ISA/IEC 62443: How to gain insight in your assets and how to protect them

Arjan Aelmans – OT Specialist Systems Engineer

NSE7 OT & ATP, ISA/IEC 62443 Expert certified

Jeffrey Noya – Regional Systems Engineer

NNCE, NNAT, NSE4, NSE5, NSE7 OT & EFW certified

Agenda

Session 1:

Optimizing Segmentation with ISA/IEC 62443

Q&A

BREAK

Session 2:

Network and asset based attack perspective

Q&A

IEC 62443

General	**IEC TS 62443-1-1** Concepts and Models	**IEC TR 62443-1-2** Master Glossary of Terms and Abbreviations	**IEC TS 62443-1-3** System Security Conformance Metrics	**IEC TS 62443-1-4** IACS Security Life Cycle and Use Cases	
Policies and Procedures	**IEC TS 62443-2-1** Security Program Requirement for IAC Asset Owners	**IEC 62443-2-2** IACS Protection Levels	**IEC TR 62443-2-3** Patch Management in an IACS Environment	**IEC 62443-2-4** Patch Management in an IACS Environment	**IEC TR 62443-2-5** Implementation Guidance for IACS Users
System	**IEC TS 62443-3-1** Security Technology for IACS	**IEC TS 62443-3-2** Security Risk Assessment and System Design	**IEC TS 62443-3-3** System Security Requirements and Security Levels		
Component	**IEC TS 62443-4-1** Security Product Development Lifecycle Requirements	**IEC 62443-4-2** Technical Security Requirements for IACS Components			

IEC 62443 Security Levels

Asset Owner, System Integrator, and Product Supplier

What are the different protection levels?

To achieve optimum level of security i.e. SL-T (Target Security Level) and meet the security requirements, the SRs (Security Requirements) and REs (Requirement Enhancements) are deployed depending on the protection required against the specific threats. The IEC 62443 protection levels are mentioned below.

Protection Levels		SRs + REs
SL 0:	No specific requirements or security protection necessary	No specific security controls required
SL 1:	Protection against casual or coincidental violation	Security controls against basic threats
SL 2:	Protection against intentional violation using simple means with low resources, generic skills and low motivation	Security controls against moderate threats
SL 3:	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation	Security controls against sophisticated threats
SL 4:	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation	Security controls against highly advanced threats

IEC 62443-3-3

IEC 62443 Foundational Requirements

Asset Owner, System Integrator, and Product Supplier

What are Foundational Requirements (FRs)?

As defined in IEC 62443-1-1 there are a total of seven FRs:

Foundational Requirements (FRs)

FR1 – Identification and authentication control (IAC),
FR2 – Use control (UC),
FR3 – System integrity (SI),
FR4 – Data confidentiality (DC),
FR5 – Restricted data flow (RDF),
FR6 – Timely response to events (TRE), and
FR7 – Resource availability (RA).

IEC 62443-1-1

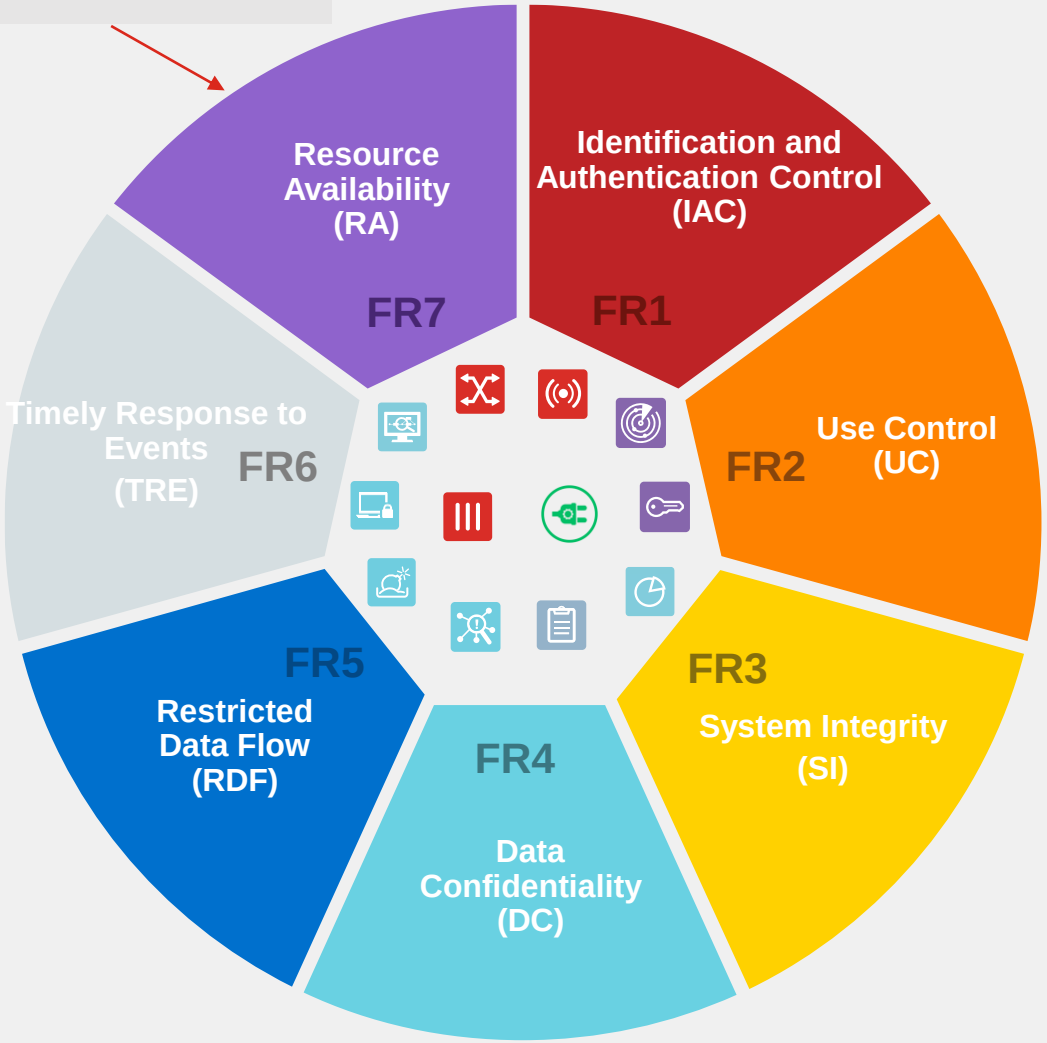
Example high-level operational controls mapping to FRs

FR1 – Passwords and user authentication
FR2 – User roles and authorization enforcement (RBAC)
FR3 – Session handling, mechanism to recognize change
FR4 – Encryption
FR5 – Network segmentation
FR6 – Logging and monitoring
FR7 – System backup and recovery

Fortinet Security Solutions support Asset Owners to achieve these requirements.

IEC 62443 expands the seven FRs defined in IEC 62443-1-1 into a series of SRs. Each SR has a baseline requirement and zero or more Requirement Enhancements (REs) to strengthen security.

NOZOMI NETWORKS



1 FortiGate, FortiWiFi/FortiAP, FortiNAC FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSIEM

2 FortiGate, FortiWiFi/FortiAP, FortiNAC, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM

3 FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM, FortiTester, FortiResponder

4 FortiGate, FortiSwitch, FortiAP, FortiEDR

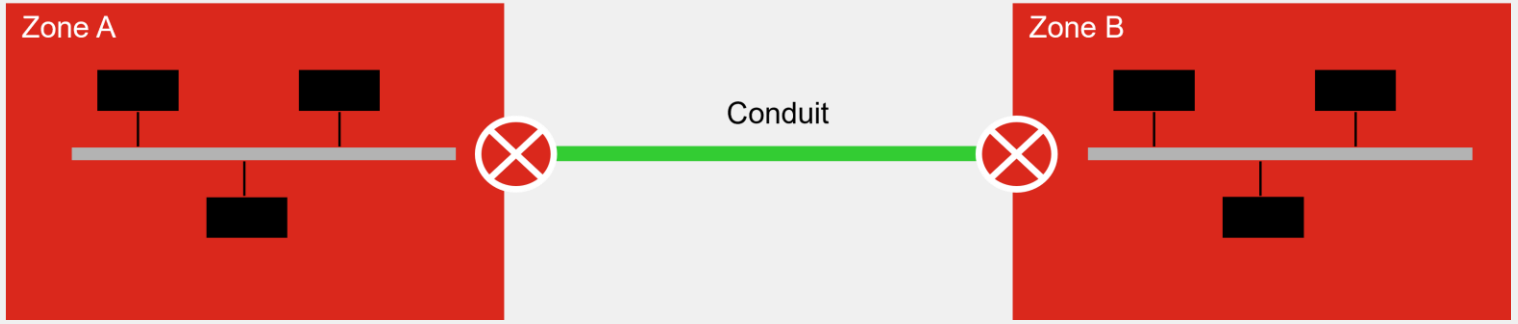
5 FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer

6 FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiSIEM, FortiManager

7 FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions

Zones and Conduits – East/West Segmentation

- IEC 62443 introduces the concept of Zones and Conduits, and this is pivotal to it's core principles.



- A **Zone** is a logical or physical area where assets of the same criticality are grouped together
  - A zone could be a defined as a single process area, safety critical systems, or systems critical to operations.
    - Assets can also include data and intellectual property
    - Impact assessments may help identify zones
    - IEC62443-3-3 defines Security Levels (SL) that are to be assigned for a given zone
- A **conduit** is a communication link between two or more zones
  - A conduit is most frequently an ethernet communications link
  - But discrete conduits must also be accounted for – e.g USB sticks
  - Conduits must be subject to security policy enforcement

IEC/ISA 62443-3-3

9.3 SR 5.1 – Network segmentation

9.3.1 Requirement

The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

9.3.2 Rationale and supplemental guidance

Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or ingress, of network traffic into a control system and reduce the spread, or egress, of network traffic from a control system. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

FR 5 – Restricted data flow (RDF)		SL1	SL2	SL3	SL4
SR 5.1 – Network segmentation	9.3	✓	✓	✓	✓

IEC/ISA 62443-3-3

9.4 SR 5.2 – Zone boundary protection

9.4.1 Requirement

The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

SRs and REs		SL 1	SL 2	SL 3	SL 4
SR 5.2 – Zone boundary protection	9.4	✓	✓	✓	✓

IEC/ISA 62443-3-3

6.3 SR 2.1 – Authorization enforcement

6.3.1 Requirement

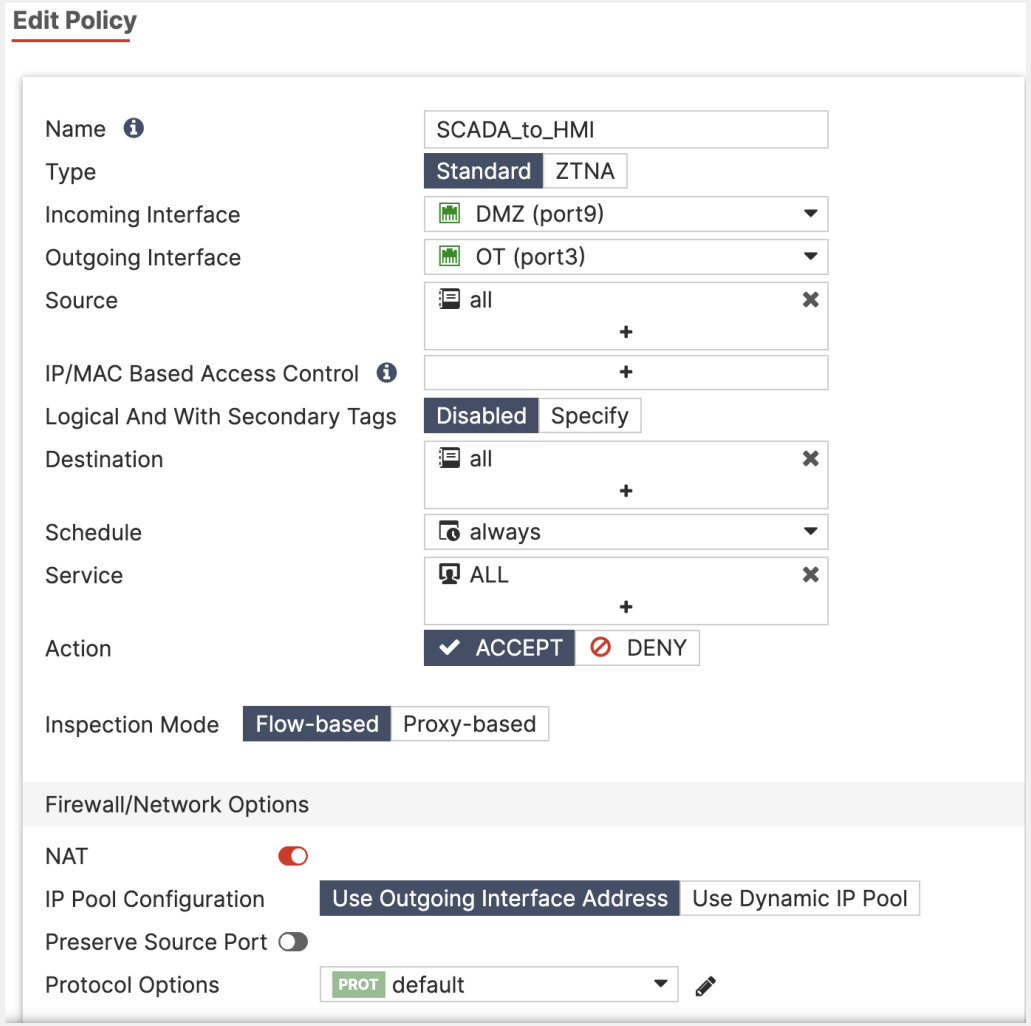
On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.

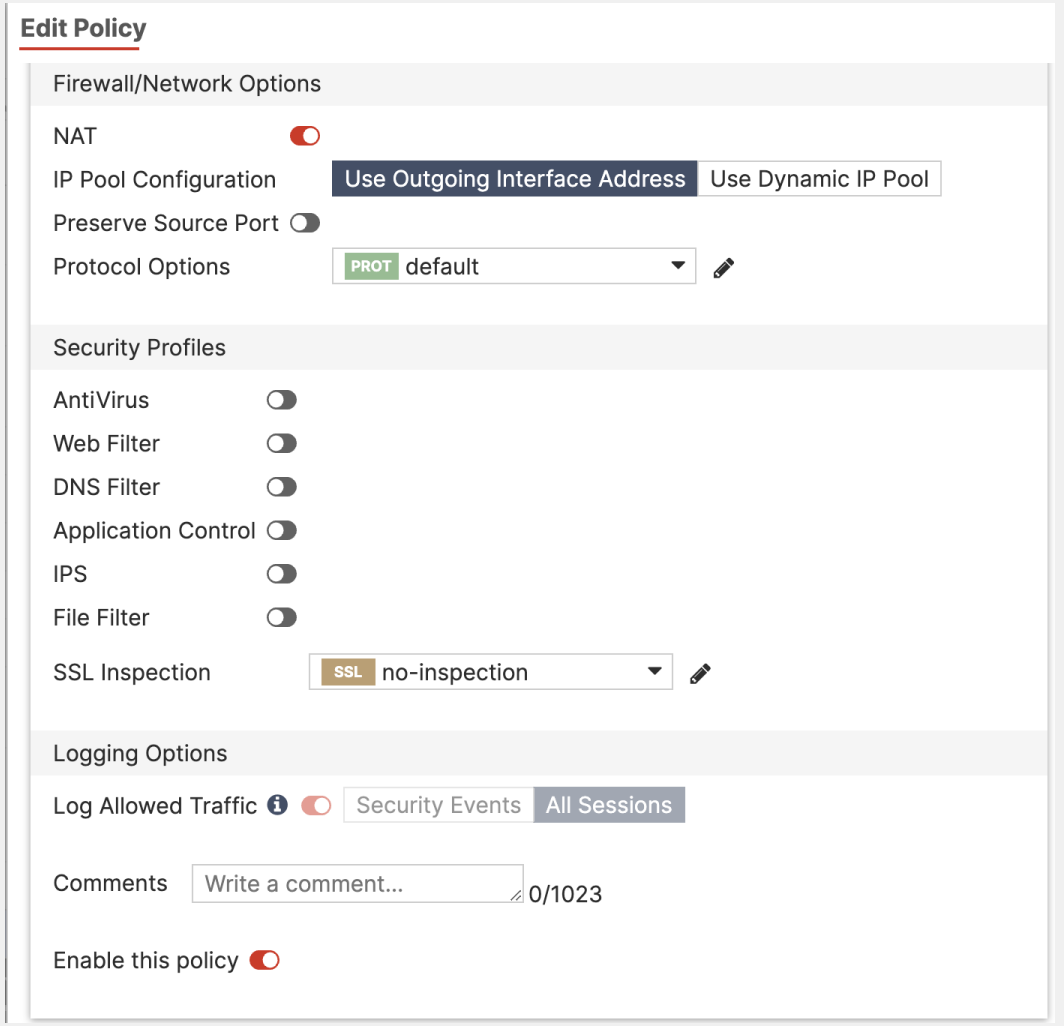
6.3.2 Rationale and supplemental guidance

Use control policies (for example, identity-based policies, role-based policies and rule-based policies) and associated read/write access enforcement mechanisms (for example, access control lists, access control matrices and cryptography) are employed to control usage between users (humans, software processes and devices) and assets (for example, devices, files, records, software processes, programs and domains).

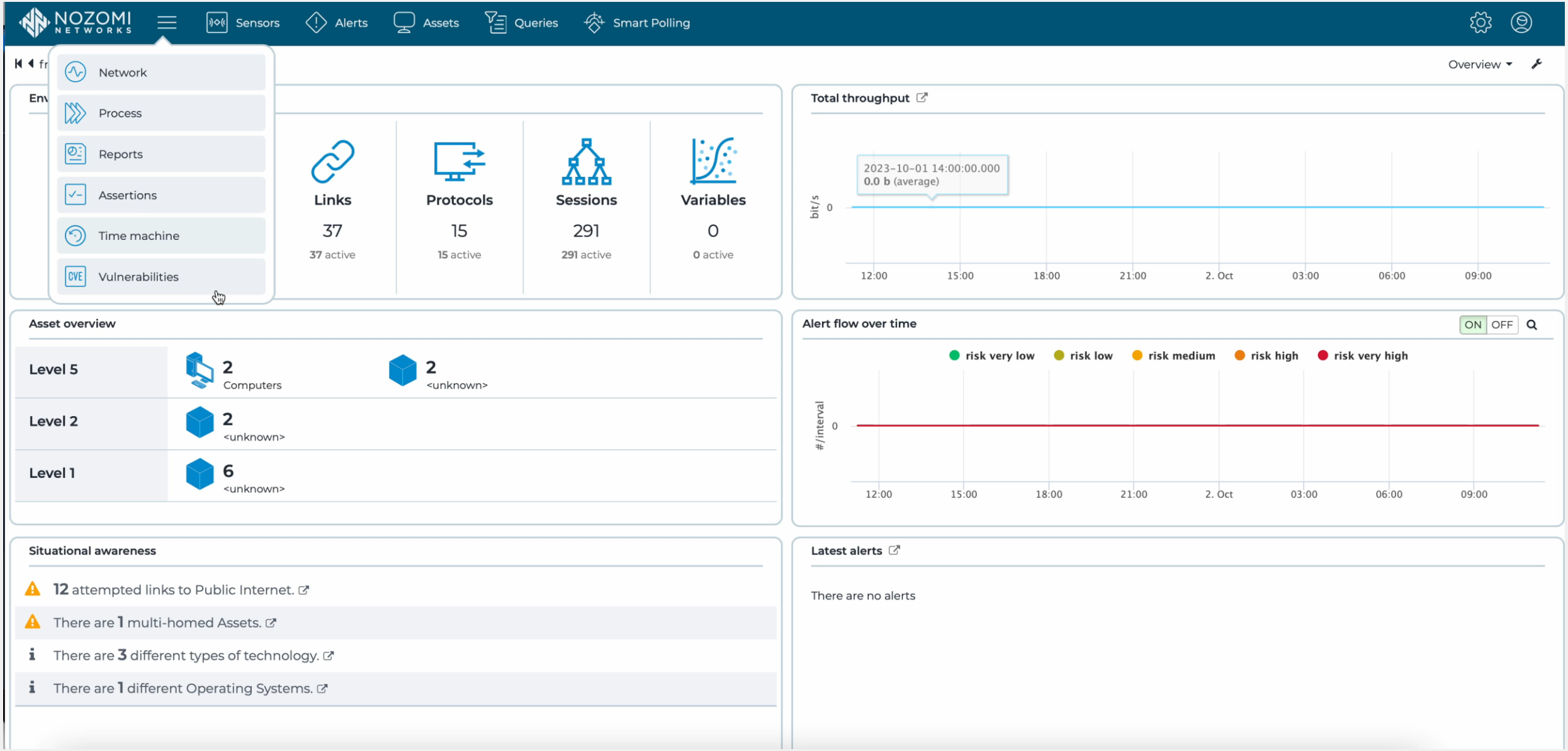
FR 2 – Use control (UC)		SL1	SL2	SL3	SL4
SR 2.1 – Authorization enforcement	6.3	✓	✓	✓	✓

Network segmentation improvement

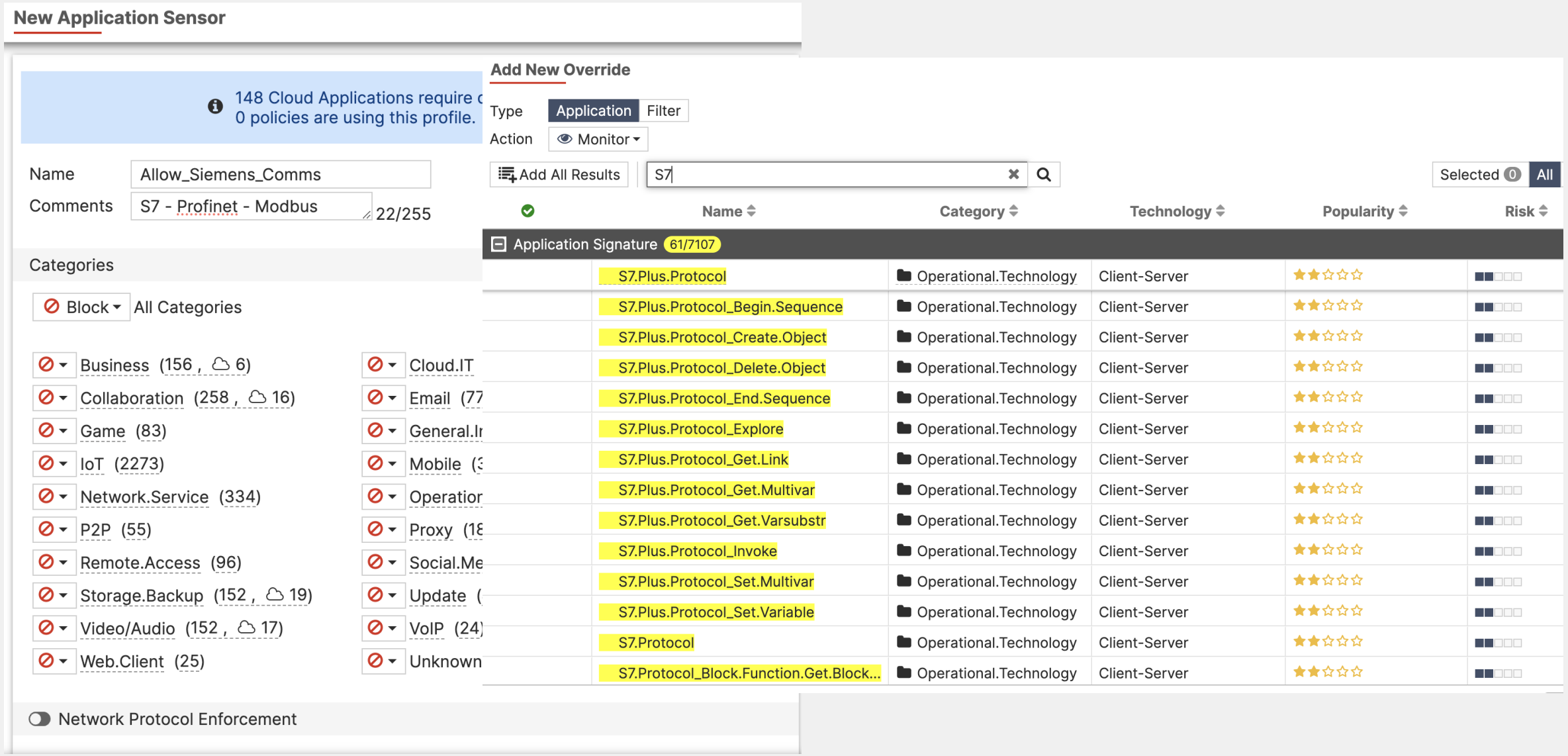




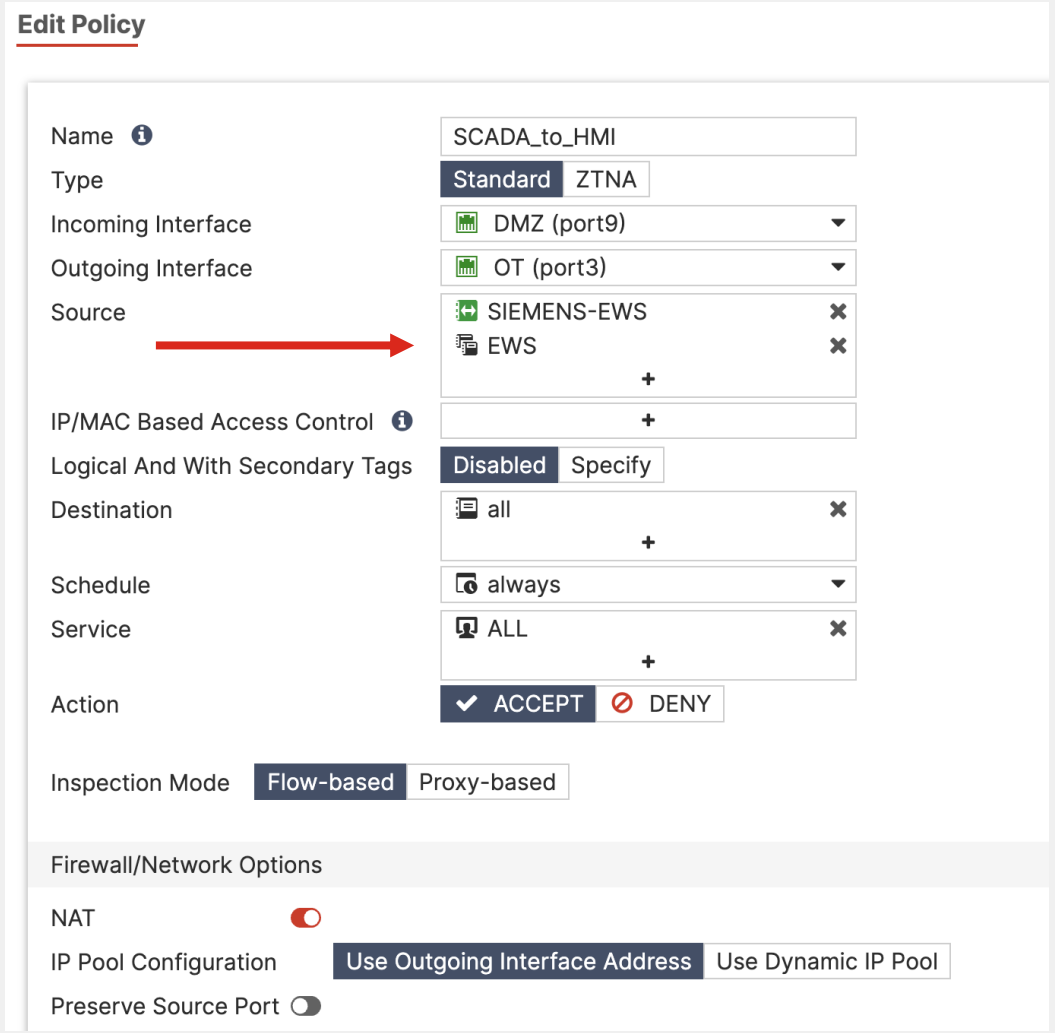
Firewall Integration Video Attacker

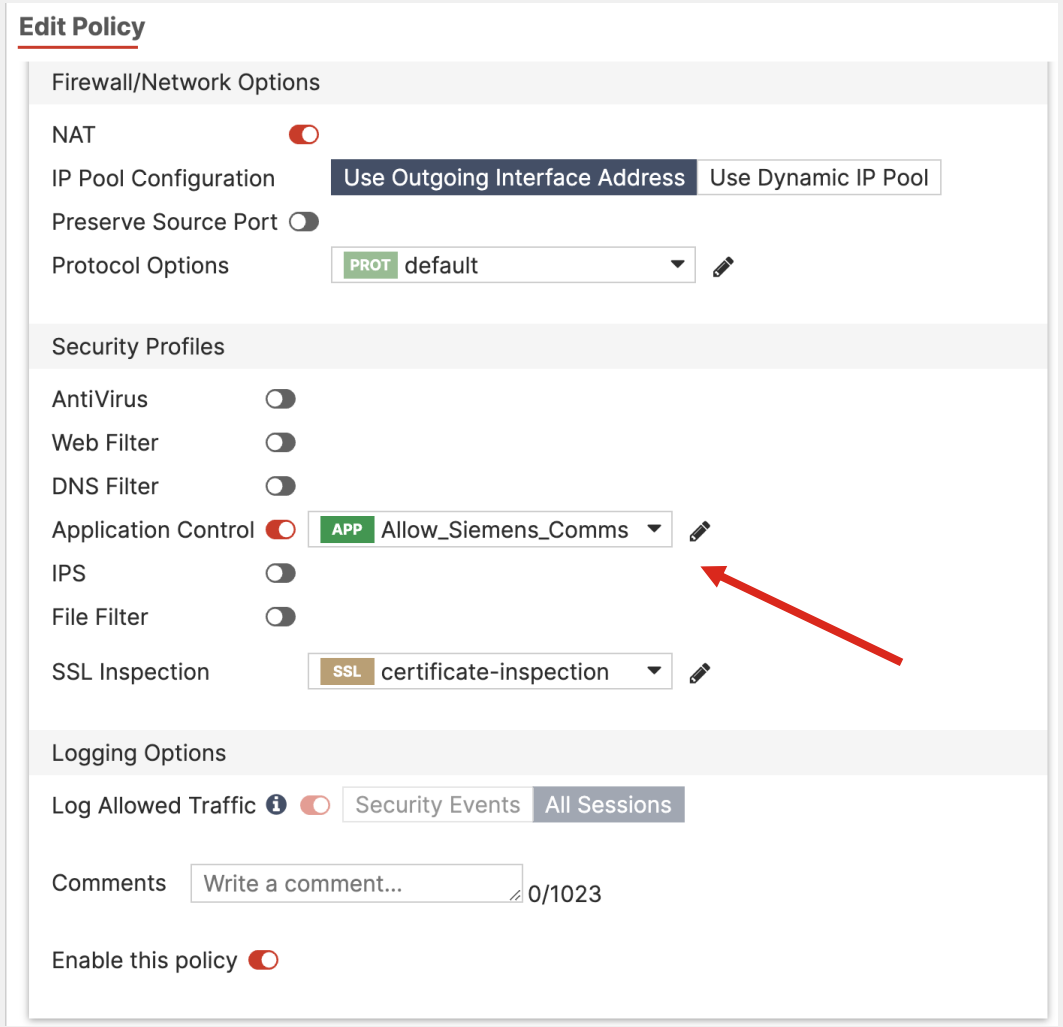


Network segmentation improvement



Network segmentation improvement





Pascal Ackerman · Following

OT/ICS/IOT Pentester | Threat Hunter | Incident Responder | Hacker | Tinkere...

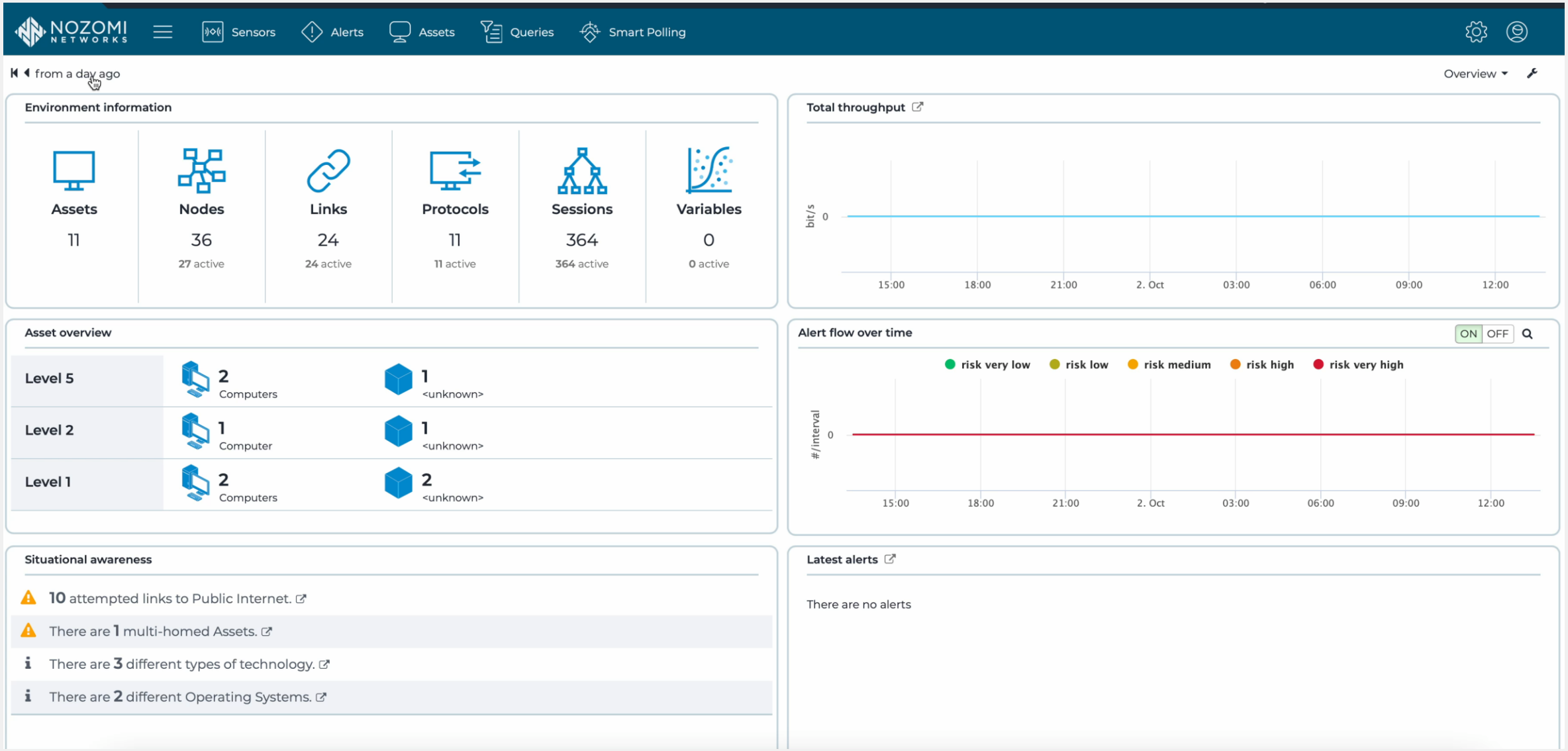
11h ·

The top 10 most observed network missconfigurations, discovered during Red and Blue team assessments by NSA and CISA Hunt and Incident Response teams include:

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

76 3 comments · 8 reposts

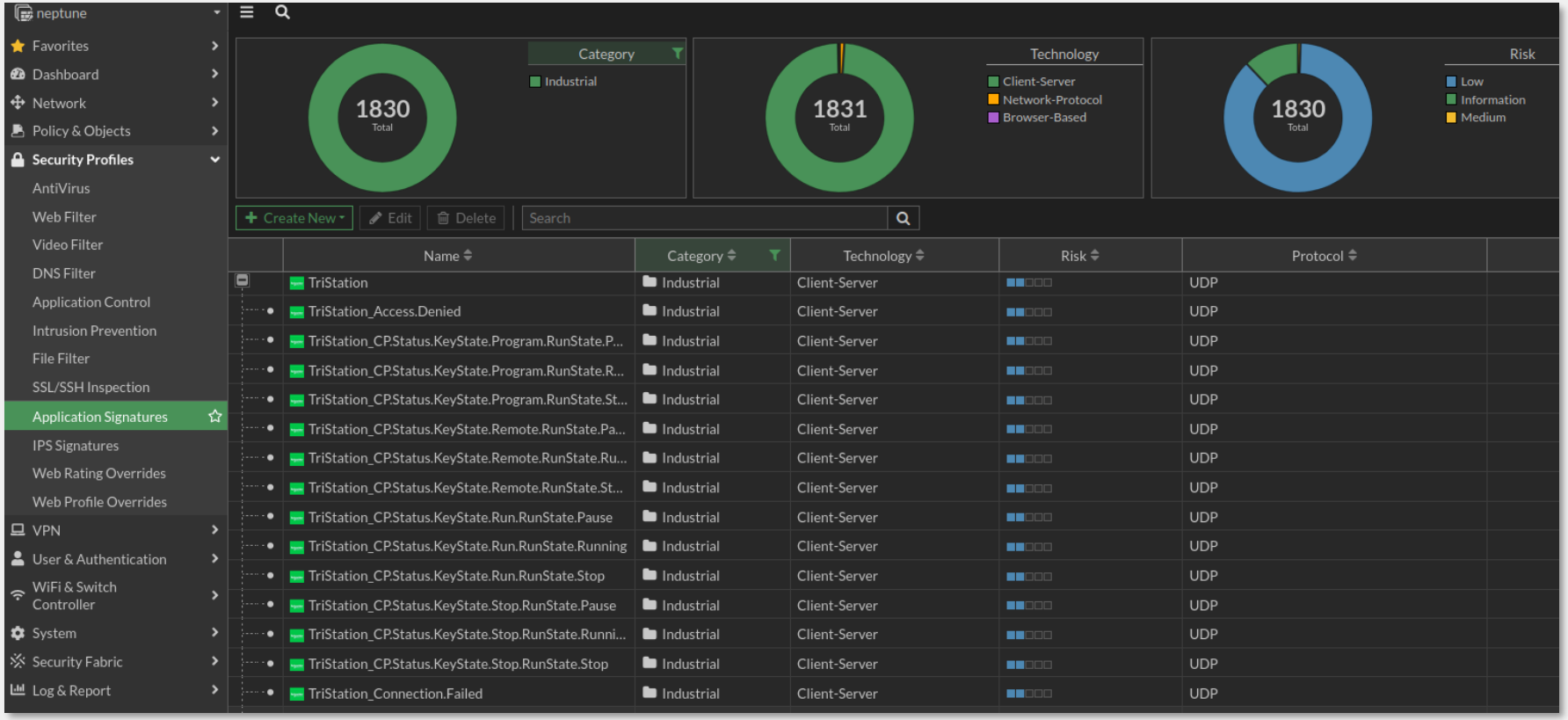
Firewall Integration Video: Engineering Workstation Compromised



16

FortiGuard Industrial Services for ICS and OT

2100+ Application Control Selectors giving visibility and control over OT & ICS protocols.



- Application Control intelligence provided through the FortiGuard Industrial Security Service.
- FortiGuard Labs, our industry-leading vulnerability research organization delivers broad industrial application intelligence offering World Class ICS communications granularity at the policy level.

Filter by Industrial Security:

- ○ Industrial Security - IPS (612)
- ○ Industrial Security - APP Control (2147)
- ○ IoT Intrusion Prevention (117)
- ○ IoT Application Control (1322)

Application Control, Deep Packet Inspection (DPI), and Intrusion Prevention System (IPS) Signatures for ICS Protocols and Applications Context Logging to Syslog, FortiAnalyzer, FortiSIEM, and more

Application Control for Industrial Control Systems

2,100+ Granular OT/ICSApplication Controls (DNP3 Example)

- DNP3
- DNP3_Abort.File
- DNP3_Activate.Config
- DNP3_Assign.Class
- DNP3_Authenticate.File
- DNP3_Authentication.Error
- DNP3_Authentication.Request
- DNP3_Close.File
- DNP3_Cold.Restart
- DNP3_Confirm
- DNP3_Delay.Measurement
- DNP3_Delete.File
- DNP3_Direct.Operate
- DNP3_Direct.Operate.Without.Ack
- DNP3_Disable.Spontaneous.Messages
- DNP3_Enable.Spontaneous.Messages
- DNP3_Freeze.And.Clear
- DNP3_Freeze.And.Clear.Without.Ack
- DNP3_Freeze.With.Time
- DNP3_Freeze.With.Time.Without.Ack
- DNP3_Get.File.Info
- DNP3_Immediate.Freeze
- DNP3_Immediate.Freeze.Without.Ack
- DNP3_Initialize.Application
- DNP3_Initialize.Data
- DNP3_Open.File
- DNP3_Operate
- DNP3_Read
- DNP3_Record.Current.Time
- DNP3_Response
- DNP3_Save.Configuration
- DNP3_Select
- DNP3_Start.Application
- DNP3_Stop.Application
- DNP3_Unsolicited.Message
- DNP3_Warm.Restart
- DNP3_Write

SEP 2023

FortiGuard Industrial Security Service

IPS & Application Control Signatures for ICS/OT Protocols

Allen-Bradley DF-1 →	Ether-S-Bus →	MMS →	Profinet IO →
Allen-Bradley PCCC →	Ether-S-I/O →	Modbus TCP/IP ⇉	Rockwell FactoryTalk View SE
Beckhoff AMS →	EtherCAT →	Moxa Modbus RTU →	**Rockwell FactoryTalk ViewPoint**
BSAP	Ethernet POWERLINK	Moxa UDP Device Discovery	Schneider UMAS →
BACnet →	EtherNet/IP-CIP →	MTConnect	**SECS-II/GEM →**
CC-Link →	FactorySuite NMXSVC	Niagara Fox	**Siemens OCG ATCS →**
CN/IP CEA-852 →	FL-NET →	oBIX	Siemens LOGO →
CoAP →	GE EGD	**OCPP →**	Siemens S7 →
DDSI-RTPS	GE SRTP →	Omron FINS →	Siemens S7 1200 →
Digi ADDP →	Hart IP →	OPC AE →	Siemens S7 Plus →
Digi RealPort (Net C/X)	IEC 60870-5-104 ⇉	OPC Common →	Siemens SIMATIC CAMP →
Digi RealPort (Net C/X) DNP3 ⇉	IEC 60870-6 (ICCP/TASE.2) →	OPC DA →	STANAG 4406 Military Messaging
Direct Message Profile →	IEC 61850 →	OPC DA Automation	STANAG 5066
DLMS/COSEM(IEC62056) →	IEC 61850-90-5 R-GOOSE	OPC HDA →	Triconex TSAA →
DNP3 →	IEC 61850-90-5 R-SV	OPC HDA Automation →	TriStation →
ECHONET Lite →	IEEE 1278.2 DIS →	OPC UA →	Veeder-Root ATG
ECOM100	IEEE C37.118 Synchrophasor →	OpenADR →	Vnet/IP
ELCOM 90 →	KNXnet/IP (EIBnet/IP) →	OSIsoft Asset Framework	**WITS0**
Emerson DeltaV	LonTalk IEC14908-1 CNP →	OSISoft PI	
Emerson ROC	Mitsubishi MELSEC →	Profinet CBA →	

Recent additions/ updates

→ message layer policy ⇉ message and parameter policy (FortiOS v6.4 and above)

FortiGuard Industrial Security Service provides broader coverage for Industrial Control System and Operational Technology applications and protocols through Application Control (AppCtrl) and IPS signatures. **For up to date list of supported signatures, please visit fortiguard.com.**

Entire list: https://www.fortiguard.com/appcontrol?category=Industrial **Submit new (signature) request:** https://www.fortiguard.com/learnmore#is

Q&A

NOZOMI NETWORKS + FORTINET

ISA/IEC 62443: How to gain insight in your assets and how to protect them

Jeffrey Noya - Regional Systems Engineer

NNCE, NNAT, NSE4, NSE5, NSE7 OT & EFW certified

Arjan Aelmans - OT Specialist Systems Engineer

NSE7 OT & ATP, ISA/IEC 62443 Expert certified

Agenda

Session 1:

Optimizing Segmentation with ISA/IEC 62443

Q&A

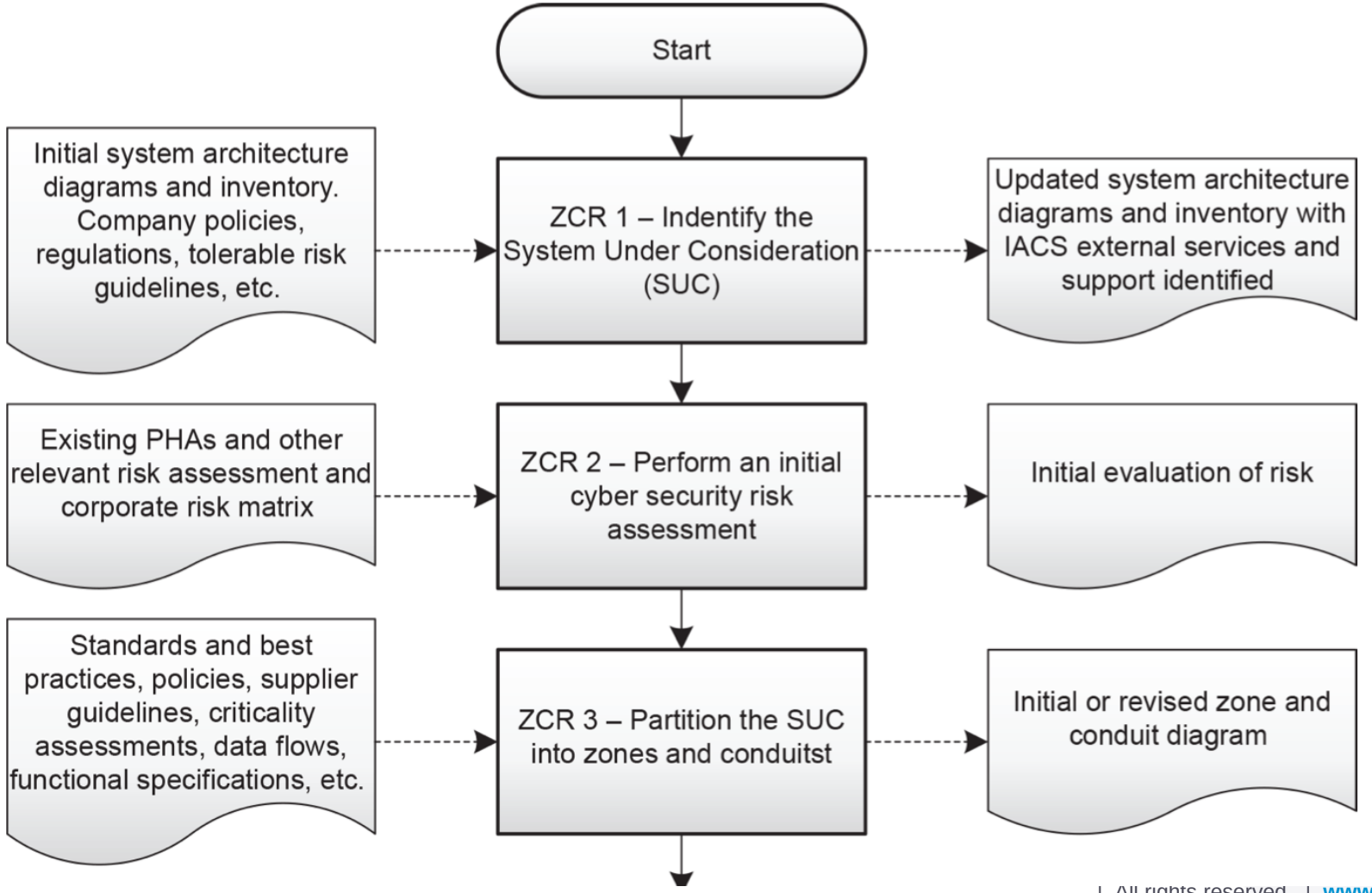
BREAK

Session 2:

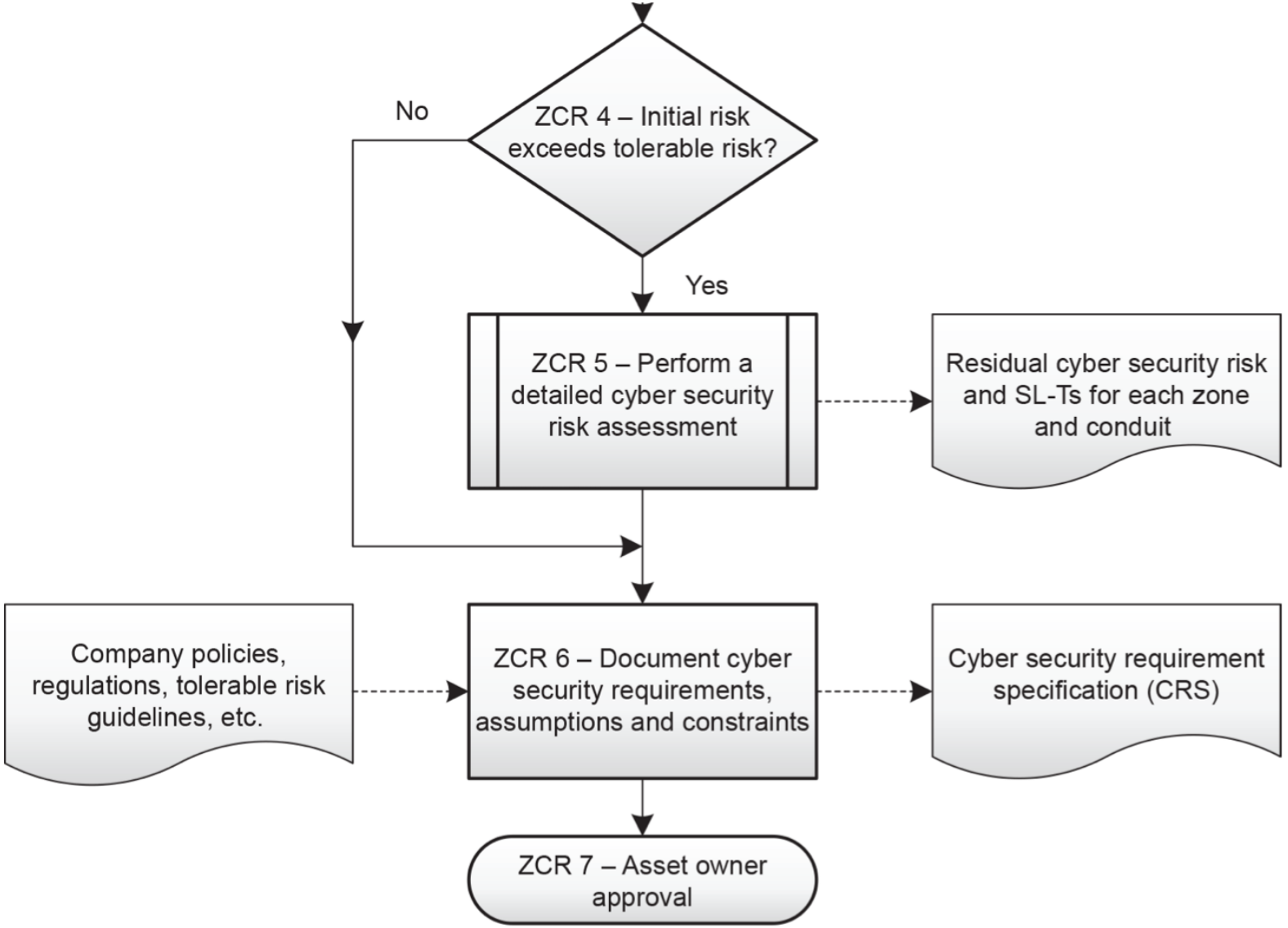
Network and asset based attack perspective

Q&A

62443-3-2: Primary steps required to establish zones and conduits, as well as to assess risk – part 1



62443-3-2: Primary steps required to establish zones and conduits, as well as to assess risk – part 2



4.2.1 ZCR 1.1: Identify the SUC perimeter and access points

4.2.1.1 Requirement

The organization shall clearly identify the SUC, including clear demarcation of the security perimeter and identification of all access points to the SUC.

4.2.1.2 Rationale and supplemental guidance

Organizations typically own and operate multiple control systems, especially larger organizations with multiple industrial facilities. Any of these control systems may be defined as a SUC. For example, there is generally at least one control system at an industrial facility, but oftentimes there are several systems that control various functions within the facility.

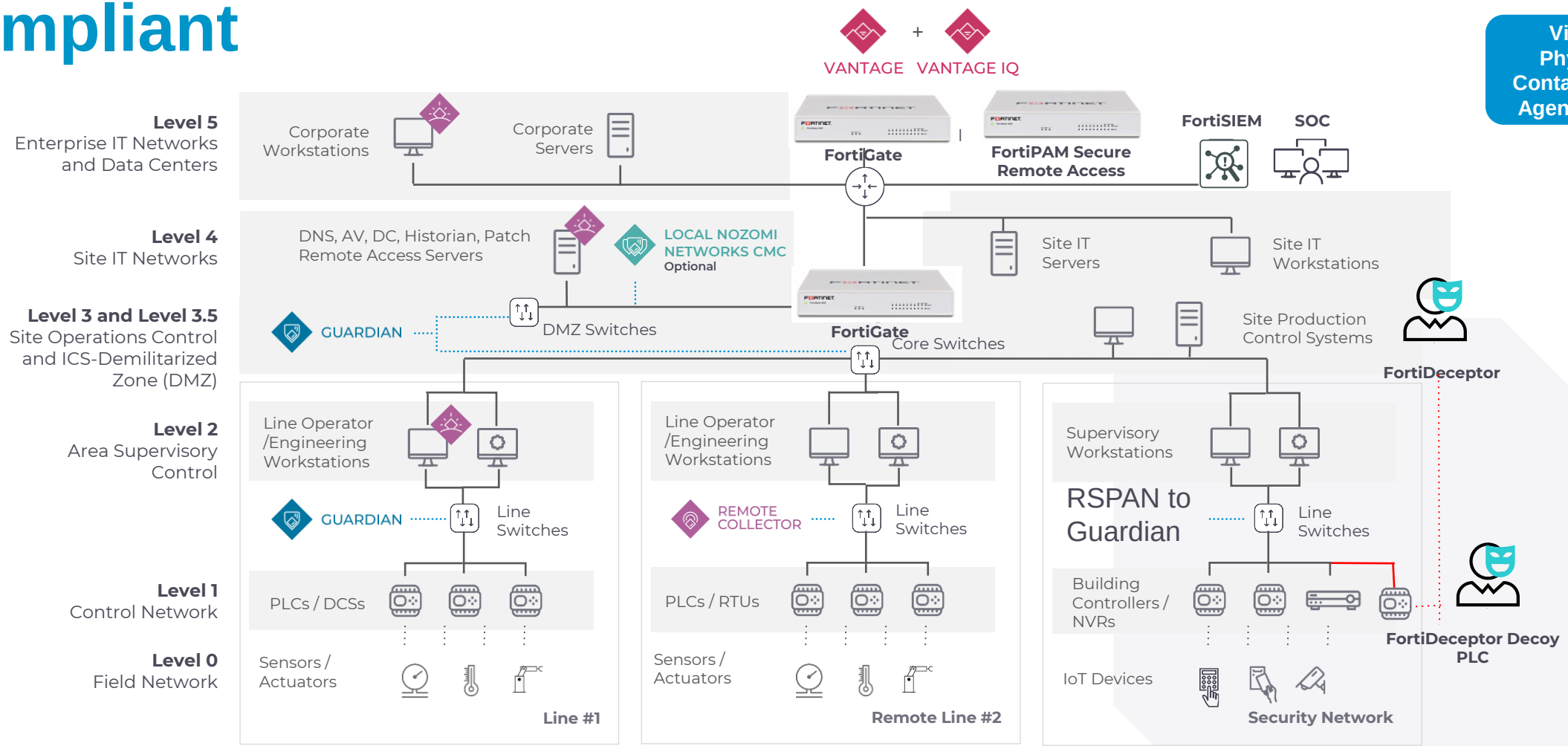
This requirement specifies that SUCs are identified for the purpose of performing cyber security analysis. The definition of a SUC is intended to include all IACS assets that are needed to provide a complete automation solution.

System inventory, architecture diagrams, network diagrams and dataflows can be used to determine and illustrate the IACS assets that are included in the SUC description.

NOTE The SUC can include multiple subsystems such as basic process control systems (BPCSs), distributed control systems (DCSs), safety instrumented systems (SISs), supervisory control and data acquisition (SCADA) and IACS product supplier's packages. This could also include emerging technologies such as the industrial Internet of Things (IIoT) or cloud-based solutions.

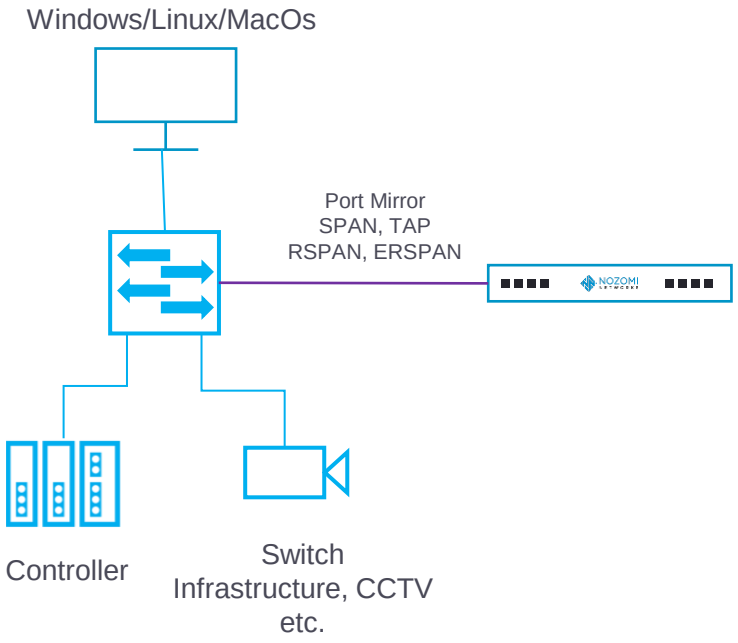
Nozomi Networks + Fortinet Architecture - IEC 62443 Compliant

Virtual
Physical
Containerized
Agent Based



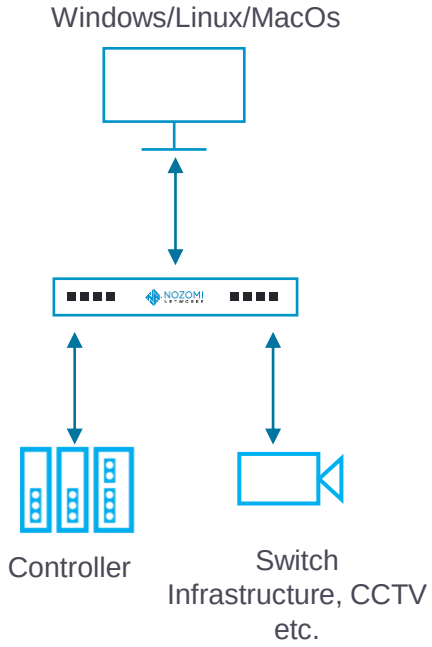
Asset Inventory

Passive Network Monitoring
(Deep Packet Inspection)



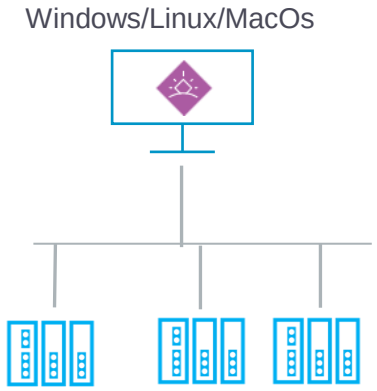
Monitors network traffic

Active Querying
(Nozomi Smart Polling)



Queries assets using native protocols

Host Based Monitoring
(Nozomi Arc Sensor)



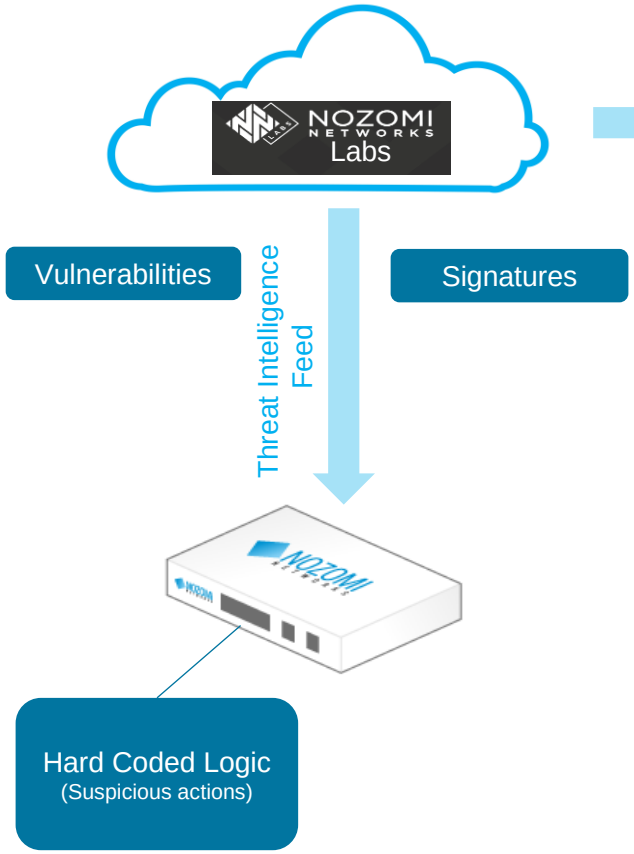
Detailed host information
Sigma Rules (indication of Compromise)
USB Detection
Deep Packet Inspection

Make, model, OS/firmware, serial no. etc. → NOZOMI NETWORKS LABS (Defending Critical Assets Against Cyber Risk) → Vulnerability Matching

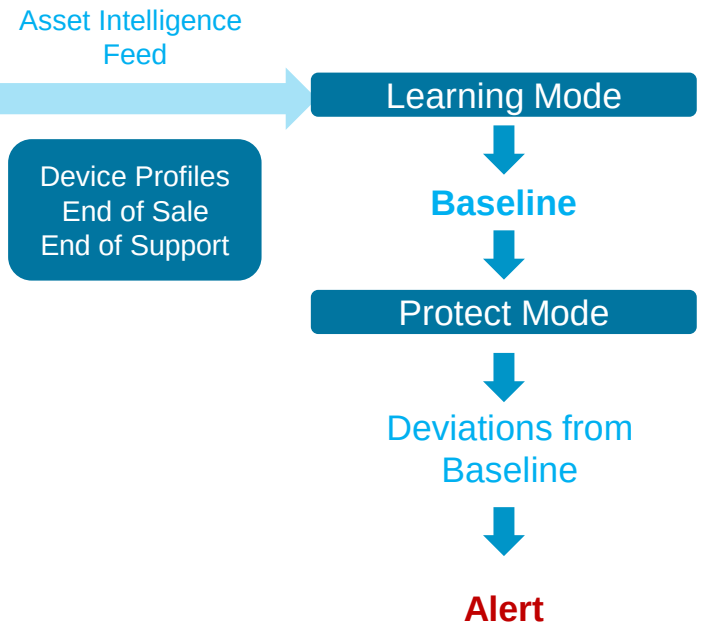
CVE Numbering Authority

Security and Operational Capabilities

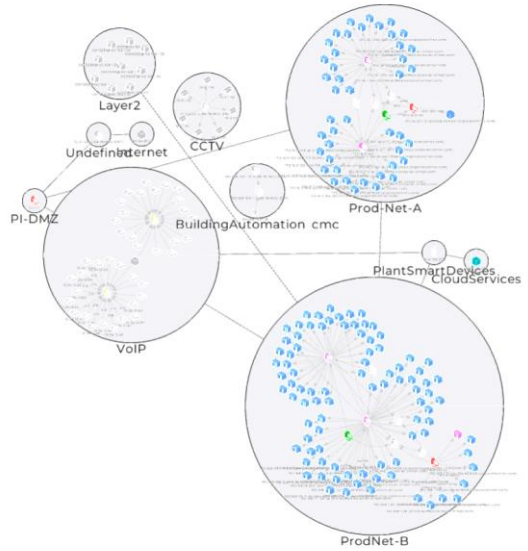
Known Threat Detection



Anomaly-Based Intrusion Detection (Zero Days)



Operational Insights



Communication Issues
Failed Devices
Virtual segmentation (IEC62443)

Advanced Deception and Honeypot

Deceive

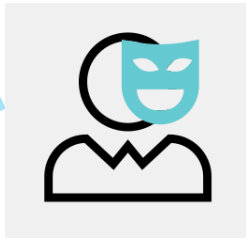
- Decoy OT Controllers and PLC's
- Feedback access attempts
- Learn about your attacker

Expose

Threat Intelligence Feed

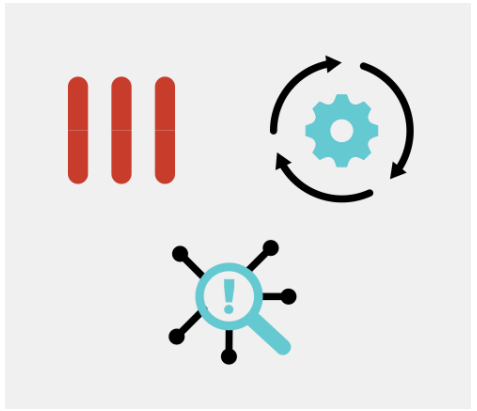
Provide feedback of events

Mimic real controllers



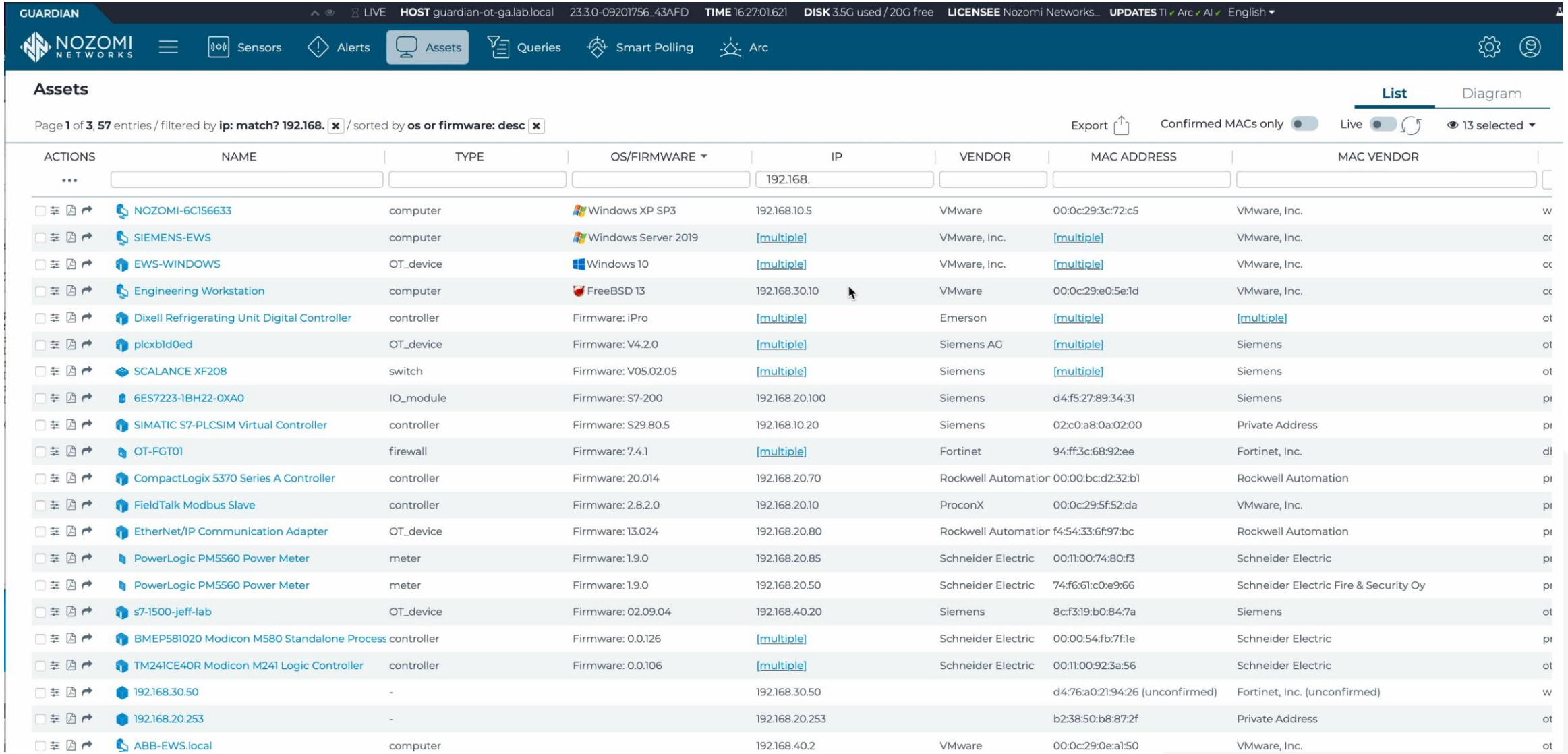
- Increase cost of attacker
- Cut down breach detection time

Eliminate



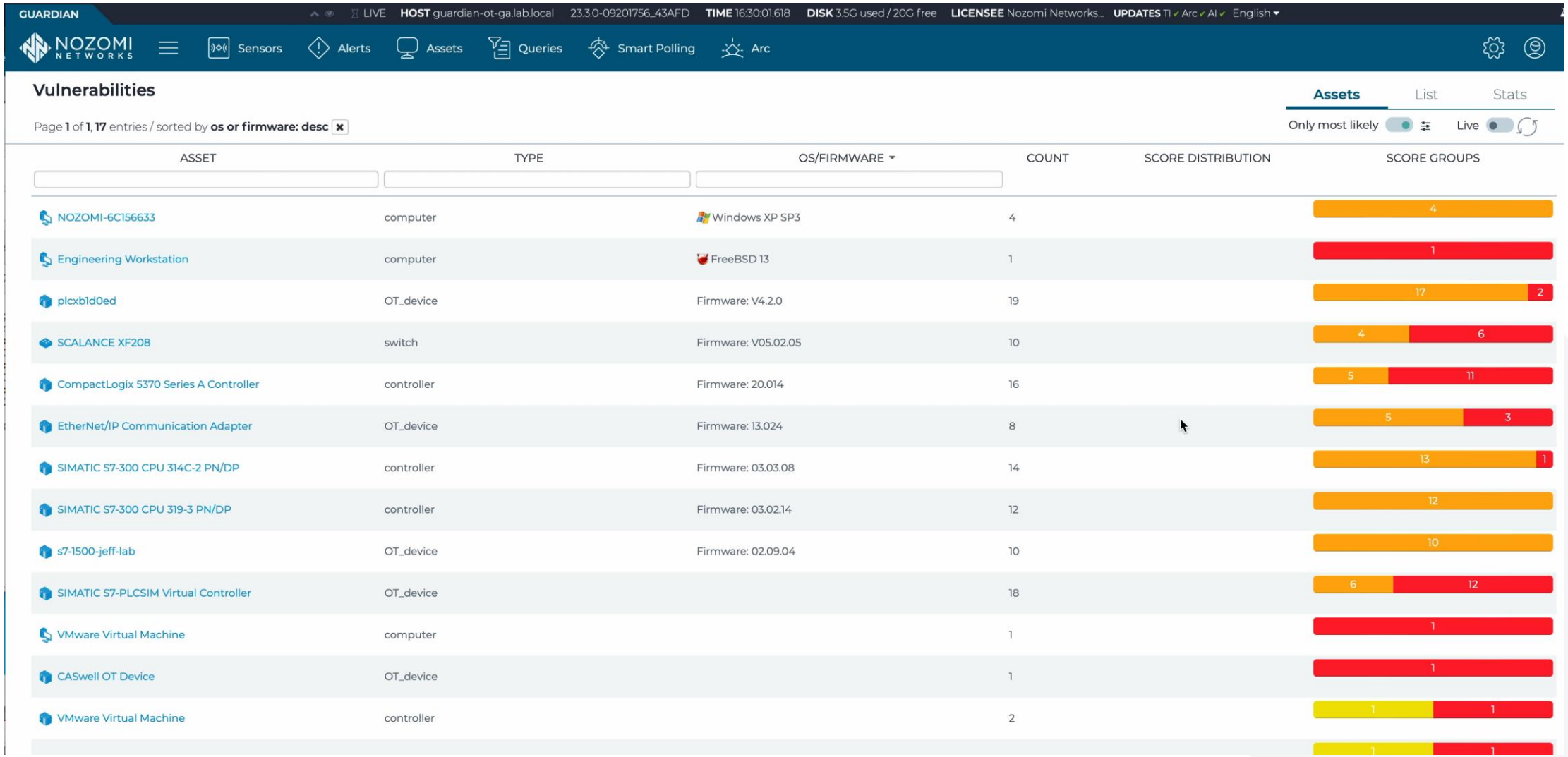
- Alerting send to SIEM, SOAR, Firewall
- Auto-Quarantaine

Identifying the assets

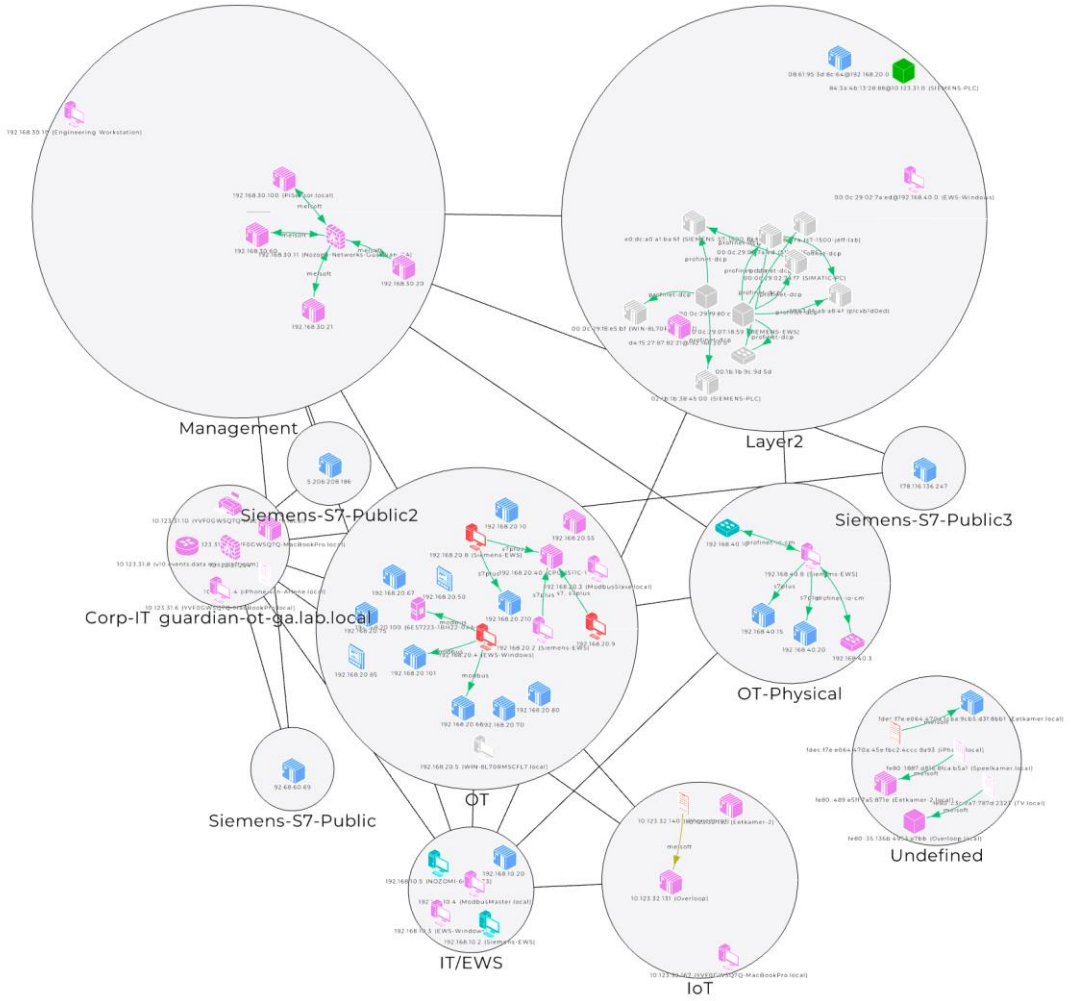


ACTIONS	NAME	TYPE	OS/FIRMWARE	IP	VENDOR	MAC ADDRESS	MAC VENDOR
				192.168.			
	NOZOMI-6C156633	computer	Windows XP SP3	192.168.10.5	VMware	00:0c:29:3c:72:c5	VMware, Inc.
	SIEMENS-EWS	computer	Windows Server 2019	[multiple]	VMware, Inc.	[multiple]	VMware, Inc.
	EWS-WINDOWS	OT_device	Windows 10	[multiple]	VMware, Inc.	[multiple]	VMware, Inc.
	Engineering Workstation	computer	FreeBSD 13	192.168.30.10	VMware	00:0c:29:e0:5e:1d	VMware, Inc.
	Dixell Refrigerating Unit Digital Controller	controller	Firmware: iPro	[multiple]	Emerson	[multiple]	[multiple]
	plcxb1d0ed	OT_device	Firmware: V4.2.0	[multiple]	Siemens AG	[multiple]	Siemens
	SCALANCE XF208	switch	Firmware: V05.02.05	[multiple]	Siemens	[multiple]	Siemens
	6ES7223-1BH22-0XA0	IO_module	Firmware: S7-200	192.168.20.100	Siemens	d4:f5:27:89:34:31	Siemens
	SIMATIC S7-PLCSIM Virtual Controller	controller	Firmware: S29.80.5	192.168.10.20	Siemens	02:c0:a8:0a:02:00	Private Address
	OT-FGT01	firewall	Firmware: 7.4.1	[multiple]	Fortinet	94:ff:3c:68:92:ee	Fortinet, Inc.
	CompactLogix 5370 Series A Controller	controller	Firmware: 20.014	192.168.20.70	Rockwell Automatior	00:00:bc:d2:32:b1	Rockwell Automation
	FieldTalk Modbus Slave	controller	Firmware: 2.8.2.0	192.168.20.10	ProconX	00:0c:29:5f:52:da	VMware, Inc.
	EtherNet/IP Communication Adapter	OT_device	Firmware: 13.024	192.168.20.80	Rockwell Automatior	f4:54:33:6f:97:bc	Rockwell Automation
	PowerLogic PM5560 Power Meter	meter	Firmware: 1.9.0	192.168.20.85	Schneider Electric	00:11:00:74:80:f3	Schneider Electric
	PowerLogic PM5560 Power Meter	meter	Firmware: 1.9.0	192.168.20.50	Schneider Electric	74:f6:61:c0:e9:66	Schneider Electric Fire & Security Oy
	s7-1500-jeff-lab	OT_device	Firmware: 02.09.04	192.168.40.20	Siemens	8c:f3:19:b0:84:7a	Siemens
	BMEP581020 Modicon M580 Standalone Process	controller	Firmware: 0.0.126	[multiple]	Schneider Electric	00:00:54:fb:7f:1e	Schneider Electric
	TM241CE40R Modicon M241 Logic Controller	controller	Firmware: 0.0.106	[multiple]	Schneider Electric	00:11:00:92:3a:56	Schneider Electric
	192.168.30.50	-		192.168.30.50		d4:76:a0:21:94:26 (unconfirmed)	Fortinet, Inc. (unconfirmed)
	192.168.20.253	-		192.168.20.253		b2:38:50:b8:87:2f	Private Address
	ABB-EWS.local	computer		192.168.40.2	VMware	00:0c:29:0e:a1:50	VMware, Inc.

Vulnerability assements (multiple assets)



Mapping and visualizing your network

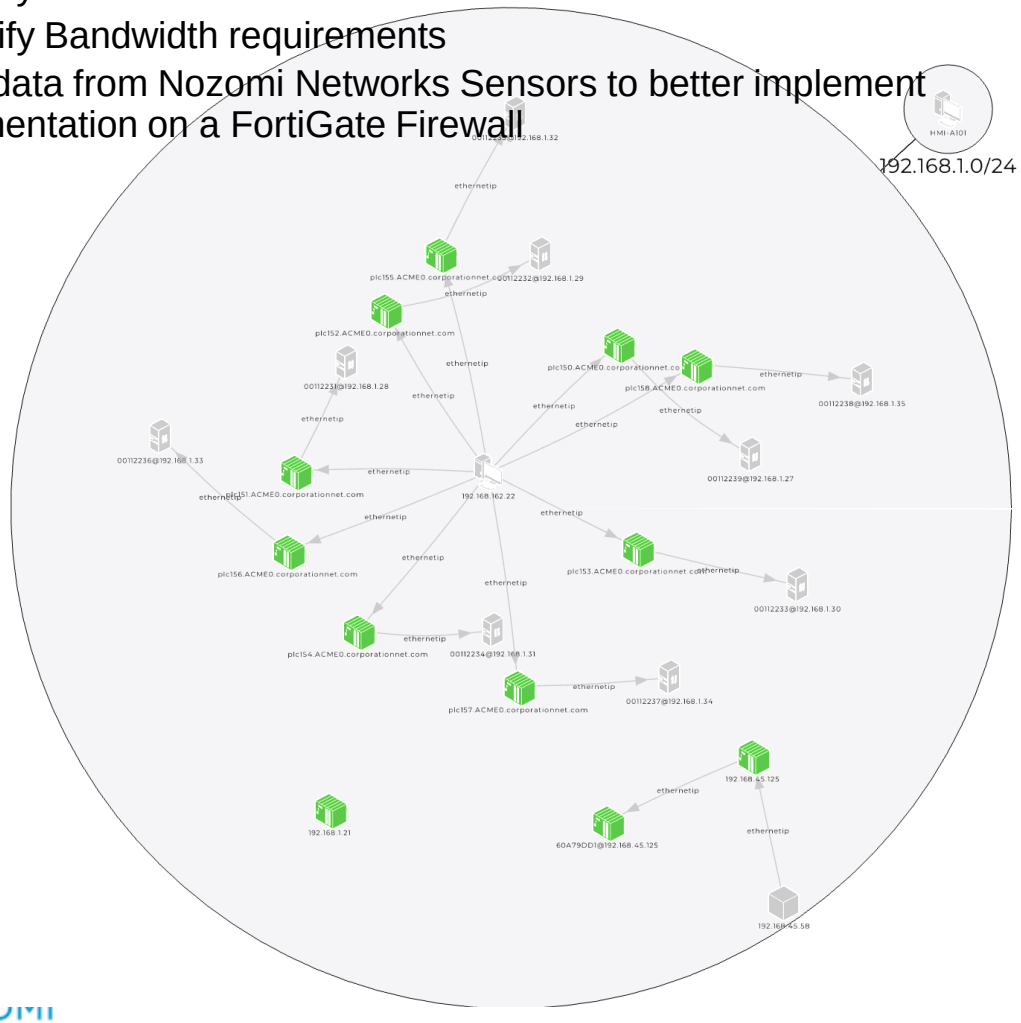


 www.nozominetworks.com

Segmentation

See who is communicating with who even within the same Layer 2 segment

- Identify Source Ports
- Identify Destination Ports
- Identify Bandwidth requirements
- Use data from Nozomi Networks Sensors to better implement segmentation on a FortiGate Firewall



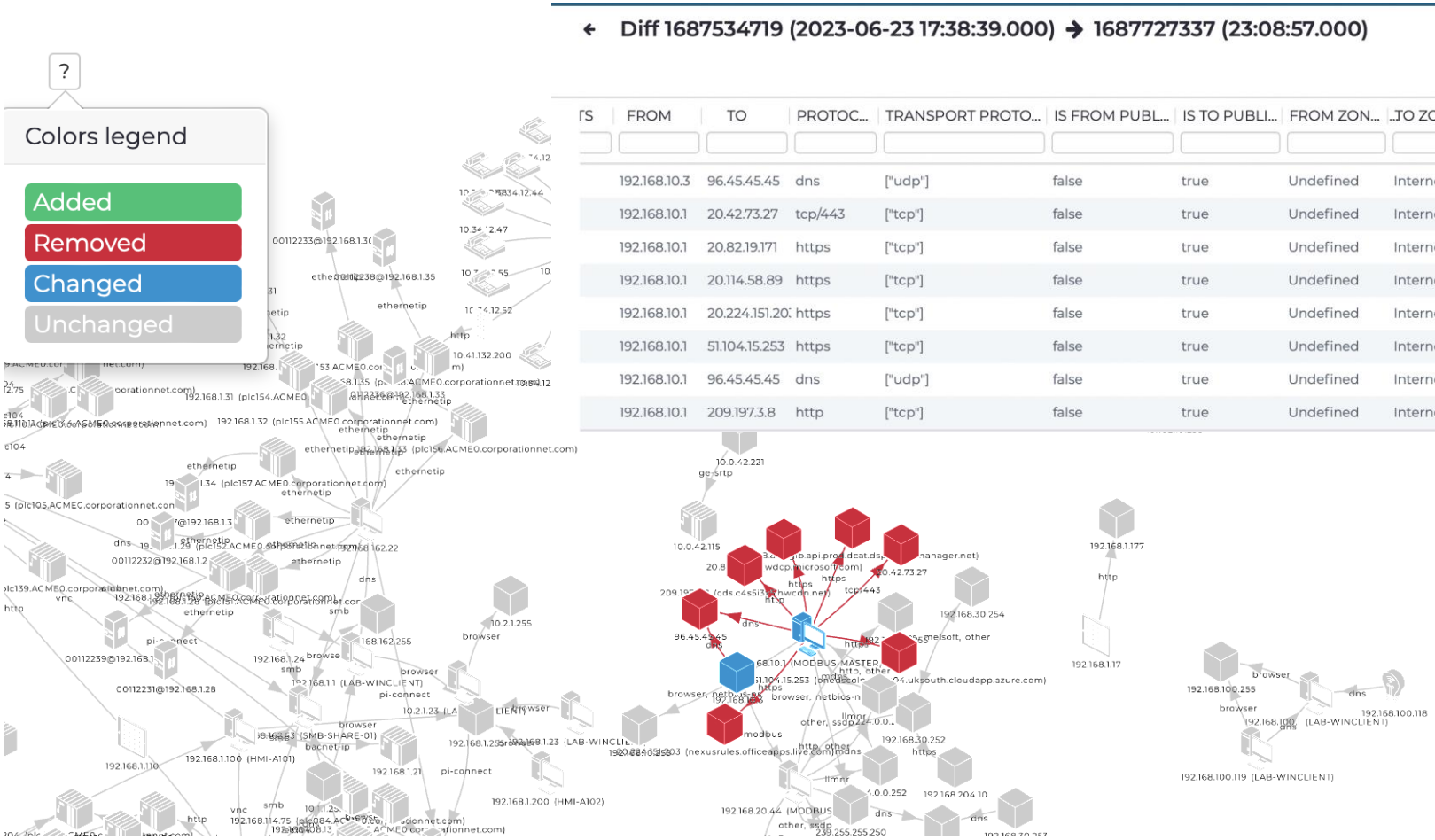
Network view

Page **1** of **48**, **1190** entries

ACTIONS	STATUS	FROM	TO	PROTOC...	TRANSPORT PROT...	FROM POR...	TO PORT ...	THROUGHP...
	CLOSED	10.105.113.99	10.102.164.17	http	tcp	25082	80	0.0 b/s
	CLOSED	172.16.4.89	192.168.175.10	cotp	tcp	49391	102	0.0 b/s
	CLOSED	172.16.4.89	192.168.115.74	cotp	tcp	49391	102	0.0 b/s
	CLOSED	172.16.4.89	192.168.20.20	cotp	tcp	49391	102	0.0 b/s
	CLOSED	172.16.4.89	192.168.114.20	cotp	tcp	49391	102	0.0 b/s
	CLOSED	172.16.4.89	192.168.114.74	cotp	tcp	49391	102	0.0 b/s
	CLOSED	172.16.4.89	192.168.170.14	cotp	tcp	49391	102	0.0 b/s
	CLOSED	172.16.4.89	192.168.107.25	cotp	tcp	49391	102	0.0 b/s
	CLOSED	172.16.4.89	192.168.231.74	cotp	tcp	49391	102	0.0 b/s
	CLOSED	172.16.4.89	192.168.19.76	cotp	tcp	49391	102	0.0 b/s
	CLOSED	172.16.4.89	192.168.21.10	cotp	tcp	49391	102	0.0 b/s
	CLOSED	10.5.1.253	10.4.1.31	rtsp	tcp	58854	560	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	50369	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	42505	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	49449	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	49281	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	57640	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	62256	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	34169	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	51400	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	52528	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	36913	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	37081	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	63328	53	0.0 b/s
	ACTIVE	192.168.100.11	192.168.100.1	dns	udp	33793	53	0.0 b/s

Know what changes on your network

Timemachine allows you to compare snapshots of the network with eachother to track changes.



Diff 1687534719 (2023-06-23 17:38:39.000) → 1687727337 (23:08:57.000)

Nodes | Links | Variables | Graph

+ Added (0) − Removed (8) ⇄ Changed (0)

TS	FROM	TO	PROTOC...	TRANSPORT PROTO...	IS FROM PUBL...	IS TO PUBLI...	FROM ZON...	TO ZONE	FROM POR...	TO PORT...	FIRST ACTIVI...	LAST ACTIVI...	LAST HANDSHA...	# ALERT...	LAST
	192.168.10.3	96.45.45.45	dns	["udp"]	false	true	Undefined	Internet	-	-	2023-06-20 11:41:5	2023-06-20 11:41:!	never	2	never
	192.168.10.1	20.42.73.27	tcp/443	["tcp"]	false	true	Undefined	Internet	-	-	2023-06-21 10:38:4	2023-06-21 10:38:	2023-06-21 10:38:48.3	3	never
	192.168.10.1	20.82.19.171	https	["tcp"]	false	true	Undefined	Internet	-	-	2023-06-21 10:38:4	2023-06-21 10:38:	2023-06-21 10:38:46.3	1	never
	192.168.10.1	20.114.58.89	https	["tcp"]	false	true	Undefined	Internet	-	-	2023-06-21 08:54:	2023-06-21 08:56	2023-06-21 08:54:06.4	1	never
	192.168.10.1	20.224.151.20	https	["tcp"]	false	true	Undefined	Internet	-	-	2023-06-21 08:54:	2023-06-21 08:56	2023-06-21 08:54:59.3	1	never
	192.168.10.1	51.104.15.253	https	["tcp"]	false	true	Undefined	Internet	-	-	2023-06-21 10:37:1	2023-06-21 10:37:	2023-06-21 10:37:23.9	1	never
	192.168.10.1	96.45.45.45	dns	["udp"]	false	true	Undefined	Internet	-	-	2023-06-20 10:12:	2023-06-21 10:39:	never	0	never
	192.168.10.1	209.197.3.8	http	["tcp"]	false	true	Undefined	Internet	-	-	2023-06-21 08:54:	2023-06-21 09:02	2023-06-21 08:56:07.6	4	never

Compliancy reporting

- Nozomi provides a robust reporting engine with a number of default report templates that can provide a starting point for customization.
- Prebuild reports such as:
  - IEC 62443 2-1
  - IEC 62443 3-3

NOZOMI NETWORKS

CONFIDENTIAL

CREATED 2023-06-05 21:33 [CEST]
BY GUARDIAN guardian.nozomi.local

SR 3.4

Software and information integrity

The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.

Ensure that detections of the following actions are authorized changes to software at rest:
Firmware change, Program change, Program upload, A potentially unwanted application payload
Improve protection capabilities against the unauthorized changes if needed.

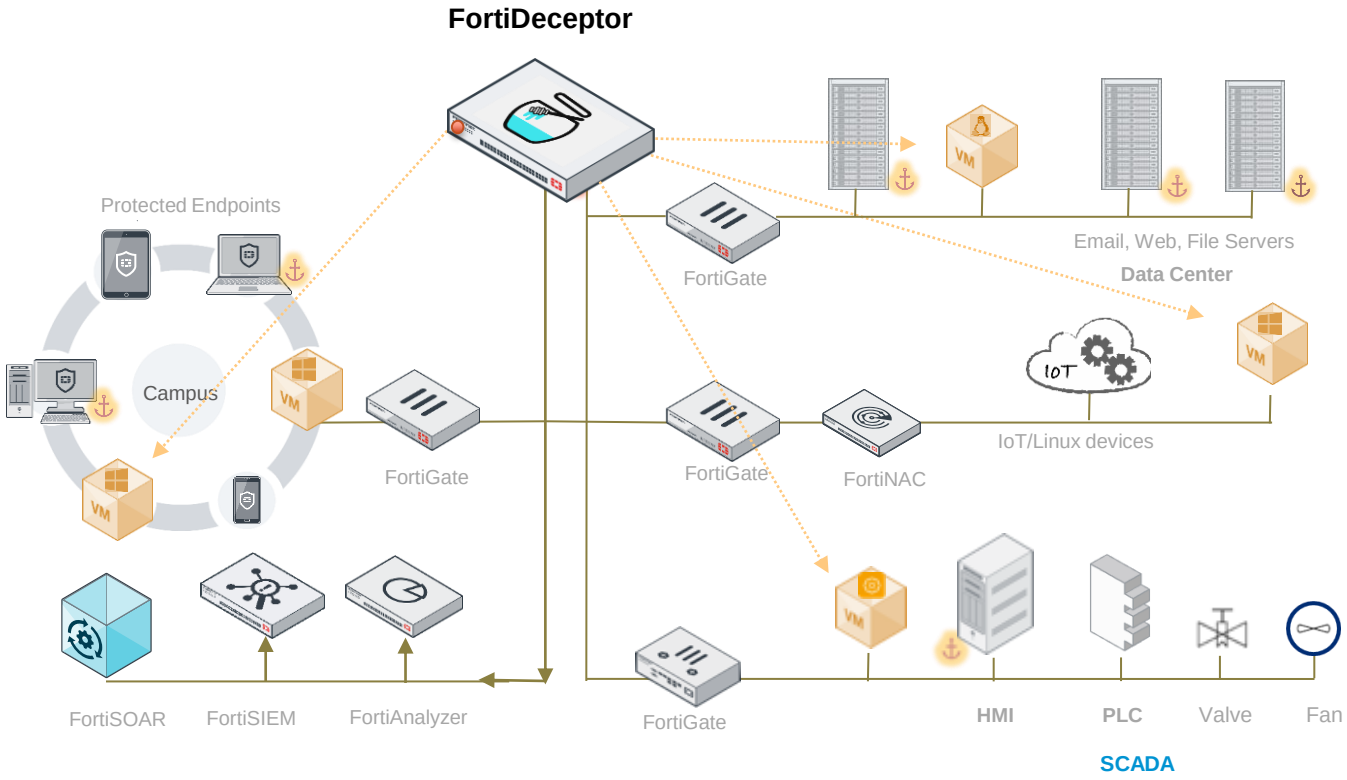
ISA62443_3-3 / SR 3-4

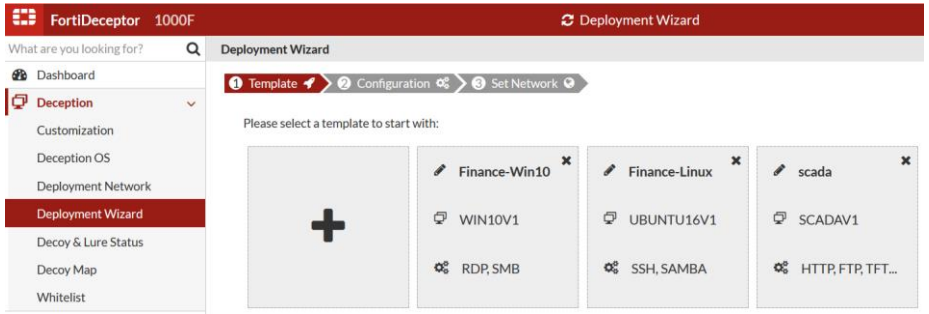
ID	TYPE	STATUS	MAC SRC	MAC DST	IP SRC	IP DST	RISK	PROTOCOL	DESCRIPTION	TIME
38edb94b-6827-48c2-b974-7eb3c13d016d	SIGN:PROGRAM:TRANSFER	open	00:0c:29:01:98:be	f4:54:33:9f:22:3d	192.168.45.58	192.168.45.125	6.0	ethernetip	Program transfer from device 192.168.45.58 to device 192.168.45.125	2023-05-30 15:27:27
ffdac73a-3daa-4f76-9137-07a20e2c1010	SIGN:PROGRAM:TRANSFER	open	00:50:56:a6:be:7b	00:09:91:03:a7:8a	10.0.42.221	10.0.42.115	6.0	ge-srtp	Program transfer from device 10.0.42.115 to device 10.0.42.221	2023-05-30 15:27:27
746ecd88-118e-49a0-a49f-6c7c934bc97f	SIGN:PROGRAM:TRANSFER	open	00:50:56:a6:be:7b	00:09:91:03:a7:8a	10.0.42.221	10.0.42.115	6.0	ge-srtp	Program transfer from device 10.0.42.115 to device 10.0.42.221	2023-05-30 15:27:27
18c3baca-d000-46aa-b88e-84c7ad731821	SIGN:PROGRAM:TRANSFER	open	00:50:56:a6:be:7b	00:09:91:03:a7:8a	10.0.42.221	10.0.42.115	6.0	ge-srtp	Program transfer from device 10.0.42.115 to device 10.0.42.221	2023-05-30 15:27:27
c4f6a8a3-f323-4d29-8aa5-29d4d77cfee9	SIGN:PROGRAM:TRANSFER	open	00:50:56:a6:be:7b	00:09:91:03:a7:8a	10.0.42.221	10.0.42.115	6.0	ge-srtp	Program transfer from device 10.0.42.115 to device 10.0.42.221	2023-05-30 15:27:27

NOZOMI NETWORKS

Deception: LifeCycle

Deceive



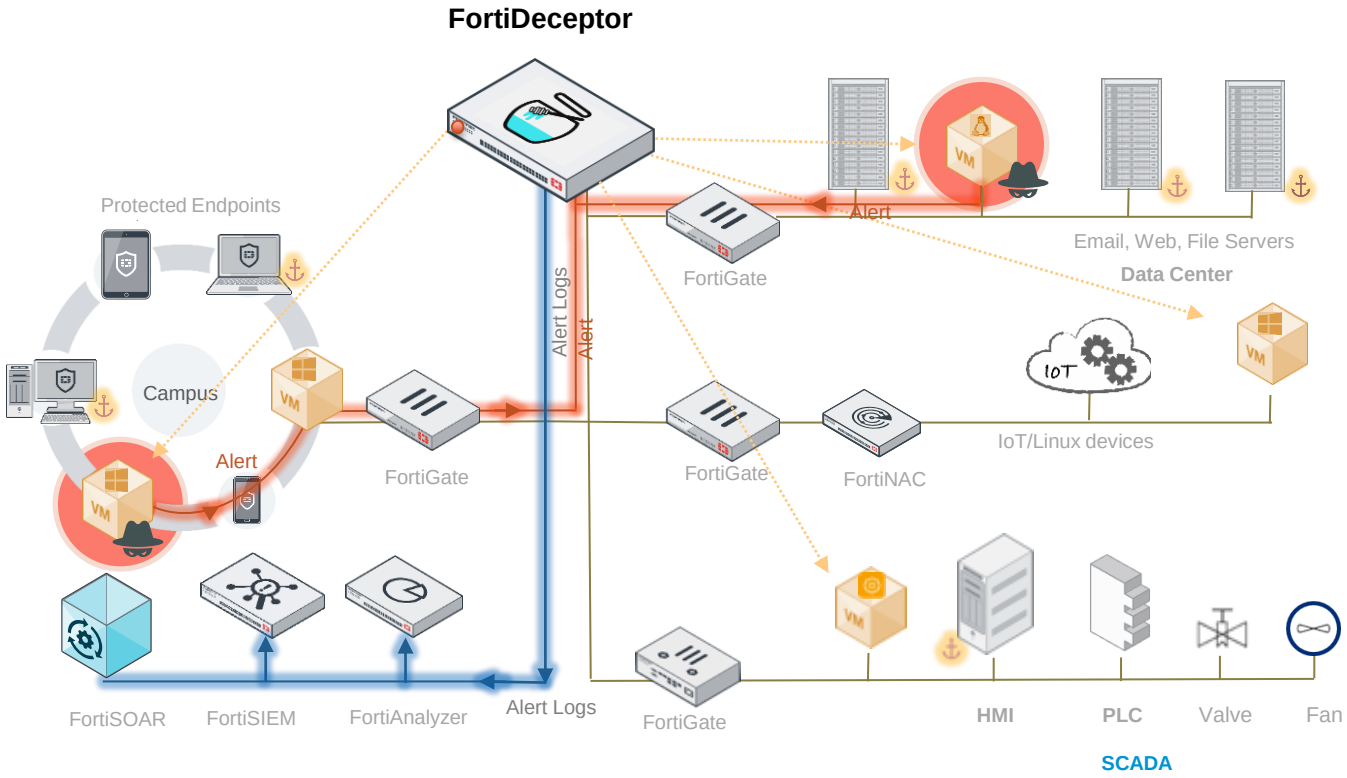


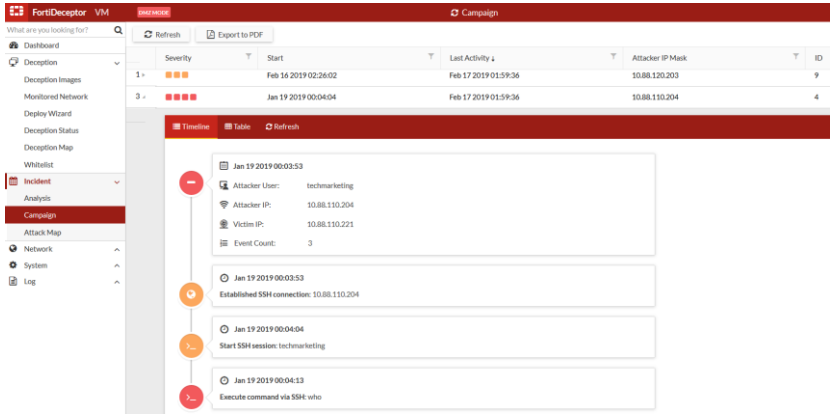
- Lure attackers to decoys that appear indistinguishable from real IT and OT assets and are highly interactive
- Centrally manage and automate the deployment of decoy VMs (Windows, Linux, ICS/SCADA) and generation of lures (data, application /services*)

OT Lures: MODBUS, S7-200, IPMI, Bacnet, Triconex, Guardian-AST, IEC104, ENIP
IoT Lures: Medical PACS, DICOM, infusion pump, ERP, POS, GIT
IT Lures: SSL VPN, RDP, SMB, SQL, SSH, SAMBA, etc

Deception: LifeCycle

Deceive > Expose

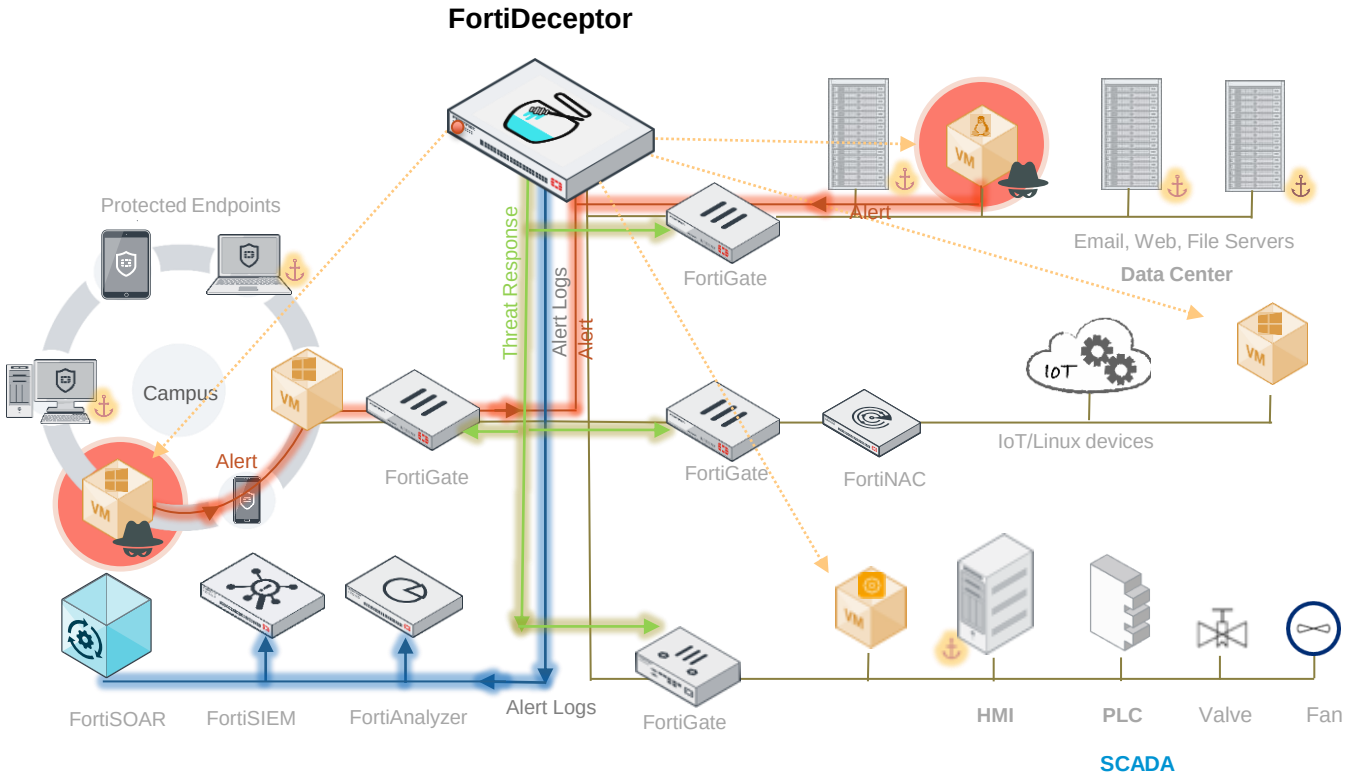


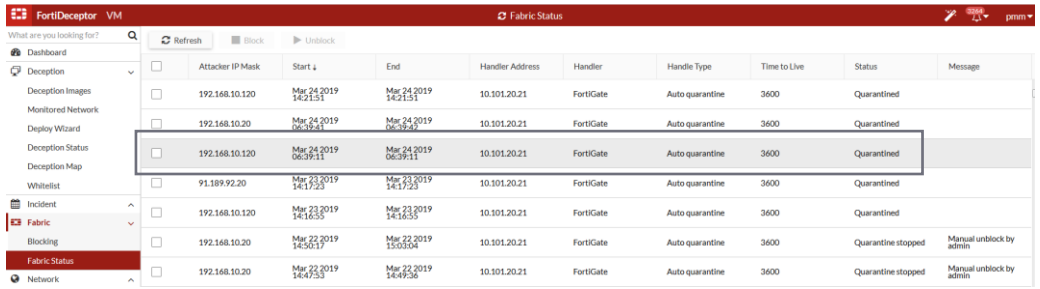


- Acts as an early warning system that generates alerts for review and validation
- Consolidate detection and correlation of external and internal actor activities into a single pane view of threat campaign

Deception: LifeCycle

Deceive > Expose > Eliminate



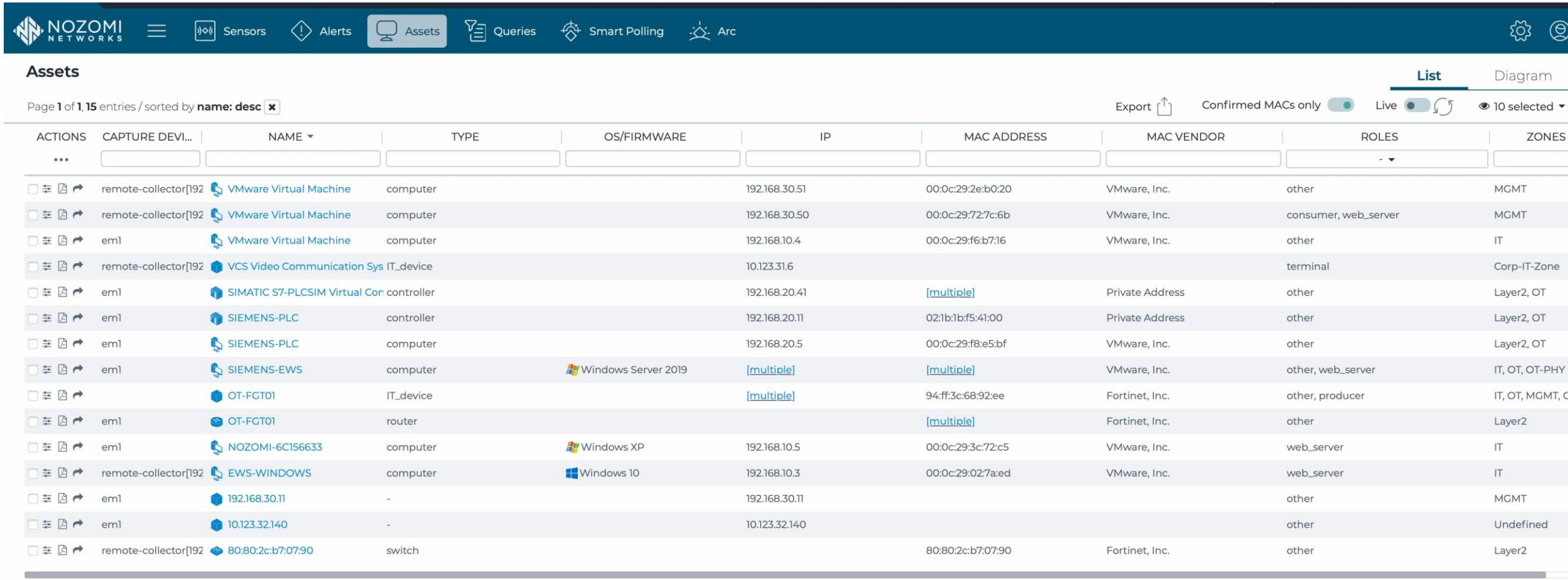


- Manual/Automatic severity-based blocking of attackers before any real damage occurs
- Fabric integration
  - FortiGate: Quarantine IP address
  - FortiNAC: Isolate devices
  - FortiSOAR: Trigger playbooks
  - FortiSIEM: Visibility and threat hunting
  - 3rd Party: Fabric Connector

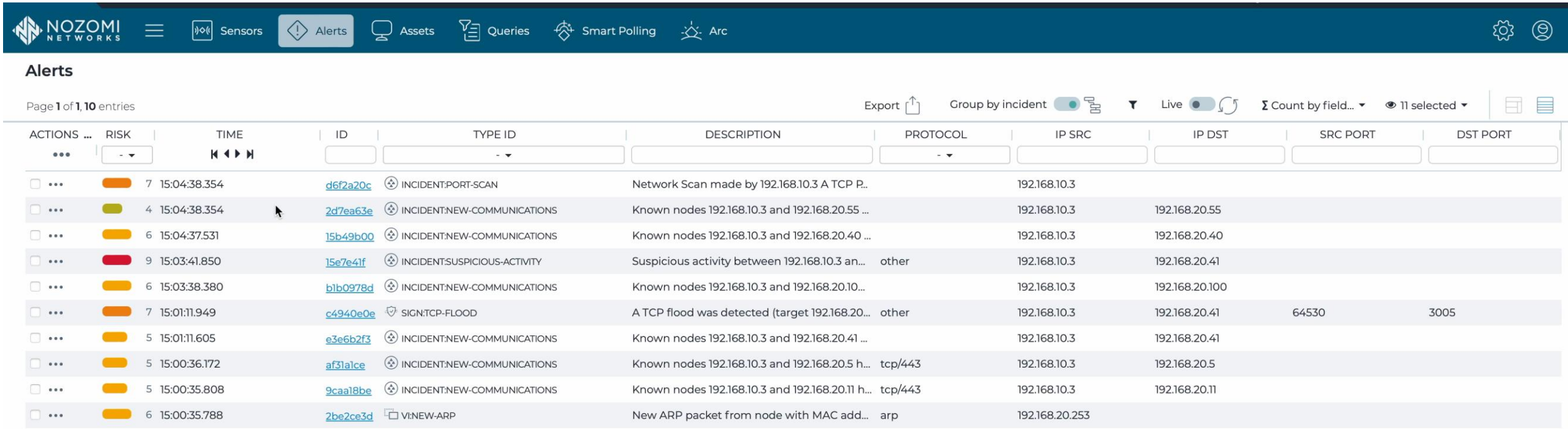
Demo’s

- Honeypot Deception Detection Only
- IDS Detection Only
- Detection by IDS and Deception technology combined

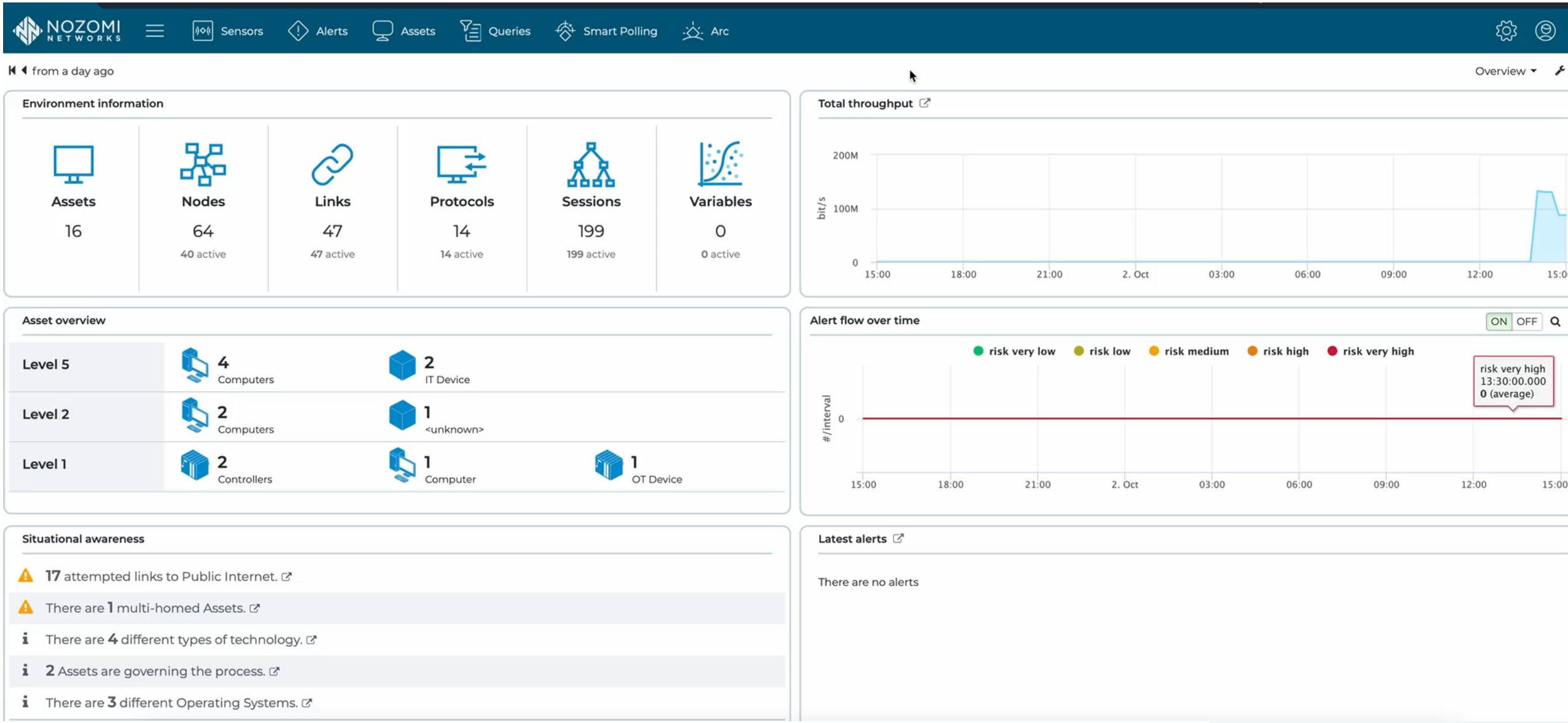
Deception Detection only



IDS Detection only



Detection by IDS and Deception combined



Q&A

Contact details

- Jeffrey Noya | Regional Systems Engineer Nozomi Networks | jeffrey.noya@nozominetworks.com
- Celine van der Winkel | Regional Sales Director Nozomi Networks | celine.vanderwinkel@nozominetworks.com
- Arjan Aelmans | SSE OT Fortinet | aaelmans@fortinet.com
- Jasper Wubben | BDM Fortinet | jwubben@fortinet.com