NOZOMI NETWORKS

Improving Visibility & Security for Cyber Physical Systems

The current challenge and risks, and the recommended approach to finding and monitoring all connected devices, including IoT, IIoT, and OT

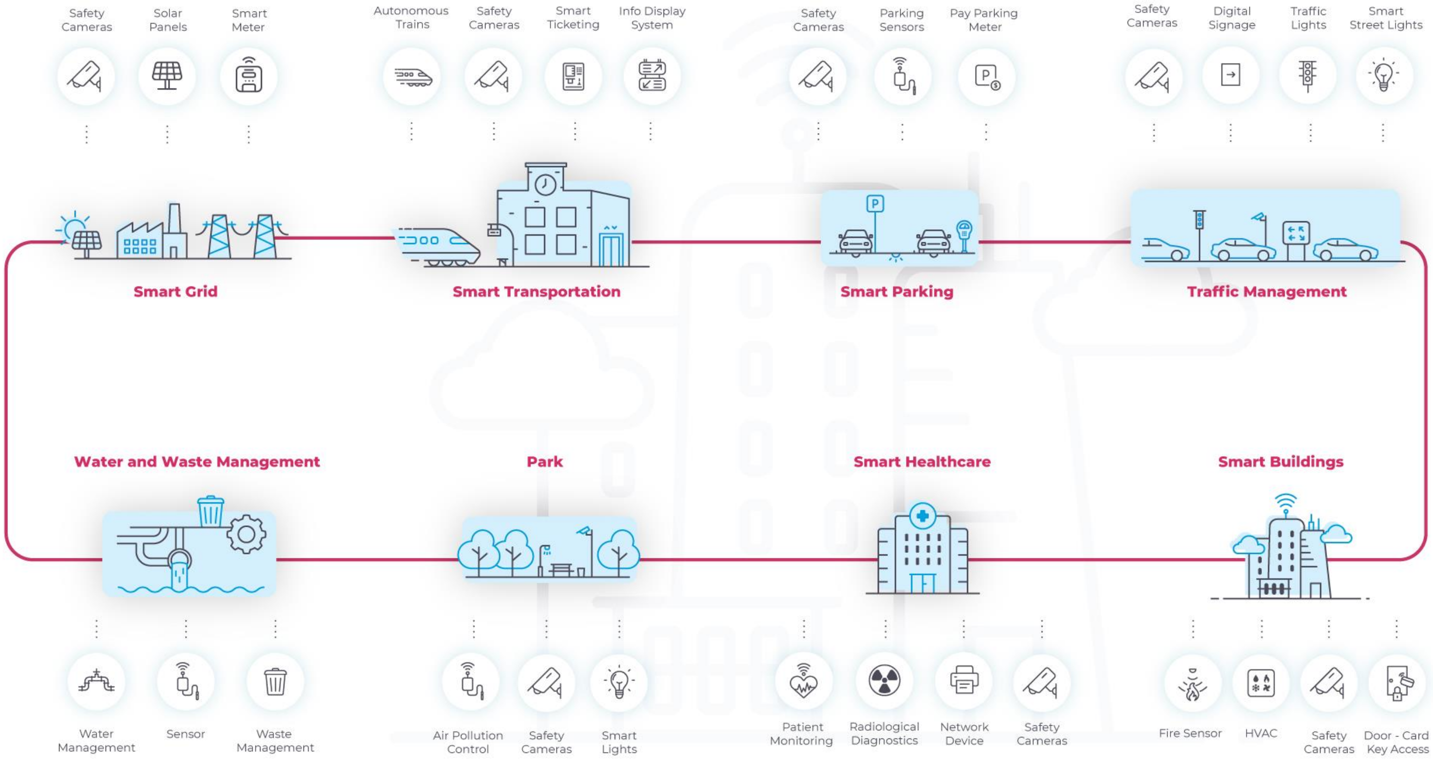
Presenter

Michael Dugent – IoT Director

Today's complex and increasingly connected smart environments and cyber physical systems are vulnerable to cyber threats and disruption of vital systems.

To keep people safe and comfortable and keep all operations working as expected, cyber security teams need to be able to identify and monitor all connected devices so problems can be fixed before they cause disruptions.

Cyber Physical devices (IoT / IIoT / OT) are now ubiquitous



Best Practices

Developing Best Practices for OT / IoT Cyber Security

What are the Challenges?

Understanding the full Attack Surface

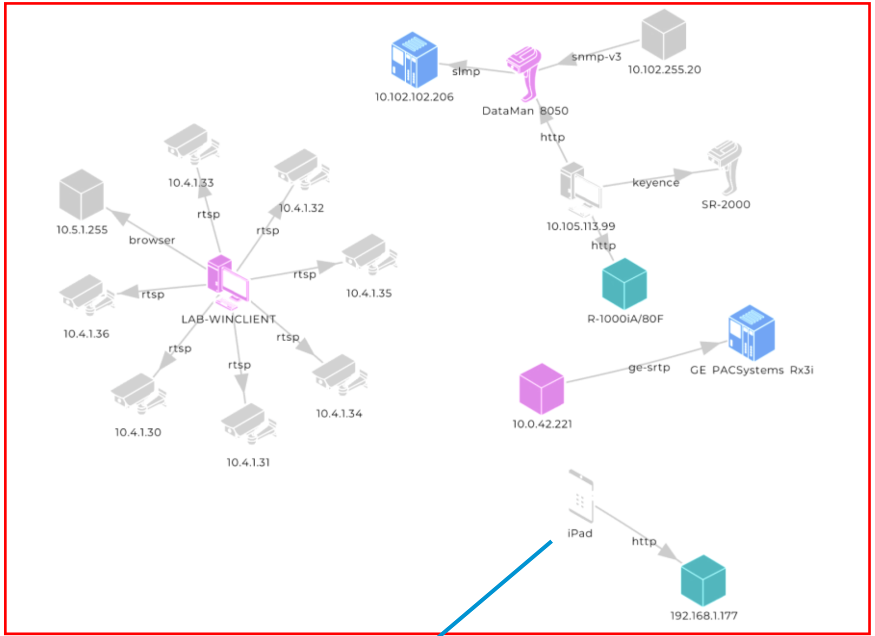
As more and more devices become connected, do I know what devices can talk – and who are they talking to? How do I control that?

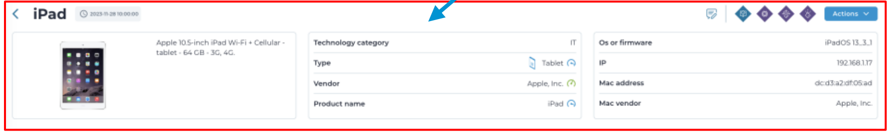
Are these devices secure?

Once know what is out there and how it communicates – how to ensure up to date firmware / patches, firmware integrity, proper encryption and authentication, etc? Who's responsibility is this?

If they're compromised – how to isolate and respond?

Regardless of protective measures, it's possible and maybe even likely these devices are occasionally compromised. Can we protect the rest of the network, and respond to an incident, and get things working again?





Apple 10.5-inch iPad Wi-Fi + Cellular - tablet - 64 GB - 3G, 4G.

Technology category	IT
Type	Tablet
Vendor	Apple, Inc.
Product name	iPad

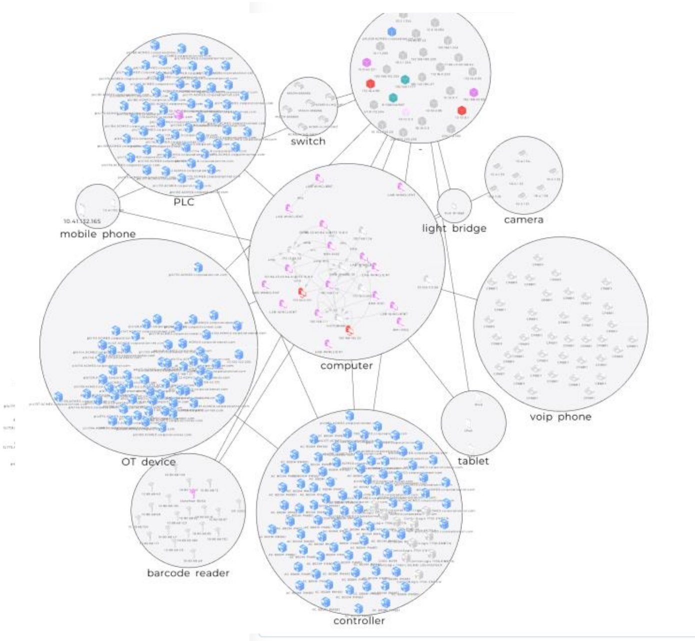
Os or firmware	iPadOS 13..3..1
IP	192.168.1.17
Mac address	dc:d3:a2:df:05:ad
Mac vendor	Apple, Inc.

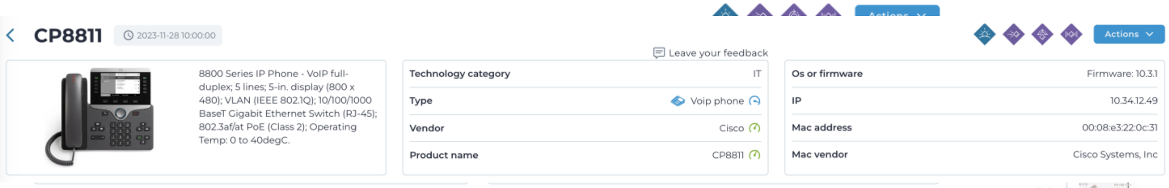
Functionality Needed to meet these Best Practices?

Security Challenge	Examples of Targeted Outcomes	Technology and Process Capabilities to Solve
Visibility	**Asset Visibility** **Communications Mapping** **Vulnerability Management**	• Passive Asset Discovery / Network Visualization • Vulnerability Database / Workbooks / Asset Intelligence • Active Asset Discovery and Scanning • Endpoint Sensors for Detection and Response
Detection	**Threat Detection** **Anomaly Detection** **Root Cause Analysis**	• DPI Traffic Monitoring / Anomaly Detection • Process Monitoring and Threat Detection • Threat Intelligence Ingestion and Use • Cross Platform Integration
Response	**Forensic Tools** **Playbooks** **Actionable Intelligence**	• Dashboards / Queries / Alerts / Reports • In-Line Blocking or Disruption via Technical Integrations • Response Playbooks / Planning

Asset Discovery and Network Visualization

Passively or Actively Identify Assets and Communication Flows, and aggregate across all environments and sites. Visibility and awareness of all devices that are a part of the full attack surface is foundational for cyber security for IoT / IIoT / OT





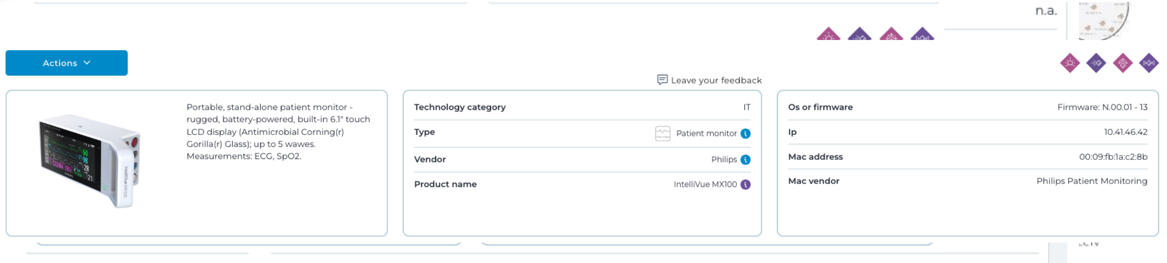
CP8811

2023-11-28 10:00:00

8800 Series IP Phone - VoIP full-duplex; 5 lines; 5-in. display (800 x 480); VLAN (IEEE 802.1Q); 10/100/1000 BaseT Gigabit Ethernet Switch (RJ-45); 802.3af/at PoE (Class 2); Operating Temp: 0 to 40degC.

Technology category	IT
Type	Voip phone
Vendor	Cisco
Product name	CP8811

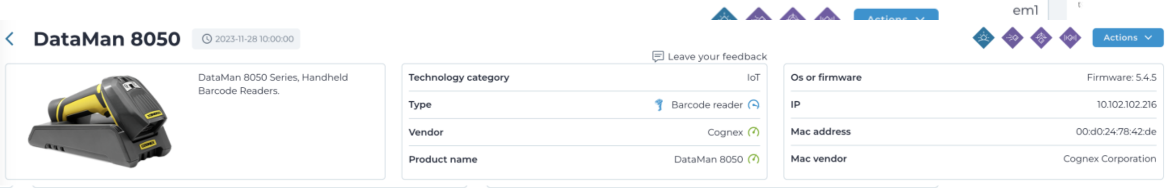
Os or firmware	Firmware: 10.3.1
IP	10.34.12.49
Mac address	00:08:e3:22:0c:31
Mac vendor	Cisco Systems, Inc



Portable, stand-alone patient monitor - rugged, battery-powered, built-in 6.1" touch LCD display (Antimicrobial Corning(r) Gorilla(r) Glass); up to 5 wawes. Measurements: ECG, SpO2.

Technology category	IT
Type	Patient monitor
Vendor	Philips
Product name	IntelliVue MX100

Os or firmware	Firmware: N.00.01 - 13
Ip	10.41.46.42
Mac address	00:09:fb:1a:c2:8b
Mac vendor	Philips Patient Monitoring



DataMan 8050

2023-11-28 10:00:00

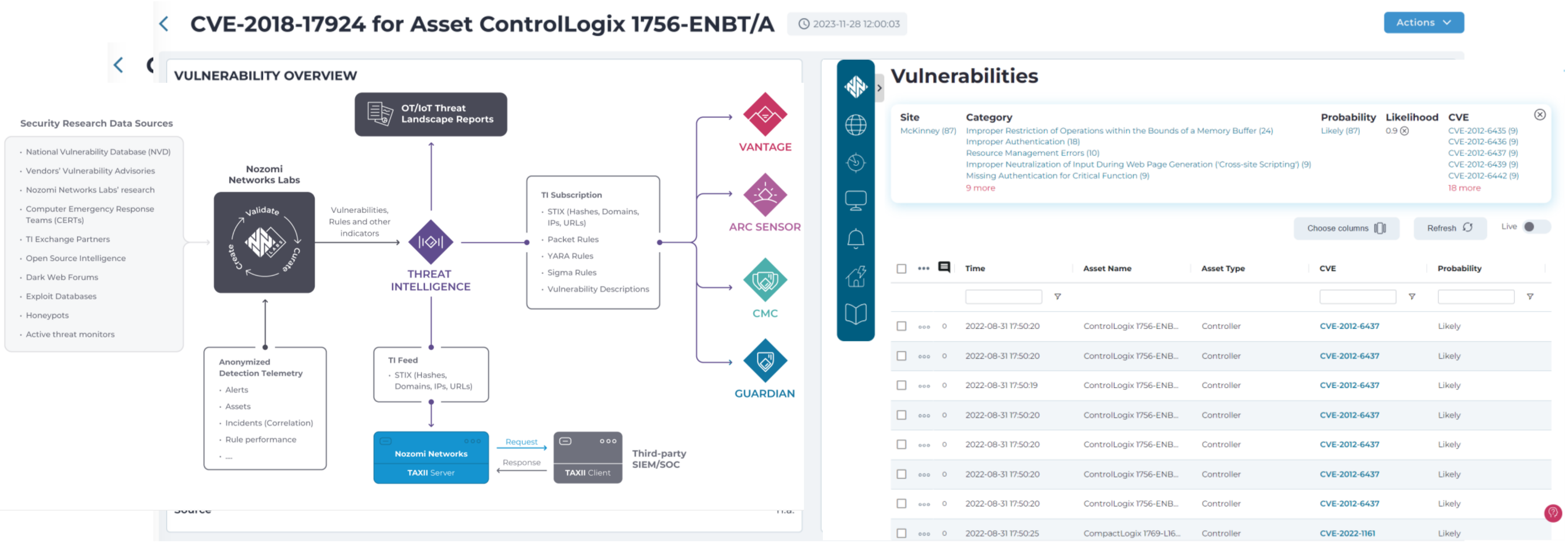
DataMan 8050 Series, Handheld Barcode Readers.

Technology category	IoT
Type	Barcode reader
Vendor	Cognex
Product name	DataMan 8050

Os or firmware	Firmware: 5.4.5
IP	10.102.102.216
Mac address	00:d0:24:78:42:de
Mac vendor	Cognex Corporation

Identify Vulnerabilities and Risks

Having a database of device vulnerability information enhanced by threat research that references against the assets and communications database enables quick, and ideally automated identification of potential risks.

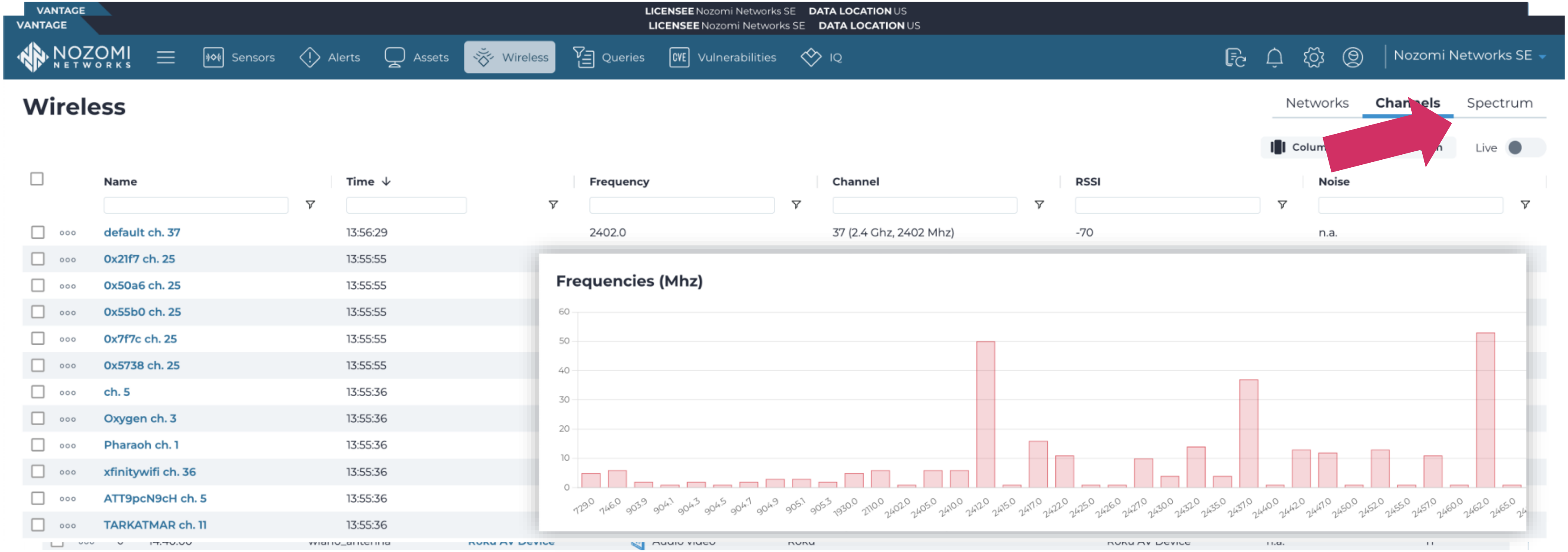


Site	Category	Probability	Likelihood	CVE
McKinney (87)	Improper Restriction of Operations within the Bounds of a Memory Buffer (24) Improper Authentication (18) Resource Management Errors (10) Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (9) Missing Authentication for Critical Function (9) 9 more	Likely (87)	0.9 ⊗	CVE-2012-6435 (9) CVE-2012-6436 (9) CVE-2012-6437 (9) CVE-2012-6439 (9) CVE-2012-6442 (9) 18 more

□	•••		Time	Asset Name	Asset Type	CVE	Probability
□	ooo	0	2022-08-31 17:50:20	ControlLogix 1756-ENB...	Controller	CVE-2012-6437	Likely
□	ooo	0	2022-08-31 17:50:20	ControlLogix 1756-ENB...	Controller	CVE-2012-6437	Likely
□	ooo	0	2022-08-31 17:50:19	ControlLogix 1756-ENB...	Controller	CVE-2012-6437	Likely
□	ooo	0	2022-08-31 17:50:20	ControlLogix 1756-ENB...	Controller	CVE-2012-6437	Likely
□	ooo	0	2022-08-31 17:50:20	ControlLogix 1756-ENB...	Controller	CVE-2012-6437	Likely
□	ooo	0	2022-08-31 17:50:20	ControlLogix 1756-ENB...	Controller	CVE-2012-6437	Likely
□	ooo	0	2022-08-31 17:50:20	ControlLogix 1756-ENB...	Controller	CVE-2012-6437	Likely
□	ooo	0	2022-08-31 17:50:25	CompactLogix 1769-L16...	Controller	CVE-2022-1161	Likely

Identify Wireless Networks and Devices

Some of these devices won't be easily seen on the wire – understanding the wireless networks that exist (and especially those that shouldn't) and which devices are using them (and how) a critical puzzle piece.

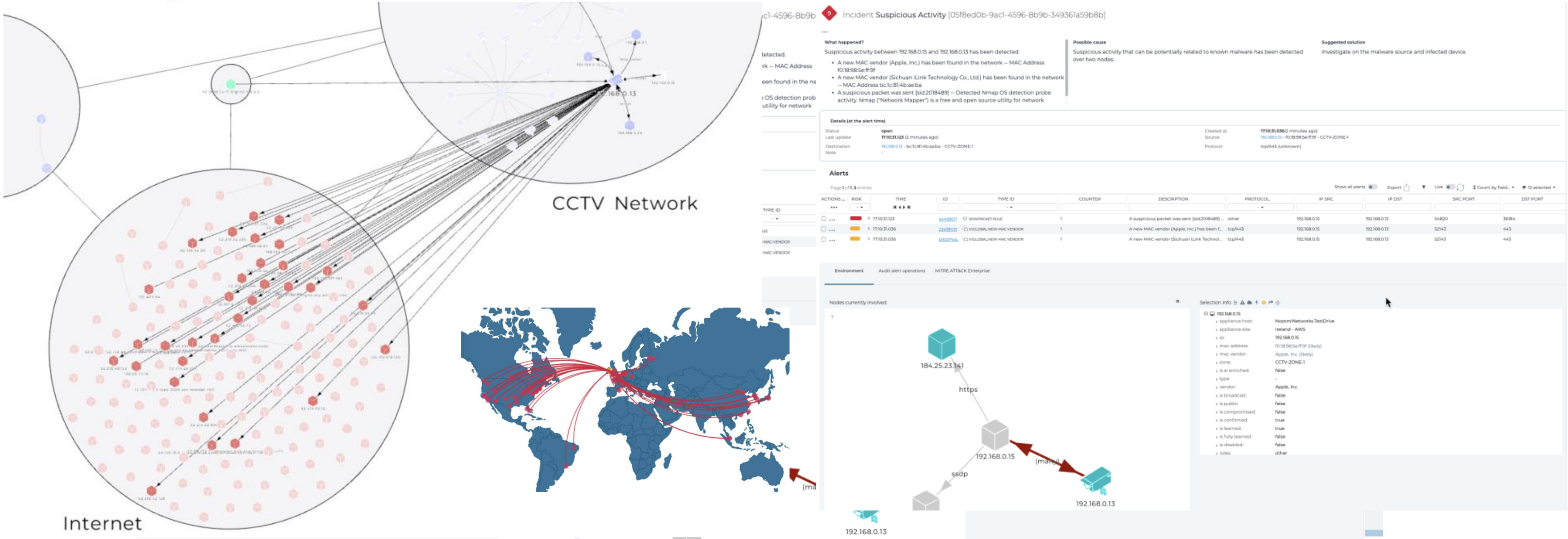


Wireless

	Name	Time ↓	Frequency	Channel	RSSI	Noise
□	default ch. 37	13:56:29	2402.0	37 (2.4 Ghz, 2402 Mhz)	-70	n.a.
□	0x21f7 ch. 25	13:55:55				
□	0x50a6 ch. 25	13:55:55				
□	0x55b0 ch. 25	13:55:55				
□	0x7f7c ch. 25	13:55:55				
□	0x5738 ch. 25	13:55:55				
□	ch. 5	13:55:36				
□	Oxygen ch. 3	13:55:36				
□	Pharaoh ch. 1	13:55:36				
□	xfinitywifi ch. 36	13:55:36				
□	ATT9pcN9cH ch. 5	13:55:36				
□	TARKATMAR ch. 11	13:55:36				

Detect Potential Threats and Plan Response

Utilize a Hybrid Threat Detection approach including signature, indicator, behavior, and anomaly based detections at the network and endpoint level to capture events, group into incidents and playbooks, and plan mitigation.



9 Incident **Suspicious Activity** [05f8ed0b-9ac1-4596-8b9b-349361a59b8b]

What happened?

Suspicious activity between 192.168.0.15 and 192.168.0.13 has been detected.

- A new MAC vendor (Apple, Inc.) has been found in the network -- MAC Address f0:18:98:5e:ff:9f
- A new MAC vendor (Sichuan iLink Technology Co., Ltd.) has been found in the network -- MAC Address bc:1c:81:4b:ae:ba
- A suspicious packet was sent [sid:2018489] -- Detected Nmap OS detection probe activity. Nmap ("Network Mapper") is a free and open source utility for network

Possible cause

Suspicious activity that can be potentially related to known malware has been detected over two nodes.

Suggested solution

Investigate on the malware source and infected device.

Details (at the alert time)

Status	open	Created at	17:10:31.036(2 minutes ago)
Last update	17:10:31.123 (2 minutes ago)	Source	192.168.0.15 - f0:18:98:5e:ff:9f - CCTV-ZONE-1
Destination	192.168.0.13 - bc:1c:81:4b:ae:ba - CCTV-ZONE-1	Protocol	tcp/443 (unknown)
Note	-		

Alerts

Page 1 of 1, 3 entries

Show all alerts | Export | Live | Count by field... | 12 selected

ACTIONS ...	RISK	TIME	ID	TYPE ID	COUNTER	DESCRIPTION	PROTOCOL	IP SRC	IP DST	SRC PORT	DST PORT
□ ...	🟥 9	17:10:31.123	ee458617	SIGN:PACKET-RULE	1	A suspicious packet was sent [sid:2018489] ...	other	192.168.0.15	192.168.0.13	54820	36184
□ ...	🟧 5	17:10:31.036	23a98109	VI:GLOBAL:NEW-MAC-VENDOR	1	A new MAC vendor (Apple, Inc.) has been f...	tcp/443	192.168.0.15	192.168.0.13	52143	443
□ ...	🟧 5	17:10:31.036	b90374dc	VI:GLOBAL:NEW-MAC-VENDOR	1	A new MAC vendor (Sichuan iLink Technol...	tcp/443	192.168.0.15	192.168.0.13	52143	443

Environment | Audit alert operations | MITRE ATT&CK Enterprise

Nodes currently involved

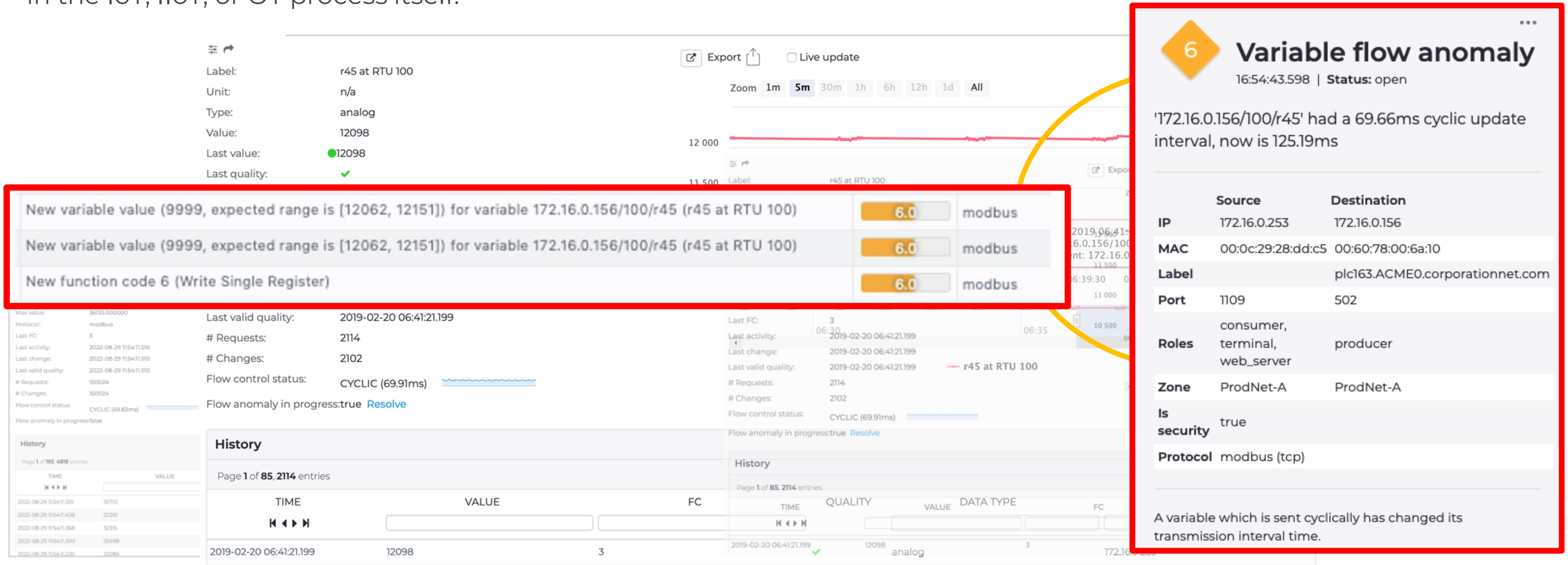
Selection info

192.168.0.15

appliance host:	NozomiNetworks.TestDrive
appliance site:	Ireland - AWS
ip:	192.168.0.15
mac address:	f0:18:98:5e:ff:9f (likely)
mac vendor:	Apple, Inc. (likely)
zone:	CCTV-ZONE-1
is ai enriched:	false
type:	-
vendor:	Apple, Inc.
is broadcast:	false
is public:	false
is compromised:	false
is confirmed:	true
is learned:	true
is fully learned:	false
is disabled:	false
roles:	other

Use Deep Inspection of Traffic to Monitor OT / IoT Processes

Advanced Deep Packet Inspection capability allows a security team to monitor, illustrate, and detect anomalous behavior in the IoT, IIoT, or OT process itself.



Label:	r45 at RTU 100
Unit:	n/a
Type:	analog
Value:	12098
Last value:	● 12098
Last quality:	✓

New variable value (9999, expected range is [12062, 12151]) for variable 172.16.0.156/100/r45 (r45 at RTU 100)	6.0	modbus
New variable value (9999, expected range is [12062, 12151]) for variable 172.16.0.156/100/r45 (r45 at RTU 100)	6.0	modbus
New function code 6 (Write Single Register)	6.0	modbus

Last valid quality:	2019-02-20 06:41:21.199
# Requests:	2114
# Changes:	2102
Flow control status:	CYCLIC (69.91ms)
Flow anomaly in progress:	true Resolve

History

Page 1 of 85, 2114 entries

TIME	VALUE	FC
2019-02-20 06:41:21.199	12098	3

6 Variable flow anomaly

16:54:43.598 | **Status:** open

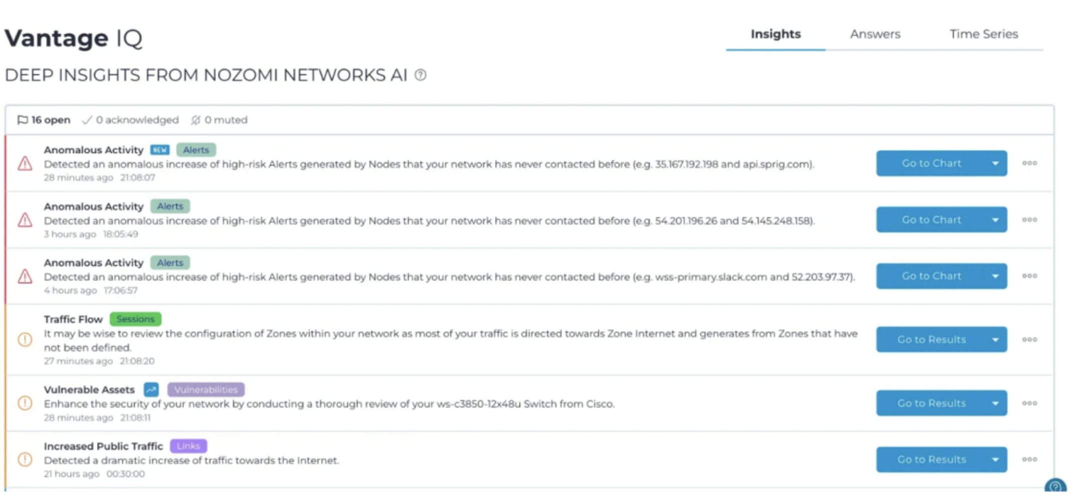
'172.16.0.156/100/r45' had a 69.66ms cyclic update interval, now is 125.19ms

	Source	Destination
IP	172.16.0.253	172.16.0.156
MAC	00:0c:29:28:dd:c5	00:60:78:00:6a:10
Label		plc163.ACME0.corporationnet.com
Port	1109	502
Roles	consumer, terminal, web_server	producer
Zone	ProdNet-A	ProdNet-A
Is security	true	
Protocol	modbus (tcp)	

A variable which is sent cyclically has changed its transmission interval time.

Robust Reporting and Insights

The ability to automatically generate complete reports for regulatory or internal requirements and get executive level summaries of threats and risks is crucial. Use AI to act as an analyst and automate where possible.



Vantage IQ

DEEP INSIGHTS FROM NOZOMI NETWORKS AI

16 open ✓ 0 acknowledged 0 muted

Anomalous Activity NEW Alerts
Detected an anomalous increase of high-risk Alerts generated by Nodes that your network has never contacted before (e.g. 35.167.192.198 and api.sprig.com).
28 minutes ago 21:08:07

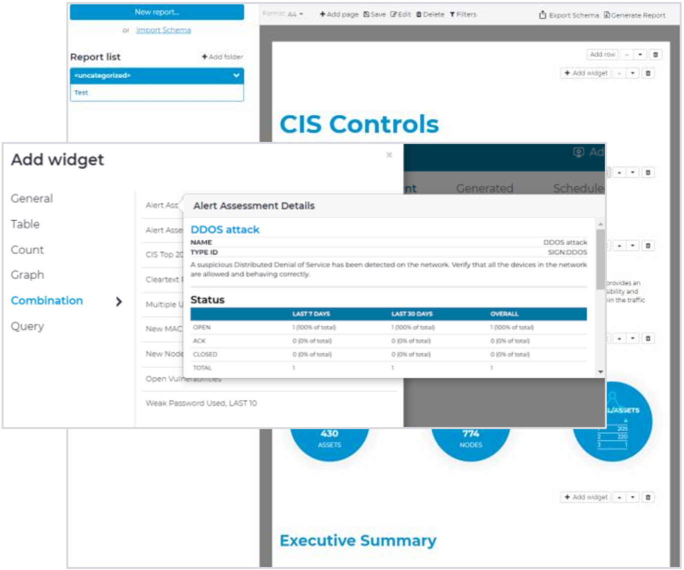
Anomalous Activity Alerts
Detected an anomalous increase of high-risk Alerts generated by Nodes that your network has never contacted before (e.g. 54.201.196.26 and 54.145.248.158).
3 hours ago 18:05:49

Anomalous Activity Alerts
Detected an anomalous increase of high-risk Alerts generated by Nodes that your network has never contacted before (e.g. wss-primary.slack.com and 52.203.97.37).
4 hours ago 17:06:57

Traffic Flow Sessions
It may be wise to review the configuration of Zones within your network as most of your traffic is directed towards Zone Internet and generates from Zones that have not been defined.
27 minutes ago 21:08:20

Vulnerable Assets Vulnerabilities
Enhance the security of your network by conducting a thorough review of your ws-c3850-12x48u Switch from Cisco.
28 minutes ago 21:08:11

Increased Public Traffic Links
Detected a dramatic increase of traffic towards the Internet.
21 hours ago 00:30:00



CIS Controls

Add widget

Alert Assessment Details

DDOS attack

NAME: DDOS attack
TYPE ID: SIGN:DDOS

A suspicious Distributed Denial of Service has been detected on the network. Verify that all the devices in the network are allowed and behaving correctly.

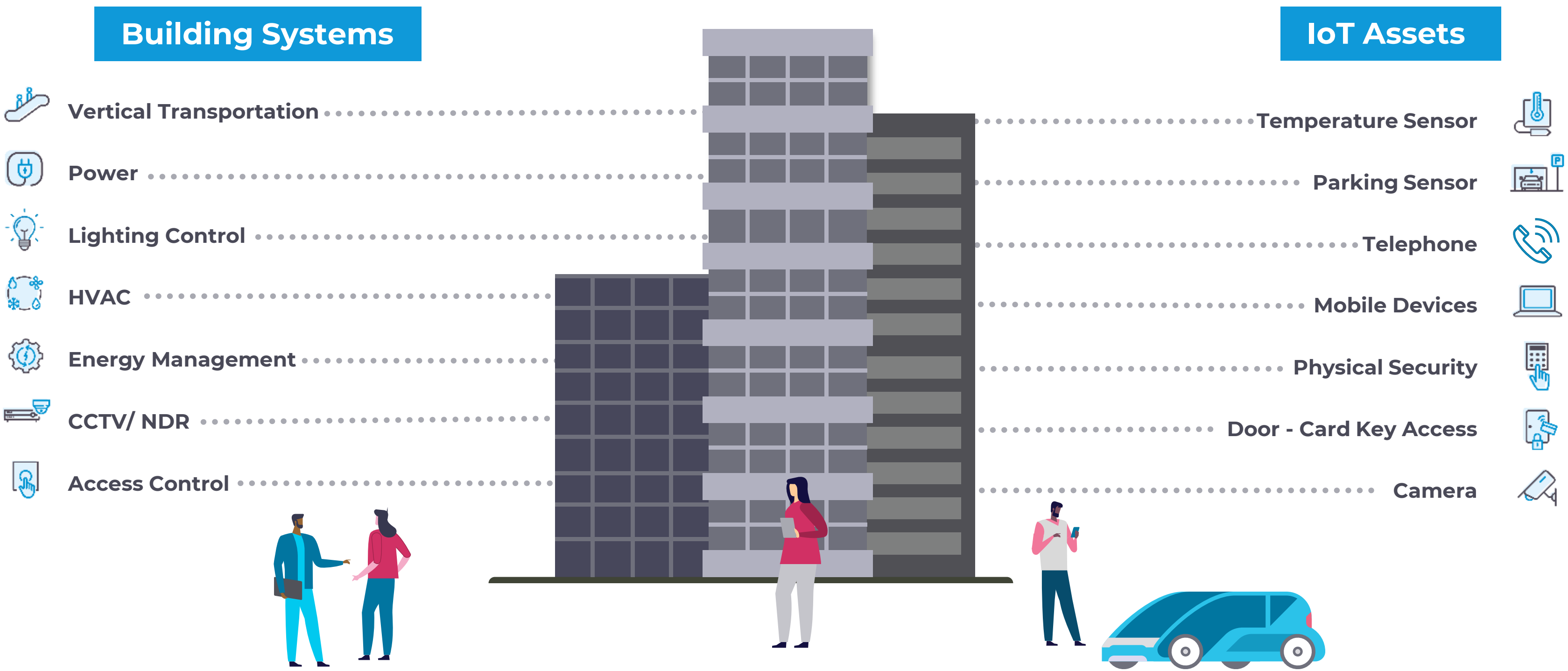
Status

	LAST 7 DAYS	LAST 30 DAYS	OVERALL
OPEN	1 (100% of total)	1 (100% of total)	1 (100% of total)
ACK	0 (0% of total)	0 (0% of total)	0 (0% of total)
CLOSED	0 (0% of total)	0 (0% of total)	0 (0% of total)
TOTAL	1	1	1

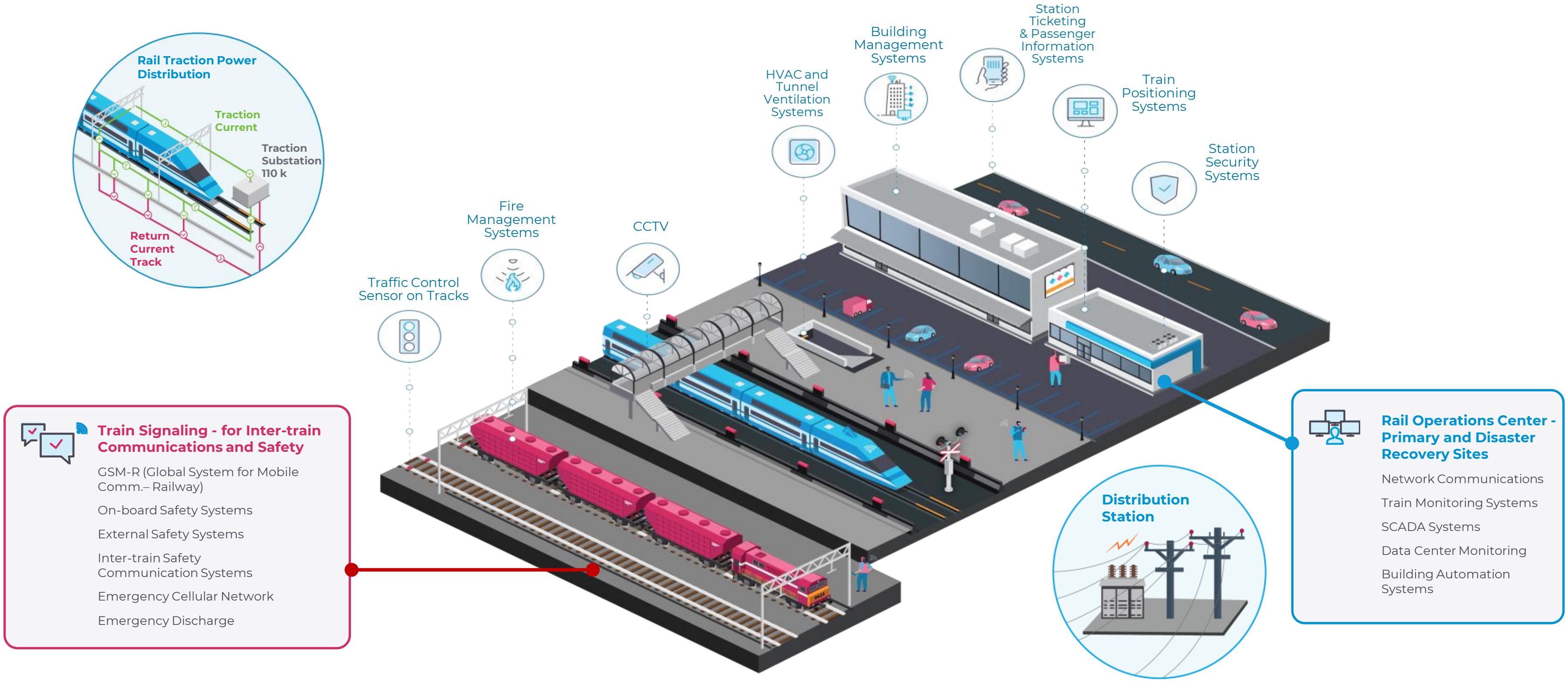
Executive Summary

Examples and Use Cases

Cyber Physical Attack Surface: Standard Building



Cyber Physical Attack Surface Example – Rail


Rail Traction Power Distribution
Traction Current
Traction Substation 110 k
Return Current Track
Traffic Control Sensor on Tracks
Fire Management Systems
CCTV
HVAC and Tunnel Ventilation Systems
Building Management Systems
Station Ticketing & Passenger Information Systems
Train Positioning Systems
Station Security Systems
Distribution Station

Train Signaling - for Inter-train Communications and Safety

GSM-R (Global System for Mobile Comm.– Railway)

On-board Safety Systems

External Safety Systems

Inter-train Safety Communication Systems

Emergency Cellular Network

Emergency Discharge

Rail Operations Center - Primary and Disaster Recovery Sites

Network Communications

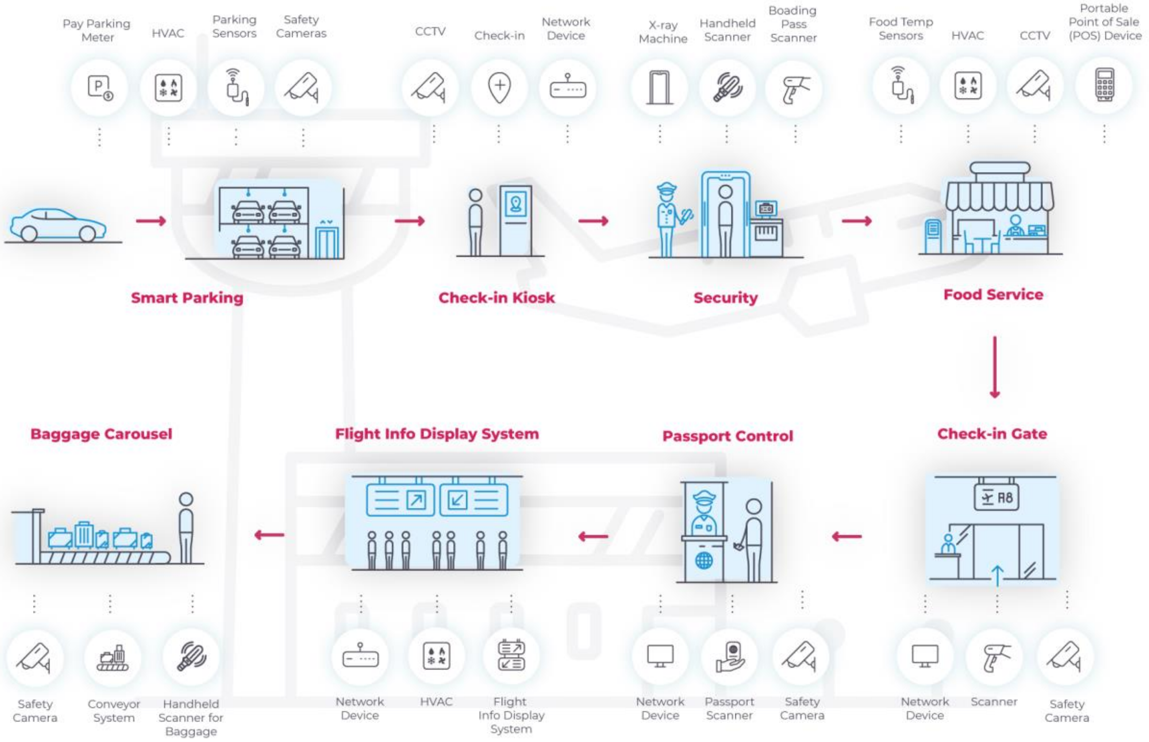
Train Monitoring Systems

SCADA Systems

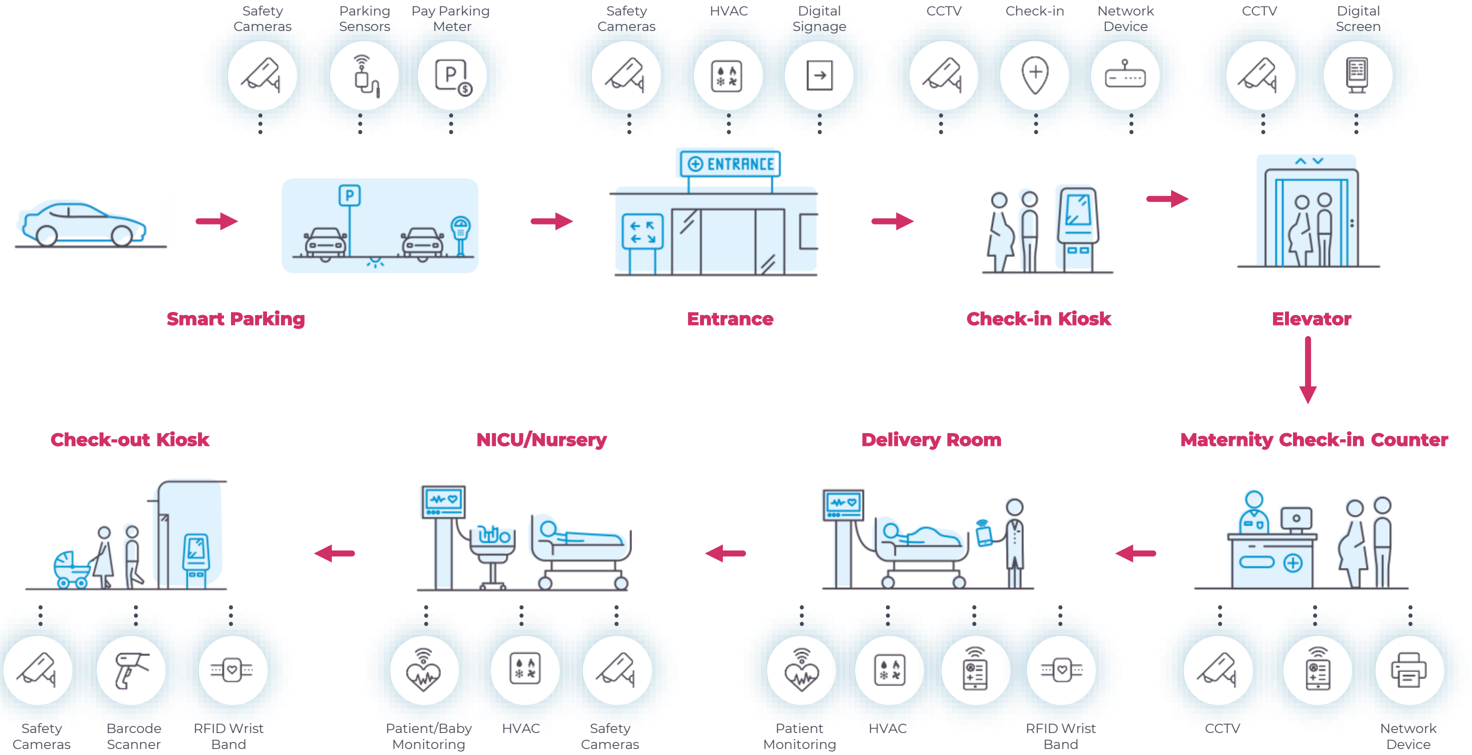
Data Center Monitoring

Building Automation Systems

Cyber Physical Attack Surface Example – Airport



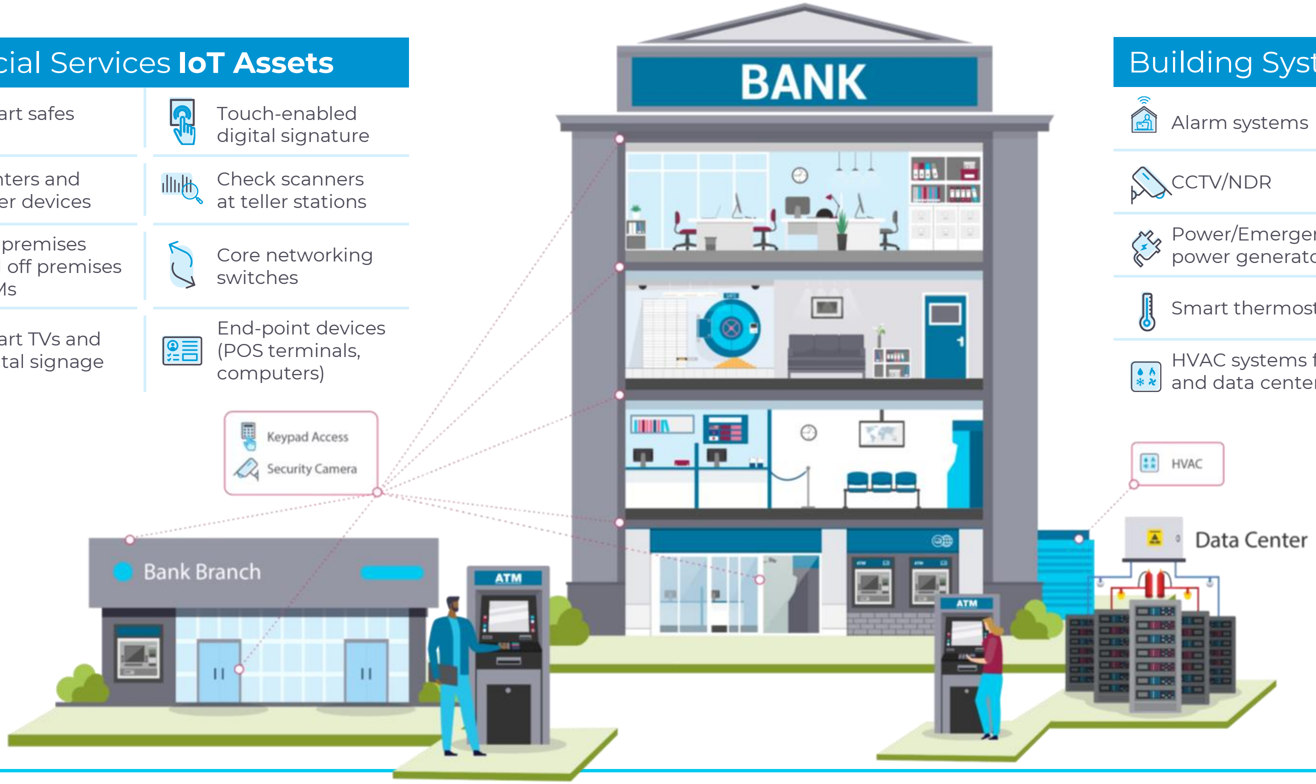
Cyber Physical Attack Surface Example – Healthcare



Cyber Physical Attack Surface Example: Financial Institution

Financial Services **IoT Assets**

- Smart safes
- Printers and other devices
- On-premises and off premises ATMs
- Smart TVs and digital signage
- Touch-enabled digital signature
- Check scanners at teller stations
- Core networking switches
- End-point devices (POS terminals, computers)



Building Systems **OT Assets**

- Alarm systems
- CCTV/NDR
- Power/Emergency power generator
- Smart thermostats
- HVAC systems for bank building and data center heating/ cooling
- Fire detection
- Lighting control
- Door locks/keypad access/badge systems
- Data center cooling system

Risk Examples: Targeting Cyber Physical Systems

Managing a large number of completely disparate types and vendors of systems.

Networks in buildings are large and comprised of a variety of types of systems and OEM vendors, some with third-party access or even control of networks. Nozomi Networks helps to give visibility into this large distribution of assets.

CCTV used as an entry point to secure networks or to monitor secure areas.

Significant security flaws in CCTV and security monitoring systems have allowed attacks to compromise these systems to remotely monitor the feeds to plan physical attacks, or as a point of presence to launch further cyber attack.

Using OT / IoT as a pivot point to bypass perimeter cyber security.

Lack of attention to OT and IoT systems like CCTV cameras and temperature sensors that use stripped down operating systems and minimal encryption or authentication creates a potential pivot point to critical systems.

Risk Examples: Targeting Cyber Physical Systems

IP Cameras Compromised and used as a botnet.

A targeted vendor's IP cameras were compromised using a 0 day and thousands of cameras across numerous organizations were tied together as a large botnet that targeted other organizations for DDoS attacks.

Building Management System Compromised for crypto mining.

A prospective client reported high resource load on BMS environment, installing Guardian on the network detected cryptocurrency mining software installed managed from an external location.

Vendors managing Physical Security ignoring firmware updates

An assessment at a large government institution found that the firmware on multiple vendors' alarm systems hadn't been updated in years, leaving critical vulnerabilities with simple exploits in place.

About Nozomi Networks

11K+

Worldwide Installations

102M+

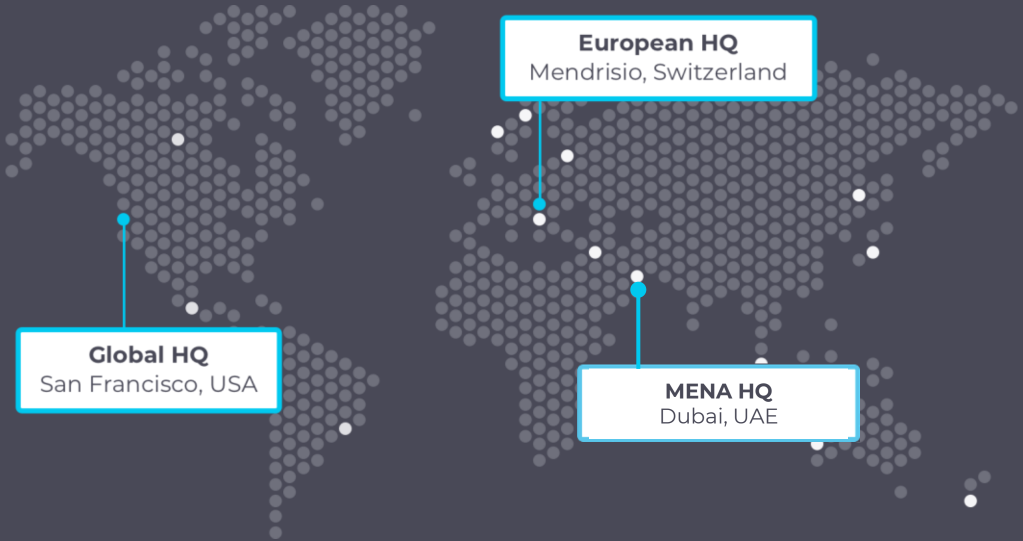
Devices Monitored Across Converged OT/IoT

6 Continents

Scalable Deployments Across 6 Continents

Global Expertise

Worldwide Network of Partners and 1,500+ Certified Professionals



Nozomi Networks Industry Expertise

Cyber Security Expertise for Cyber Physical Systems Across all key Verticals

- Airports
- Automotive
- Rail Systems
- Data Centers
- Federal Government
- Financial Services

- Manufacturing
- Maritime
- Military
- Mining
- Oil & Gas
- Pharma

- Retail
- Smart Cities
- Transportation & Logistics
- Utilities
- Water & Wastewater
- Healthcare

Nozomi Networks Differentiators and R&D

The only vendor with full platform coverage of all cyber physical systems.

Leading Platform Scalability

Proven Large Deployments
Deployed with some of the largest customers in the world – including single sensors monitoring 1M+ devices

Cloud-Based Scale
Option to aggregate and analyze data on-premises through Guardian or with Vantage cloud

Consolidated Management
Management through CMC or from the cloud

Ease of Deployment

Sensor Options to Fit Your Environment
Physical, virtual, cloud, edge, endpoint, container sensors

Cloud Architecture
SaaS platform speeds onboarding, eliminates sizing issues

Industry's Largest Partner Ecosystem and Open API
Minimizes integration complexity

Actionable Intelligence

Power of AI
Only vendor with AI/ML engine for more analysis of data and anomalies

Prioritized Remediation
Workbooks and customized playbooks prioritize and guide remediation efforts

Overcoming the Skills Gap
Intelligent automation to deal with low alerts, data deluge and security issues

Ongoing R&D Projects

Onboard Vehicle Monitoring

Monitoring Encrypted Communications

Wireless Communication Monitoring

NOZOMI NETWORKS

nozominetworks.com

Thank You

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.