EVOLUTION OF SIEM AND SOAR

WE IMPROVE YOUR CYBERSECURITY

Lieuwe Jan Koning

Co-Founder and CTO

ON2IT

● Classification –

ON2IT
ZERO TRUST INNOVATORS

90 % OF OUR CYBER BUDGET SHOULD FOCUS ON ENHANCING PREVENTION

WE ARE ON2IT

2005

COMPANY FOUNDED

by Marcel van Eemeren CEO and Lieuwe Jan Koning CTO

24/7/365

SOC

ZALTBOMMEL
The Netherlands

PLANO
Texas, USA

AUXO

proprietary Zero Trust platform

EUROPEAN COMMISSION

SEAL OF EXCELLENCE

300+

Customers worldwide

<1% CHURN
>100 MONTHS

100% ZERO TRUST
Make
Zero Trust
Happen

AICPA™

ISO

SOC2 / ISO9001 / ISO27001

ZERO TRUST

The only Cybersecurity Strategy that prevents data breaches

STRATEGIC

AUXO™

The platform to deliver Zero Trust & to provide 99.999% automated event resolution

TACTICAL

mSOC™

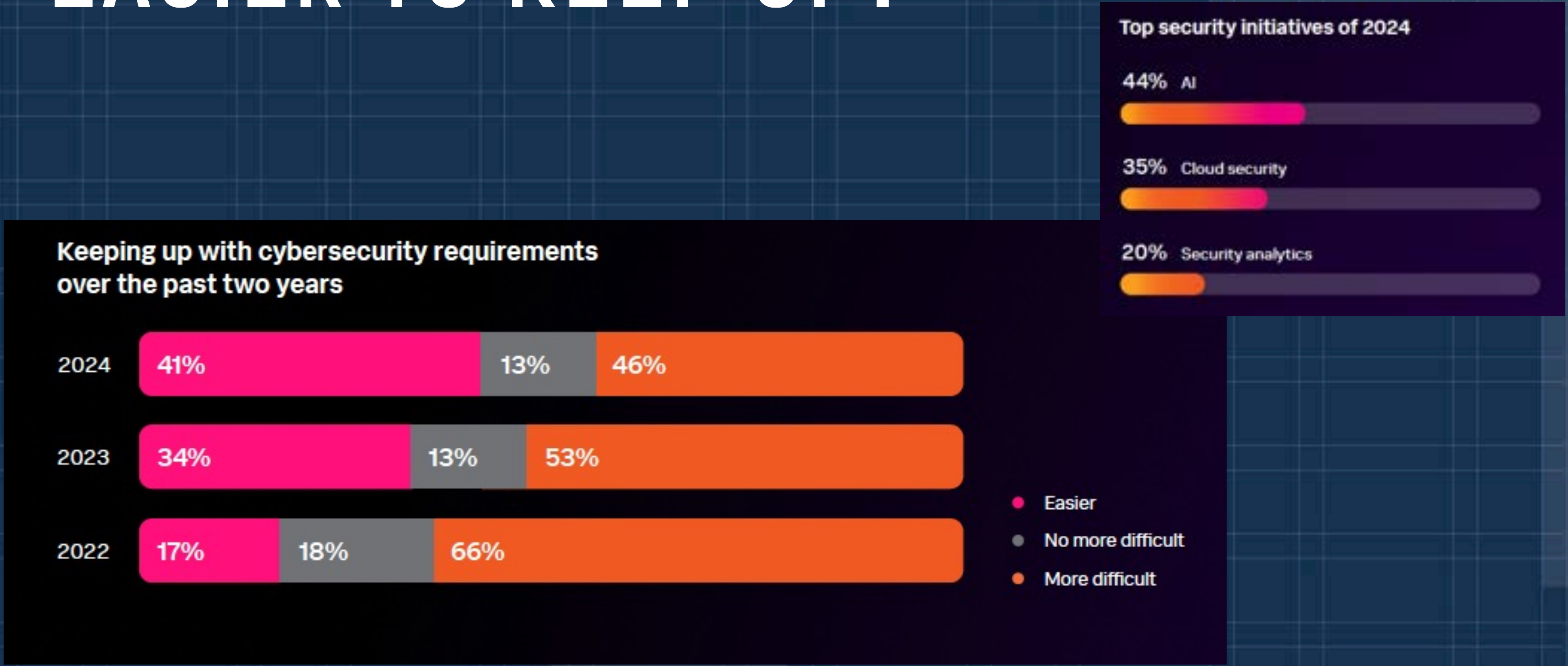
Our mSOC™,

our Cyber Defenders

SECURITY OPERATIONS CENTER
2.
on2it
CYBERSECURITY INCIDENT RESPONSE TEAM
2.
on2it

OPERATIONAL

EASIER TO KEEP UP?

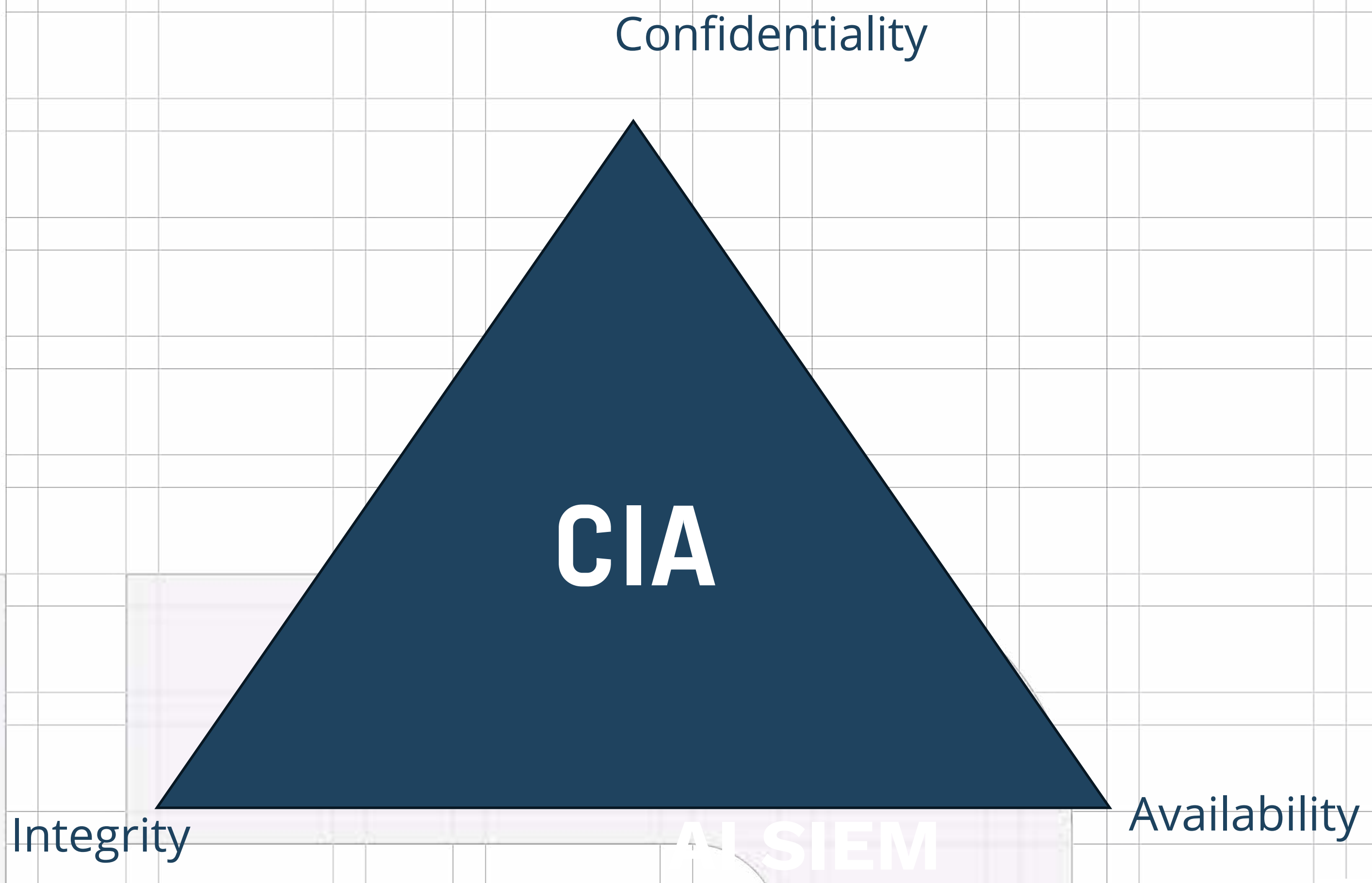


Top security initiatives of 2024

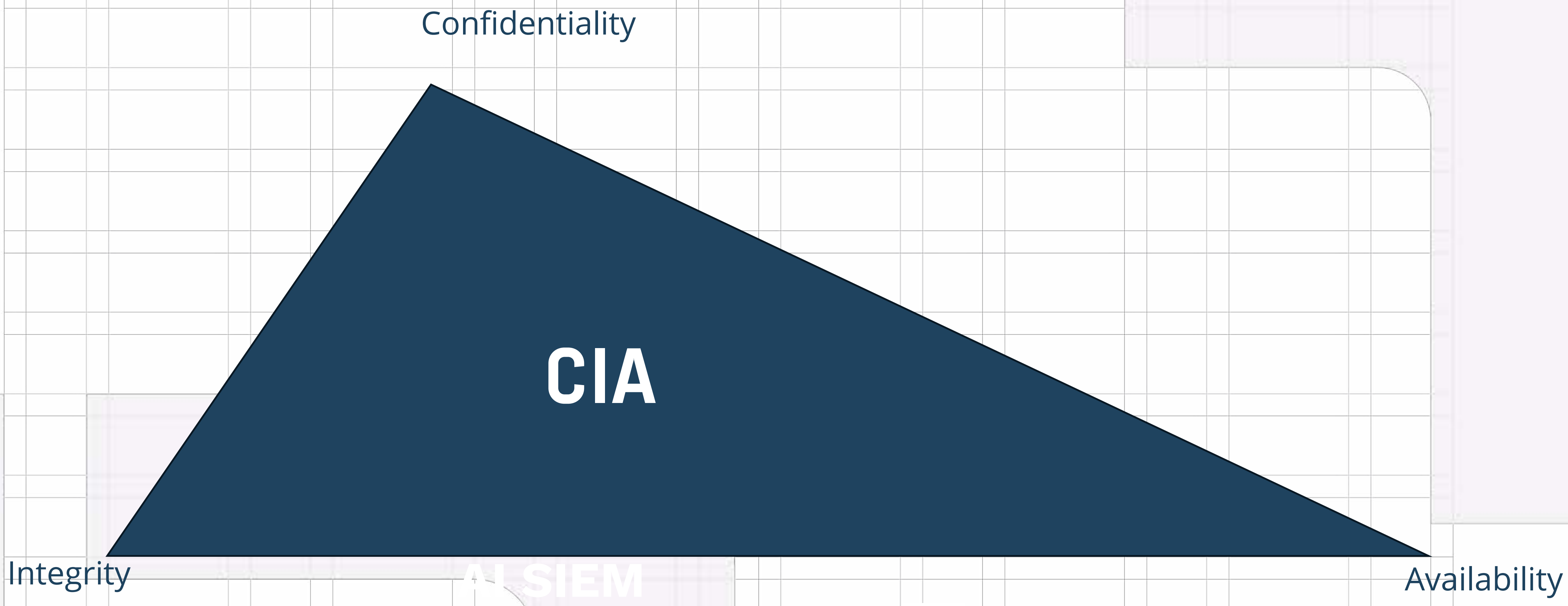
Keeping up with cybersecurity requirements over the past two years

source: State of Security 2024 | Splunk

CIA TRIAD



CIA TRIAD IN MANY ORGANIZATIONS



Security
is
Tomorrows Availability

RESULT

- Must the IPS be in blocking mode?
- Should we do application based rules in the datacenter?
- Can we apply content updates continuously?
- Contractors get access to webmail
- Let’s implement a DLP solution

SHOULD BE

- Do our top-10 applications have protection against all applicable attack techniques?
- Who needs access to application X?
- What do we do to prevent exfiltration of data?
- When do we have 0 applications without MFA?
- When do we have phishing-resistant MFA? (FIDO2/WebAuthn)
- Is our prevention compliant with DORA? NIS2?

WHAT WE PROCURE

- SIEM
- MDR
- Retainer / CSIRT
- A SOC service

“When we had our first breach, we had no idea what happened, we were helpless.

Then we implemented MDR and invested in a SIEM and a SOC.

When we got hacked recently, we knew exactly how we were breached.

We still got hacked.”

- *A CISO (who wishes to remain anonymous)*

WHAT SHOULD WE DO?

- Let’s Make Zero Trust Happen
- Role of SIEM + SOAR + SOC

ZERO TRUST

1. DEFINE THE PROTECT SURFACE

2. MAP THE TRANSACTION FLOWS

3. A ZERO TRUST ARCHITECTURE

4. CREATE ZERO TRUST POLICY

5. MONITOR AND MAINTAIN THE NETWORK

THE PRESIDENT'S NATIONAL SECURITY
TELECOMMUNICATIONS ADVISORY COMMITTEE

NSTAC REPORT TO THE PRESIDENT

Zero Trust and Trusted Identity Management

February 23, 2022

ZERO TRUST

1. DEFINE THE PROTECT SURFACE

2. MAP THE TRANSACTION FLOWS

3. A ZERO TRUST ARCHITECTURE

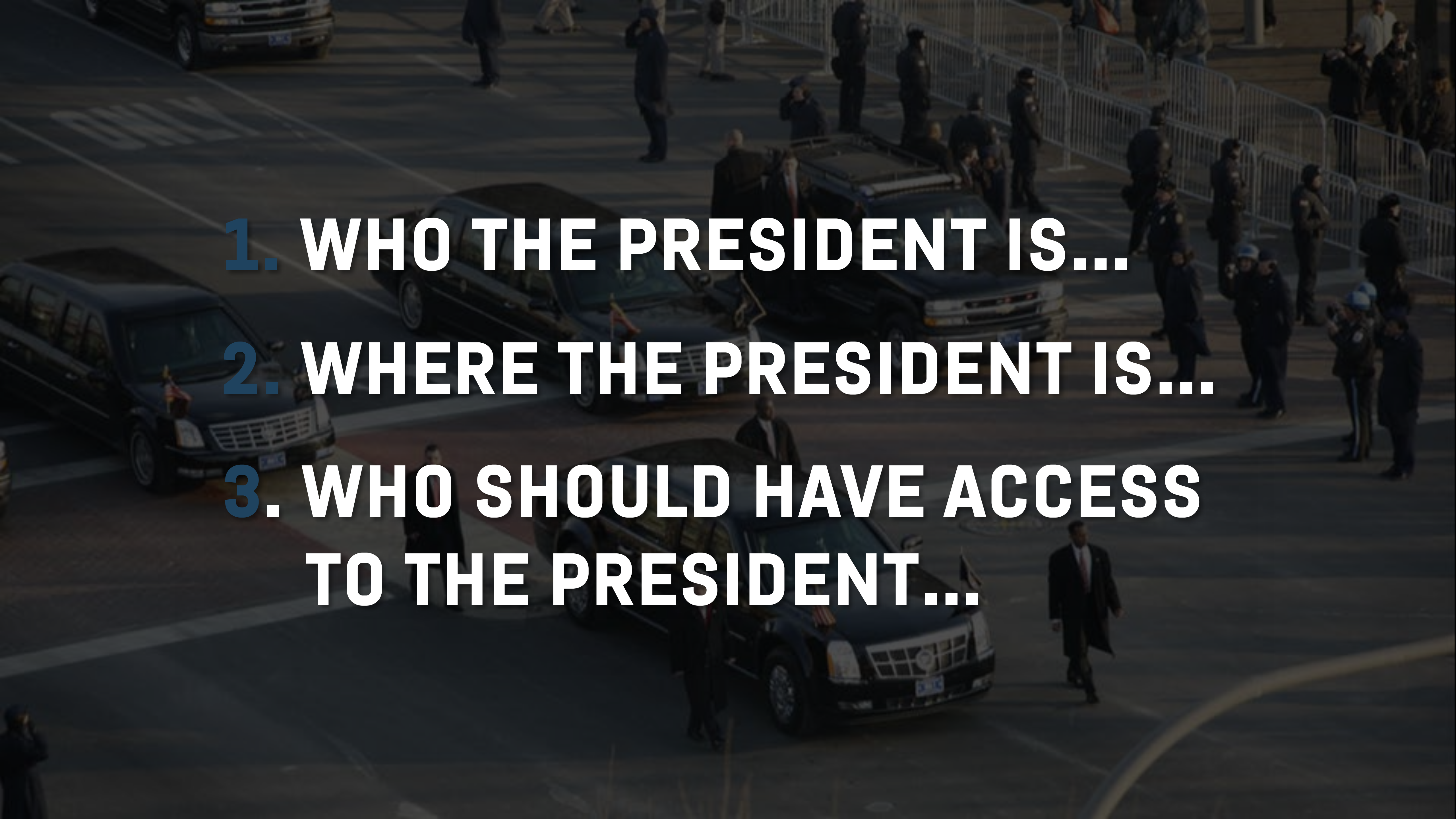
4. CREATE ZERO TRUST POLICY

5. MONITOR AND MAINTAIN THE NETWORK

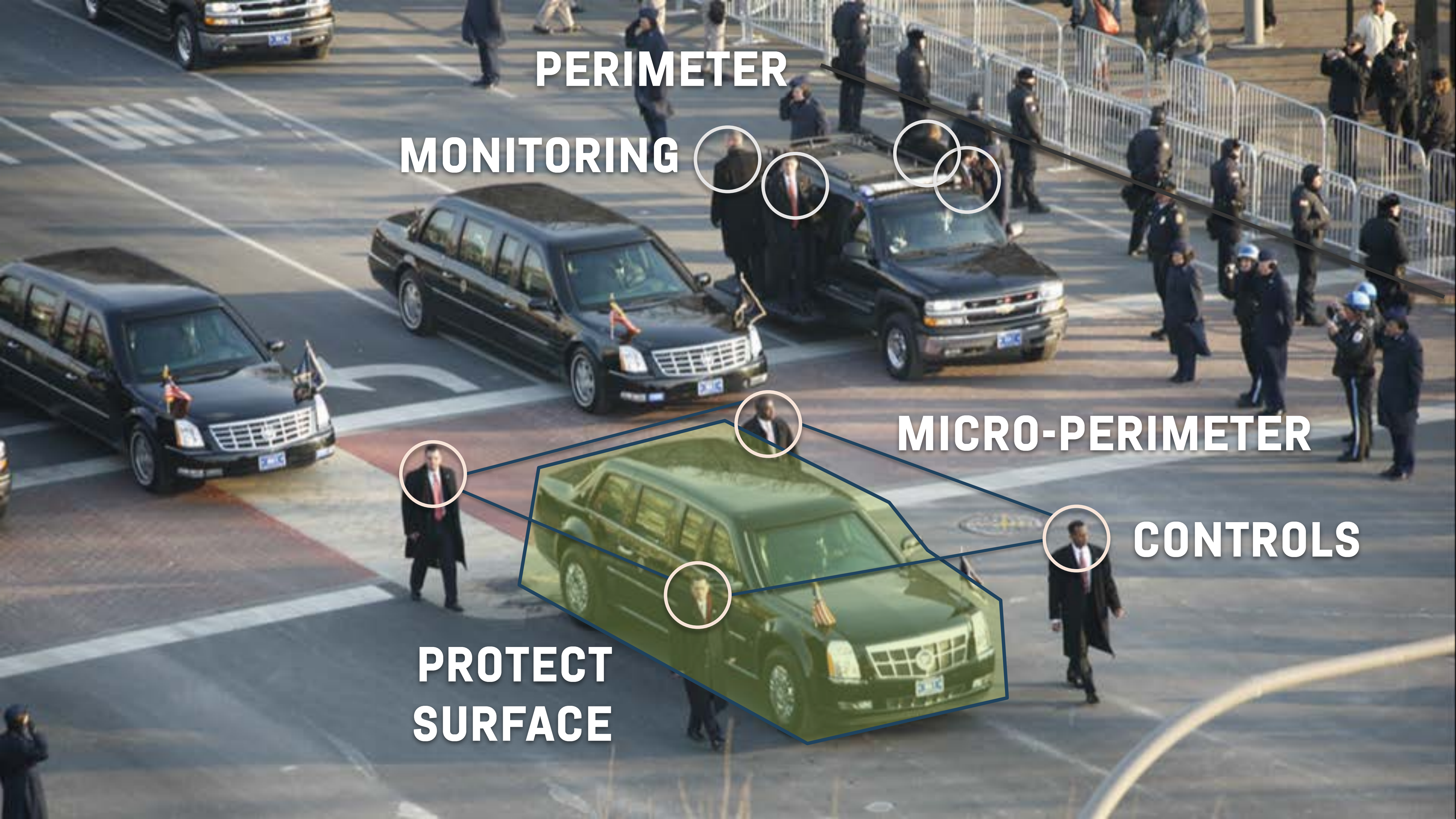
PROTECT SURFACE

1. DEFINE THE PROTECT SURFACE

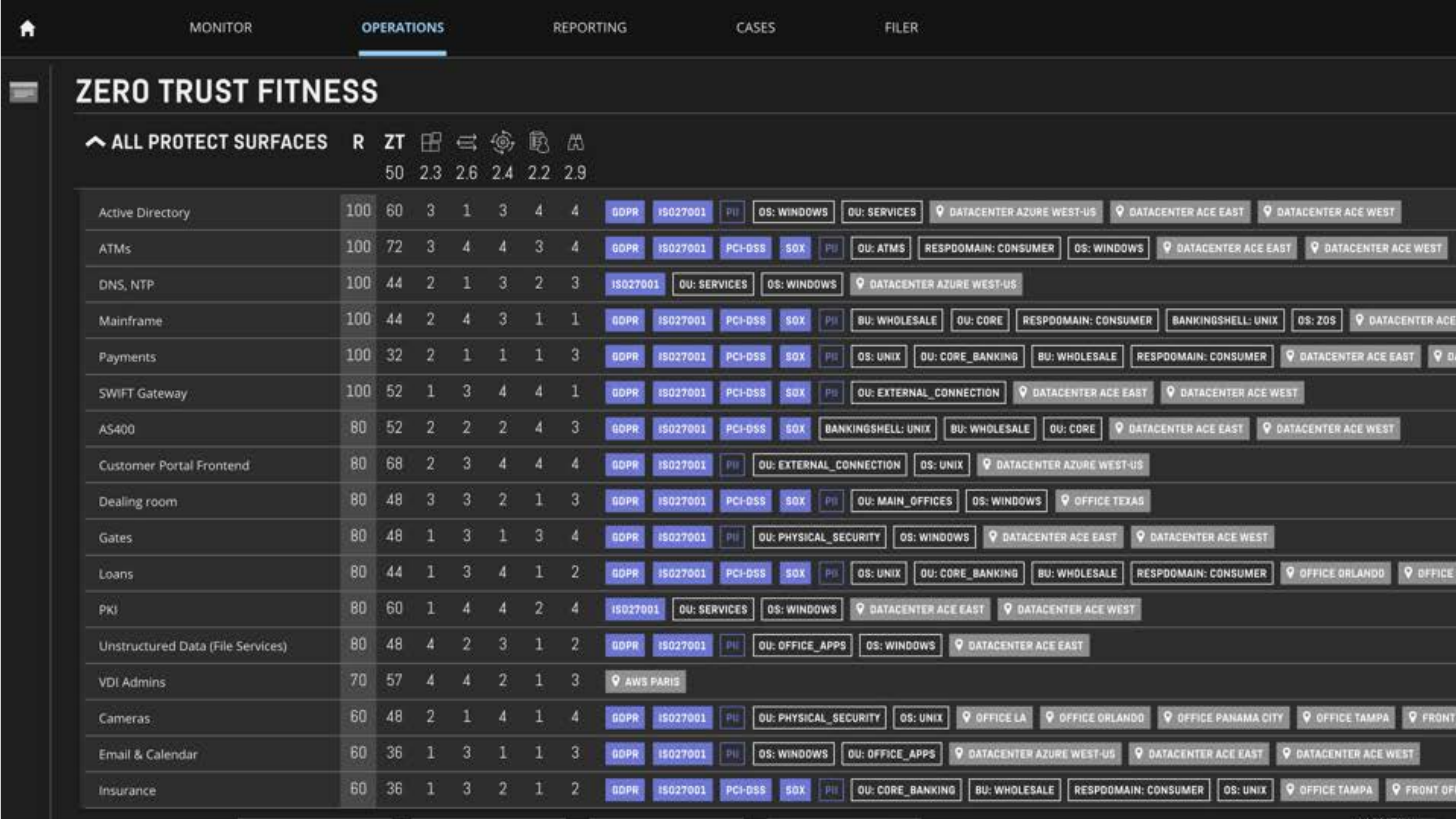
ONLY



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



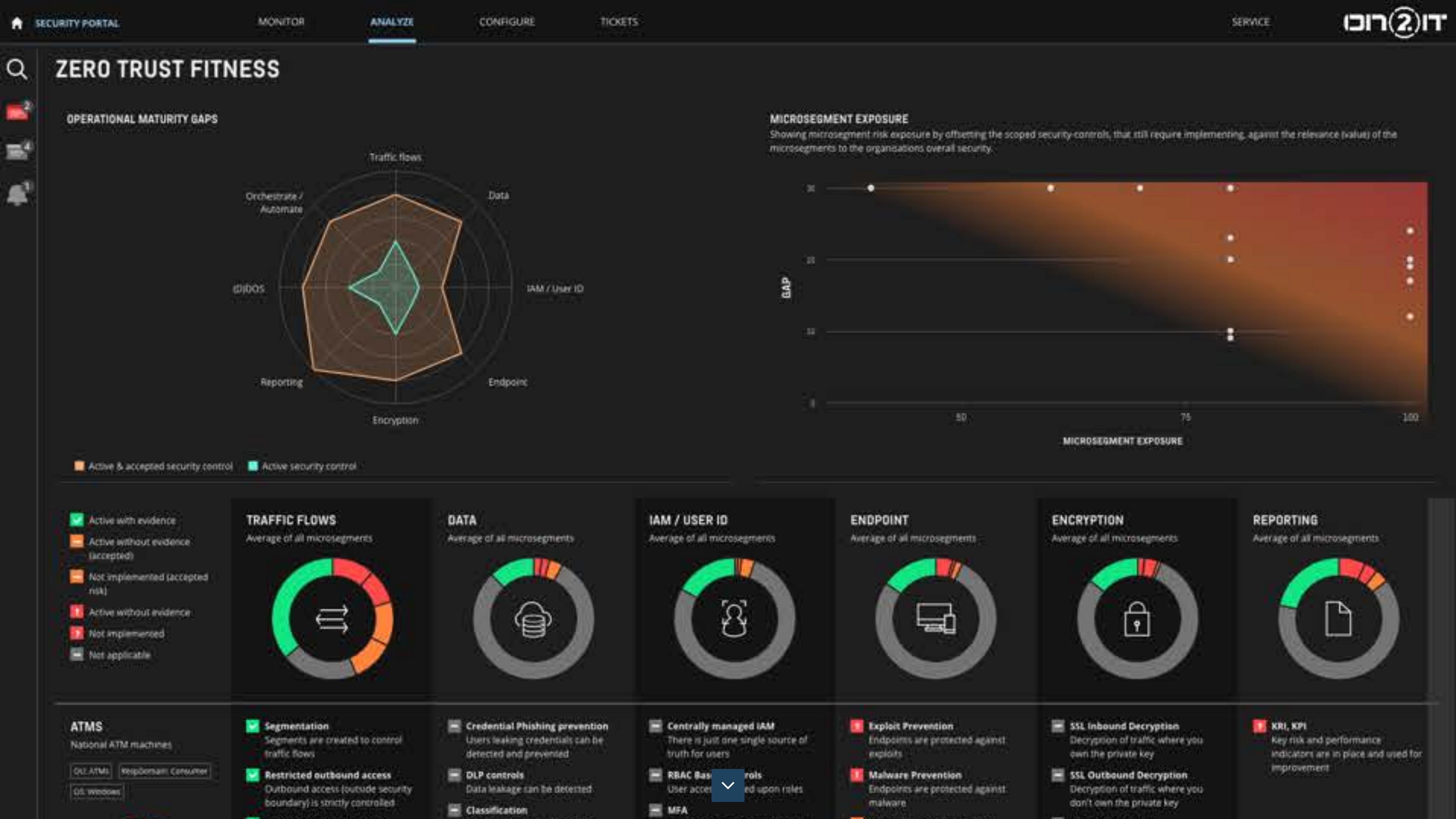
ZERO TRUST FITNESS

ALL PROTECT SURFACES

ALL PROTECT SURFACES	R	ZT						
		50	2.3	2.6	2.4	2.2	2.9	
Active Directory	100	60	3	1	3	4	4	GDPR ISO27001 PII OS: WINDOWS OU: SERVICES DATACENTER AZURE WEST-US DATACENTER ACE EAST DATACENTER ACE WEST
ATMs	100	72	3	4	4	3	4	GDPR ISO27001 PCI-DSS SOX PII OU: ATMS RESPDOMAIN: CONSUMER OS: WINDOWS DATACENTER ACE EAST DATACENTER ACE WEST
DNS, NTP	100	44	2	1	3	2	3	ISO27001 OU: SERVICES OS: WINDOWS DATACENTER AZURE WEST-US
Mainframe	100	44	2	4	3	1	1	GDPR ISO27001 PCI-DSS SOX PII BU: WHOLESALE OU: CORE RESPDOMAIN: CONSUMER BANKINGSHELL: UNIX OS: ZOS DATACENTER ACE
Payments	100	32	2	1	1	1	3	GDPR ISO27001 PCI-DSS SOX PII OS: UNIX OU: CORE_BANKING BU: WHOLESALE RESPDOMAIN: CONSUMER DATACENTER ACE EAST D
SWIFT Gateway	100	52	1	3	4	4	1	GDPR ISO27001 PCI-DSS SOX PII OU: EXTERNAL_CONNECTION DATACENTER ACE EAST DATACENTER ACE WEST
AS400	80	52	2	2	2	4	3	GDPR ISO27001 PCI-DSS SOX BANKINGSHELL: UNIX BU: WHOLESALE OU: CORE DATACENTER ACE EAST DATACENTER ACE WEST
Customer Portal Frontend	80	68	2	3	4	4	4	GDPR ISO27001 PII OU: EXTERNAL_CONNECTION OS: UNIX DATACENTER AZURE WEST-US
Dealing room	80	48	3	3	2	1	3	GDPR ISO27001 PCI-DSS SOX PII OU: MAIN_OFFICES OS: WINDOWS OFFICE TEXAS
Gates	80	48	1	3	1	3	4	GDPR ISO27001 PII OU: PHYSICAL_SECURITY OS: WINDOWS DATACENTER ACE EAST DATACENTER ACE WEST
Loans	80	44	1	3	4	1	2	GDPR ISO27001 PCI-DSS SOX PII OS: UNIX OU: CORE_BANKING BU: WHOLESALE RESPDOMAIN: CONSUMER OFFICE ORLANDO OFFICE
PKI	80	60	1	4	4	2	4	ISO27001 OU: SERVICES OS: WINDOWS DATACENTER ACE EAST DATACENTER ACE WEST
Unstructured Data (File Services)	80	48	4	2	3	1	2	GDPR ISO27001 PII OU: OFFICE_APPS OS: WINDOWS DATACENTER ACE EAST
VDI Admins	70	57	4	4	2	1	3	AWS PARIS
Cameras	60	48	2	1	4	1	4	GDPR ISO27001 PII OU: PHYSICAL_SECURITY OS: UNIX OFFICE LA OFFICE ORLANDO OFFICE PANAMA CITY OFFICE TAMPA FRONT
Email & Calendar	60	36	1	3	1	1	3	GDPR ISO27001 PII OS: WINDOWS OU: OFFICE_APPS DATACENTER AZURE WEST-US DATACENTER ACE EAST DATACENTER ACE WEST
Insurance	60	36	1	3	2	1	2	GDPR ISO27001 PCI-DSS SOX PII OU: CORE_BANKING BU: WHOLESALE RESPDOMAIN: CONSUMER OS: UNIX OFFICE TAMPA FRONT OF

ZERO TRUST STEP 3

3. A ZERO TRUST ARCHITECTURE



ZERO TRUST FITNESS

OPERATIONAL MATURITY GAPS

🟧 Active & accepted security control 🟦 Active security control

MICROSEGMENT EXPOSURE

Showing microsegment risk exposure by offsetting the scoped security-controls, that still require implementing, against the relevance (value) of the microsegments to the organisations overall security.

- ✓ Active with evidence
- 🟧 Active without evidence (accepted)
- 🟧 Not implemented (accepted risk)
- ! Active without evidence
- ! Not implemented
- – Not applicable

TRAFFIC FLOWS

Average of all microsegments

DATA

Average of all microsegments

IAM / USER ID

Average of all microsegments

ENDPOINT

Average of all microsegments

ENCRYPTION

Average of all microsegments

REPORTING

Average of all microsegments

ATMS

National ATM machines

OU: ATMs | RespDomain: Consumer | OS: Windows

☑ **Segmentation**
Segments are created to control traffic flows

☑ **Restricted outbound access**
Outbound access (outside security boundary) is strictly controlled

– **Credential Phishing prevention**
Users leaking credentials can be detected and prevented

– **DLP controls**
Data leakage can be detected

– **Classification**

– **Centrally managed IAM**
There is just one single source of truth for users

– **RBAC Bas** **rols**
User acce ed upon roles

– **MFA**

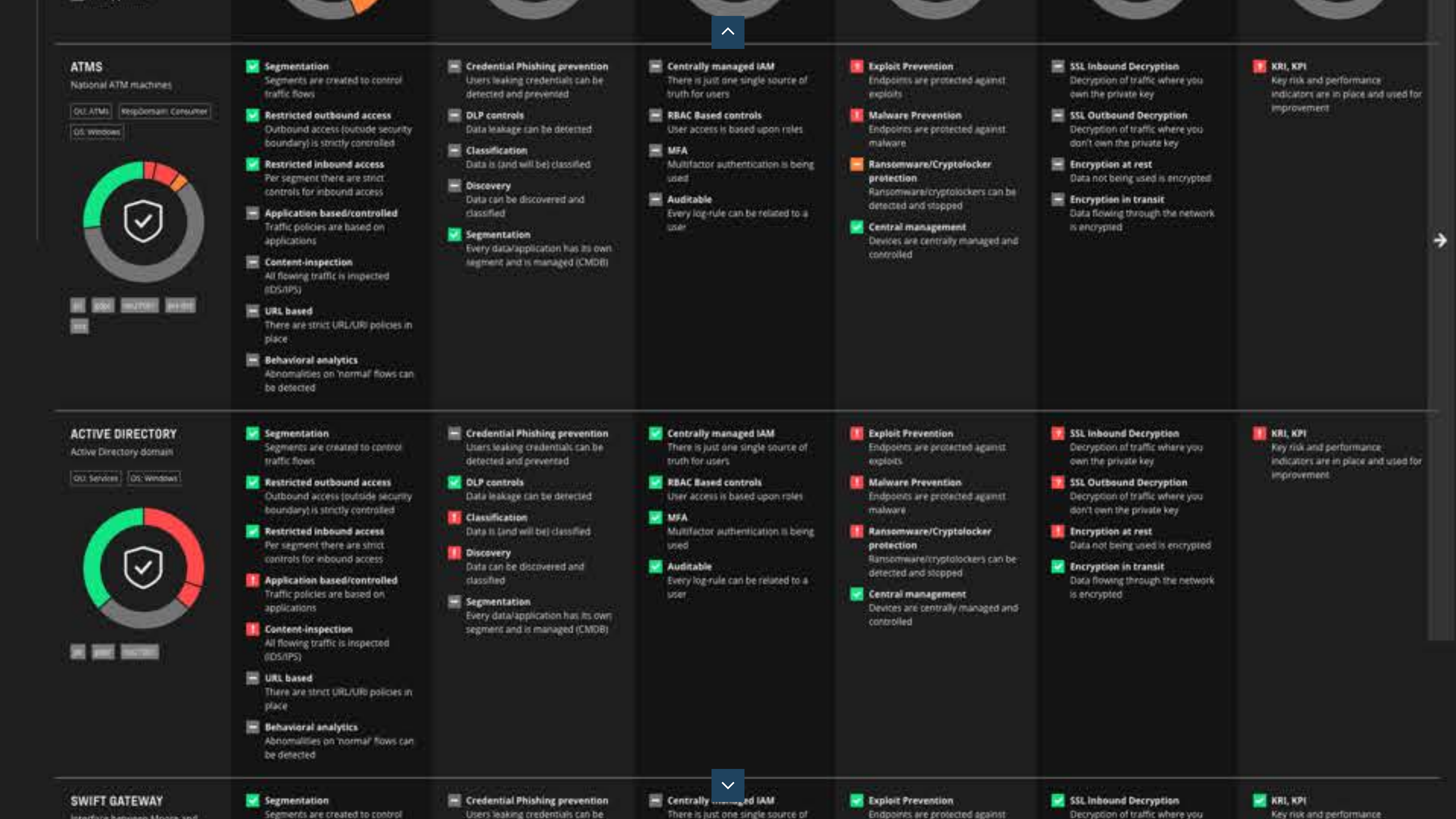
! **Exploit Prevention**
Endpoints are protected against exploits

! **Malware Prevention**
Endpoints are protected against malware

– **SSL Inbound Decryption**
Decryption of traffic where you own the private key

– **SSL Outbound Decryption**
Decryption of traffic where you don't own the private key

! **KRI, KPI**
Key risk and performance indicators are in place and used for improvement



ATMS

National ATM machines

OU: ATMs | RespDomain: Consumer | OS: Windows

✓ **Segmentation**
Segments are created to control traffic flows

✓ **Restricted outbound access**
Outbound access (outside security boundary) is strictly controlled

✓ **Restricted inbound access**
Per segment there are strict controls for inbound access

– **Application based/controlled**
Traffic policies are based on applications

– **Content-inspection**
All flowing traffic is inspected (IDS/IPS)

– **URL based**
There are strict URL/URI policies in place

– **Behavioral analytics**
Abnomalities on 'normal' flows can be detected

– **Credential Phishing prevention**
Users leaking credentials can be detected and prevented

– **DLP controls**
Data leakage can be detected

– **Classification**
Data is (and will be) classified

– **Discovery**
Data can be discovered and classified

✓ **Segmentation**
Every data/application has its own segment and is managed (CMDB)

– **Centrally managed IAM**
There is just one single source of truth for users

– **RBAC Based controls**
User access is based upon roles

– **MFA**
Multifactor authentication is being used

– **Auditable**
Every log-rule can be related to a user

! **Exploit Prevention**
Endpoints are protected against exploits

! **Malware Prevention**
Endpoints are protected against malware

! **Ransomware/Cryptolocker protection**
Ransomware/cryptolockers can be detected and stopped

✓ **Central management**
Devices are centrally managed and controlled

– **SSL Inbound Decryption**
Decryption of traffic where you own the private key

– **SSL Outbound Decryption**
Decryption of traffic where you don't own the private key

– **Encryption at rest**
Data not being used is encrypted

– **Encryption in transit**
Data flowing through the network is encrypted

! **KRI, KPI**
Key risk and performance indicators are in place and used for improvement

ACTIVE DIRECTORY

Active Directory domain

OU: Services | OS: Windows

✓ **Segmentation**
Segments are created to control traffic flows

✓ **Restricted outbound access**
Outbound access (outside security boundary) is strictly controlled

✓ **Restricted inbound access**
Per segment there are strict controls for inbound access

! **Application based/controlled**
Traffic policies are based on applications

! **Content-inspection**
All flowing traffic is inspected (IDS/IPS)

– **URL based**
There are strict URL/URI policies in place

– **Behavioral analytics**
Abnomalities on 'normal' flows can be detected

– **Credential Phishing prevention**
Users leaking credentials can be detected and prevented

✓ **DLP controls**
Data leakage can be detected

! **Classification**
Data is (and will be) classified

! **Discovery**
Data can be discovered and classified

– **Segmentation**
Every data/application has its own segment and is managed (CMDB)

✓ **Centrally managed IAM**
There is just one single source of truth for users

✓ **RBAC Based controls**
User access is based upon roles

✓ **MFA**
Multifactor authentication is being used

✓ **Auditable**
Every log-rule can be related to a user

! **Exploit Prevention**
Endpoints are protected against exploits

! **Malware Prevention**
Endpoints are protected against malware

! **Ransomware/Cryptolocker protection**
Ransomware/cryptolockers can be detected and stopped

✓ **Central management**
Devices are centrally managed and controlled

! **SSL Inbound Decryption**
Decryption of traffic where you own the private key

! **SSL Outbound Decryption**
Decryption of traffic where you don't own the private key

! **Encryption at rest**
Data not being used is encrypted

✓ **Encryption in transit**
Data flowing through the network is encrypted

! **KRI, KPI**
Key risk and performance indicators are in place and used for improvement

SWIFT GATEWAY

Interface between Moore and

✓ **Segmentation**
Segments are created to control

– **Credential Phishing prevention**
Users leaking credentials can be

– **Centrally managed IAM**
There is just one single source of

✓ **Exploit Prevention**
Endpoints are protected against

✓ **SSL Inbound Decryption**
Decryption of traffic where you

✓ **KRI, KPI**
Key risk and performance

ZERO TRUST STEP 3

4. CREATE ZERO TRUST POLICY

NOW A WORLDWIDE DE FACTO STANDARD: FIVE STEPS

5. MONITOR AND MAINTAIN THE NETWORK

CLOSER LOOK AT STEP 5

Why it matters?

- Validation that prevention works
- Respond to threats, especially APT
- Evidence (DORA, NIS2; non-repudiation)
- PDCA continuous improvement

2005

SIEM 1.0

LOG COLLECTION

2010

SIEM 2.0

DATA OVERLOAD

2015

SIEM 3.0

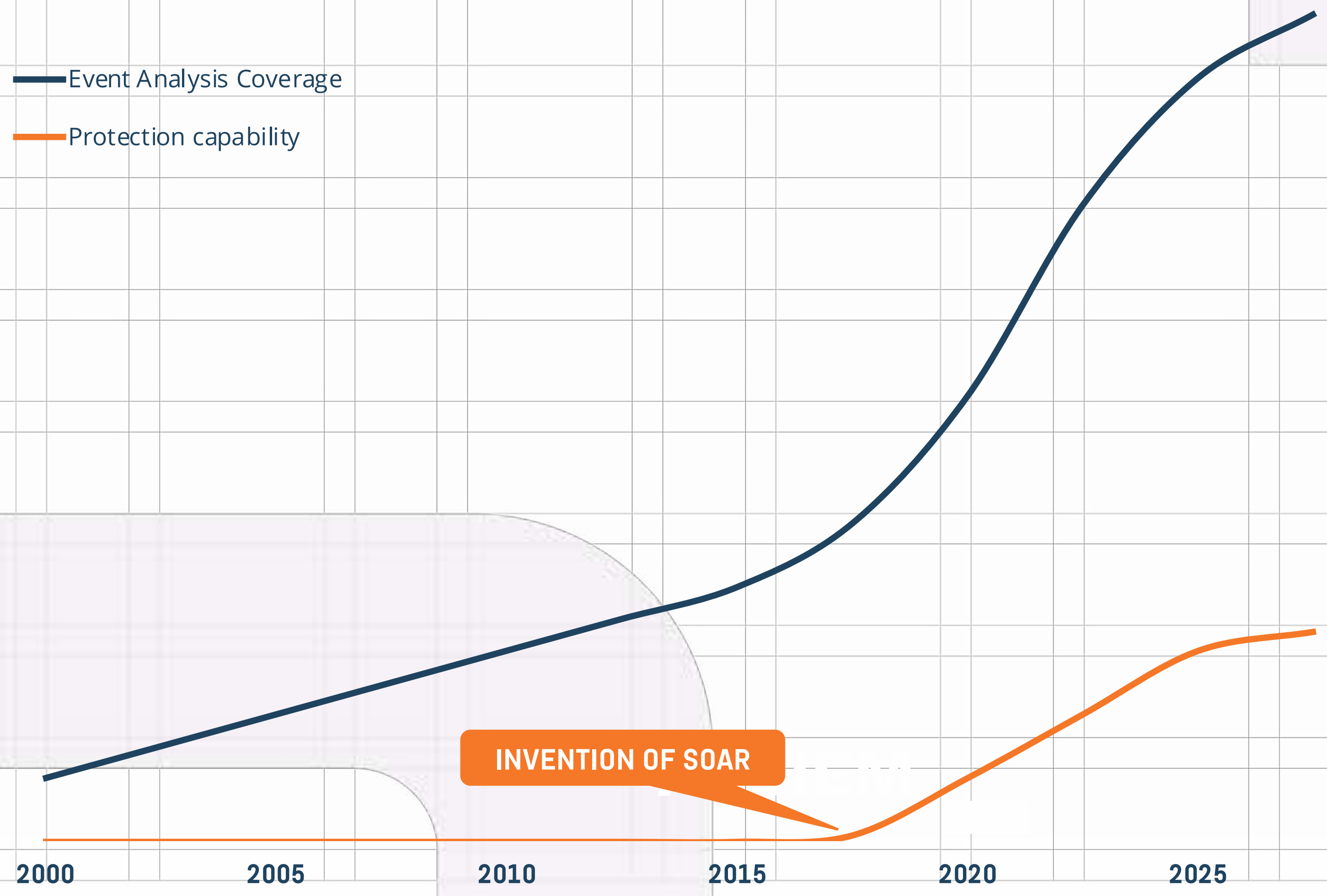
MACHINE LEARNING

2020

SIEM 3.0

SOAR + AI

EVOLUTION OF SIEM + SOAR CAPABILITY



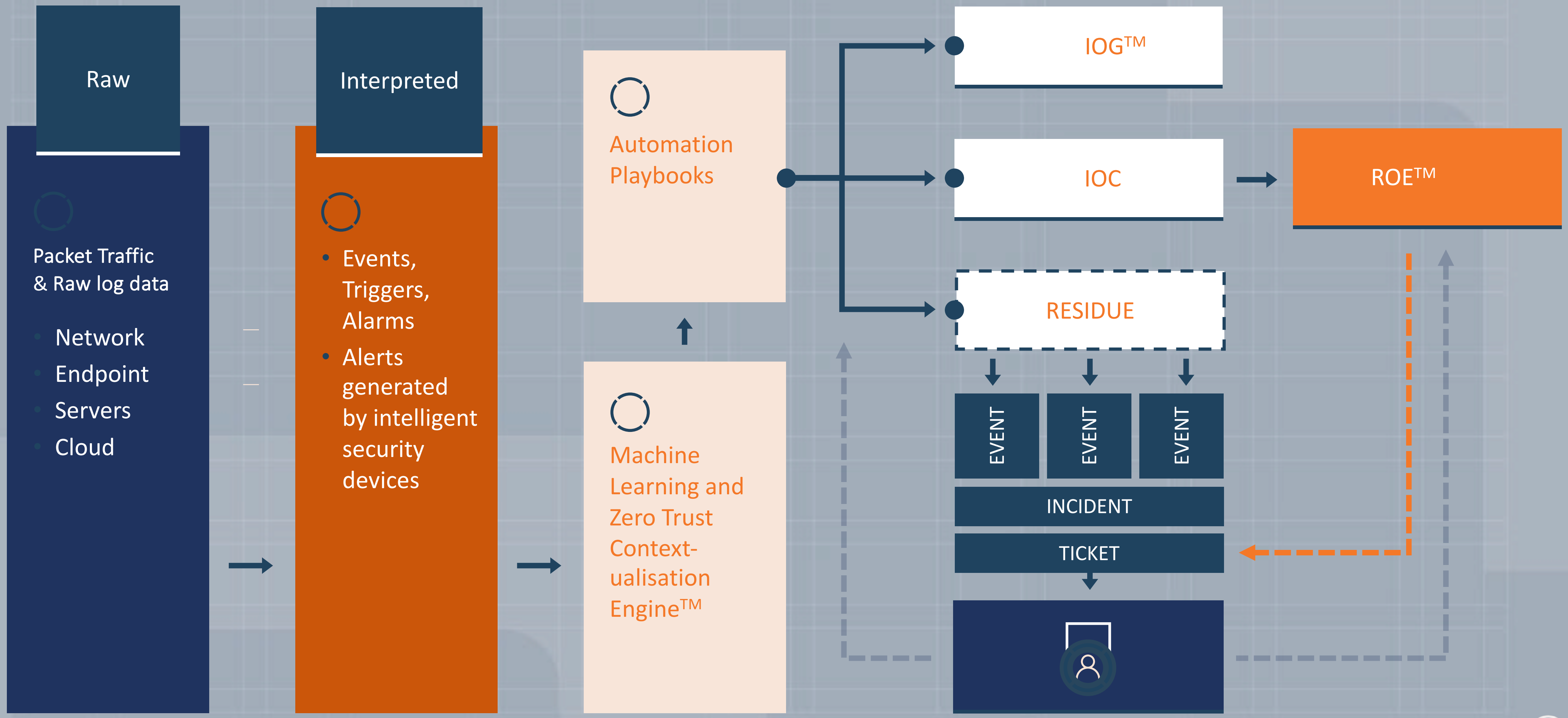
● Classification –

ON2IT
ZERO TRUST INNOVATORS

RESULT OF SIEM EVOLUTION

- Better coverage of log analysis
- However: still rearview mirror
- Protection capability is very limited – SOAR acts at end of killchain

AUXO



Raw

Packet Traffic & Raw log data

- Network
- Endpoint
- Servers
- Cloud

Interpreted

- Events, Triggers, Alarms
- Alerts generated by intelligent security devices

Automation Playbooks

Machine Learning and Zero Trust Contextualisation Engine^{TM}

IOG^{TM}

IOC

RESIDUE

ROE^{TM}

EVENT

EVENT

EVENT

INCIDENT

TICKET

KEY TAKEAWAYS

- Balance shift from **A only** to **CIA**
- SOC + SOAR must focus on prevention
- Make Zero Trust happen!

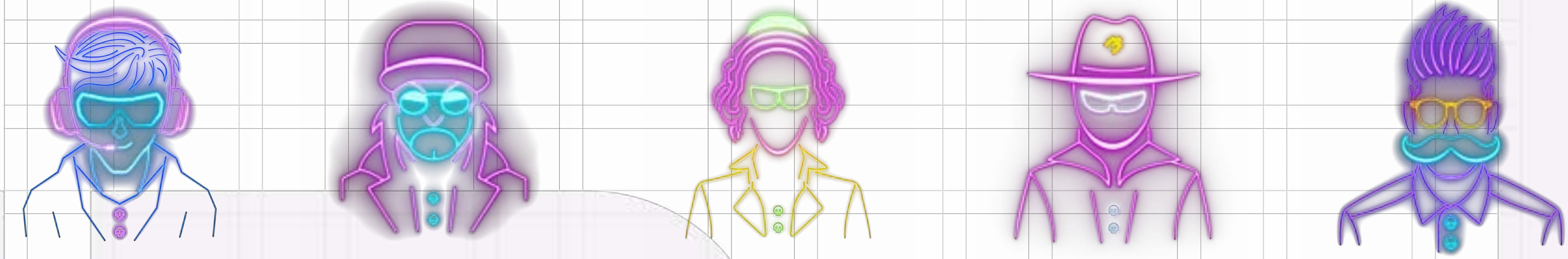
THREAT-TALKS.COM

Listen on Spotify

Listen on amazon music

Listen on Apple Podcasts

Listen on YouTube



● Classification – Confidential

THANK YOU!

Lieuwe Jan Koning

Co-Founder and CTO

ON2IT

ZERO TRUST INNOVATORS