

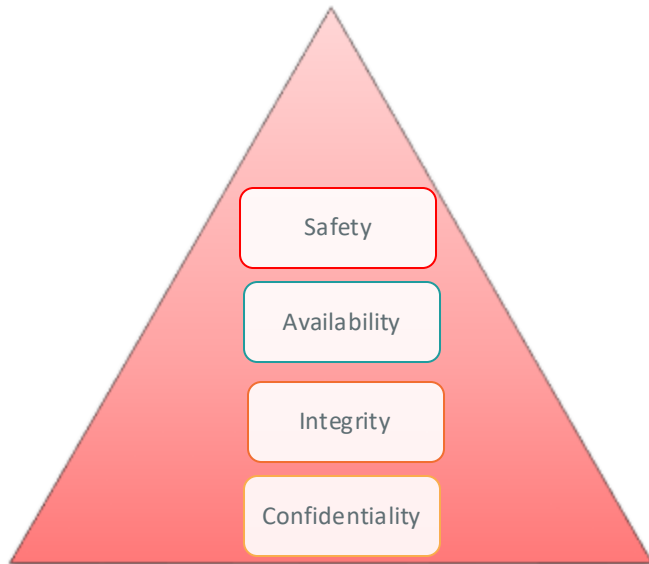


Compliance and Regulatory Challenges in OT: Best Practices for Adherence

Sebastian Erler-Yates, Technical Sales Engineer, EMEA

Telonic Gipfeltreffen 27.03.2025

Defining OT/IoT Cyber Risk

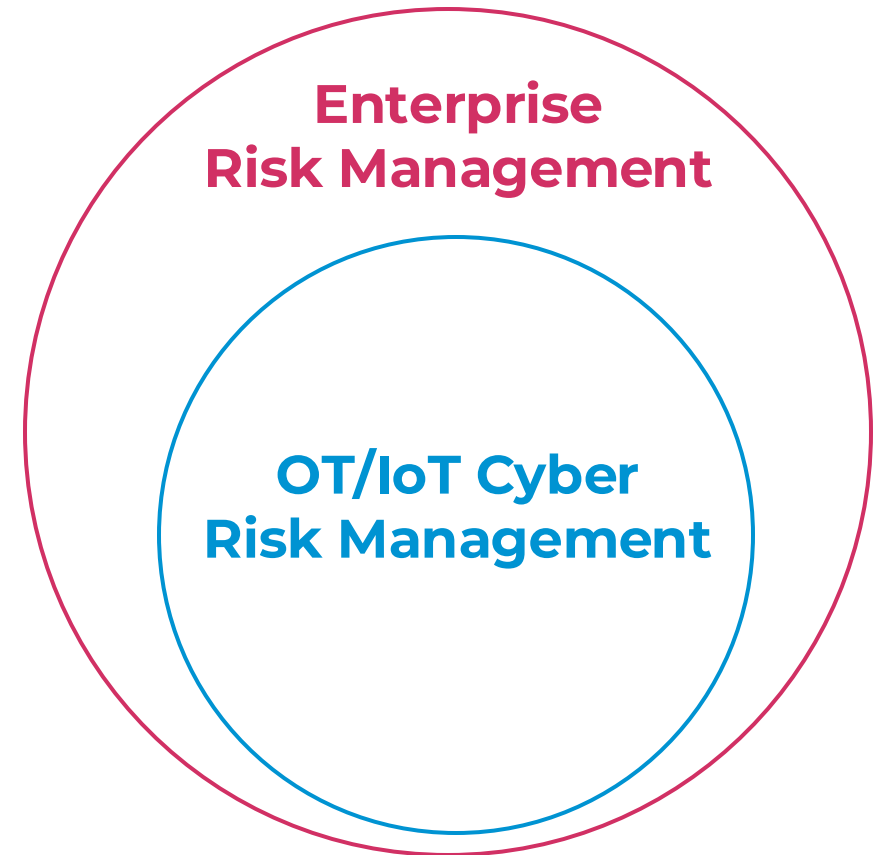


OT/IoT Cyber Risk is the potential for **loss of life, injuries, equipment damage, environmental damage, financial harm, and operational disruptions** caused by the failure, misuse, or cyber compromise of connected operational technology and internet of things systems that support industrial and critical infrastructure operations.

OT/IoT Cyber Risk is a Business Risk

Cyber Risk: More Than an IT Issue—A Key Part of the Larger Ecosystem

The growing OT/IoT cyber threat landscape makes cyber risks as crucial as safety, legal, financial, and reputational risks, necessitating their integration into Enterprise Risk Management (ERM) programs



OT/IoT Cyber Risk Frameworks

Key Frameworks Shaping the Risk Management Process

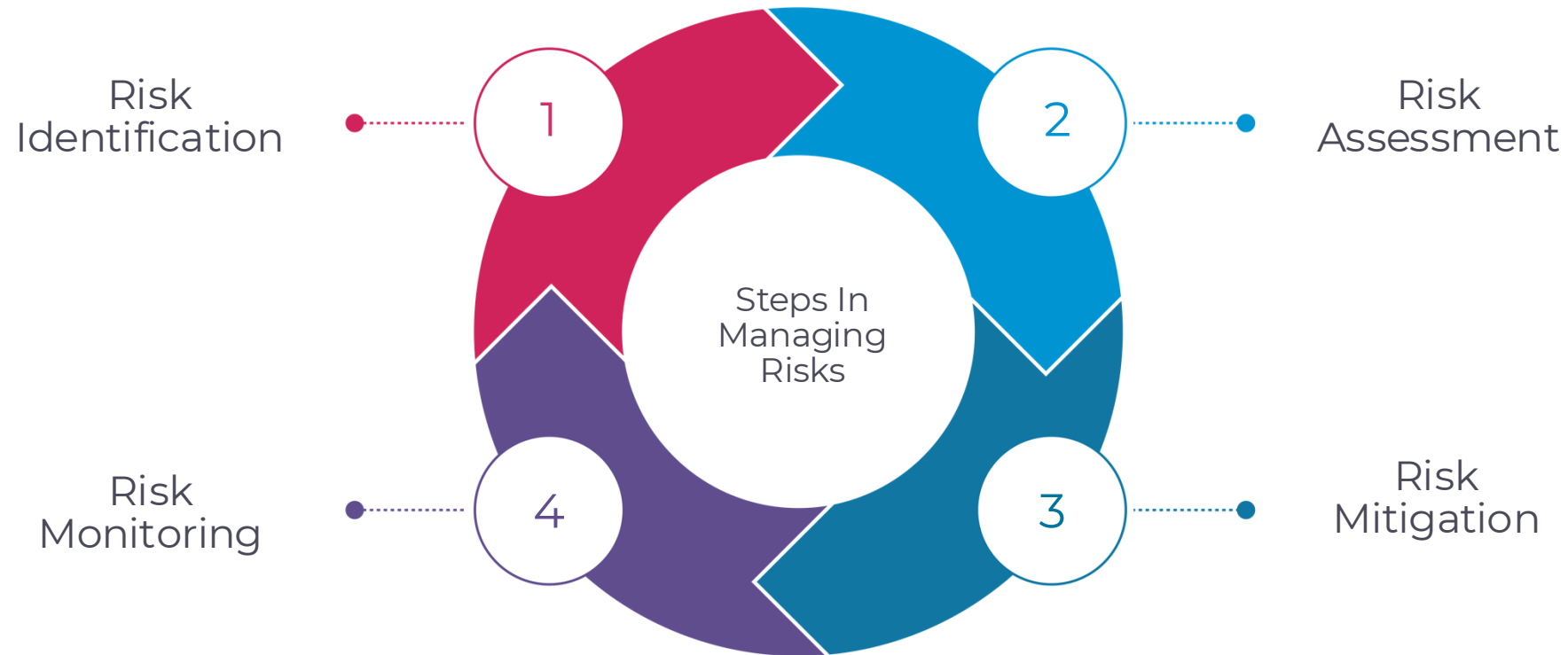
- **ISO 31000:2018:** Principles and guidelines for risk management
- **IEC 31010:2019:** Risk assessment techniques
- **NIST Risk Management Framework (RMF):** A structured process for integrating cybersecurity and risk management activities into the system development lifecycle.
- **ISO/IEC 27005:2022:** Guidance on managing information security risks
- **ISA/IEC 62443-3-2:** Security risk assessment for industrial automation and control system design
- **NIS2 Directive (EU 2022/2555):** – Updated EU cybersecurity directive that strengthens security requirements for critical and essential entities
- **EU Cyber Resilience Act (CRA):** – Proposed regulation to ensure cybersecurity requirements for products with digital elements
- **KRITIS-Verordnung (BSI-KritisV, Germany):** – National regulation for critical infrastructure operators, defining security obligations and reporting requirements

OT specific

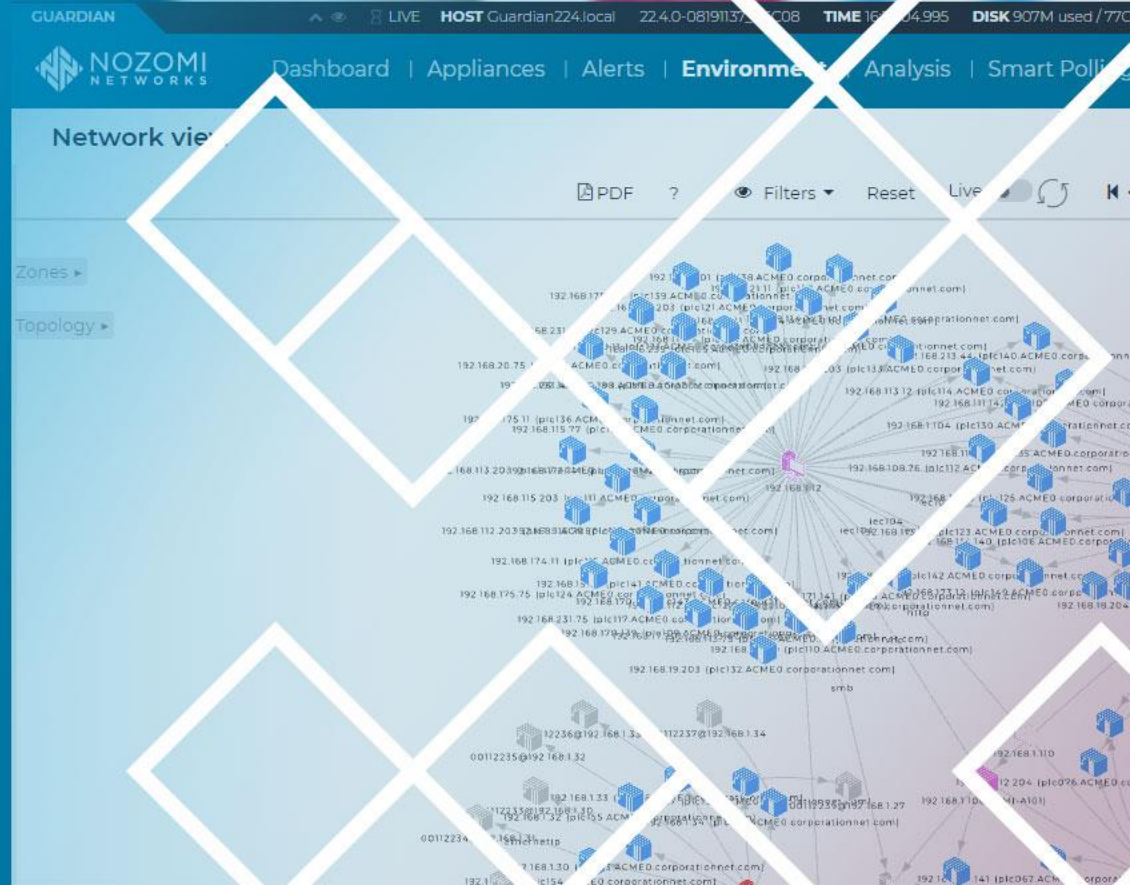


OT/IoT Cyber Risk Management Process

The Continuous Nature of Risk Management



OT/IoT Risk Management with Nozomi Networks

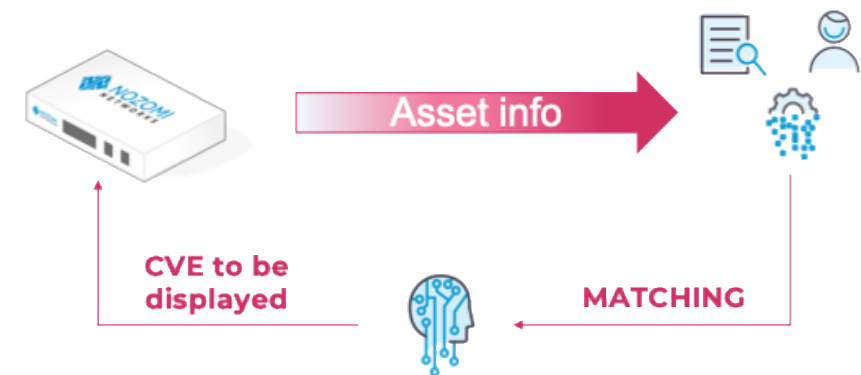
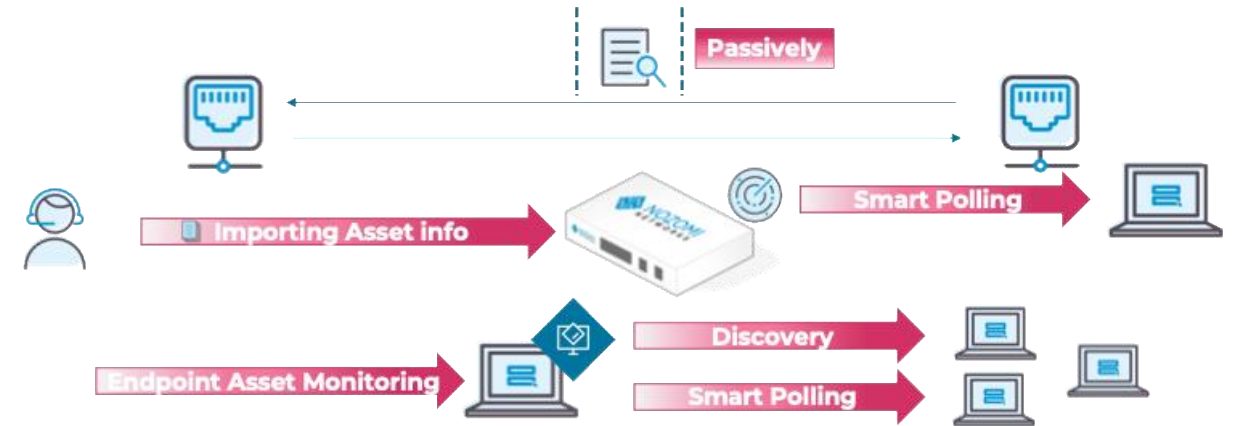


Asset Inventory

Risk Identification Starts with Asset Inventory

- Comprehensive Asset Visibility through
 - **Passive Network** Inventory
 - Active **Discovery** packets
 - Active **Smart Polling**
 - Asset Data **Import**, and **Integrations**
 - **Asset Intelligence** service
 - **Endpoint** Sensor-Based Inventory
 - **Wireless** Asset inventory

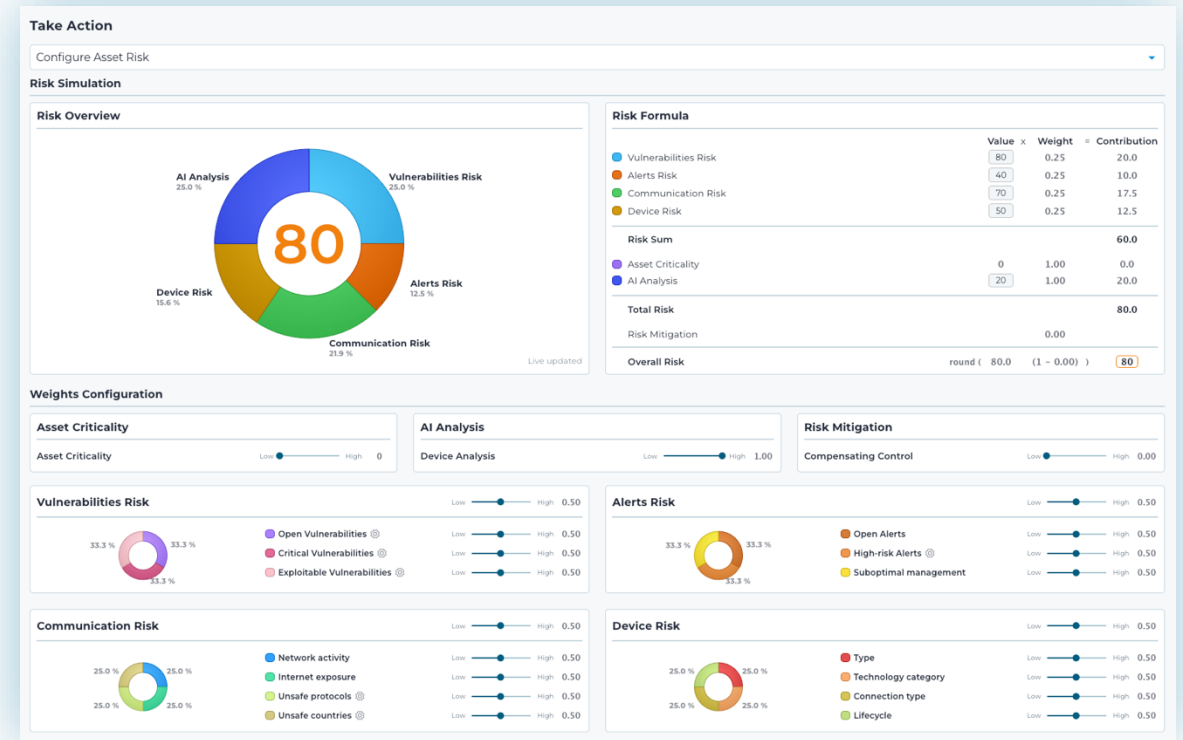
- Extensive Asset Data Attributes, including:
 - **Network**, User, Process, Software, **Hardware**
 - Utilization, **Lifecycle**, Asset Criticality & **CVE**



Risk Score Calculation

Asset-Centric Risk Assessment Approach

- Each **asset** and related entity (**sensor, zone, site, enterprise**) is assigned a unique Risk Score.
- Asset Risk Scores are calculated using weighted risk factors and sub-factors reflecting **Threat, Vulnerability, Controls Effectiveness**, and **Impact** identified during the Risk Identification step:
 - Asset Criticality
 - Device Risk
 - Communication Risk
 - Vulnerability Risk
 - Alert Risk
- **The asset risk score calculation can be customized** to suit the asset owner's environment.



Risk Remediation

Focused Cyber Risk Mitigation Recommendations



- **AI/ML-driven** prioritized risk remediation actions
- **Out-of-the-box integrations** with:
 - SIEMs & Log Management
 - SOARs
 - Firewalls & Endpoint Security
 - NACs and SDNs
 - Alert & Ticketing Systems
 - Secure Remote Access, and more
- **Limitless integrations with OpenAPI** enable easy integration with any existing tools and systems

Upgrade Internet Explorer to Edge
This action reduces your overall Risk by **1%** and resolves or mitigates **114 CVEs** across **114 Assets**.
Software Update

Stop using HTTP
This action reduces your overall Risk by **3%** and affects **12157** recently active Links across **5593 Assets**.
Protocol Policy



RESTful Services

Threat & Risk Overview and Details

Multidimensional Risk Dynamics Monitoring

Risk
Monitoring



- A properly configured individual asset risk score enables effective monitoring of **risk context**
- Calculation of **sensor, zone, site**, and ultimately the overall **company risk score**.
- Actionable threat insights powered by **Mandiant Threat Intelligence**:
 - Threat descriptions
 - Exploitation status and vectors
 - MITRE ATT&CK details
 - Mitigation suggestions and more

APT28 Kimsuky Group 74 Forest Blizz... +36 more

APT28 is a highly active cyber espionage group that has employed a variety of malware and TTPs, including spear phishing, watering holes, credential collection, and the exploitation of mobile platforms, toward intelligence collection intended to provide political and military advantage. APT28 operations have primarily impacted entities across the public and private sectors in North America and Europe, and the group, which multiple governments have attributed to Unit 26165 within the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), has heavily targeted Ukraine in particular following Russia's February 2022 full-scale invasion. However, we have also observed APT28's targeting of government and military entities in other regions such as the Middle East and Asia, and open source reporting further corroborates our observations of the group's activity in these regions.

First seen: 2015-01-01
Last seen: 2024-05-07

Associated malware and vulnerabilities

- DROVORUB** (BAT, TROJAN) - Drovorub is a sophisticated malware family associated with Russian state-sponsored threat actors. It is a Linux malware designed to create backdoors...
- CVE-2015-1641** - Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Office Compatibility Pack SP3, Word Autom...
- CVE-2012-1856** - The TabStrip ActiveX control in the Common C Microsoft Office 2003 SP3, Office 2003 Web Con and ...

Targeted Countries

References

- Microsoft. (2023, July 12). How Microsoft names threat actors. Retrieved Novemb...
- Microsoft Threat Actor Naming July 2023. Ref. [link]
- Billy Leonard. (2023, April 19). Ukraine remains Russia's biggest cyber focus in...
- Leonard TAO 2023. Ref. [link]
- NSA, CIA, FBI, INSC. (2020, July). Russian GRU Conducting Global Brute Force Ca...
- Cybersecurity Advisory GRU Brute Force Campaign July 2021. Ref. [link]
- Hacquebord, F., Remorin, L. (2020, December 17). Pawn Storm's Lack of Sophistica...
- ThreatIntel Pawn Storm Dec 2020. Ref. [link]
- Microsoft Threat Intelligence Center (MSTIC). (2020, September 10). STRONTIUM: O...
- https://www.microsoft.com/en-us/security/blog/2020/09/10/strontium-0/

Enterprise

MITRE ATT&CK for ENTERPRISE techniques detection

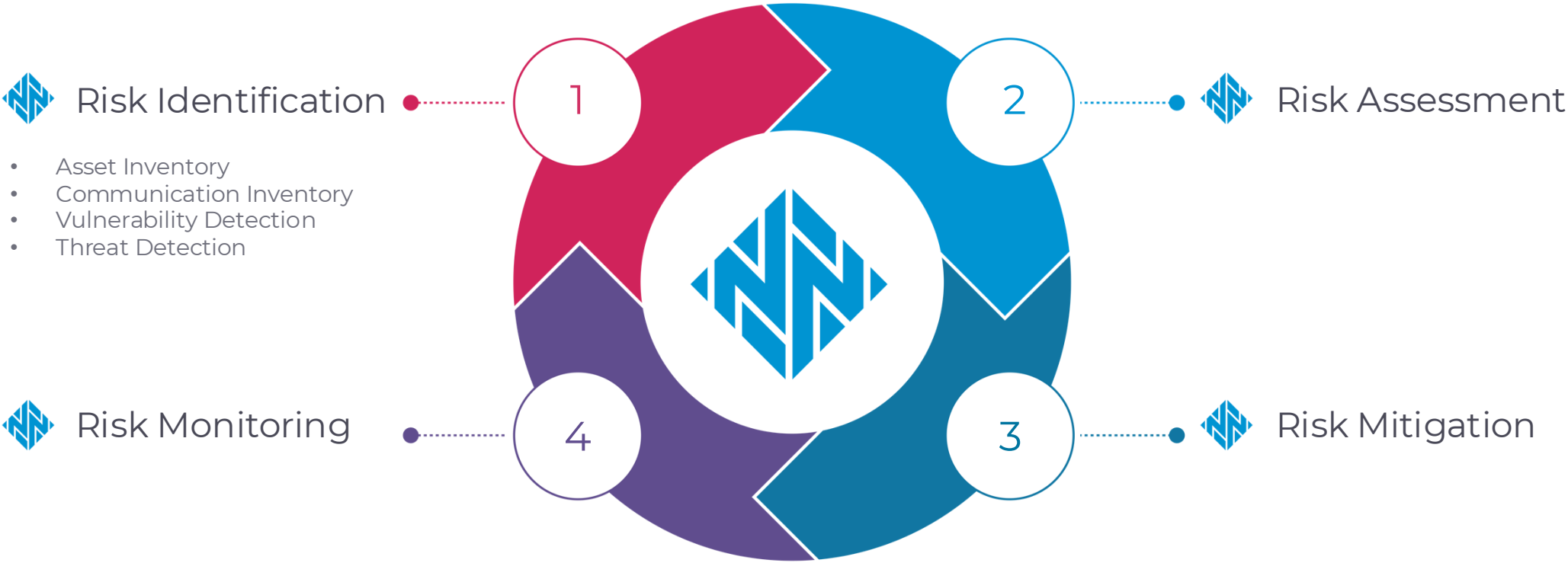
Comprehensive visualization

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Gather Victim Identity Information	Acquire Infrastructure	Exploit Public-Facing Application	Windows Management Instrumentation	Boot or Logon Initialization Scripts	Exploitation for Privilege Escalation	Rootkit	Adversary-in-the-Middle	System Owner/User Discovery	Replication Through Removable Media	Screen Capture	Application Layer Protocol	Exfiltration Over Web Service

Risk Management in Action

The background features a blue gradient with a globe in the center. Overlaid on the globe are binary digits (0s and 1s) in yellow and white. A white diamond-shaped grid pattern is superimposed on the right side of the image. The text "Risk Management in Action" is written in white, bold, sans-serif font on the left side.

Manage OT/IoT Cyber Risks Effectively with Nozomi Networks



Assets 381

IT
305

OT
45

IoT
31

Active

381

High Risk

18

Types

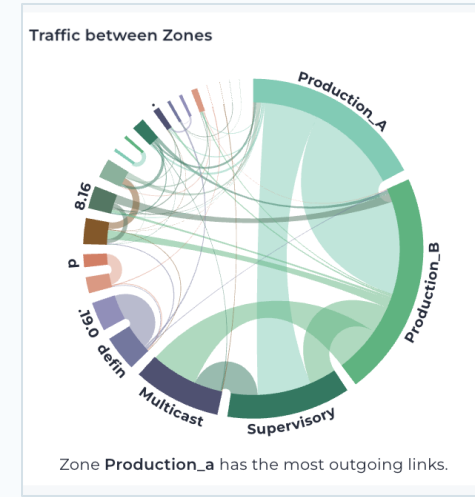
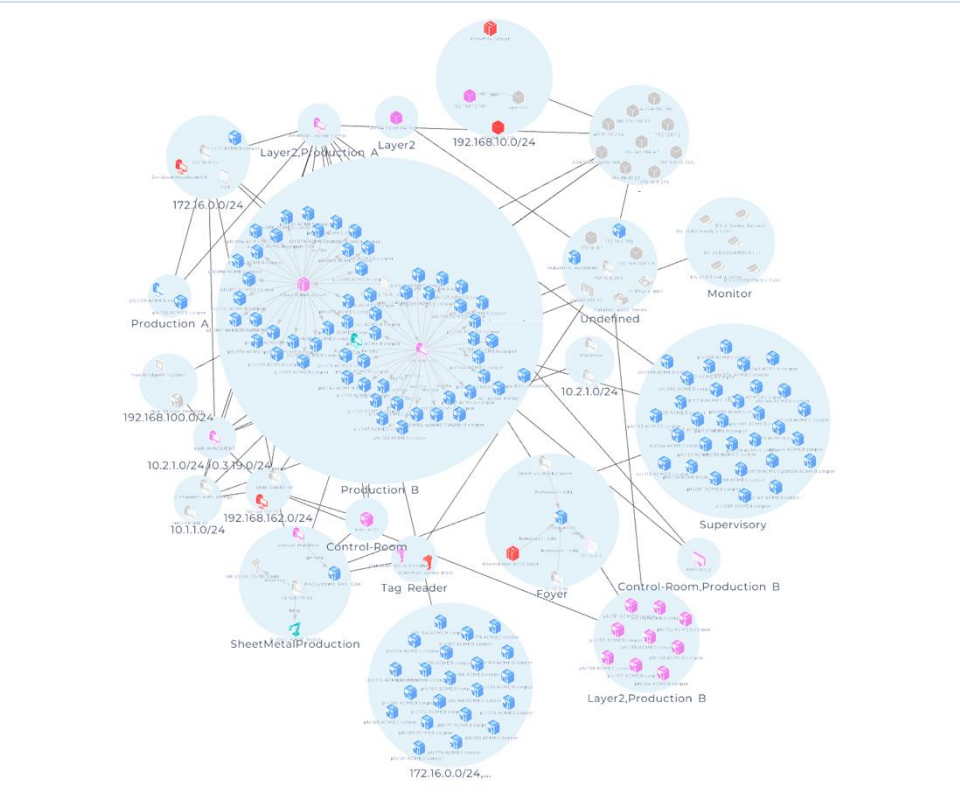
Type	Assets	%
Computer	134	35.2%
IT device	99	26.0%
Mobile phone	39	10.2%
Other	20	5.2%
Controller	20	5.2%
OT device	15	3.9%

Vendors

Vendor	Assets	%
Apple	74	37.8%
VMware	36	18.4%
ROOMZ	8	4.1%
Rockwell Aut...	6	3.1%
Mitsubishi EL	4	2.0%
WAGO	3	1.5%

OS

OS	Assets	%
macOS	31	34.1%
Windows	17	18.7%
Linux	10	11.0%
tvOS	7	7.7%
iOS	4	4.4%
Windows XP	3	3.3%



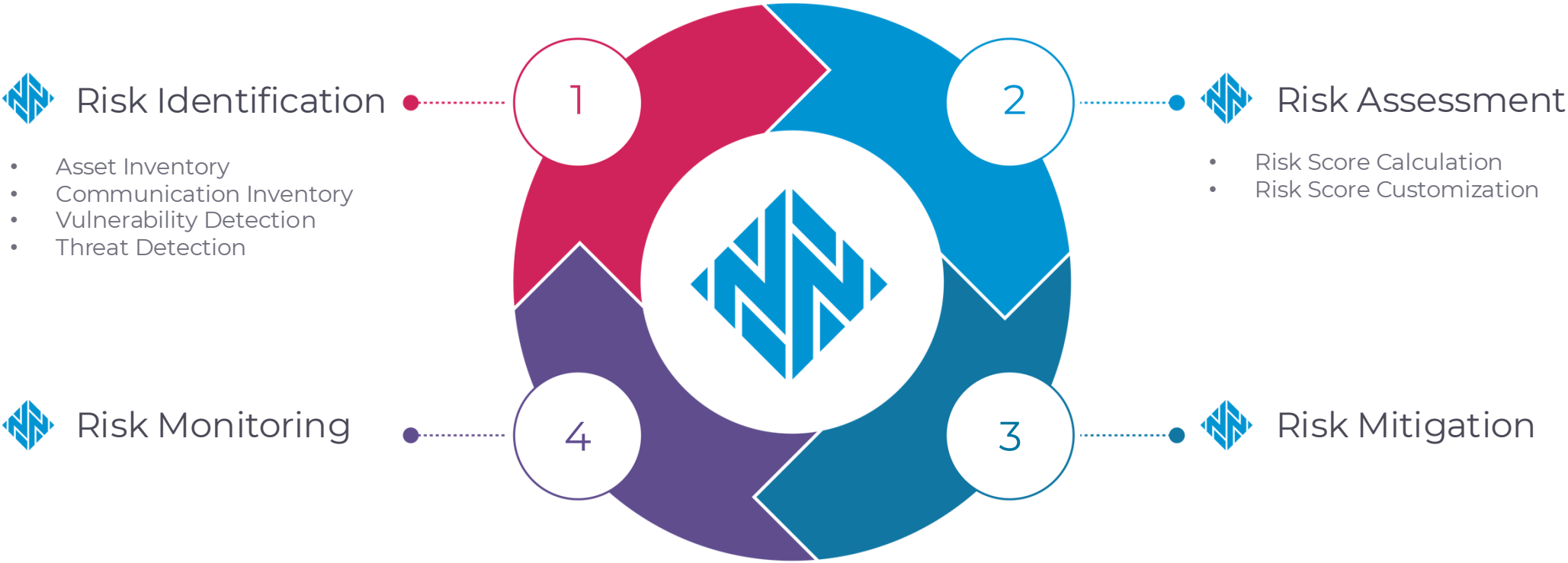
Open Alerts

Name	Alerts	%
Device state change	787	15.4%
Duplicated IP	718	14.0%
Malicious USB device	621	12.1%
Protocol packet injection	398	7.8%
MITM attack	347	6.8%
OT device stop request	286	5.6%

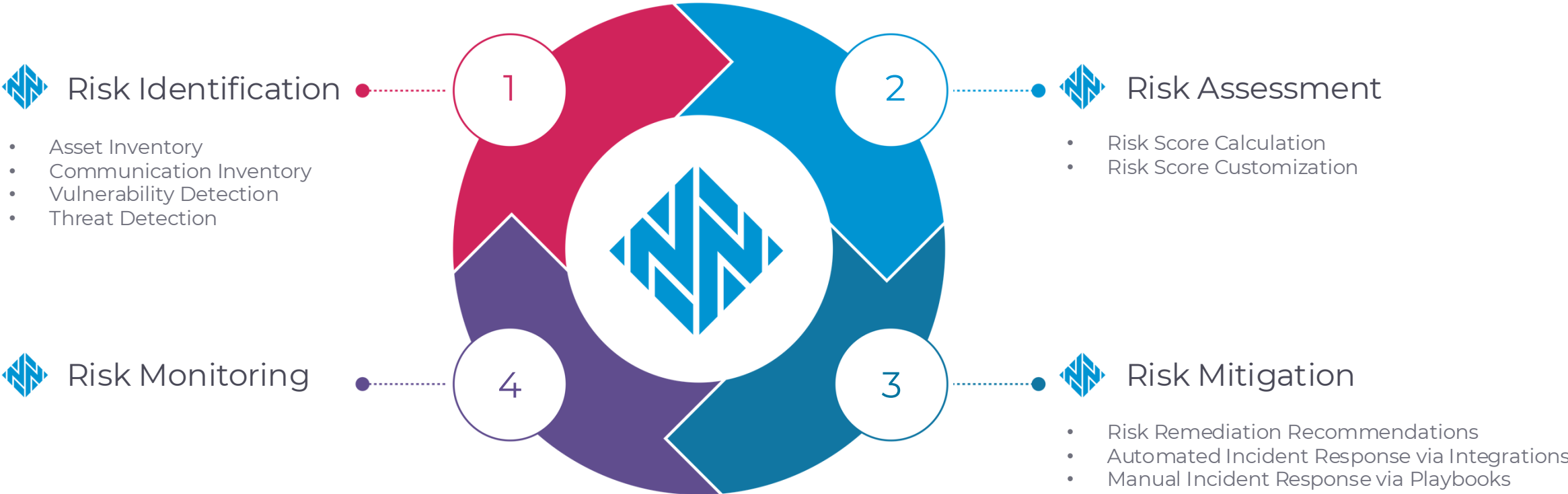
Alert Sources

Asset	Alerts	%
R04ENCPU iQ-R Series PLC CPU	1.64K	43.5%
LE-DEMO-BA	744	19.7%
SEL-401 Protection Automation and Control Mergin...	368	9.8%
Bosch Nexa Tools	213	5.6%
ch-demo-motor-rpi.local	184	4.9%
Safety_PLC	147	3.9%

Manage OT/IoT Cyber Risks Effectively with Nozomi Networks



Manage OT/IoT Cyber Risks Effectively with Nozomi Networks





Asset Risk

Overview Remediations Details Benchmarks

Remediations ⓘ

Software Remediations

Applying **2** Remediations → Will mitigate **305** Vulnerabilities → Reducing by **2%** Overall Risk



Upgrade Internet Explorer to Edge

This action reduces your overall Risk by **1%** and resolves or mitigates **114** CVEs across 114 Assets.

Software Update



Upgrade Windows 7 to Windows 10

This action reduces your overall Risk by **1%** and resolves or mitigates **191** CVEs across 191 Assets.

OS Update

Communication Remediations

Applying **3** Remediations → Will block **22.0K** Unsafe Links → Reducing by **6%** Overall Risk



Stop using HTTP

This action reduces your overall Risk by **3%** and affects 12157 recently active Links across 5593 Assets.

Protocol Policy



Stop using SMB

This action reduces your overall Risk by **1%** and affects 5324 recently active Links across 2406 Assets.

Protocol Policy

Hardware Remediations

Applying **1** Remediation → Will replace **12** Assets → Reducing by **1%** Overall Risk



Replace unsupported hardware

This action reduces your overall Risk by **1%** across 12 Assets.

Hardware Upgrade

Malicious USB device ⓘ 21:00:36

Actions ▾



What happened

Suspicious key inputs. This Human Interface Device (HID) [vendor: Atmel Corp.] [product: unregistered/unknown] connected to [192.168.45.192] has shown suspicious behavior, possibly related to automatically injected commands rather than a human interaction.

Possible cause

Suspicious behaviour detected in a device announcing itself as Human Interface Device (HID). It may be compromised, including malicious software running on it and performing dangerous actions targeting the main system it is connected to.

Suggested solution

Disconnect the Human Interface Device (HID) and inspect it carefully, it might have a miniature embedded chip inside. Find the root cause of the unexpected behavior.

Actor details

Source	
Site	Building Automation
Zone	n.a.
Label	LE-DEMO-BA
IP	192.168.45.192
MAC	n.a.
TCP/IP port	n.a.
Roles	n.a.
Users	4

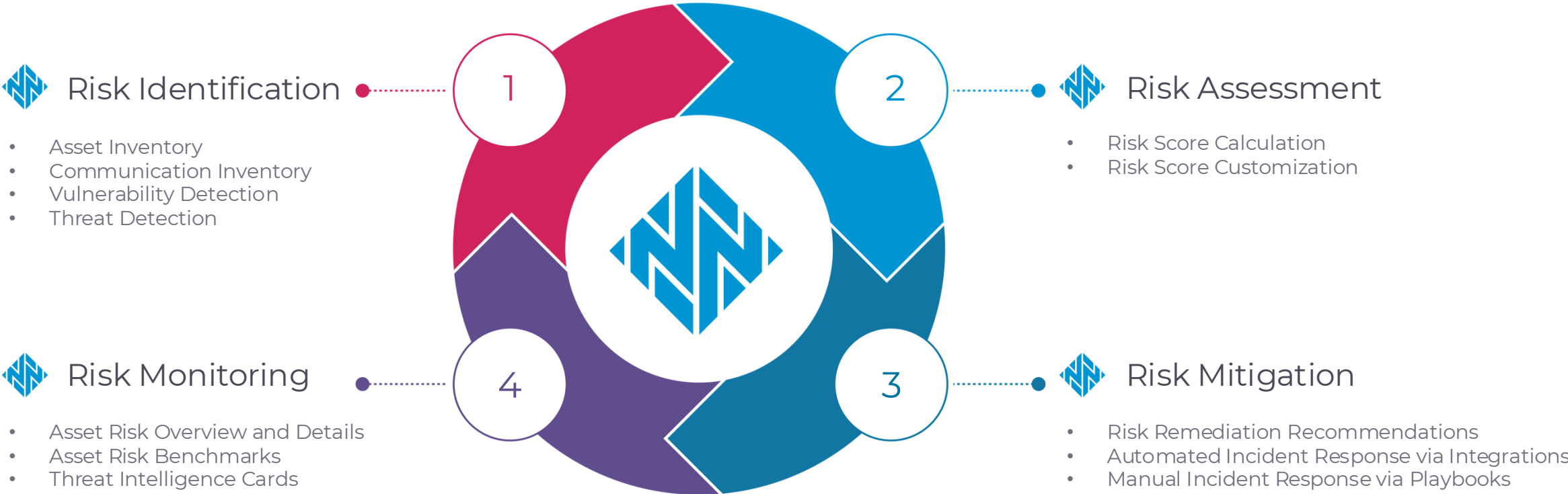
Playbook ✎

Malicious Hardware Device

- For malicious USB injection you must follow the **System Intrusion Process for external hardware devices** (SIPE).
 - Do **not** remove the malicious devices and do **not** power down the affected system.
 - Contact the incident response team (internal number: **012-25423-12452**) and the SO of the affected department.
 - Send an email to the head of the department and the CISO with information about the alert and about the activation of the SIPE process.
- Consult the **Incident Response** team. The following items must be executed in order expect of extraordinary circumstances:
 - Initiate** forensic investigation
 - Collect forensic artifacts from the affected system. (Memory dump, system logs, etc)
 - Collect traffic logs
 - Examine** access control of the system.
 - Consider affected number of systems and users.
 - Activate** incident and isolation policies.
 - Enable appropriate blocking firewall rules
 - Restrict User accessibility
 - Remove** the malicious device and consult the recover policy for the system according to impact.
- Support the activation of the **Business Continuity Plan** if required.
 - Evaluate the requirements for data recovery and access recovery.
 - Evaluate the activation of USB blocking policies at the end points of the organization.

The content of this process should be documented in a report and emailed to the head of the department and CISO.

Manage OT/IoT Cyber Risks Effectively with Nozomi Networks



Asset Risk

Overview Remediations Details Benchmarks

Overview 1w 1m 1q 1y All

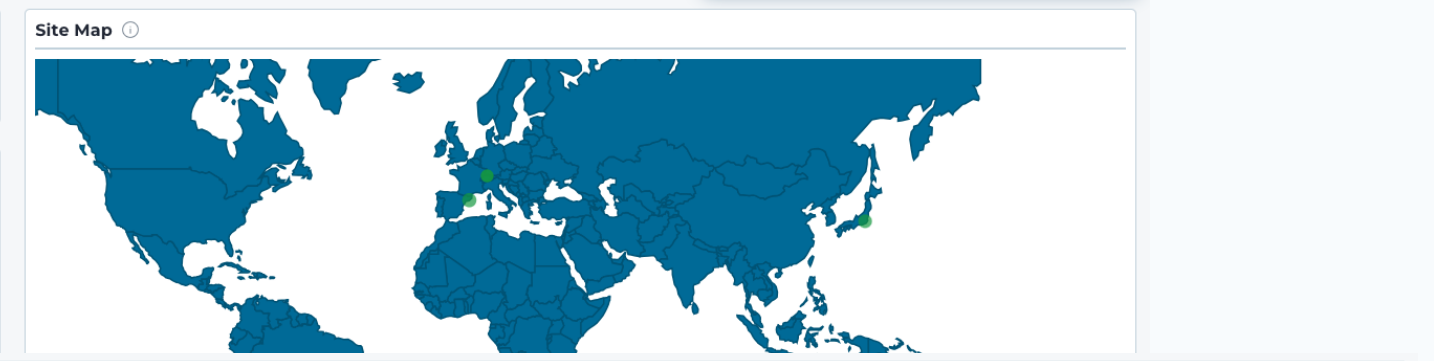
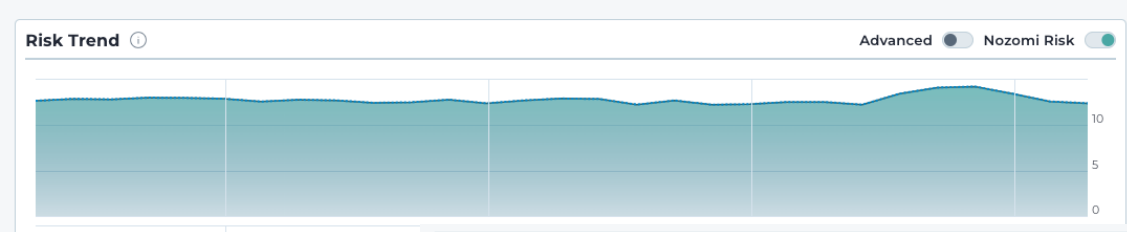
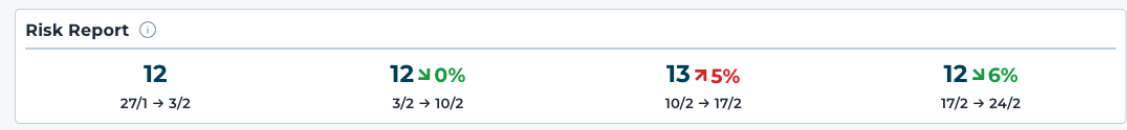
12 ↓2%
Low
Custom Risk
Overall in your organization

12 ↓2%
Low
Nozomi Risk
Overall in your organization

18 Low
Riskiest Site
Building Automation

18 ↑2%
Low
Riskiest Sensor
ch-demo-production-line-guardian-air

95 ↑956%
High
Riskiest Zone
Unspecified



Riskiest Sites

Building Automation	18 Low
Production Line	15 ↓4% Low
Mendrisio	12 ↑1% Low
North City	9 ↓27% Low
South City	9 ↓21% Low

Riskiest Sensors

ch-demo-production-line-guardian-air	18 ↑2% Low
ch-demo-building-automation-arc.intra.nozominetworks.com	18 Low
ch-demo-production-line-arc-embedded.intra.nozominetworks...	15 ↓4% Low
ch-demo-nozomiville-sensor-1.intra.nozominetworks.com	12 ↑1% Low
ch-demo-nozomiville-sensor-3.intra.nozominetworks.com	9 ↓21% Low

Riskiest Zones

Unspecified	95 ↑956% High
production_line	27 ↑39% Low
production_line_field	23 ↓8% Low
production_line_control	23 ↓7% Low
power_production	20 ↑3% Low

Riskiest Sites

Building Automation

18 Low

Risk	Name	Type	Vendor
18	LE-DEMO-BA	Computer	Intel

Production Line

15 ↓4% Low

Risk	Name	Type	Vendor
100	R04ENCPU iQ-R ...	Controller	Mitsubishi El...
44	5069-L306ERMS...	Controller	Rockwell Au...
40	1734-AENTR Ser...	IO	Rockwell Au...

Mendrisio

12 ↑1% Low

Risk	Name	Type	Vendor
49	Android.local	HMI	Advantech
47	Safety_PLC	Controller	Rockwell Au...
46	DESKTOP-4GAN...	Computer	Avalue Tech...

North City

9 ↓27% Low

Risk	Name	Type	Vendor
22	192.168.40.5	Other	VMware
8	ID_OnLogic2.local	Computer	OnLogic
8	USW-Flex-XC 2.5...	Switch	Ubiquiti

South City

9 ↓21% Low

Top 3 Riskiest Assets

No Assets available for this trend.

Not enough data in the selected time frame.

Global Leadership Footprint

12K+

Worldwide Installations

105M+

Devices Monitored Across
Converged OT/IoT

6 Continents

Scalable Deployments
Across 6 Continents

Global Expertise

Worldwide Network of Partners
and 1,500+ Certified Professionals



Securing the World's Largest Organizations



9 of Top 20
Oil & Gas



7 of Top 10
Pharma



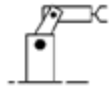
5 of Top 10
Mining



5 of Top 10
Utilities



Chemicals



Manufacturing



Automotive



Airports



Water



Building Automation



Food & Retail



Logistics



Smart Cities



Transportation

OT

OT/IloT

IloT

Nozomi Networks Labs



Through research and collaboration with industry and institutions, we're helping defend the critical assets and systems that support everyday life.



Research Reports



Tools



Projects



Labs Blogs



Threat Advisories



Threat and Asset Intelligence

90%

of the time, vulnerabilities/threats found within 24 hours of installation

Hundreds

of industrial device vulnerabilities responsibly disclosed



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.