

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

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

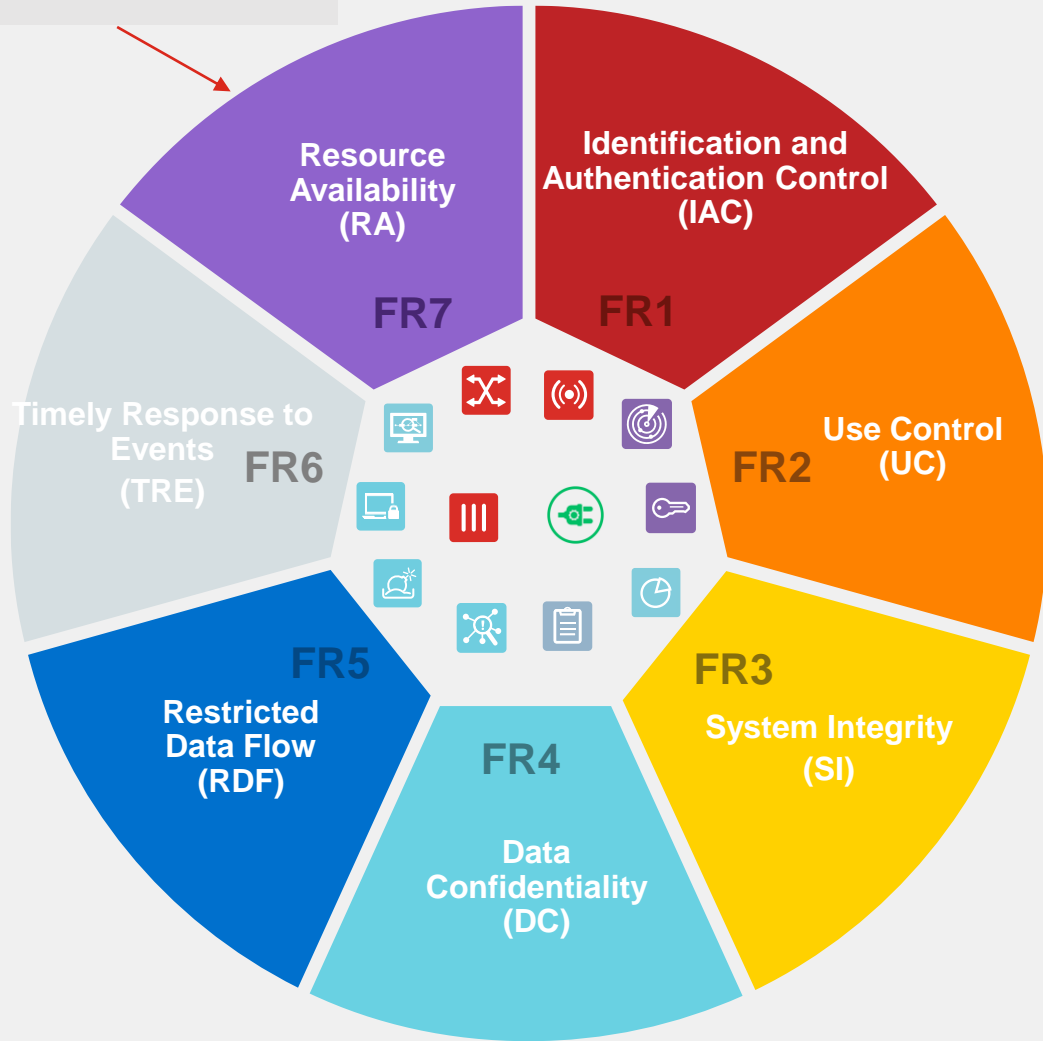
Example high-level operational controls mapping to FRs

- 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.





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

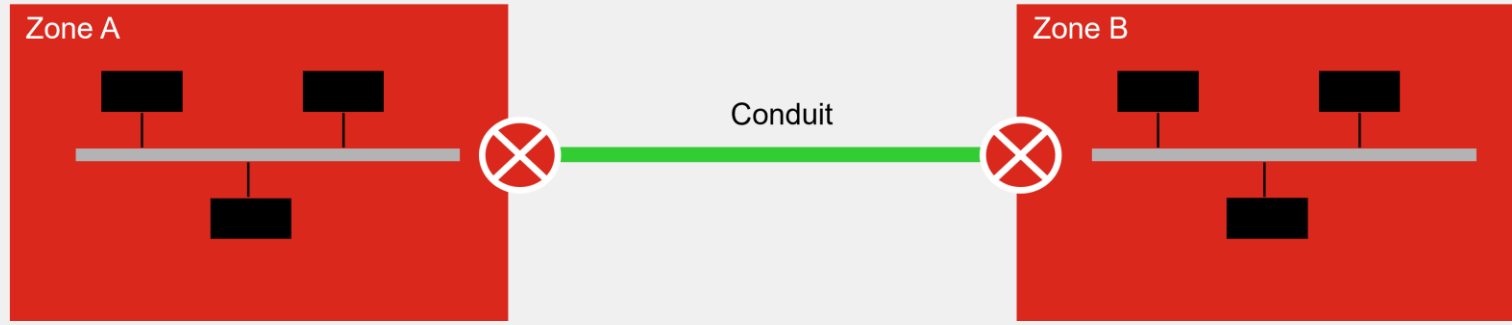
5 FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer

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 its core principles.



- A **Zone** is a logical or physical area where assets of the same criticality are grouped together
 - A zone could be 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



Edit Policy

Name **i** SCADA_to_HMI

Type **Standard** ZTNA

Incoming Interface **DMZ (port9)**

Outgoing Interface **OT (port3)**

Source **all** **x**

IP/MAC Based Access Control **i** **+**

Logical And With Secondary Tags **Disabled** Specify

Destination **all** **x**

Schedule **always**

Service **ALL** **x**

Action **ACCEPT** **DENY**

Inspection Mode **Flow-based** Proxy-based

Firewall/Network Options

NAT **o**

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port **o**

Protocol Options **PROT** default **✎**

Edit Policy

Firewall/Network Options

NAT **o**

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port **o**

Protocol Options **PROT** default **✎**

Security Profiles

AntiVirus **o**

Web Filter **o**

DNS Filter **o**

Application Control **o**

IPS **o**

File Filter **o**

SSL Inspection **SSL** no-inspection **✎**

Logging Options

Log Allowed Traffic **i** **o** **Security Events** All Sessions

Comments **Write a comment...** 0/1023

Enable this policy **o**



Firewall Integration Video Attacker

The dashboard features a top navigation bar with the Nozomi Networks logo and menu items: Sensors, Alerts, Assets, Queries, and Smart Polling. A sidebar on the left contains a menu with options: Network, Process, Reports, Assertions, Time machine, and Vulnerabilities. The main content area is divided into several sections:

- Summary Cards:** Links (37 active), Protocols (15 active), Sessions (291 active), and Variables (0 active).
- Total throughput:** A line chart showing throughput in bit/s over time, with a callout for 2023-10-01 14:00:00.000 at 0.0 b (average).
- Asset overview:** A table showing asset counts by level: Level 5 (2 Computers, 2 <unknown>), Level 2 (2 <unknown>), and Level 1 (6 <unknown>).
- Alert flow over time:** A chart showing the number of alerts per interval, with a legend for risk levels: risk very low, risk low, risk medium, risk high, and risk very high.
- Latest alerts:** A section indicating there are no alerts.
- Situational awareness:** A list of alerts: 12 attempted links to Public Internet, 1 multi-homed Asset, 3 different types of technology, and 1 different Operating System.

Network segmentation improvement

New Application Sensor

148 Cloud Applications require 0 policies are using this profile.

Name: Allow_Siemens_Comms
 Comments: S7 - Profinet - Modbus 22/255

Categories

- Block All Categories
- Business (156, 6)
- Collaboration (258, 16)
- Game (83)
- IoT (2273)
- Network.Service (334)
- P2P (55)
- Remote.Access (96)
- Storage.Backup (152, 19)
- Video/Audio (152, 17)
- Web.Client (25)

- Cloud.IT
- Email (77)
- General.Ir
- Mobile (3)
- Operatio
- Proxy (18)
- Social.Me
- Update (
- VoIP (24)
- Unknown

Add New Override

Type: Application Filter
 Action: Monitor

Add All Results S7

Selected 0 All

Name	Category	Technology	Popularity	Risk
Application Signature 61/7107				
S7.Plus.Protocol	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Begin.Sequence	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Create.Object	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Delete.Object	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_End.Sequence	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Explore	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Get.Link	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Get.Multivar	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Get.Varsubstr	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Invoke	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Set.Multivar	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Plus.Protocol_Set.Variable	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Protocol	Operational.Technology	Client-Server	★★★★☆	■■■■
S7.Protocol_Block.Function.Get.Block...	Operational.Technology	Client-Server	★★★★☆	■■■■

Network Protocol Enforcement



Network segmentation improvement



Edit Policy

Name **i** SCADA_to_HMI

Type **Standard** ZTNA

Incoming Interface DMZ (port9)

Outgoing Interface OT (port3)

Source **SIEMENS-EWS** **EWS**

IP/MAC Based Access Control **i**

Logical And With Secondary Tags **Disabled** Specify

Destination **all**

Schedule **always**

Service **ALL**

Action **ACCEPT** DENY

Inspection Mode **Flow-based** Proxy-based

Firewall/Network Options

NAT

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port

Edit Policy

Firewall/Network Options

NAT

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port

Protocol Options **PROT** default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control **APP** Allow_Siemens_Comms

IPS

File Filter

SSL Inspection **SSL** certificate-inspection

Logging Options

Log Allowed Traffic **i** Security Events All Sessions

Comments Write a comment... 0/1023

Enable this policy





Pascal Ackerman · Following
OT/ICS/IOT Pentester | Threat Hunter |
Incident Responder | Hacker | Tinkere...
11h · 🌐



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

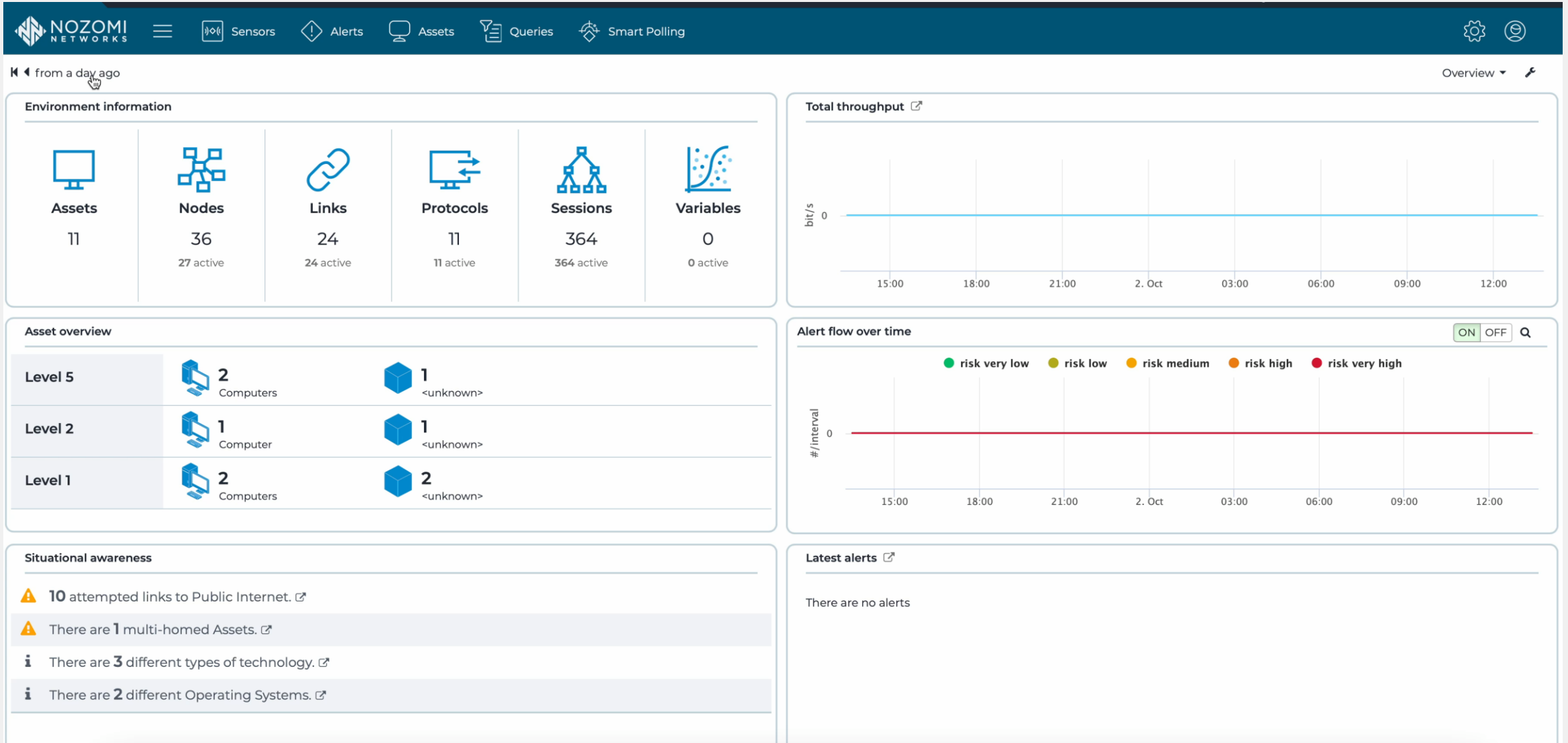
1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
- 3. Insufficient internal network monitoring
- 4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication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



3 comments · 8 reposts

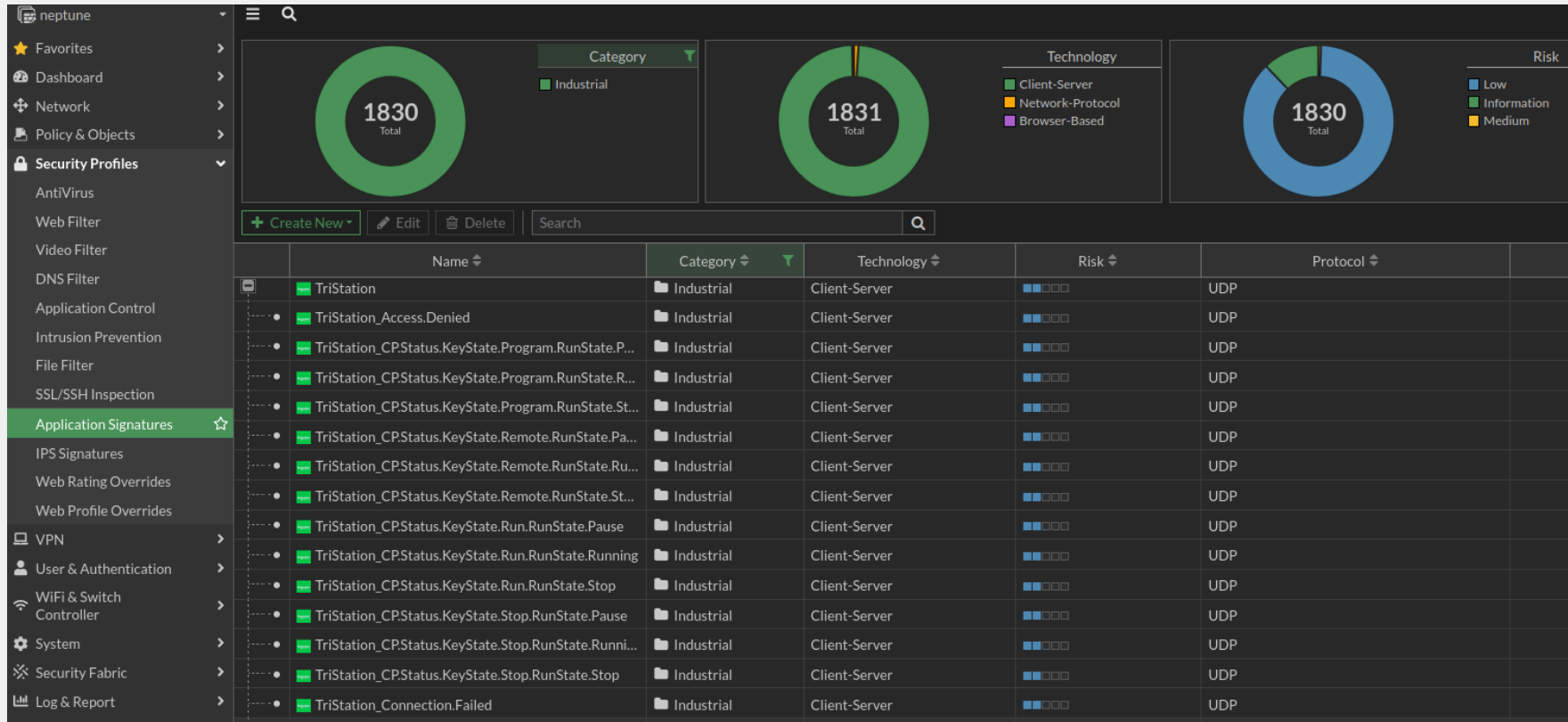


Firewall Integration Video: Engineering Workstation Compromised



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/ICS Application 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



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	WITSO
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 [fortiguards.com](https://www.fortiguards.com).**

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



Q&A





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

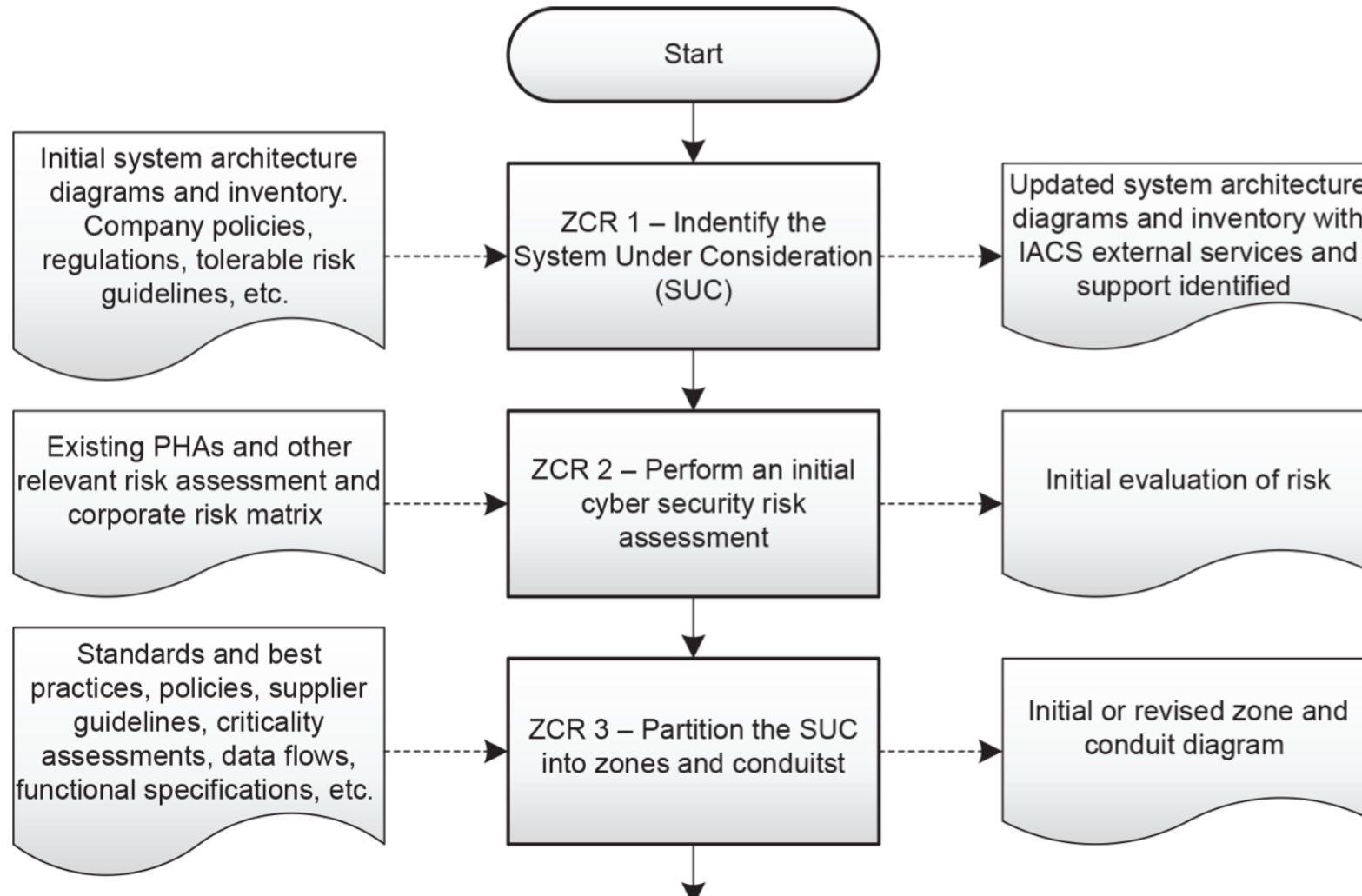
BREAK

Session 2:

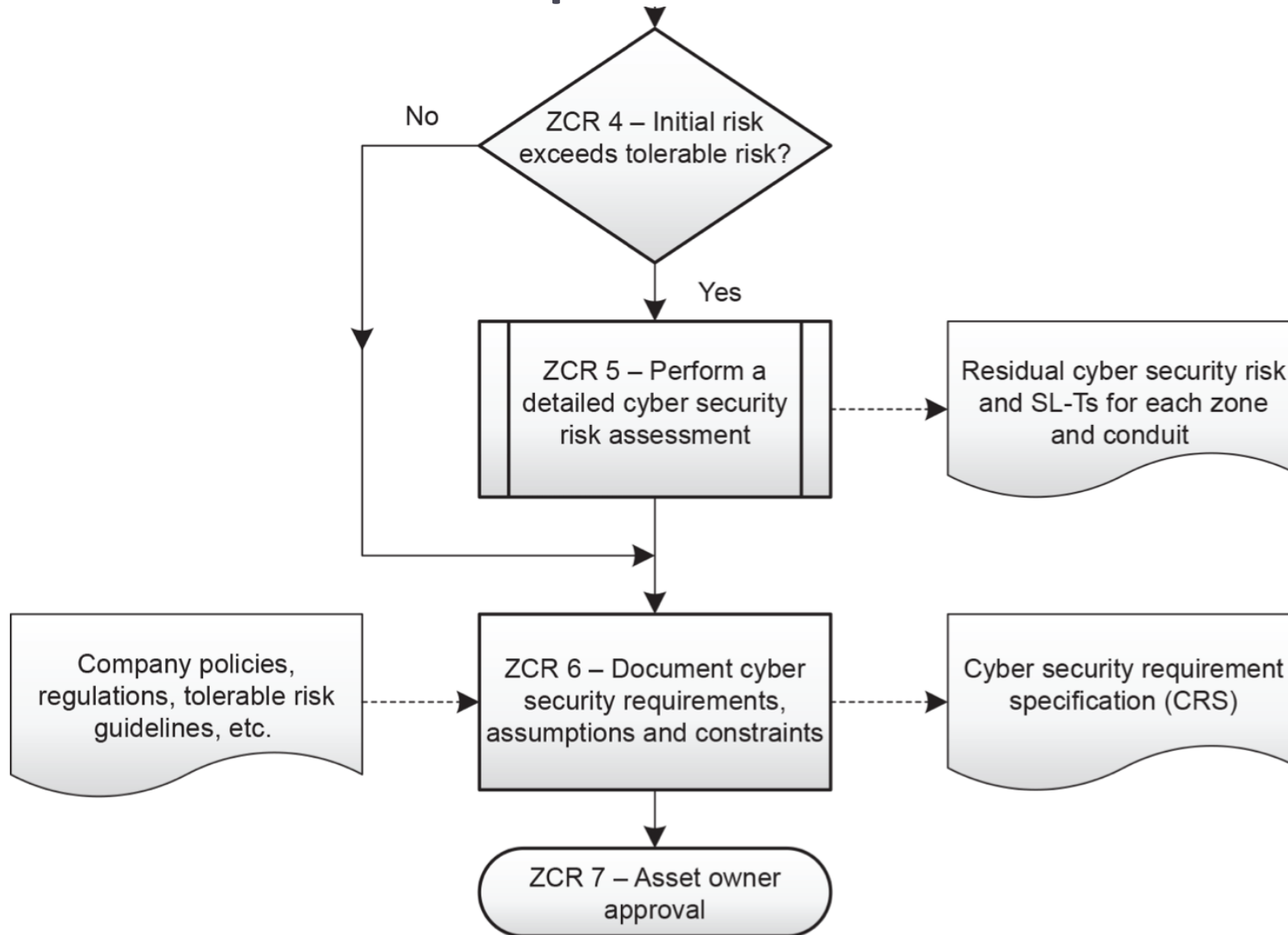
Network and asset based attack perspective

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

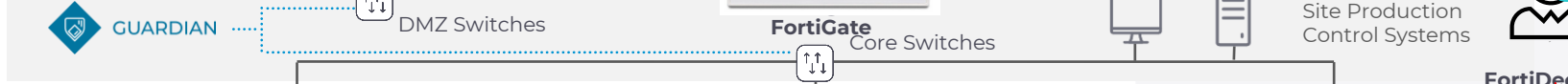
Level 5
Enterprise IT Networks
and Data Centers



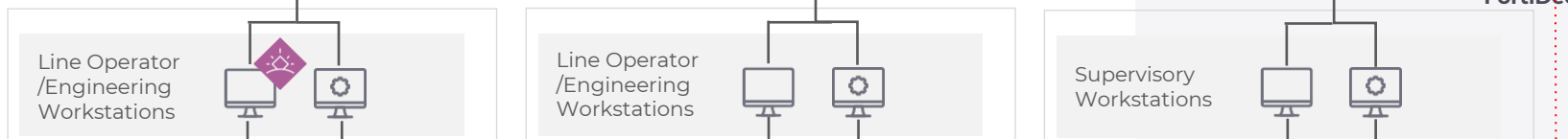
Level 4
Site IT Networks



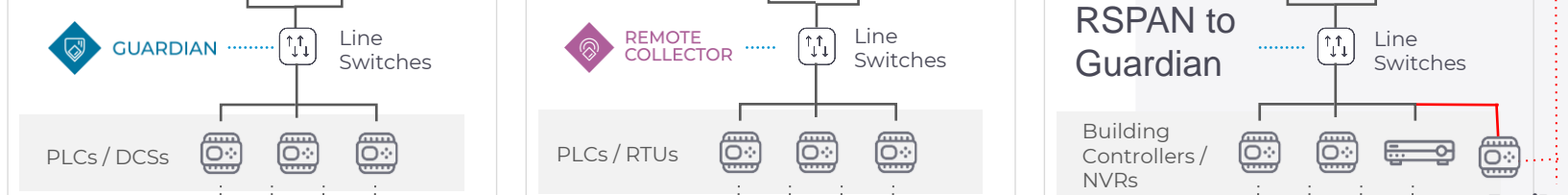
Level 3 and Level 3.5
Site Operations Control
and ICS-Demilitarized
Zone (DMZ)



Level 2
Area Supervisory
Control



Level 1
Control Network



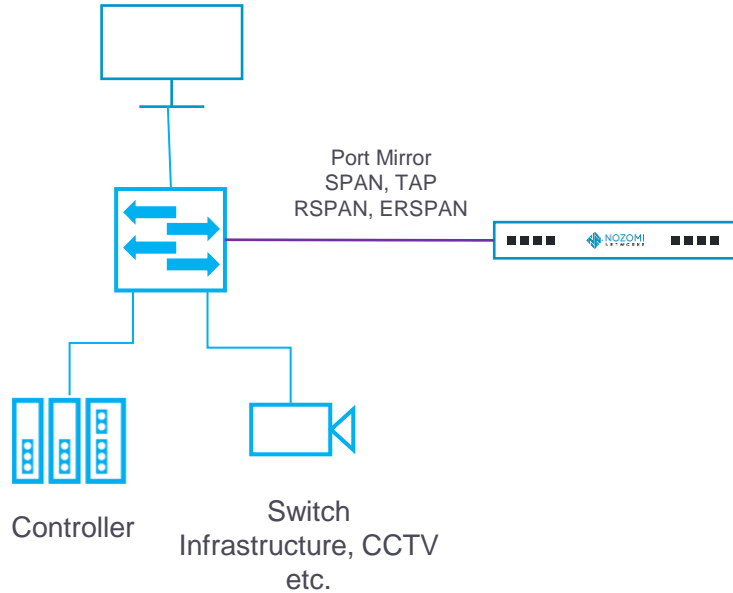
Level 0
Field Network



Asset Inventory

Passive Network Monitoring (Deep Packet Inspection)

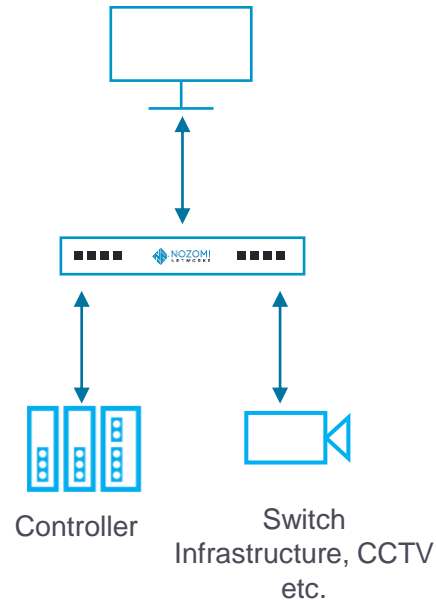
Windows/Linux/MacOs



Monitors network traffic

Active Querying (Nozomi Smart Polling)

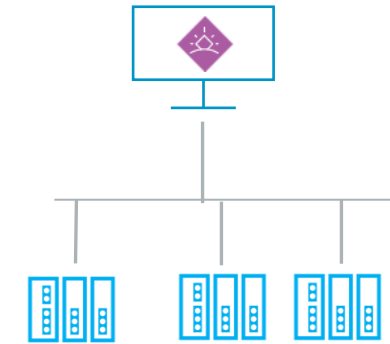
Windows/Linux/MacOs



Queries assets using native protocols

Host Based Monitoring (Nozomi Arc Sensor)

Windows/Linux/MacOs



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

Make, model, OS/firmware,
serial no. etc.



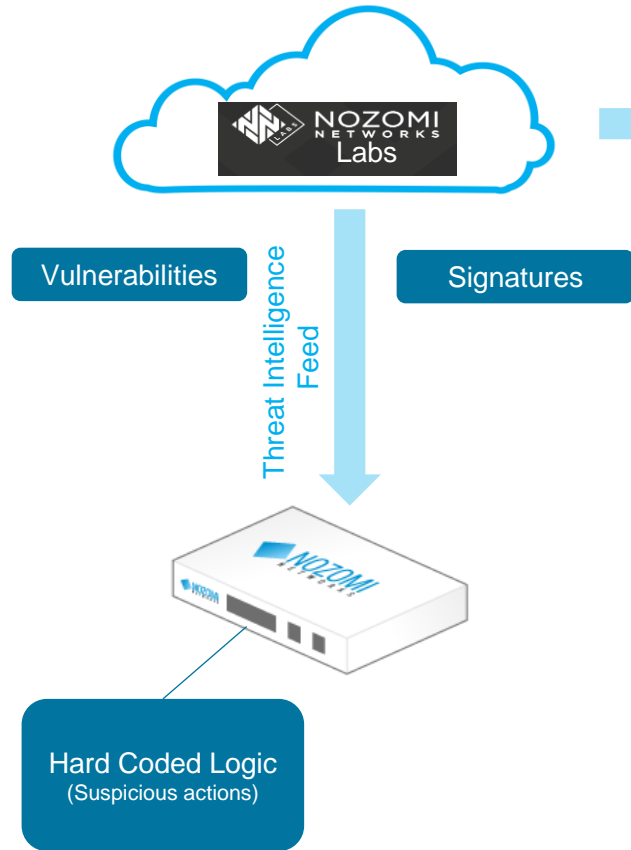
CVE Numbering Authority



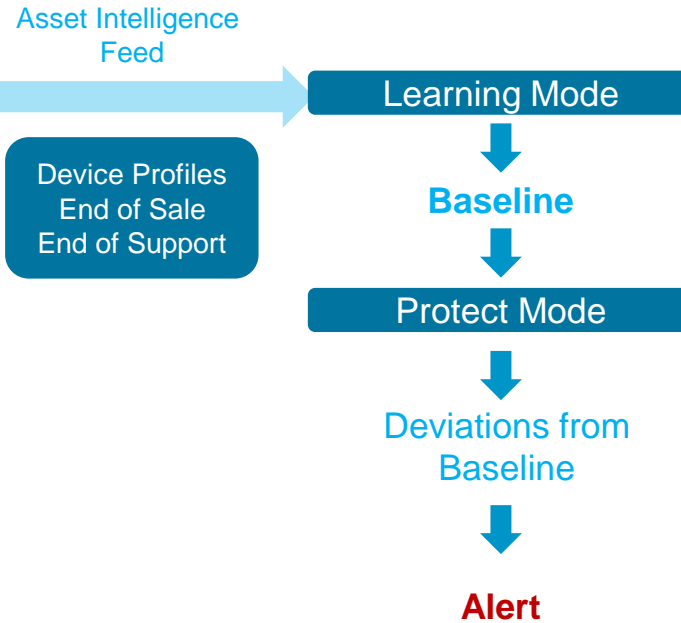
Vulnerability Matching

Security and Operational Capabilities

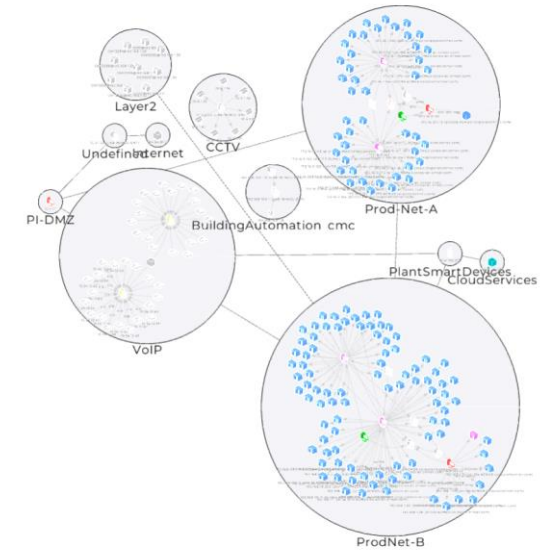
Known Threat Detection



Anomaly-Based Intrusion Detection (Zero Days)



Operational Insights



Communication Issues
Failed Devices
Virtual segmentation (IEC62443)

Advanced Deception and Honeypot

Deceive

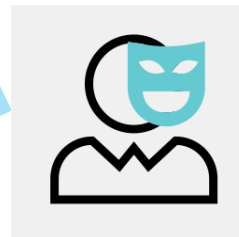


- Decoy OT Controllers and PLC's
- Feedback access attempts
- Learn about your attacker

Expose



Threat Intelligence Feed

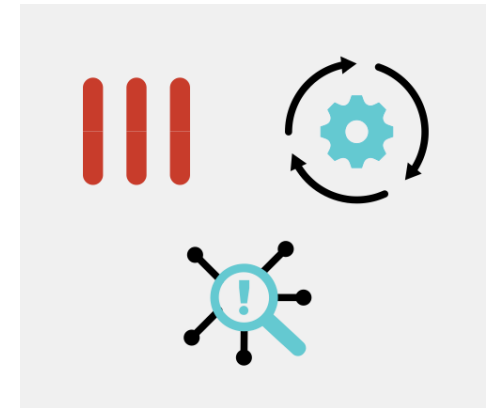


Provide feedback of events

Mimic real controllers

- Increase cost of attacker
- Cut down breach detection time

Eliminate



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

Identifying the assets

GUARDIAN LIVE HOST guardian-ot-ga.lab.local 23.3.0-09201756_43AFD TIME 16:27:01.621 DISK 3.5G used / 20G free LICENSEE Nozomi Networks... UPDATES TI Arc AI English

NOZOMI NETWORKS Sensors Alerts Assets Queries Smart Polling Arc

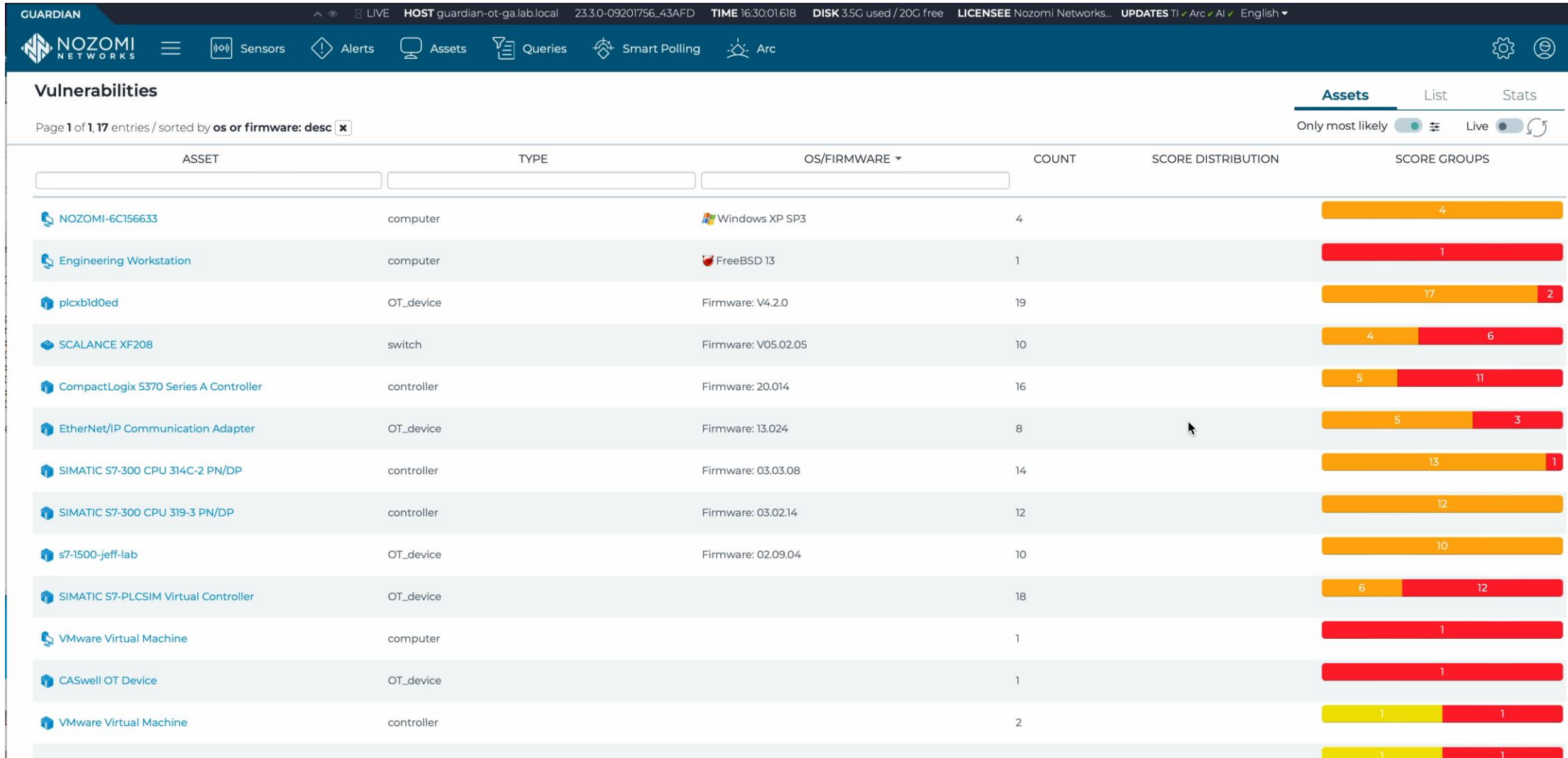
Assets

Page 1 of 3, 57 entries / filtered by ip: match? 192.168. / sorted by os or firmware: desc

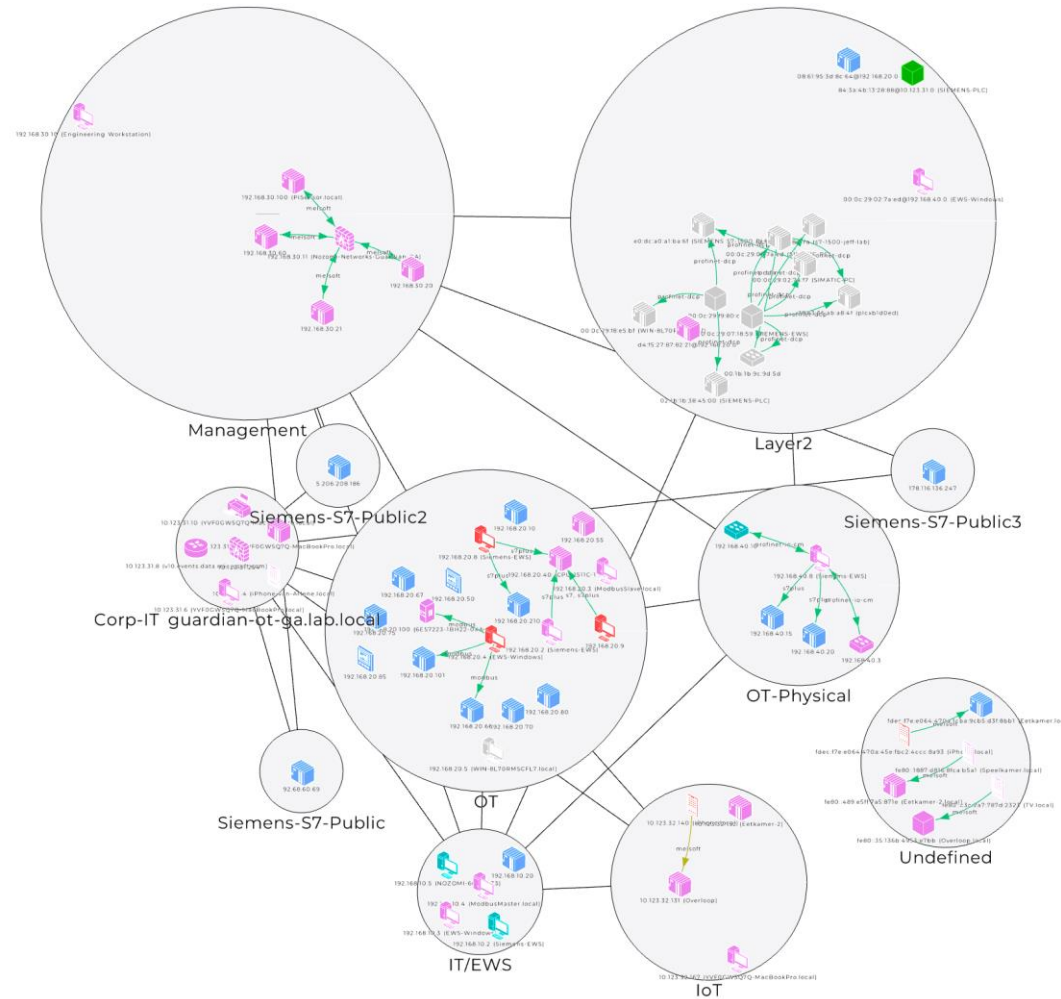
Export Confirmed MACs only Live 13 selected

ACTIONS	NAME	TYPE	OS/FIRMWARE	IP	VENDOR	MAC ADDRESS	MAC VENDOR
...				192.168.			
<input type="checkbox"/>	NOZOMI-6C156633	computer	Windows XP SP3	192.168.10.5	VMware	00:0c:29:3c:72:c5	VMware, Inc.
<input type="checkbox"/>	SIEMENS-EWS	computer	Windows Server 2019	[multiple]	VMware, Inc.	[multiple]	VMware, Inc.
<input type="checkbox"/>	EWS-WINDOWS	OT_device	Windows 10	[multiple]	VMware, Inc.	[multiple]	VMware, Inc.
<input type="checkbox"/>	Engineering Workstation	computer	FreeBSD 13	192.168.30.10	VMware	00:0c:29:e0:5e:1d	VMware, Inc.
<input type="checkbox"/>	Dixell Refrigerating Unit Digital Controller	controller	Firmware: iPro	[multiple]	Emerson	[multiple]	[multiple]
<input type="checkbox"/>	plcxbd0ed	OT_device	Firmware: V4.2.0	[multiple]	Siemens AG	[multiple]	Siemens
<input type="checkbox"/>	SCALANCE XF208	switch	Firmware: V05.02.05	[multiple]	Siemens	[multiple]	Siemens
<input type="checkbox"/>	6ES7223-1BH22-0XA0	IO_module	Firmware: S7-200	192.168.20.100	Siemens	d4:f5:27:89:34:31	Siemens
<input type="checkbox"/>	SIMATIC S7-PLCSIM Virtual Controller	controller	Firmware: S29.80.5	192.168.10.20	Siemens	02:c0:a8:0a:02:00	Private Address
<input type="checkbox"/>	OT-FGT01	firewall	Firmware: 7.4.1	[multiple]	Fortinet	94:ff:3c:68:92:ee	Fortinet, Inc.
<input type="checkbox"/>	CompactLogix 5370 Series A Controller	controller	Firmware: 20.014	192.168.20.70	Rockwell Automati	00:00:bc:d2:32:b1	Rockwell Automation
<input type="checkbox"/>	FieldTalk Modbus Slave	controller	Firmware: 2.8.2.0	192.168.20.10	ProconX	00:0c:29:5f:52:da	VMware, Inc.
<input type="checkbox"/>	EtherNet/IP Communication Adapter	OT_device	Firmware: 13.024	192.168.20.80	Rockwell Automati	f4:54:33:6f:97:bc	Rockwell Automation
<input type="checkbox"/>	PowerLogic PM5560 Power Meter	meter	Firmware: 1.9.0	192.168.20.85	Schneider Electric	00:11:00:74:80:f3	Schneider Electric
<input type="checkbox"/>	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
<input type="checkbox"/>	s7-1500-jeff-lab	OT_device	Firmware: 02.09.04	192.168.40.20	Siemens	8c:f3:19:b0:84:7a	Siemens
<input type="checkbox"/>	BMEP581020 Modicon M580 Standalone Process controller	controller	Firmware: 0.0.126	[multiple]	Schneider Electric	00:00:54:fb:7f:1e	Schneider Electric
<input type="checkbox"/>	TM241CE40R Modicon M241 Logic Controller	controller	Firmware: 0.0.106	[multiple]	Schneider Electric	00:11:00:92:3a:56	Schneider Electric
<input type="checkbox"/>	192.168.30.50	-		192.168.30.50		d4:76:a0:21:94:26 (unconfirmed)	Fortinet, Inc. (unconfirmed)
<input type="checkbox"/>	192.168.20.253	-		192.168.20.253		b2:38:50:b8:87:2f	Private Address
<input type="checkbox"/>	ABB-EWS.local	computer		192.168.40.2	VMware	00:0c:29:0e:a1:50	VMware, Inc.

Vulnerability assessments (multiple assets)



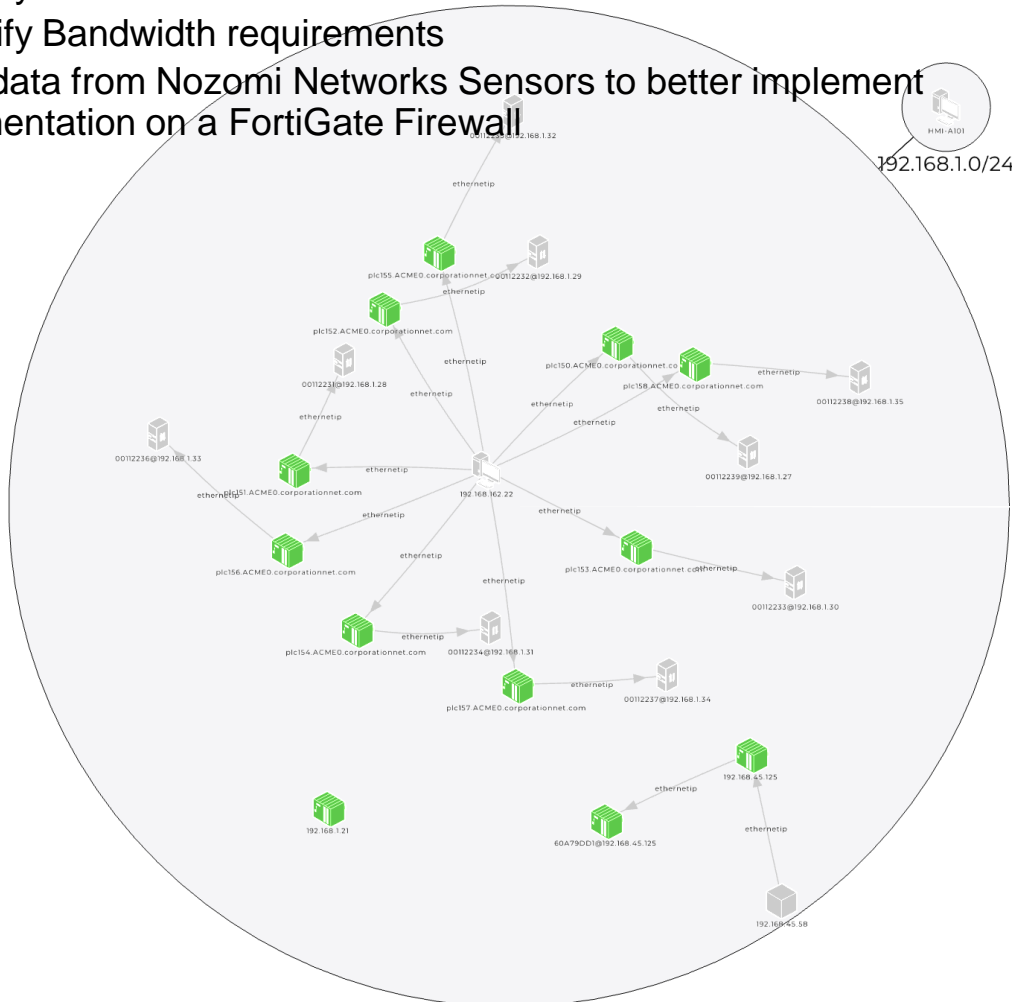
Mapping and visualizing your network



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



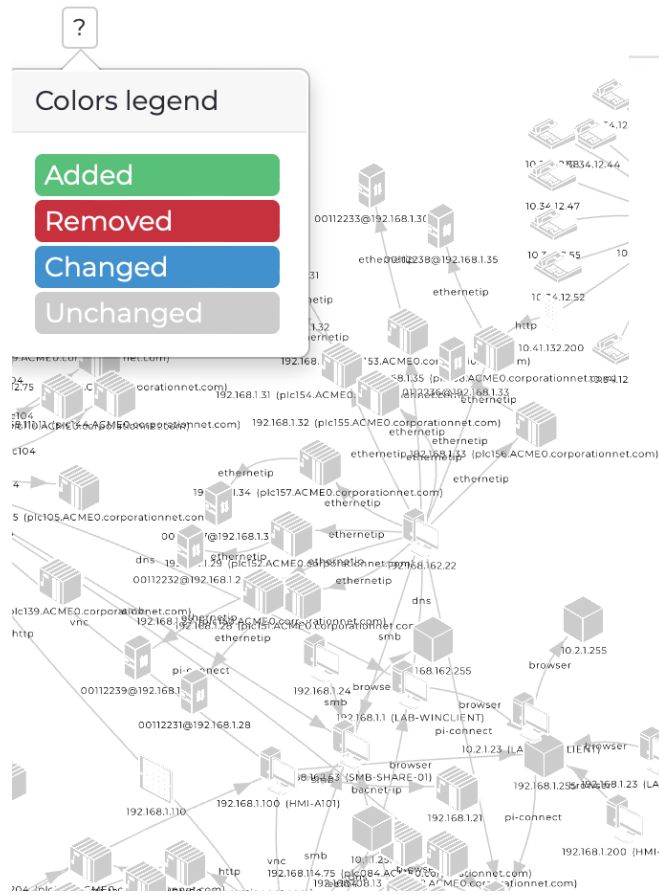
Network view

Page 1 of 48, 1190 entries

ACTIONS	STATUS	FROM	TO	PROT...	TRANSPORT PROT...	FROM POR...	TO PORT ...	THROUGH...
			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	192.168.100.111	192.168.100.1	dns	udp	50369 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	42505 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	49449 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	49281 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	57640 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	62256 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	34169 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	51400 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	52528 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	36913 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	37081 53 0.0 b/s
			ACTIVE	192.168.100.111	192.168.100.1	dns	udp	63328 53 0.0 b/s
			ACTIVE	192.168.100.111	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 each other 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)

IS	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 11:41:5	never	2	never
	192.168.10.1	20.42.73.27	tcp/443	["tcp"]	false	true	Undefined	Internet	-	-	2023-06-21 10:38:7	2023-06-21 10:38:7	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 10:38:7	2023-06-21 10:38:7	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 08:54:7	2023-06-21 08:56:7	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 08:54:7	2023-06-21 08:56:7	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 10:37:7	2023-06-21 10:37:7	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 10:12:7	2023-06-21 10:39:7	never	0	never
	192.168.10.1	209.197.3.8	http	["tcp"]	false	true	Undefined	Internet	-	-	2023-06-21 08:54:7	2023-06-21 09:02:7	2023-06-21 08:56:07.6	4	never

Compliance 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



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

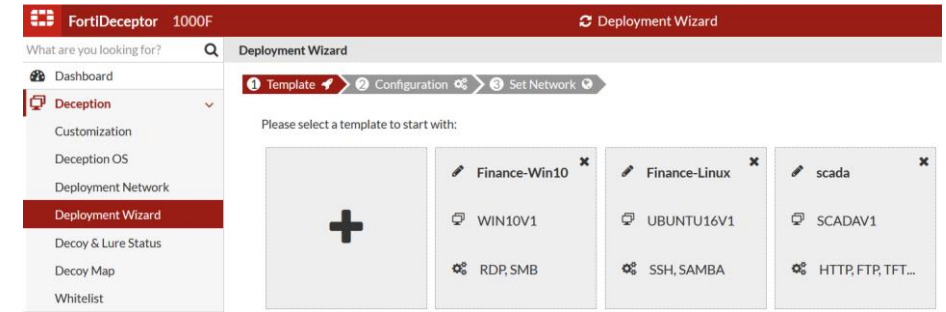
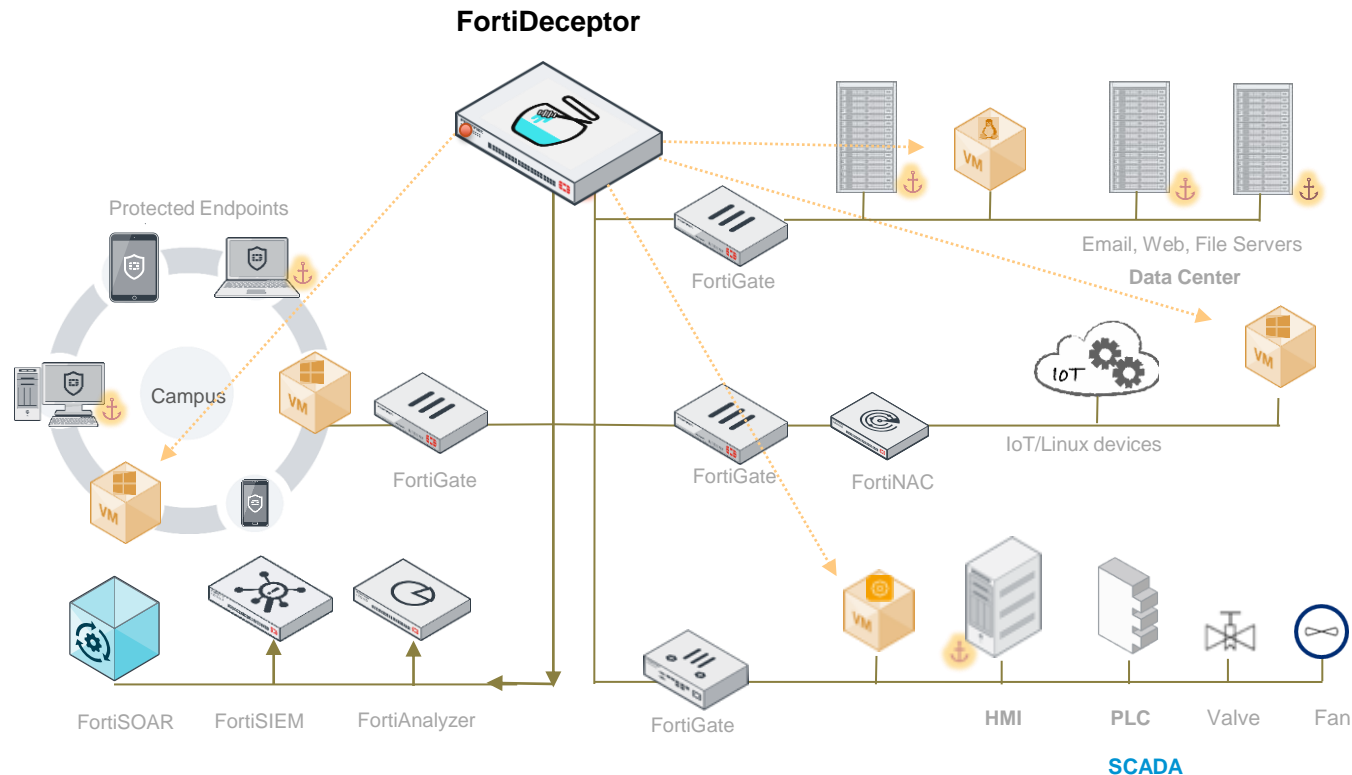
Improve protection capabilities against the unauthorized changes if needed.

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	etherne tip	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

Deception: LifeCycle

Deceive

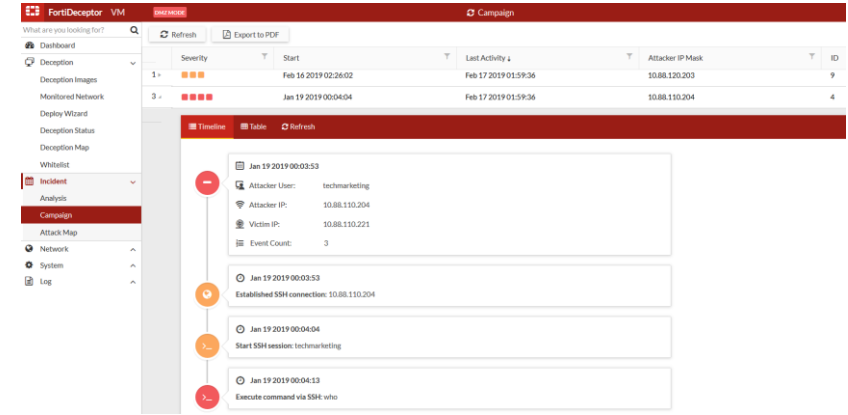
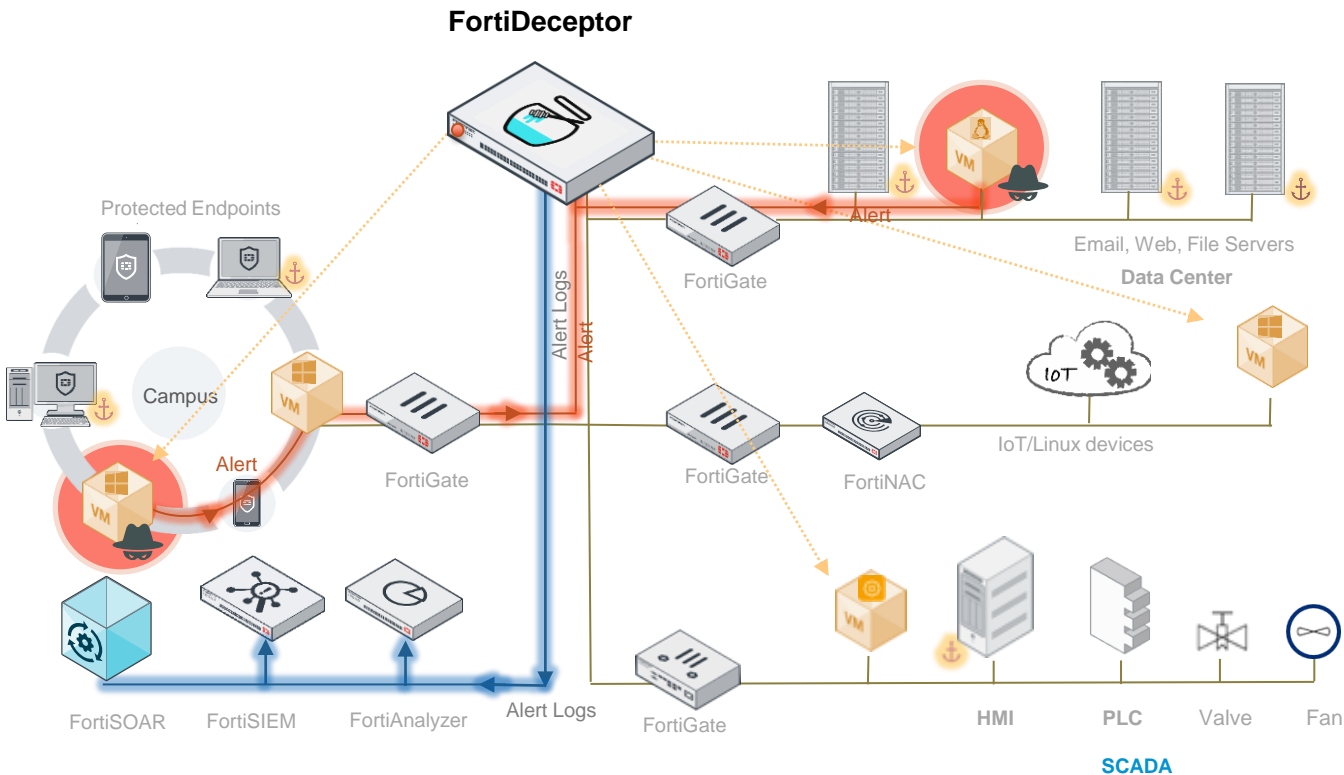


- Lure attackers to decoys that appear indistinguishable from real IT and OT assets and are highly interactive
- Centrally manage and automate the deployment of decoy VMs (Windows, Linux, ICS/SCADA) and generation of lures (data, application /services*)

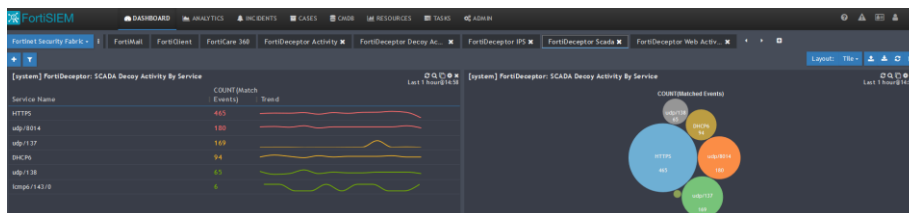
OT Lures: MODBUS, S7-200, IPMI, Bacnet, Triconex, Guardian-AST, IEC104, ENIP
IoT Lures: Medical PACS, DICOM, infusion pump, ERP, POS, GIT
IT Lures: SSL VPN, RDP, SMB, SQL, SSH, SAMBA, etc

Deception: LifeCycle

Deceive > Expose

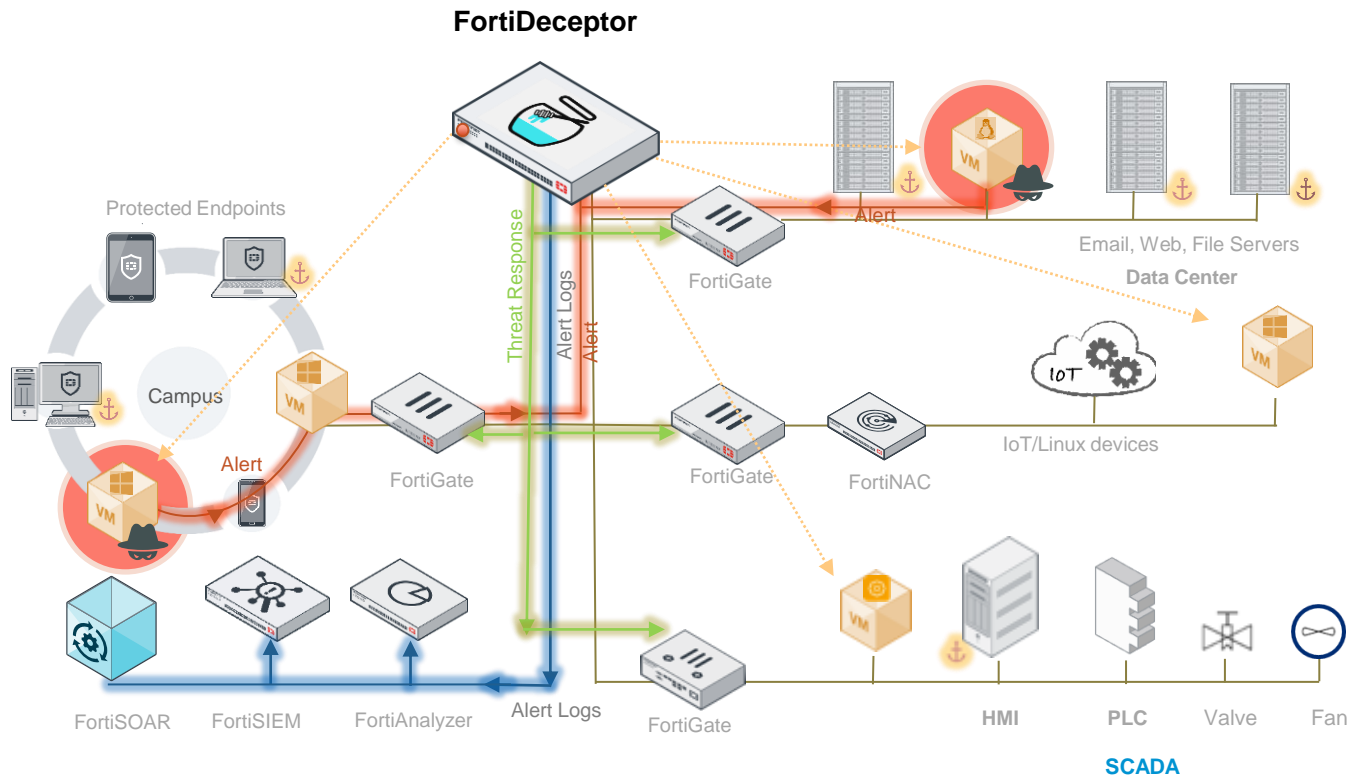


- Acts as an early warning system that generates alerts for review and validation
- Consolidate detection and correlation of external and internal actor activities into a single pane view of threat campaign



Deception: LifeCycle

Deceive > Expose > Eliminate



Attacker IP Mask	Start	End	Handler Address	Handler	Handle Type	Time to Live	Status	Message
192.168.10.120	Mar 24 2019 14:21:51	Mar 24 2019 14:21:51	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
192.168.10.20	Mar 24 2019 06:19:41	Mar 24 2019 06:19:41	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
192.168.10.120	Mar 24 2019 06:39:11	Mar 24 2019 06:39:11	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
91.189.92.20	Mar 23 2019 14:11:23	Mar 23 2019 14:11:23	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
192.168.10.120	Mar 23 2019 14:16:33	Mar 23 2019 14:16:33	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantined	
192.168.10.20	Mar 22 2019 14:50:17	Mar 22 2019 15:00:04	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantine stopped	Manual unblock by admin
192.168.10.20	Mar 22 2019 14:47:53	Mar 22 2019 14:49:58	10.101.20.21	FortiGate	Auto quarantine	3600	Quarantine stopped	Manual unblock by admin

- 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



Sensors

Alerts

Assets

Queries

Smart Polling

Arc



Assets

List

Diagram

Page 1 of 1,15 entries / sorted by name: desc

Export

Confirmed MACs only

Live

10 selected

ACTIONS	CAPTURE DEVI...	NAME	TYPE	OS/FIRMWARE	IP	MAC ADDRESS	MAC VENDOR	ROLES	ZONES
<input type="checkbox"/>	remote-collector[192]	VMware Virtual Machine	computer		192.168.30.51	00:0c:29:2e:b0:20	VMware, Inc.	other	MGMT
<input type="checkbox"/>	remote-collector[192]	VMware Virtual Machine	computer		192.168.30.50	00:0c:29:72:7c:6b	VMware, Inc.	consumer, web_server	MGMT
<input type="checkbox"/>	em1	VMware Virtual Machine	computer		192.168.10.4	00:0c:29:f6:b7:16	VMware, Inc.	other	IT
<input type="checkbox"/>	remote-collector[192]	VCS Video Communication Sys	IT_device		10.123.31.6			terminal	Corp-IT-Zone
<input type="checkbox"/>	em1	SIMATIC S7-PLCSIM Virtual Con	controller		192.168.20.41	[multiple]	Private Address	other	Layer2, OT
<input type="checkbox"/>	em1	SIEMENS-PLC	controller		192.168.20.11	02:1b:1b:f5:41:00	Private Address	other	Layer2, OT
<input type="checkbox"/>	em1	SIEMENS-PLC	computer		192.168.20.5	00:0c:29:f8:e5:bf	VMware, Inc.	other	Layer2, OT
<input type="checkbox"/>	em1	SIEMENS-EWS	computer	Windows Server 2019	[multiple]	[multiple]	VMware, Inc.	other, web_server	IT, OT, OT-PHY
<input type="checkbox"/>		OT-FGT01	IT_device		[multiple]	94:ff:3c:68:92:ee	Fortinet, Inc.	other, producer	IT, OT, MGMT, C
<input type="checkbox"/>	em1	OT-FGT01	router			[multiple]	Fortinet, Inc.	other	Layer2
<input type="checkbox"/>	em1	NOZOMI-6C156633	computer	Windows XP	192.168.10.5	00:0c:29:3c:72:c5	VMware, Inc.	web_server	IT
<input type="checkbox"/>	remote-collector[192]	EWS-WINDOWS	computer	Windows 10	192.168.10.3	00:0c:29:02:7a:ed	VMware, Inc.	web_server	IT
<input type="checkbox"/>	em1	192.168.30.11	-		192.168.30.11			other	MGMT
<input type="checkbox"/>	em1	10.123.32.140	-		10.123.32.140			other	Undefined
<input type="checkbox"/>	remote-collector[192]	80:80:2c:b7:07:90	switch			80:80:2c:b7:07:90	Fortinet, Inc.	other	Layer2

IDS Detection only

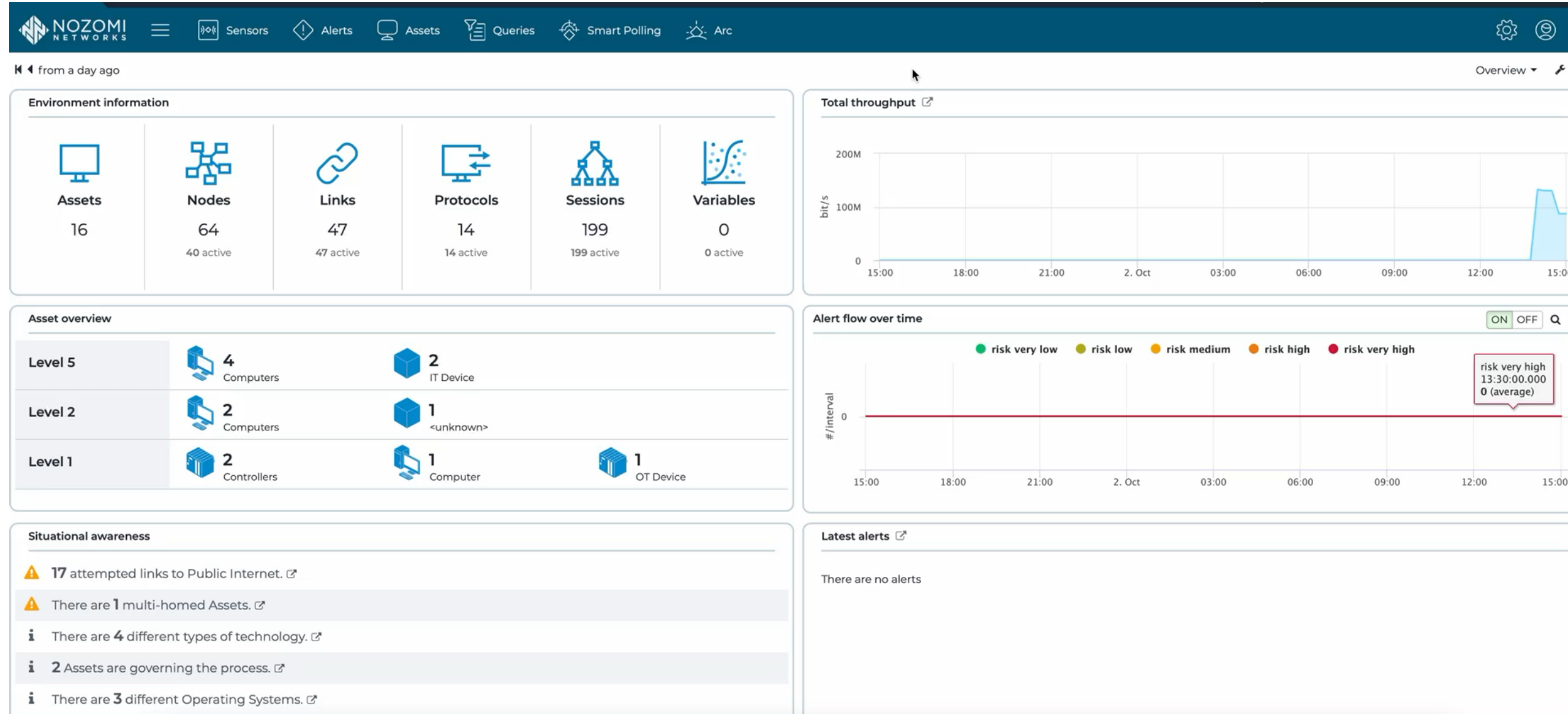
Alerts

Page 1 of 1,10 entries

Export 
 Group by incident 
 Live 
 Count by field... 
 11 selected  

ACTIONS ...	RISK	TIME	ID	TYPE ID	DESCRIPTION	PROTOCOL	IP SRC	IP DST	SRC PORT	DST PORT
<input type="checkbox"/> ...	7	15:04:38.354	d6f2a20c	INCIDENT:PORT-SCAN	Network Scan made by 192.168.10.3 A TCP P...		192.168.10.3			
<input type="checkbox"/> ...	4	15:04:38.354	2d7ea63e	INCIDENT:NEW-COMMUNICATIONS	Known nodes 192.168.10.3 and 192.168.20.55 ...		192.168.10.3	192.168.20.55		
<input type="checkbox"/> ...	6	15:04:37.531	15b49b00	INCIDENT:NEW-COMMUNICATIONS	Known nodes 192.168.10.3 and 192.168.20.40 ...		192.168.10.3	192.168.20.40		
<input type="checkbox"/> ...	9	15:03:41.850	15e7e41f	INCIDENT:SUSPICIOUS-ACTIVITY	Suspicious activity between 192.168.10.3 an...	other	192.168.10.3	192.168.20.41		
<input type="checkbox"/> ...	6	15:03:38.380	b1b0978d	INCIDENT:NEW-COMMUNICATIONS	Known nodes 192.168.10.3 and 192.168.20.10...		192.168.10.3	192.168.20.100		
<input type="checkbox"/> ...	7	15:01:11.949	c4940e0e	SIGN:TCP-FLOOD	A TCP flood was detected (target 192.168.20...	other	192.168.10.3	192.168.20.41	64530	3005
<input type="checkbox"/> ...	5	15:01:11.605	e3e6b2f3	INCIDENT:NEW-COMMUNICATIONS	Known nodes 192.168.10.3 and 192.168.20.41 ...		192.168.10.3	192.168.20.41		
<input type="checkbox"/> ...	5	15:00:36.172	af31a1ce	INCIDENT:NEW-COMMUNICATIONS	Known nodes 192.168.10.3 and 192.168.20.5 h...	tcp/443	192.168.10.3	192.168.20.5		
<input type="checkbox"/> ...	5	15:00:35.808	9caa18be	INCIDENT:NEW-COMMUNICATIONS	Known nodes 192.168.10.3 and 192.168.20.11 h...	tcp/443	192.168.10.3	192.168.20.11		
<input type="checkbox"/> ...	6	15:00:35.788	2be2ce3d	VI:NEW-ARP	New ARP packet from node with MAC add...	arp	192.168.20.253			

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