NOZOMI NETWORKS

INDUSTRY BRIEF

Transportation: Improving Operational Resilience Through OT and IoT Visibility and Security

Table of Contents

1. Introduction

Improving Operational Resilience Through OT and IoT Visibility and Security

Transportation and logistics organizations are rapidly evolving to improve their service levels and efficiency. At the same time, safety has never been more important, as risks from cyber threats increase. The World Economic Forum cites cyberattacks on critical infrastructure, including transportation, as the world's fifth highest risk in 2020.[1]

Intelligent Transportation Systems (ITS) are becoming more digitized, connected and complex, increasing the need for enhanced network and asset visibility across operational technology (OT), Internet of Things (IoT) and information technology (IT) environments. Fortunately, real-time OT/IoT visibility technology can be used to improve both availability and cyber resilience, helping ensure the safety of transportation systems as they transform.

More and more components used in transportation and logistics systems are digitized and connected. From traffic signaling systems with road sensors and lidar, to tunnel lighting and ventilation systems, to railway power and control systems, the complexity of networks and the number of assets in ITS is rapidly growing.

With this increasing connectivity comes an expanded attack surface with many vulnerabilities.

For example, NotPetya ransomware was used to attack a global shipping and logistics leader. The outcome was anything but incidental: a two-week disruption of operations, a shutdown of the Port of Los Angeles' largest cargo terminal, and a loss of $300 million.[2]

Such incidents have brought OT cybersecurity to the attention of CISOs and managers of both public and private transportation systems. These leaders are under pressure to reduce risk for the entire organization, which involves going beyond enterprise IT systems to include ITS. As a result, initiatives for improving the visibility and cybersecurity of OT/IoT networks are now being embraced.

Given the risk involved, IT experts with a high level of cybersecurity skill are beginning to turn their attention to the challenges of securing ITS. For most IT teams, transportation systems are "black boxes", providing no visibility into their networks, assets and vulnerabilities. And, traditional IT tools and tactics may disrupt OT/IoT devices and networks. Furthermore, most IT pros are not attuned to the safety, environmental and uptime priorities of ITS operators.

THE ROAD TO OPERATIONAL RESILIENCE

Read this paper to learn how a unified ITS network monitoring and threat detection solution makes it easy to

achieve operational availability, visibility and security.

The result is an immediate need for comprehensive ITS security solutions that deliver asset inventory, vulnerability identification, anomaly and intrusion detection, plus fast remediation assistance. Such solutions must integrate with existing IT tools and workflows, yet be safe and provide value to operations teams.

The Nozomi Networks real-time OT and IoT visibility and security solution has been proven to deliver exactly that for major transportation systems around the world.

2. Transportation Resilience Challenges by Sector

2.1 Airports

Airports represent one of the most complex ecosystems[3] that exist in terms of the number of stakeholders, suppliers, service providers and technologies involved. They are also going through remarkable digital transformation, where COVID-19 public health measures are introducing new systems and practices, and siloed systems are becoming interconnected. More and more IoT devices, such as scanners, access control systems and security cameras are being added at a fast rate.

At the same time, airport operators are concerned about the evolving threat landscape. Cybercriminals, using ransomware for financial gain, have been successful in attacking governments such as those that manage many airport facilities. In 2019, The City of New Orleans suffered a cyberattack serious enough for it to declare a state of emergency.[4] Although airport operations were not impacted in this case, airport leadership must factor ransomware, as well as potential hacktivist or nation-state attacks, into cyber risk assessments.

In the past, airports relied extensively on physical security models,[5] but now, increasing connectivity is making cybersecurity an important part of the overall safety and security lens of airport management.

Despite the myriad challenges to improving airport security, it is possible to make significant progress.

CHALLENGES FACED BY AIRPORTS

Airports are under tremendous pressure to strengthen end-to-end security.

Some of the major challenges to improving airport security are multiple stakeholders, siloed legacy systems, too much connectivity and a quickly evolving threat landscape.[3]

One of the first steps is to have visibility to all the OT and IoT systems, networks, and devices in use. Once this is achieved, the use of best practices and real-time anomaly and threat monitoring can greatly improve cybersecurity, safety and operational resilience.

2.2 Bus, Rail and Highways

Bus, rail and highway systems, many of which are government-managed, are considered critical infrastructure, vital to the functioning of societies and economies. If traffic or rail signaling control systems are disrupted, an entire city or region could be thrown into chaos.

Today, many municipalities are re-imagining their mobility systems. They're leveraging technology, sensors, and connectivity to change the way transportation infrastructure is used, and to improve passengers' experience.

The San Diego Association of Governments, for example, is introducing fleets of on-demand, electric vehicles that connect to transit hubs to address first- and last-mile challenges.[6] While such systems solve mobility challenges, they also create an expanded attack surface for cyber threat actors to target.

Addressing the challenge of ITS operational resilience means meeting the needs of two typically siloed groups, IT and OT. IT teams want to identify assets, communications and networks, and then assess vulnerabilities in the system. Once visibility is achieved, they want to monitor for threats and verify that actions are taken to reduce vulnerabilities, whether done internally or by vendors.

OT teams, on the other hand, are more concerned about availability and safety. They need to know when a cyber incident impacts, or has the potential to impact, normal operations. In addition to malicious attacks, such an incident could be unintentional. For example, caused by the misconfiguration of an asset, poorly written software that leads to failing equipment, a degraded wireless link that leads to connectivity issues with field devices, or end-user error.

Early warning of such situations allows operators to act before downtime occurs or safety is threatened.

BRIDGING THE IT/OT DIVIDE

Reducing the cybersecurity blind spots caused by separate IT and OT teams requires leadership and the right tools.

The Nozomi Networks solution is safe for OT, and helps operators improve availability. It also provides the visibility and threat detection required by IT, while integrating with their existing systems and workflows.

Transit authorities around the world are conducting audits that unfortunately demonstrate a lack visibility into their ITS cyber and operational risks. With the added concerns of safety and the need to maintain revenue, it becomes clear why many public and private transit organizations are investing in ITS visibility and security solutions.

2.3 Maritime

The maritime industry transports 90% of the world's trade[7] and like other industries, is becoming increasingly connected, automated and remotely monitored. Shippers want to optimize voyages and monitor things like:

- Load condition of the vessel
- Fuel consumption
- Position and route
- Machinery performance
- System efficiencies

Rapid digitization is creating a path towards Maritime Autonomous Systems (MAS), where new generation ships will be remotely controlled from land.

NON-TARGETED ATTACKS CAN BE COSTLY FOR ASSET OWNERS

A cyberattack doesn't have to target an organization to disrupt operations and be costly to fix.

Email phishing led to Maersk being infected with NotPetya ransomware. Collateral damage included having to rebuild a network of 4,000 servers and 45,000 PCs.[9]

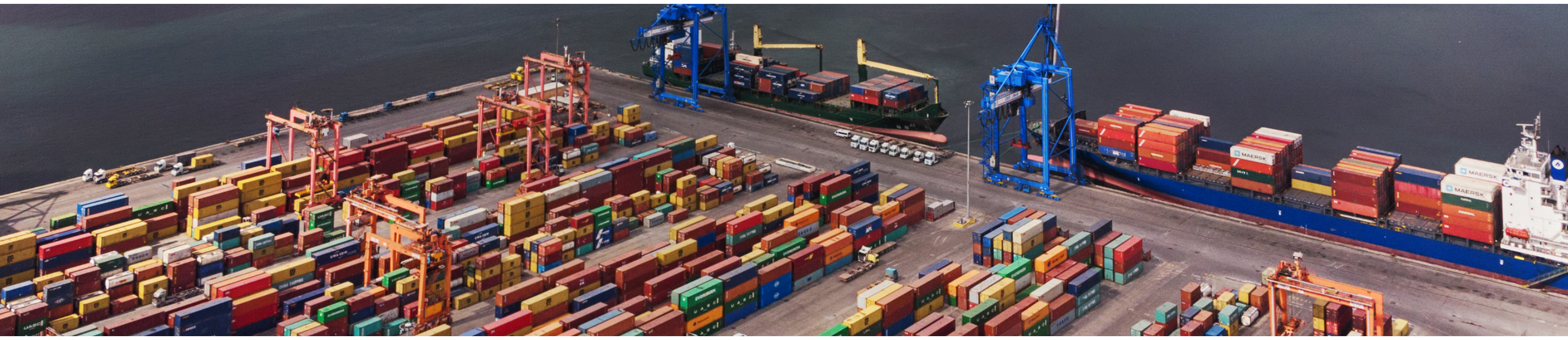
On the other hand, the level of system visibility and cybersecurity maturity in this sector is relatively low. Many ships contain devices and systems that their operators aren't even aware of. Crew are not typically trained to identify phishing emails or manage network access control.

While dramatic situations like a vessel being capsized via hacking are not out of the realm of possibility, they are still unlikely.[8] Crew constantly observe ship behavior and often have the ability to employ manual or safety systems to correct performance that is out of normal range.

Disruptive events that are more likely to occur include:

- Employees or suppliers unintentionally causing cyber incidents that threaten operational reliability or are expensive to remediate
- Cyber criminals disrupting a company's shipping operations or altering documents to facilitate drug smuggling
- Threat actors stopping ship-to-shore functions, such as crane operations, and stopping the flow of goods

Driven by the needs to reduce risk, comply with international shipping standards,[10] and meet insurer requirements, shipping companies are investing in cyber resilience. An important capability lies in identifying maritime assets and their communications. Networks should be monitored for vulnerabilities, threats, and unusual behavior that could indicate a cyberattack.



3. The Nozomi Networks Solution

3.1 How the Nozomi Networks Solution Improves Operational Resilience and Cyber Defense

Nozomi Networks helps transportation asset owners accelerate the pace of digital transformation. Our solution unifies visibility and threat detection across OT, IoT, IT and cyber-physical systems.

We make it possible for organizations to tackle escalating cyber risks to ITS networks while modernizing to succeed in the future.

SECURING GLOBAL TRANSPORTATION LEADERS

Nozomi Networks deployments safeguard the movements of billions of people and packages every year.

Nozomi Networks delivers ITS visibility, threat detection and insight to major transportation systems and thousands of the largest industrial sites around the world. Through the innovative use of artificial intelligence (AI), our solution automates the hard work of inventorying, visualizing and monitoring ITS control networks.

Asset owners benefit from the real-time visibility and threat detection needed to ensure high cyber resilience and reliability.

Following is a short description of our product line, for complete information, visit **our website**.

SAAS

Vantage

Vantage accelerates security response with unmatched threat detection and visibility across your OT, IoT and IT networks. Its scalable SaaS platform enables you to protect any number of assets, anywhere. You can respond faster and more effectively to cyber threats, ensuring operational resilience.

Requires Guardian sensors.

EDGE OR PUBLIC CLOUD

Guardian

Guardian provides industrial strength OT and IoT security and visibility. It combines asset discovery, network visualization, vulnerability assessment, risk monitoring and threat detection in a single application. Guardian shares data with both Vantage and the CMC.

EDGE OR PUBLIC CLOUD

Central Management Console

The Central Management Console (CMC) consolidates OT and IoT risk monitoring and visibility across your distributed sites, at the edge or in the public cloud. It integrates with your IT security infrastructure for streamlined workflows and faster response to threats and anomalies.

SUBSCRIPTION

Threat Intelligence

The Threat Intelligence service delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of emerging threats and new vulnerabilities, and reduce your mean-time-to-detect (MTTD).

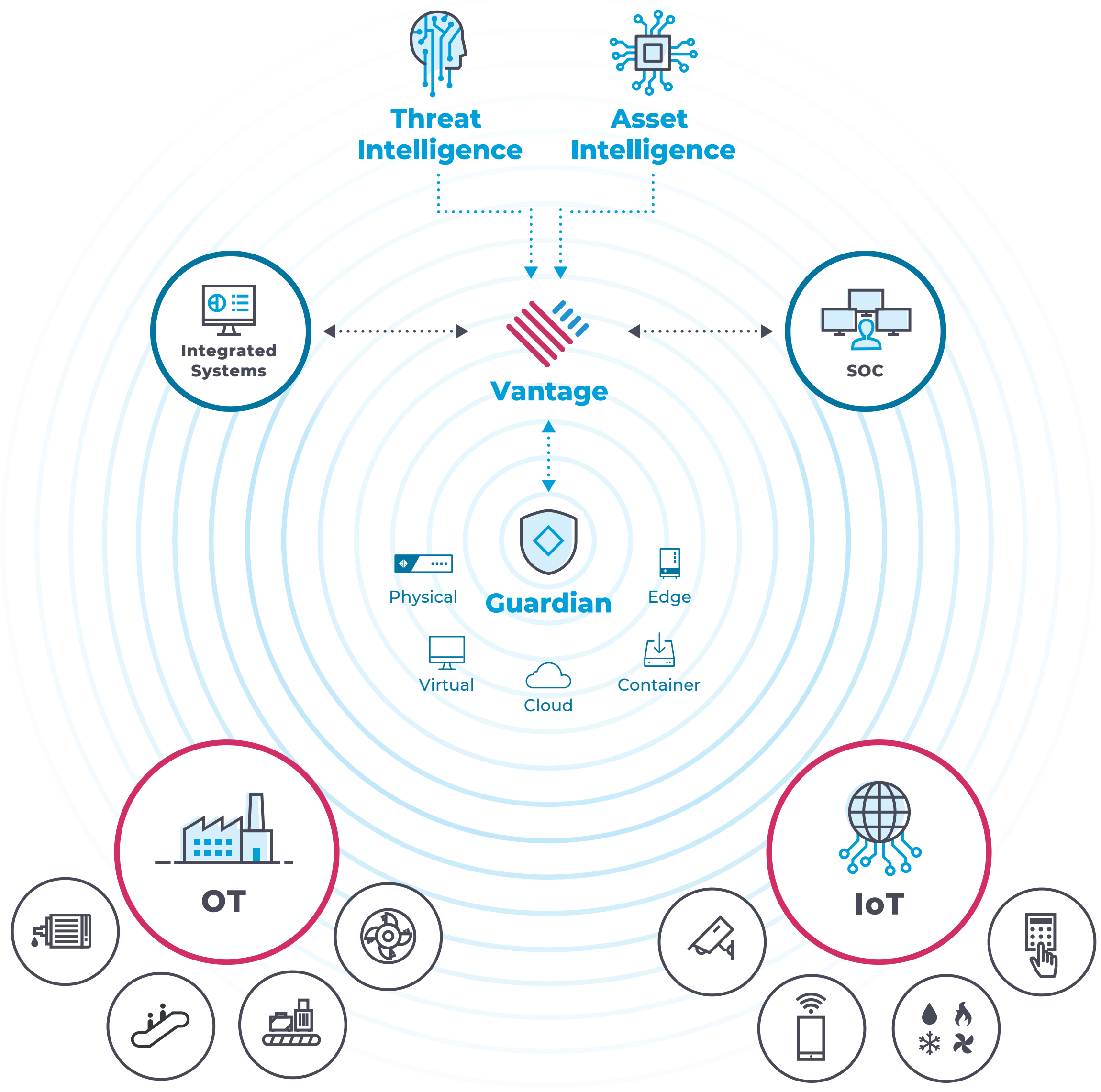
SUBSCRIPTION

Asset Intelligence

The Asset Intelligence service delivers regular profile updates for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-respond (MTTR).

3.2 Diagram: OT and IoT Security and Visibility

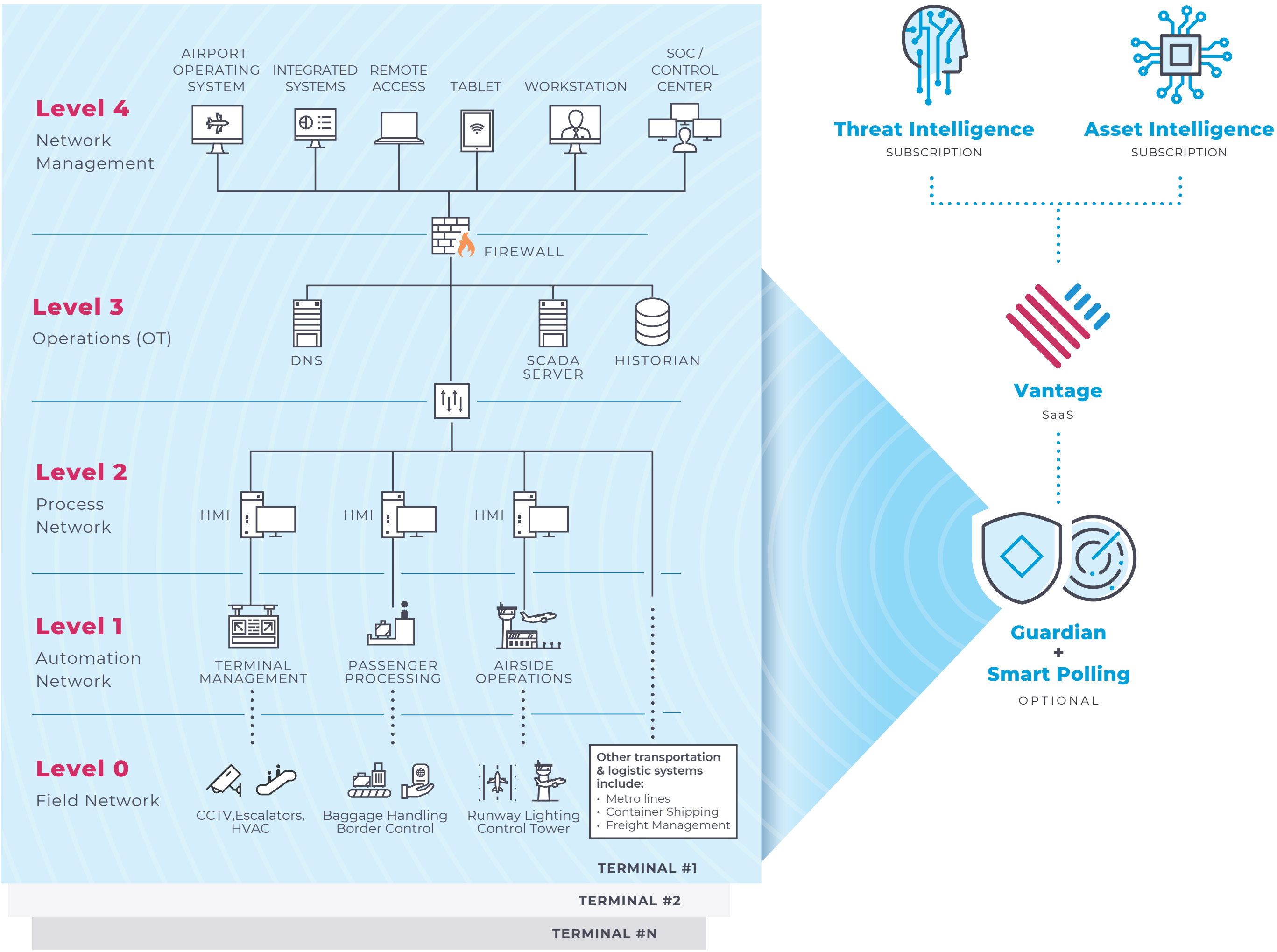
You can protect a wide variety of mixed environments with rapid asset discovery, real-time network visualization and up-to-date threat intelligence.



3.3 Deployment Architecture: Purdue Model Example

You can tailor the Nozomi Networks solution to meet your needs by utilizing its flexible architecture and integrations with other systems.

Additionally, **Remote Collectors™** can be added to Guardian sensors to capture data from remote and offsite locations.



4. Improving Network and Operational Visibility

4.1 Use Case: Gaining Deeper Visibility into Multi-System Operations

Transportation and logistics companies are leveraging automation to improve efficiencies across operational systems – from x-ray and baggage handling machines to environmental controls, ticketing and scheduling systems, and more.

This complex technology environment makes consolidated OT/IoT visibility extremely difficult. It also expands the attack surface, increasing vulnerability to cyber threats.

To keep things running smoothly, operations managers need a simple way to inventory the wide variety of devices in the IT/OT environment, along with deep visibility across all their ITS networks.

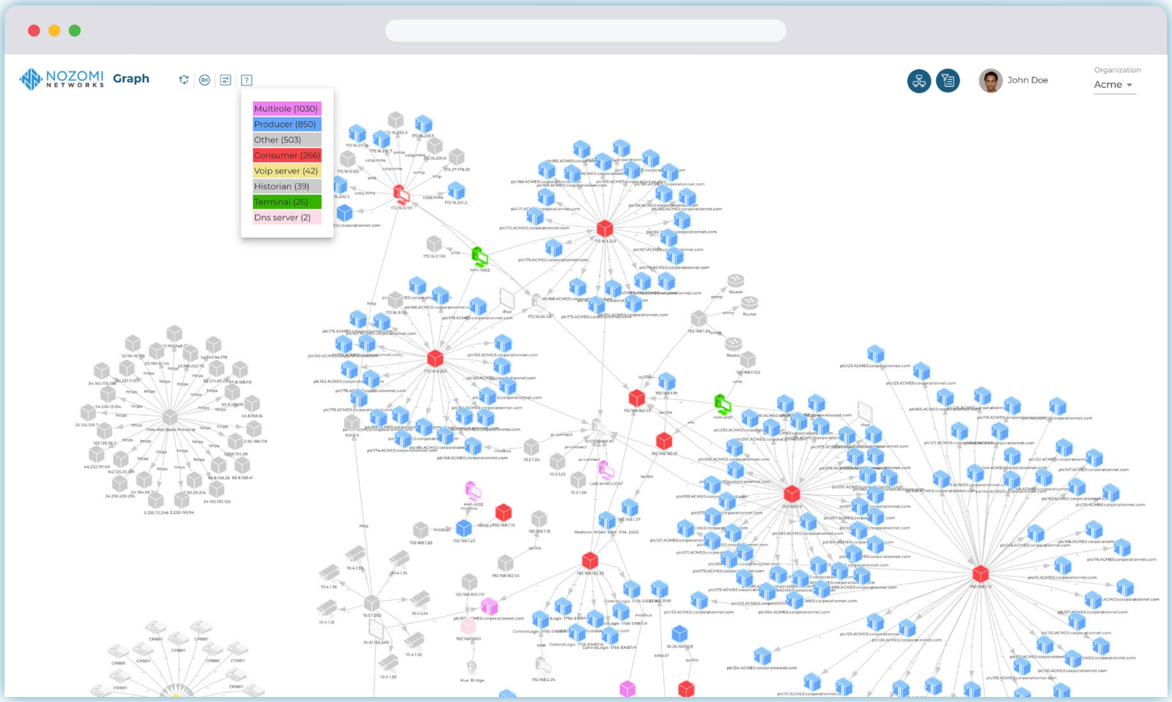
The Nozomi Networks solution easily addresses the complex operational visibility challenges found in airport, metro and other transportation management environments.

As soon as it's deployed, the solution automatically creates an accurate, centralized inventory of ITS assets and keeps it up-to-date. Detailed asset views make it easy to drill down for deeper insight, while automated alerts bring hardware, software and device changes to your attention.

Guardian sensors also analyze network traffic, using the data to build a live, interactive visualization of your operational technology systems. An extensive amount of useful information is provided, including:

- A macro view of the entire ITS environment, with the ability to filter by subnets and network segments
- The role of each node and the traffic between nodes
- The protocols used to communicate between nodes and zones
- Network traffic information such as throughput, protocols and open TCP connections
- Detailed attributes of endpoints and connections

The Nozomi Networks solution delivers consolidated visibility into your OT and IoT assets and networks. The breadth and depth of information often provides insight into previously unknown devices, connections and activity.



Nozomi Networks Solution: Network Graph View

This visualization displays all assets on your network for real-time awareness.

THE CHALLENGE

- Seeing and securing ITS assets and behavior.

THE SOLUTION

Using Automated Asset Inventorying and Real-time Network Visualization to Improve OT System Awareness

- The Nozomi Networks solution provides comprehensive visibility into operational networks and ITS/IoT assets.
- Organizations can efficiently manage and monitor processes, identify risks to reliability, and troubleshoot problems.

RESULTS

Network-wide situational awareness

Comprehensive visibility into ITS networks and systems

Better oversight of vulnerabilities and risks to reliability

Faster troubleshooting of system changes and issues

4.2 Use Case: Preventing Operational Disruption and Downtime

The global economy thrives on the seamless movement of people and goods. Individual cargo ships can transport 8,000 containers on a single voyage.[11] Mass transit systems carry over 53 billion riders each year,[12] while over 8.8 billion passengers flow through airports around the world.[13]

Think about the impact of a system outage or technology glitch on the processing of people and products. Missed connections, delayed baggage, and unsafe environments are just some of the implications.

Unplanned downtime happens for multiple reasons – a device breaks down from operating 24/7, a networking change disturbs an OT system, or a cyber incident halts a critical process. In transportation operations where every minute counts, operators can lose valuable time trying to locate, understand and address issues that arise.

In one case, an airport had a failing PLC that caused a baggage handling system to stop working.

The maintenance team had trouble pinpointing the cause, resulting in an extended outage. Imagine the benefits of proactively identifying potential equipment problems and spotting cyber threats before they disrupt operations.

The Nozomi Networks solution tackles the risk of transportation system downtime by identifying failing equipment using passive network monitoring and anomaly detection.

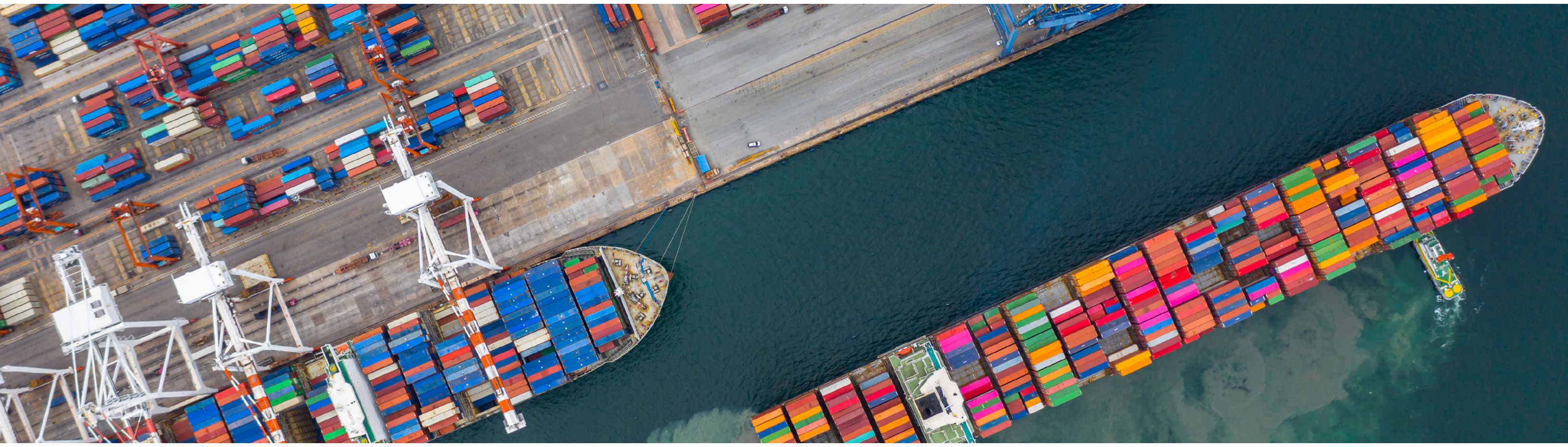
Baselining Variables

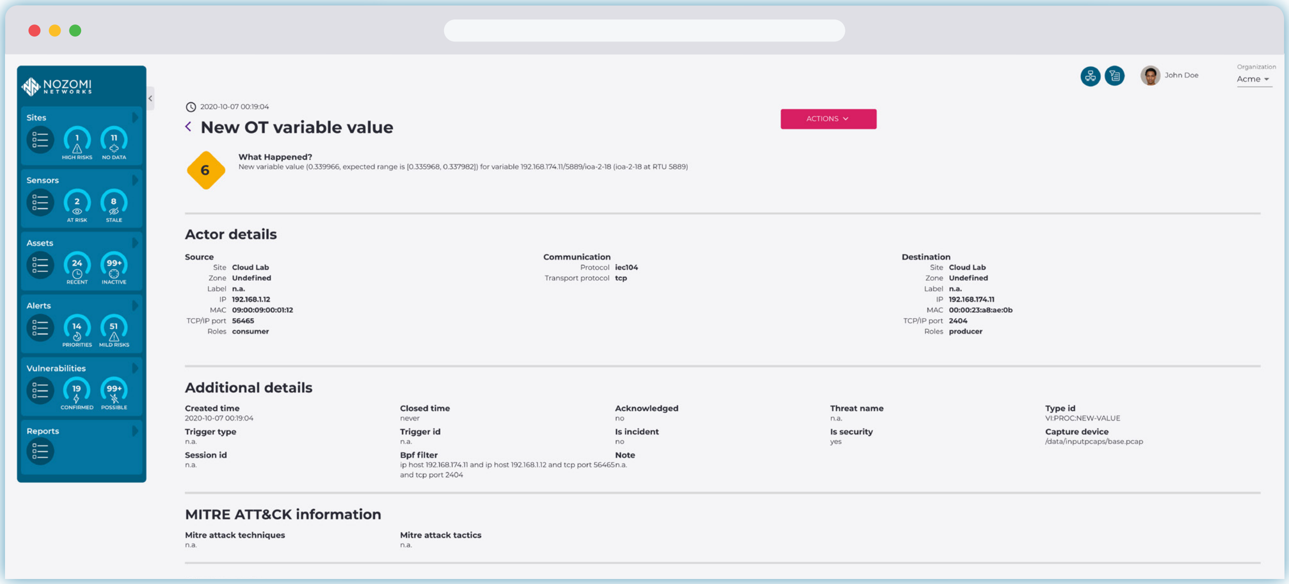
In the initial Dynamic Learning™ phase, the the Nozomi Networks solution uses machine learning and AI to observe your network traffic and create asset and operational baselines. It models behavior and correlates multiple types of data, including information about similar assets within the system, to determine what normal activity looks like.

Detecting Anomalies

In monitoring phase, the solution automatically detects when a specific device or automated operation is deviating from its baseline, and is moving towards a state that could disrupt services. It delivers a simple, consolidated view of what's happening in your multi-vendor, multi-protocol networks, and proactively alerts you that remediation may be necessary.

Anomaly detection, paired with the Nozomi Networks Asset Intelligence subscription, significantly reduces troubleshooting efforts and enables you to act before a device or automated operation fails.





2020-10-07 00:19:04

New OT variable value

6

What Happened?
New variable value (0.339966, expected range is [0.335968, 0.337982]) for variable 192.168.174.11/5889/ioa-2-18 (ioa-2-18 at RTU 5889)

Actor details

Source
Site **Cloud Lab**
Zone **Undefined**
Label **n.a.**
IP **192.168.1.12**
MAC **09:00:09:00:01:12**
TCP/IP port **56465**
Roles **consumer**

Communication
Protocol **iec104**
Transport protocol **tcp**

Destination
Site **Cloud Lab**
Zone **Undefined**
Label **n.a.**
IP **192.168.174.11**
MAC **00:00:23:a8:ae:0b**
TCP/IP port **2404**
Roles **producer**

Additional details

Created time
2020-10-07 00:19:04

Trigger type
n.a.

Session id
n.a.

Closed time
never

Trigger id
n.a.

Bpf filter
ip host 192.168.174.11 and ip host 192.168.1.12 and tcp port 56465 and tcp port 2404

Acknowledged
no

Is incident
no

Note
n.a.

Threat name
n.a.

Is security
yes

Type id
VI:PROC:NEW-VALUE

Capture device
/data/inputpcaps/base.pcap

MITRE ATT&CK information

Mitre attack techniques
n.a.

Mitre attack tactics
n.a.

Nozomi Networks Solution: OT Variable Alert

Unusual device or system behavior could lead to operational disruption and serious safety incidents.

THE CHALLENGE

- Keeping people and products moving.

THE SOLUTION

Using Anomaly Detection to Identify At-Risk Devices and Processes Before They Fail

- The Nozomi Networks solution protects against operational disruption by detecting when a specific device or automated operation is deviating from its baseline and moving towards a state that could disrupt services. It also identifies if vendor work has been completed or not, ensuring that maintenance is done on time.
- Operators leverage a simple, consolidated view of what's happening and receive alerts prompting them to act before a device or automated operation fails.

RESULTS

Continuous network monitoring

Rapid detection of failing equipment or unusual system behavior

Fast and efficient problem identification, response and remediation

Improved operational reliability

5. Detecting Cyber Risks and Improving Cyber Resilience

5.1 Use Case: Understanding Where System Vulnerabilities Lie

Transportation operational environments contain thousands of devices from multiple vendors. For example, assets that track equipment vehicle or rolling stock movement, lighting controls, traffic counters, and so much more.

Unfortunately, most operational devices lack the built-in security required to keep travellers, data and systems safe. Many OT and IoT assets are missing the authentication, encryption, and other security standards that typically apply to IT applications and systems.

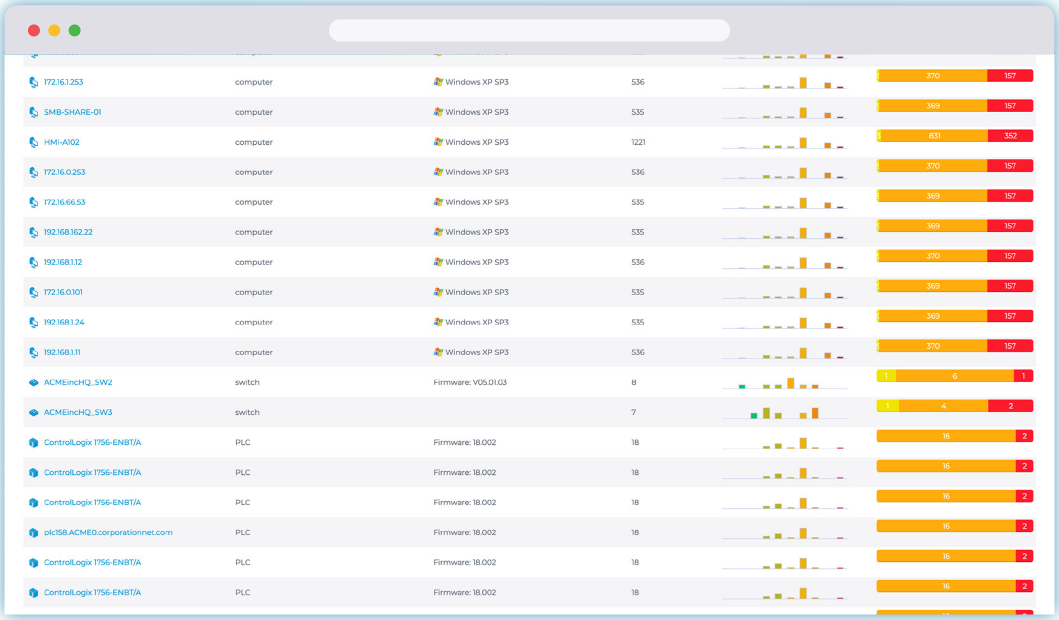
Which leaves you with more questions than answers, such as which devices are vulnerable and in need of better protection? And, which ones require firmware updates or other actions to close the door on cyber risks?

The Nozomi Networks solution addresses this challenge by automatically identifying operational system vulnerabilities. It uncovers weak spots and prioritizes critical exposure points, so you can proactively address them before they are exploited.

The solution helps you answer questions such as:

- Are devices from Vendor X vulnerable?
- How many assets on our network are still running Windows XP?
- Do I need to update certain devices because their firmware is vulnerable?

To help your security team prioritize high-level exposure points, it displays all vulnerabilities by vendor, severity level and more – all in one dedicated view. Plus, it offers drilldown on each vulnerability for deeper troubleshooting and remediation assistance



172.16.1.253	computer	Windows XP SP3	536		370	157
SMB-SHARE-01	computer	Windows XP SP3	535		369	157
HMI-A102	computer	Windows XP SP3	1221		831	352
172.16.0.253	computer	Windows XP SP3	536		370	157
172.16.66.53	computer	Windows XP SP3	535		369	157
192.168.162.22	computer	Windows XP SP3	535		369	157
192.168.1.12	computer	Windows XP SP3	536		370	157
172.16.0.101	computer	Windows XP SP3	535		369	157
192.168.1.24	computer	Windows XP SP3	535		369	157
192.168.1.11	computer	Windows XP SP3	536		370	157
ACMEincHQ_SW2	switch	Firmware: V05.01.03	8	1	6	1
ACMEincHQ_SW3	switch		7	1	4	2
ControlLogix 1756-ENBT/A	PLC	Firmware: 18.002	18		16	2
ControlLogix 1756-ENBT/A	PLC	Firmware: 18.002	18		16	2
ControlLogix 1756-ENBT/A	PLC	Firmware: 18.002	18		16	2
plc158.ACME0.corporationnet.com	PLC	Firmware: 18.002	18		16	2
ControlLogix 1756-ENBT/A	PLC	Firmware: 18.002	18		16	2
ControlLogix 1756-ENBT/A	PLC	Firmware: 18.002	18		16	2

Nozomi Networks Solution: Vulnerabilities List
Automated vulnerability assessment helps you rapidly identify which vendor's devices are at risk, and focus your remediation efforts on top priorities.

THE CHALLENGE

- Identifying which sensors, controllers, and IoT devices are vulnerable.

THE SOLUTION

Automated Vulnerability Assessment Identifies At-risk Assets

- The Nozomi Networks solution addresses this challenge by automatically determining which devices are at risk. It uses the U.S. government's NVD (National Vulnerability Database) for standardized naming, description, and scoring.
- To help your security team prioritize high level exposure points, the solution displays all vulnerabilities by vendor and severity level. Plus, it offers drilldown on each vulnerability for deeper troubleshooting and remediation assistance.

RESULTS

Automatic detection of vulnerabilities

Real-time situational awareness using vulnerability dashboards, drilldowns and reports

Efficient prioritization and remediation of risks

5.2 Use Case: Detecting Malware Before It Impacts OT/IoT Networks

In 2008 a teenager in Lodz, Poland demonstrated just how vulnerable a rail network can be. He altered a television remote control and took control of the industrial control systems managing light-rail track points in the city. The impact? Four trains derailed and 12 people injured.[14]

Why did the attack pack such a big punch? Because interconnected operational environments common to the transportation industry create an open and expanding threat surface that is highly vulnerable to malicious intrusion.

Many of the OT/IoT devices and communication protocols used in facility management, cargo handling, automated fare controls, CCTV infrastructure and other operational systems lack built-in security. Cyberattacks on these devices have the potential to endanger the safety of millions of passengers transiting through airports and metro systems, and stop the flow of goods around the world. Transportation management control services can also be the entry point for attacks that ultimately target IT networks.

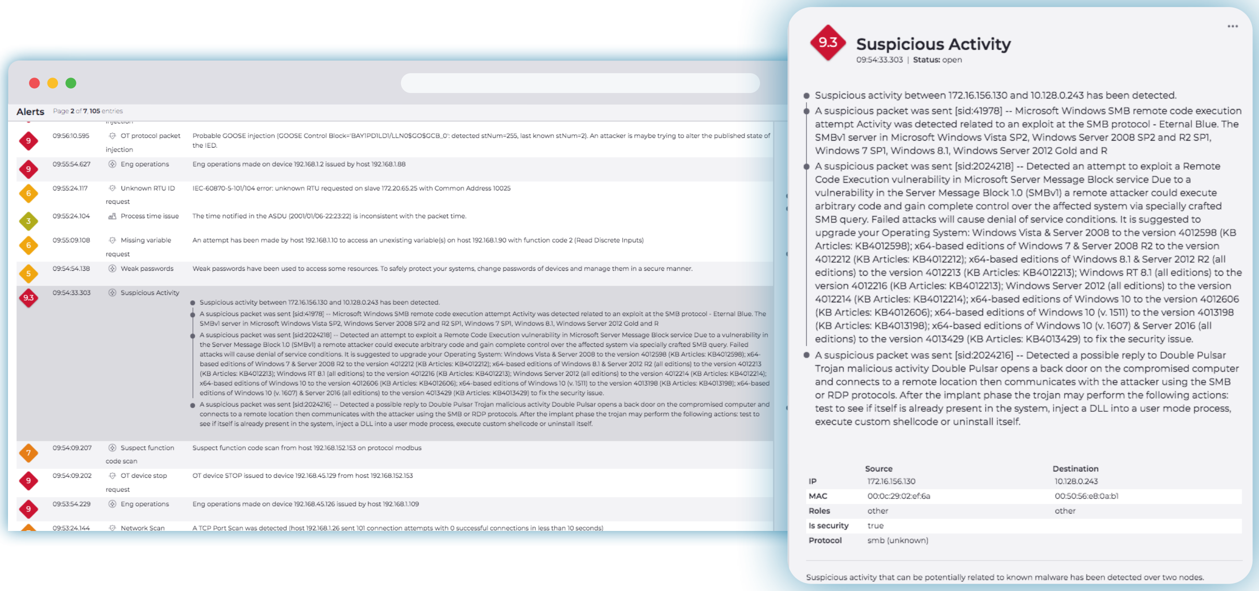
Advanced malware progresses through different phases during an attack. Early identification of the malware is essential to neutralizing it before it migrates between IT and OT network and damage occurs.

The Nozomi Networks solution uses behavior-based anomaly detection and multiple types of signature and rule-based detection to identify malware at each attack phase.

- During early stages, Guardian's anomaly detection flags irregular activity, such as malware that is beaconing out to an external Command and Control server (C&C). Its signatures detect specific content in network traffic related to the presence of the malware.
- During the reconnaissance stage, malware prepares for an attack by triggering a learning process. Here, Nozomi Networks' anomaly detection identifies new commands in the host network. Even if the malware uses standard or proprietary transport control system protocols to communicate, the messages will vary from usual baseline behavior, allowing Guardian to single them out.
- In both early and late stage attacks, Guardian enables transportation operators to implement new firewall rules to block communication or take other actions to stop further attack commands and limit harm.

Built-in integration with tools such as SIEMs and scheduling systems means that IT staff can respond to OT threats cost-effectively with existing tools and workflows.

The Asset Intelligence and Threat Intelligence subscriptions continuously update Guardian sensors, allowing teams to quickly detect and respond to cyber threats and anomalies before they can succeed.



Alerts Page 2 of 7, 105 entries

9	09:56:10.595	OT protocol packet injection	Probable GOOSE injection (GOOSE Control Block='BAY1PD1LD1/LLN0$GO$GCB_0': detected stNum=255, last known stNum=2). An attacker is maybe trying to alter the published state of the IED.
9	09:55:54.627	Eng operations	Eng operations made on device 192.168.1.2 issued by host 192.168.1.88
6	09:55:24.117	Unknown RTU ID request	IEC-60870-5-101/104 error: unknown RTU requested on slave 172.20.65.25 with Common Address 10025
3	09:55:24.104	Process time issue	The time notified in the ASDU (2001/01/06-22:23:22) is inconsistent with the packet time.
6	09:55:09.108	Missing variable request	An attempt has been made by host 192.168.1.10 to access an unexisting variable(s) on host 192.168.1.90 with function code 2 (Read Discrete Inputs)
5	09:54:54.138	Weak passwords	Weak passwords have been used to access some resources. To safely protect your systems, change passwords of devices and manage them in a secure manner.
9.3	09:54:33.303	Suspicious Activity	● Suspicious activity between 172.16.156.130 and 10.128.0.243 has been detected. ● A suspicious packet was sent [sid:41978] -- Microsoft Windows SMB remote code execution attempt Activity was detected related to an exploit at the SMB protocol - Eternal Blue. The SMBv1 server in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R ● A suspicious packet was sent [sid:2024218] -- Detected an attempt to exploit a Remote Code Execution vulnerability in Microsoft Server Message Block service Due to a vulnerability in the Server Message Block 1.0 (SMBv1) a remote attacker could execute arbitrary code and gain complete control over the affected system via specially crafted SMB query. Failed attacks will cause denial of service conditions. It is suggested to upgrade your Operating System: Windows Vista & Server 2008 to the version 4012598 (KB Articles: KB4012598); x64-based editions of Windows 7 & Server 2008 R2 to the version 4012212 (KB Articles: KB4012212); x64-based editions of Windows 8.1 & Server 2012 R2 (all editions) to the version 4012213 (KB Articles: KB4012213); Windows RT 8.1 (all editions) to the version 4012216 (KB Articles: KB4012213); Windows Server 2012 (all editions) to the version 4012214 (KB Articles: KB4012214); x64-based editions of Windows 10 to the version 4012606 (KB Articles: KB4012606); x64-based editions of Windows 10 (v. 1511) to the version 4013198 (KB Articles: KB4013198); x64-based editions of Windows 10 (v. 1607) & Server 2016 (all editions) to the version 4013429 (KB Articles: KB4013429) to fix the security issue. ● A suspicious packet was sent [sid:2024216] -- Detected a possible reply to Double Pulsar Trojan malicious activity Double Pulsar opens a back door on the compromised computer and connects to a remote location then communicates with the attacker using the SMB or RDP protocols. After the implant phase the trojan may perform the following actions: test to see if itself is already present in the system, inject a DLL into a user mode process, execute custom shellcode or uninstall itself.
7	09:54:09.207	Suspect function code scan	Suspect function code scan from host 192.168.152.153 on protocol modbus
9	09:54:09.202	OT device stop request	OT device STOP issued to device 192.168.45.129 from host 192.168.152.153
9	09:53:54.229	Eng operations	Eng operations made on device 192.168.45.126 issued by host 192.168.1.109
	09:53:24.144	Network Scan	A TCP Port Scan was detected (host 192.168.1.26 sent 101 connection attempts with 0 successful connections in less than 10 seconds)

9.3 **Suspicious Activity**

09:54:33.303 | **Status:** open

- Suspicious activity between 172.16.156.130 and 10.128.0.243 has been detected.
- A suspicious packet was sent [sid:41978] -- Microsoft Windows SMB remote code execution attempt Activity was detected related to an exploit at the SMB protocol - Eternal Blue. The SMBv1 server in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R
- A suspicious packet was sent [sid:2024218] -- Detected an attempt to exploit a Remote Code Execution vulnerability in Microsoft Server Message Block service Due to a vulnerability in the Server Message Block 1.0 (SMBv1) a remote attacker could execute arbitrary code and gain complete control over the affected system via specially crafted SMB query. Failed attacks will cause denial of service conditions. It is suggested to upgrade your Operating System: Windows Vista & Server 2008 to the version 4012598 (KB Articles: KB4012598); x64-based editions of Windows 7 & Server 2008 R2 to the version 4012212 (KB Articles: KB4012212); x64-based editions of Windows 8.1 & Server 2012 R2 (all editions) to the version 4012213 (KB Articles: KB4012213); Windows RT 8.1 (all editions) to the version 4012216 (KB Articles: KB4012213); Windows Server 2012 (all editions) to the version 4012214 (KB Articles: KB4012214); x64-based editions of Windows 10 to the version 4012606 (KB Articles: KB4012606); x64-based editions of Windows 10 (v. 1511) to the version 4013198 (KB Articles: KB4013198); x64-based editions of Windows 10 (v. 1607) & Server 2016 (all editions) to the version 4013429 (KB Articles: KB4013429) to fix the security issue.
- A suspicious packet was sent [sid:2024216] -- Detected a possible reply to Double Pulsar Trojan malicious activity Double Pulsar opens a back door on the compromised computer and connects to a remote location then communicates with the attacker using the SMB or RDP protocols. After the implant phase the trojan may perform the following actions: test to see if itself is already present in the system, inject a DLL into a user mode process, execute custom shellcode or uninstall itself.

	Source	Destination
IP	172.16.156.130	10.128.0.243
MAC	00:0c:29:02:ef:6a	00:50:56:e8:0a:b1
Roles	other	other
Is security	true	
Protocol	smb (unknown)	

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

Nozomi Networks Solution: Alerts List

The Nozomi Networks solution alerts security teams to early stage reconnaissance and compromise activities, and provides the information needed to respond before damage occurs. The Threat Intelligence service delivers up-to-date threat and vulnerability information to stay on top of the dynamic threat landscape and reduce mean-time-to-detection (MTTD).

THE CHALLENGE

- Detecting malware operating within ITS operational networks.

THE SOLUTION

Continuous, Automated Monitoring of OT and IoT Networks to Identify Threats

- The Nozomi Networks solution takes a multi-dimensional approach to identifying suspicious activity – whether it's external or internal, accidental or intentional.
- All threat detection results are correlated with operational context for detailed insight. For example, the solution checks baselines for network peculiarities such as VPN access and IP ranges assigned to known asset vendors. If activity occurs outside normal ranges, an alert is triggered.

RESULTS

Fast threat and anomaly detection

Proactive identification of unauthorized activity

Accelerated incident response by security staff

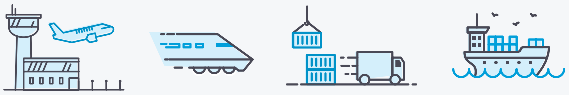
Rapid threat containment and remediation

6. Conclusion

Deep Visibility into Transportation ITS Networks Builds Operational Resilience

Transportation system operators are rapidly embracing tools and technology to gain operational efficiencies. However, digitization and high levels of connectivity increase risk and expand the threat surface. This makes it challenging to quickly address operational disruptions and deflect cyber threats.

SECURING GLOBAL TRANSPORTATION LEADERS



The answer lies in OT/IoT visibility and threat detection. Without this, it's difficult to stay on top of what's happening on ITS networks. One small change or networking issue can impact safety, system uptime, revenue and passenger/traveller experience.

Spotting and troubleshooting issues that threaten reliability requires real-time visibility. Unfortunately, many asset owners lack insight into their devices, connections, and communications.

Security gaps related to people, processes, and technology can have a big impact on operational resilience too. For example, the separation of IT and OT, combined with increasingly connected ITS control systems, can lead to blind spots and vulnerabilities. But with the right technology and a focus on best practices, transportation organizations can increase operational resilience.

With the Nozomi Networks solution, visibility and cybersecurity are easy to achieve. The solution delivers ITS visibility by automatically creating an up-to-date inventory of all assets on control networks. It then monitors their behavior for anomalies and alerts operators to changes that could indicate potential problems. The solution also provides advanced vulnerability and threat detection, along with detailed insights that lead to faster prioritization and remediation.

Tailored to meet the unique challenges of transportation asset owners, the Nozomi Networks solution helps security and operations teams gain deep visibility into ITS control networks. It significantly helps prevent operational downtime, understand vulnerabilities, detect malware and accelerate incident response.

+

FIND OUT MORE

The world's top companies have chosen our innovative solution for OT and IoT visibility to accelerate digital transformation and reduce cyber risk.

Find out how quickly the Nozomi Networks solution can boost operational resilience for your transportation system.

Contact us at **nozominetworks.com/contact**

7. Customer Reviews

Customers Give Nozomi Networks Top Score

★★★★★

Exceeded Expectations. Deeper Visibility Than Expected.

We place an emphasis that every vendor we engage with understands we are not a set up for a “cookie cutter” type of solution. I honestly expected this to be a problem for most if not all vendors. And I was correct, with Nozomi being the sole exception. Not only has their solution done as advertised, and then some.

Senior Industrial Security Manager ›

Once You Try Nozomi And Its Rich Feature Set You Cannot Imagine Operating Without It!

We put Nozomi head to head against other similar products and the Nozomi platform was able to pick out and properly categorize more L2 devices than any other tool in the market place at the time of test.

Security Analyst ›

Great Solutions For ICS.

The solution still has many features that manage the OT environment, such as inventory and vulnerability analysis capabilities. An extra point for the solution is the communication flow map of the neural network, containing information of great relevance for an incident response.

IT Analyst ›

For more reviews, visit our website.

See All Reviews

What to Look for in an OT and IoT Security and Visibility Solution

Technology advancements, such as those found in the Nozomi Networks solution, can dramatically improve security and reliability.

When choosing a solution, look for the following characteristics:

- ✓ Comprehensive OT and IoT visibility
- ✓ Advanced threat detection
- ✓ Accurate anomaly alerts
- ✓ Proven scalability across thousands of sites
- ✓ Easy IT/OT integration
- ✓ Global partner ecosystem
- ✓ Exceptional customer engagement and support

See the Nozomi Networks Solution in Action

If you would like to see our solution in action, and experience how easy it is to work with Nozomi Networks, please contact us at **nozominetworks.com/contact**

Contact Us

Want to Know More?

NOZOMI NETWORKS

SOLUTION BRIEF

OT and IoT Security and Visibility

SOLUTION BRIEF
Nozomi Networks

DOWNLOAD

NOZOMI NETWORKS

Products Solutions Partners Labs Resources Company Request a Demo

Securing OT & IoT Transportation & Logistics

White Paper

Gain visibility into your automated systems and protect them against disruption and cyberattacks.

Transportation and logistics companies are embracing digital automation as a fast track to operational efficiency. But the complex mix of operational systems makes it challenging to see and secure the entire IT and OT/IoT environment, while adhering to stringent uptime and safety requirements.

See
What's on your network and how it's behaving

Detect
Cyber threats, risks and anomalies for faster response

Unify

WEBPAGE
Transportation

VISIT

NOZOMI NETWORKS

PRODUCT OVERVIEW

Vantage

SaaS-Powered Security and Visibility of OT and IoT Networks

DATA SHEET
Vantage

DOWNLOAD

NOZOMI NETWORKS

DATA SHEET

Threat Intelligence

Detect Emerging OT and IoT Threats and Vulnerabilities

DATA SHEET
Threat Intelligence

DOWNLOAD

8. References

1. **"Global Risks Report,"** World Economic Forum, 2020.
2. **"Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks,"** L.A. Times, 2017.
3. **"Aviation Cybersecurity Understanding the Airport Ecosystem,"** The Cybersecurity Observatory.
4. **"New Orleans Declares State-of-Emergency Following Cyber Attack,"** Forbes, December 14, 2019.
5. **"Cybersecurity in Airports,"** Airport Technology, April 23, 2020.
6. **"Transportation Trends 2020,"** Deloitte Insights, 2020.
7. **"International Maritime Organization,"** Business.un.org.
8. **"Maritime Cybersecurity – Can a Hacker Capsize a Ship?,"** The Unsolicited Response Podcast, 2019.
9. **"Maritime Meets Cyber Security,"** The Maritime Executive, October 16, 2019.
10. **"Maritime Cyber Risk,"** International Maritime Organization.
11. **"Benefits of Liner Shipping: Efficiency,"** World Shipping Council, 2019.
12. **"The Global Mass Transit Revolution,"** Bloomberg CityLabs, 2018.
13. **"This is the world's busiest airport,"** CNN, 2019.
14. **"Securing the Railroads from Cyberattacks,"** Mass Transit Magazine, 2019.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

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.

nozominetworks.com