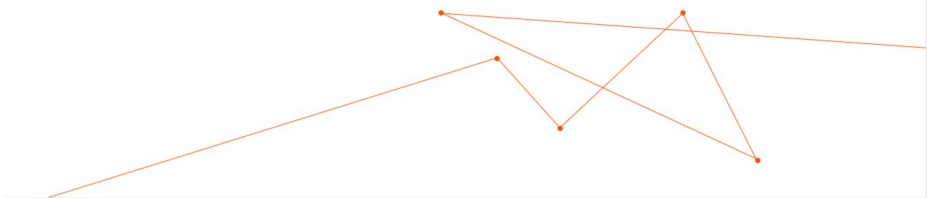

SECURITY PORTAL
MONITOR
ANALYZE
CONFIGURE
TICKETS
SERVICE
ACTIVITY
What are you looking for?
INVESTIGATION
SSL-certificate of vpn.moore-financial.com is expiring in 60 days.
2018.12.07 | 23:05
SECURITY
Rules of engagement triggered an automatic shutdown of the "collaboration" segment. Awaiting manual verification.
2018.12.07 | 23:05
ACTION NEEDED
NOTIFICATION
Renewal process started, will advise when you can expect approval form.
2018.12.07 | 23:05
INVESTIGATION
Packet loss is observed on MPLS connection between HQ and Clearwater, FL.
2018.12.07 | 23:05
INVESTIGATION
Packet loss is observed on MPLS connection between HQ and Clearwater, FL.
2018.12.07 | 23:05
ACTION NEEDED
BREAKDOWN OF THE THREAT EVENTS FROM MAY 2019
ABOUT
Lorem ipsum dolor sit amet, consectetur adipiscing elit, seddo eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
TOTAL EVENTS
9826
20%
PERIOD
Choose period
Informational 12% 22.186.288
Low 12% 100.877
Medium 12% 99.297
High 12% 4099
Critical 12% 1
FIREWALL 20%
WILDFIRE 20%
TRAPS 20%
22.186.288
2399
222
5.546.572 Spyware 12%
3.327.943 Vulnerability 11%
2.218.628 Packet 4%
6.655.886 Benign 17%
5.546.572 Malware 12%
3.327.943 Grayware 11%
90 Malware 17%
82 Spyware 12%
76 Virus 11%

The Kipling Method of Zero Trust Rule Writing

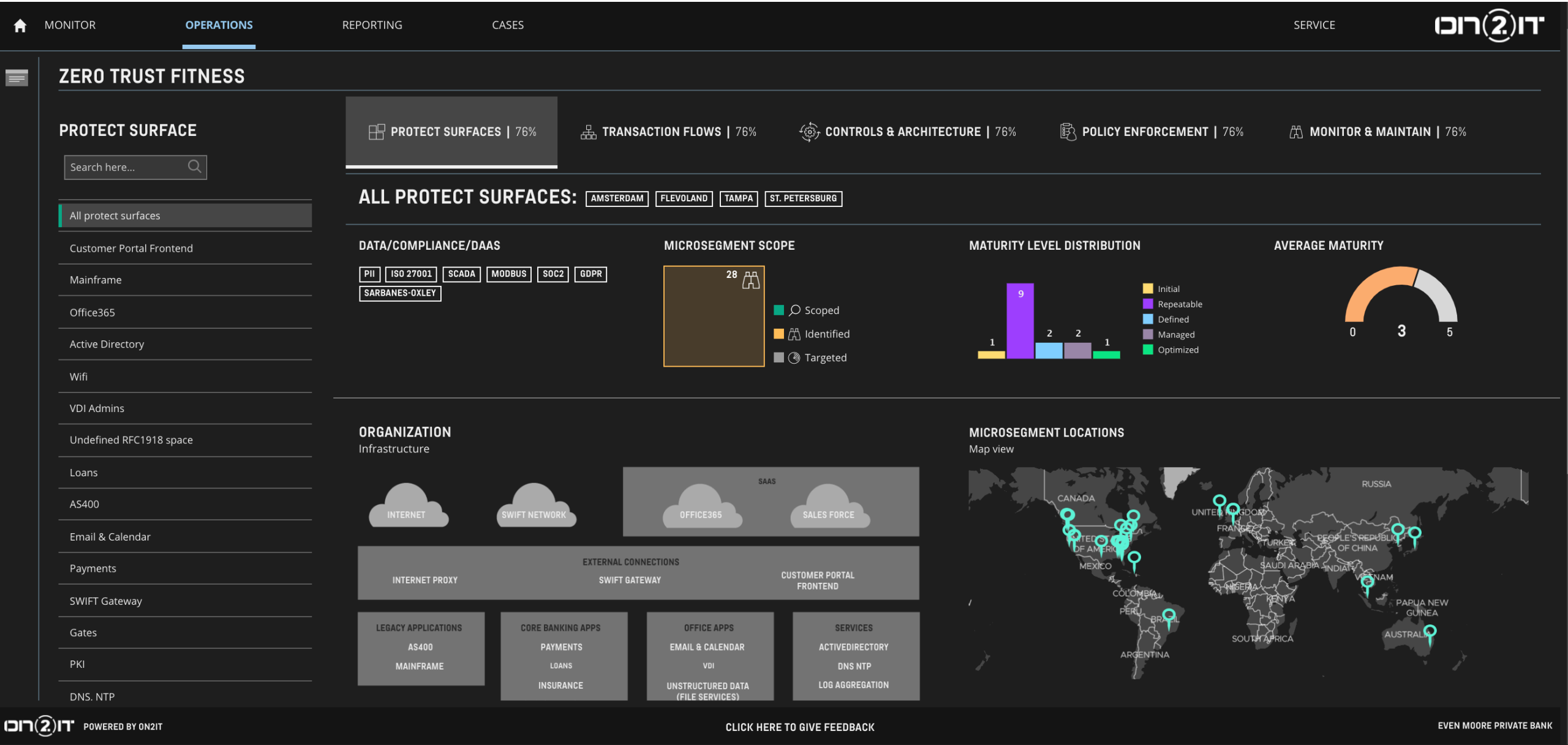
Who	What	When	Where	Why	How
User ID	**Application ID**	Time Limitations	**Device ID**	Classification	**Content ID**
Auth type			System Object	Data ID	Threat Protection
			Workload		SSL Decryption
			Geolocation		URL Filtering
					Wildfire

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

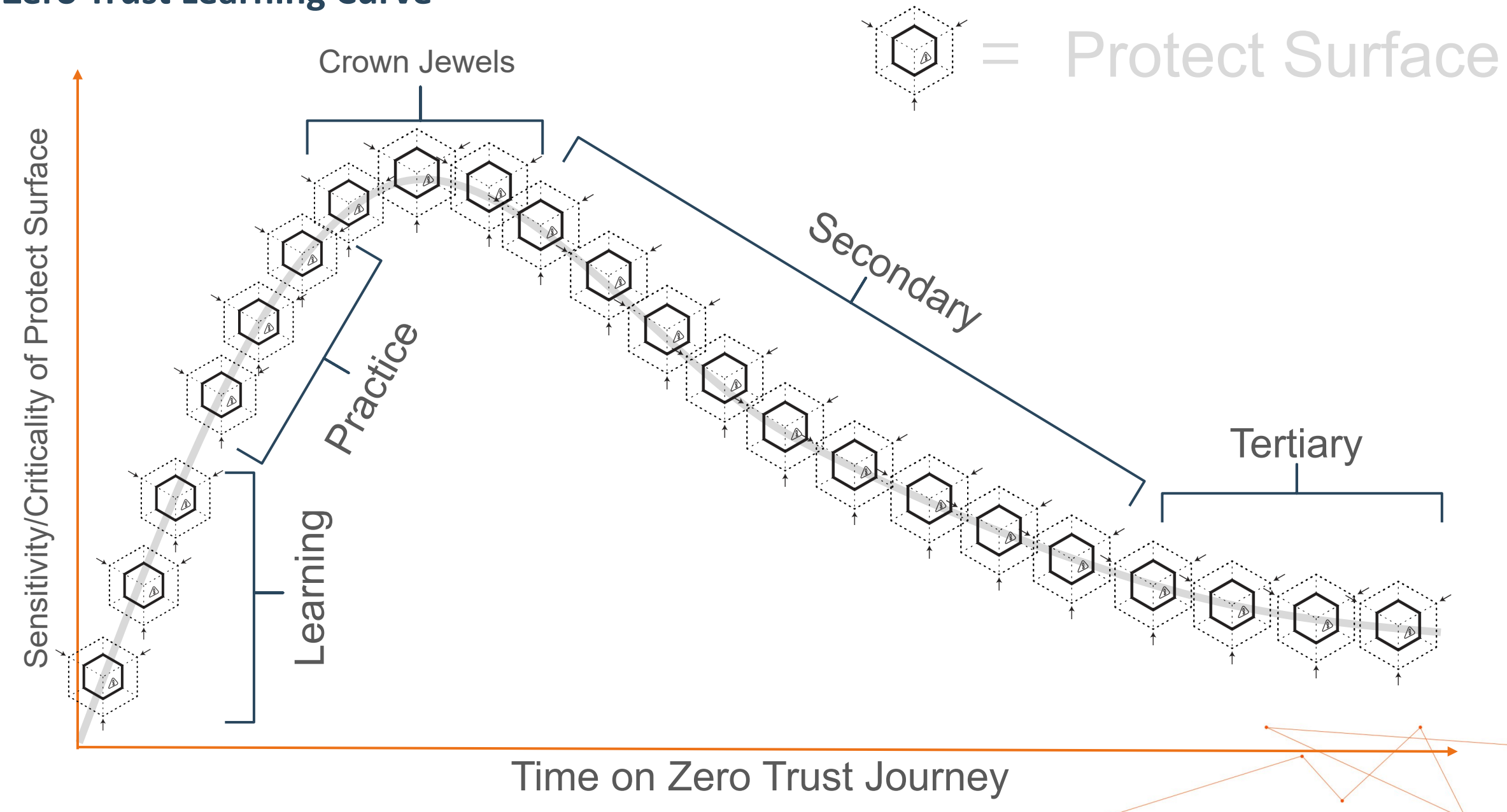
On Prem:
IF Who (UID) = Epic_Users, What (AID) = Epic, When (TOD) = Any, Where (LOC) = Epic_Srvr, Why (CLASS) = Toxic, How (CID) = Epic_CID, THEN Allow.



ZTaaS Makes Zero Trust Easy to Consume



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 _____

Zero Trust Is The World's Only Cybersecurity Strategy

"Zero trust would have profoundly limited the attacker's ability to move within OPM's network and access such sensitive data."

Source: Adopting a zero trust cyber model in government: http://federalnewsradio.com/commentary/2016/09/adopting-zero-trust-cyber-model-government/

KEEP IN TOUCH

John Kindervag

+31 88-2266200

info@on2it.net

Twitter.com/kindervag

ON2IT.net

ON2IT

ZERO TRUST INNOVATORS

ZERO TRUST INNOVATORS