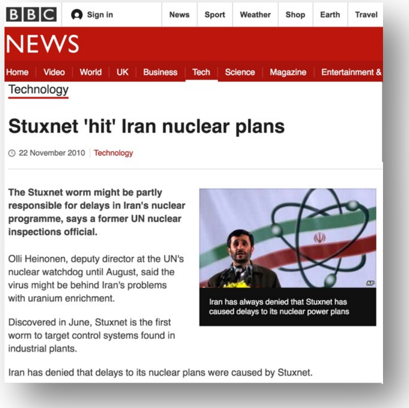
Closing blind spots & security gaps in your critical infrastructure and production networks

Klaus Eberhardt
Nozomi Networks
klaus.eberhardt@nozominetworks.com



BBC Sign in News Sport Weather Shop Earth Travel

NEWS

Home Video World UK Business Tech Science Magazine Entertainment &

Technology

Stuxnet 'hit' Iran nuclear plans

22 November 2010 | Technology

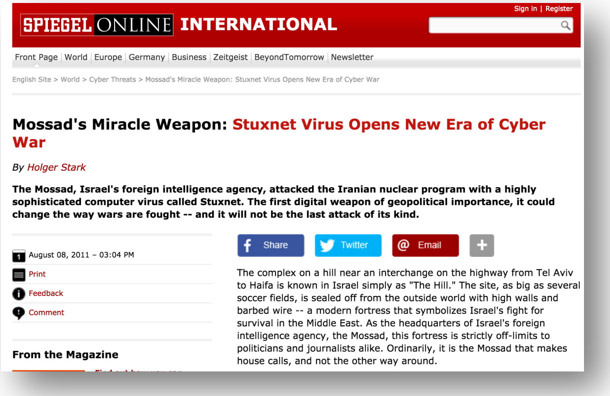
The Stuxnet worm might be partly responsible for delays in Iran's nuclear programme, says a former UN nuclear inspections official.

Iran has always denied that Stuxnet has caused delays to its nuclear power plans

Olli Heinonen, deputy director at the UN's nuclear watchdog until August, said the virus might be behind Iran's problems with uranium enrichment.

Discovered in June, Stuxnet is the first worm to target control systems found in industrial plants.

Iran has denied that delays to its nuclear plans were caused by Stuxnet.



SPIEGEL ONLINE INTERNATIONAL Sign in | Register

Front Page | World | Europe | Germany | Business | Zeitgeist | BeyondTomorrow | Newsletter

English Site > World > Cyber Threats > Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War

Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War

By Holger Stark

The Mossad, Israel's foreign intelligence agency, attacked the Iranian nuclear program with a highly sophisticated computer virus called Stuxnet. The first digital weapon of geopolitical importance, it could change the way wars are fought -- and it will not be the last attack of its kind.

August 08, 2011 – 03:04 PM

Print

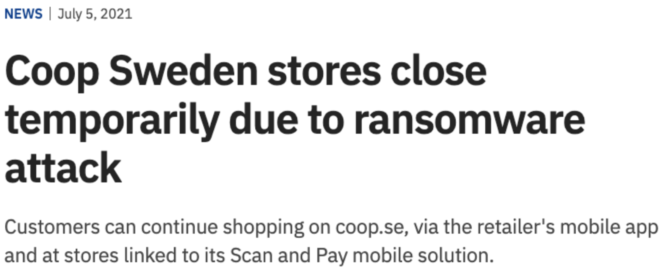
Feedback

Comment

From the Magazine

Share Twitter Email +

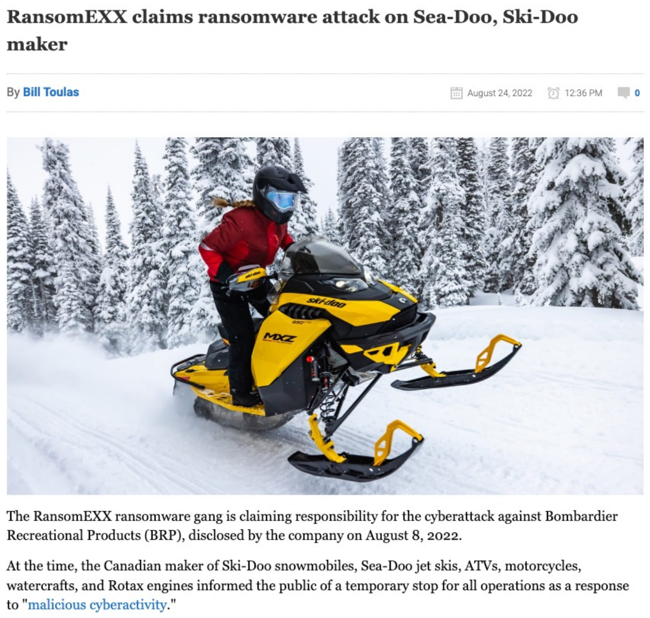
The complex on a hill near an interchange on the highway from Tel Aviv to Haifa is known in Israel simply as "The Hill." The site, as big as several soccer fields, is sealed off from the outside world with high walls and barbed wire -- a modern fortress that symbolizes Israel's fight for survival in the Middle East. As the headquarters of Israel's foreign intelligence agency, the Mossad, this fortress is strictly off-limits to politicians and journalists alike. Ordinarily, it is the Mossad that makes house calls, and not the other way around.



NEWS | July 5, 2021

Coop Sweden stores close temporarily due to ransomware attack

Customers can continue shopping on coop.se, via the retailer's mobile app and at stores linked to its Scan and Pay mobile solution.



RansomEXX claims ransomware attack on Sea-Doo, Ski-Doo maker

By Bill Toulas August 24, 2022 12:36 PM 0

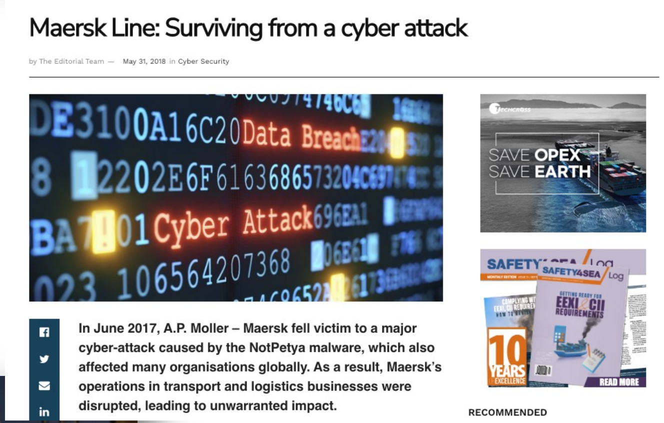
The RansomEXX ransomware gang is claiming responsibility for the cyberattack against Bombardier Recreational Products (BRP), disclosed by the company on August 8, 2022.

At the time, the Canadian maker of Ski-Doo snowmobiles, Sea-Doo jet skis, ATVs, motorcycles, watercrafts, and Rotax engines informed the public of a temporary stop for all operations as a response to "malicious cyberactivity."

Industroyer: A cyber-weapon that brought down a power grid

by André Lameiras • June 20, 2022

Five years ago, ESET researchers released their analysis of the first ever malware that was designed specifically to attack power grids

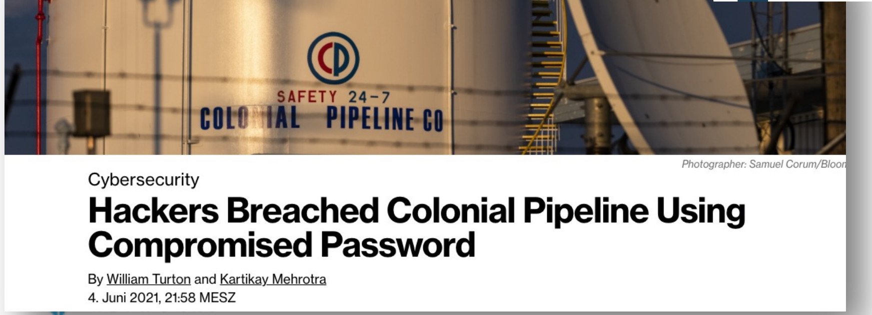


Maersk Line: Surviving from a cyber attack

by The Editorial Team — May 31, 2018 in Cyber Security

In June 2017, A.P. Moller – Maersk fell victim to a major cyber-attack caused by the NotPetya malware, which also affected many organisations globally. As a result, Maersk's operations in transport and logistics businesses were disrupted, leading to unwarranted impact.

RECOMMENDED



Photographer: Samuel Corum/Bloom

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

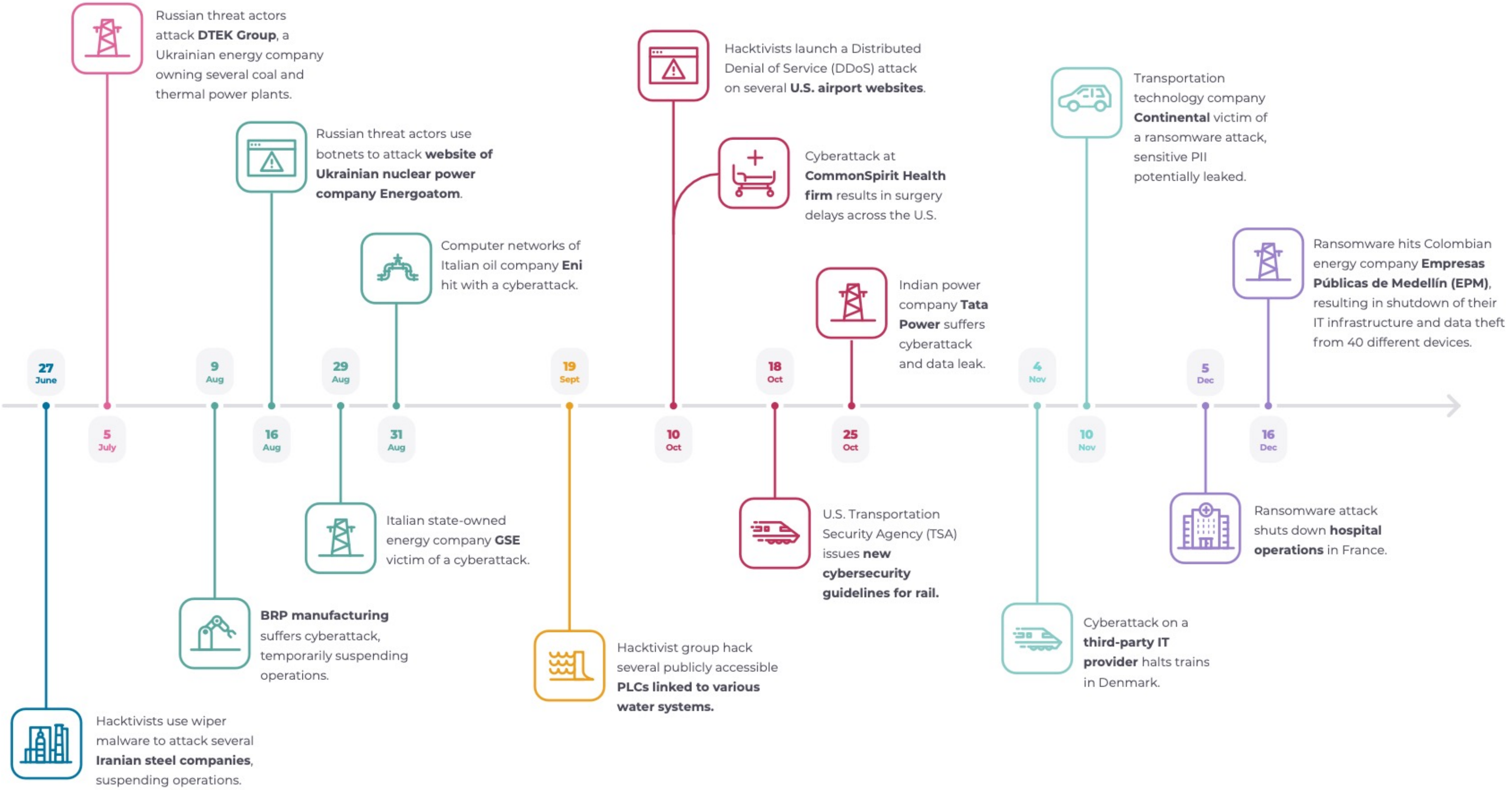
By William Turton and Kartikay Mehrotra
4. Juni 2021, 21:58 MESZ

July 22, 2022 02:53 AM

Eberspaecher reveals details of cyberattack that likely cost up to $60M

The supplier, which produces exhaust technology, air conditioning and heating systems, shut down networks and servers when cyber criminals used ransomware to gain access to its IT systems.

Notable cyber events in the second half of 2022



27 June

Hacktivists use wiper malware to attack several **Iranian steel companies**, suspending operations.

5 July

Russian threat actors attack **DTEK Group**, a Ukrainian energy company owning several coal and thermal power plants.

9 Aug

BRP manufacturing suffers cyberattack, temporarily suspending operations.

16 Aug

Russian threat actors use botnets to attack **website of Ukrainian nuclear power company Energoatom**.

29 Aug

Italian state-owned energy company **GSE** victim of a cyberattack.

31 Aug

Computer networks of Italian oil company **Eni** hit with a cyberattack.

19 Sept

Hacktivist group hack several publicly accessible **PLCs linked to various water systems.**

10 Oct

Hacktivists launch a Distributed Denial of Service (DDoS) attack on several **U.S. airport websites**.

Cyberattack at **CommonSpirit Health firm** results in surgery delays across the U.S.

18 Oct

U.S. Transportation Security Agency (TSA) issues **new cybersecurity guidelines for rail.**

25 Oct

Indian power company **Tata Power** suffers cyberattack and data leak.

4 Nov

Cyberattack on a **third-party IT provider** halts trains in Denmark.

10 Nov

Transportation technology company **Continental** victim of a ransomware attack, sensitive PII potentially leaked.

5 Dec

Ransomware attack shuts down **hospital operations** in France.

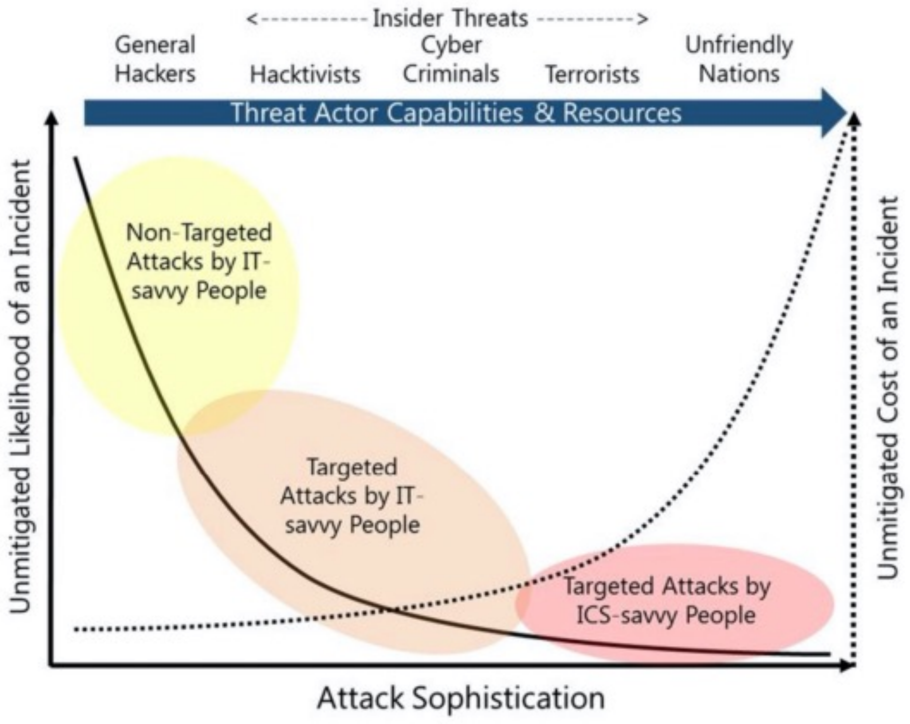
16 Dec

Ransomware hits Colombian energy company **Empresas Públicas de Medellín (EPM)**, resulting in shutdown of their IT infrastructure and data theft from 40 different devices.

Multiple threat actors/sources

- Adversarial
  - Outside Individual
  - Inside Individual
  - Trusted Insider
  - Privileged insider
  - Ad hoc group
  - Established group
  - Competitor
  - Supplier
  - Partner
  - Customer
  - Nation State
- Accidental
  - User/Privileged user/Administrator

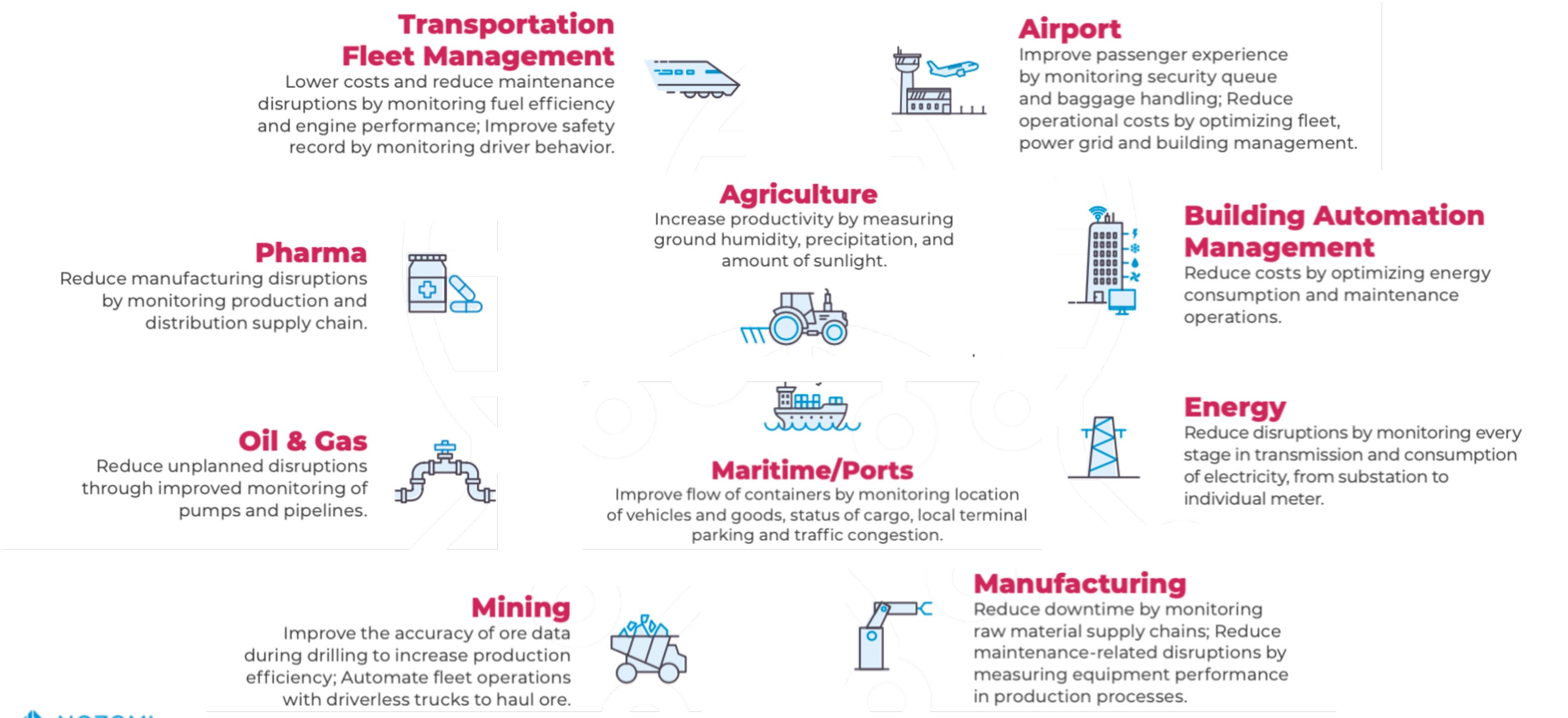
- Structural
  - IT equipment
  - Environmental controls
  - Software
- Environmental
  - Natural disaster
  - Man-made disaster
  - Infrastructure failure (e.g. telecommunications, electrical power)



Industrial Cyber Threats Vary in Sophistication

Source: https://www.arcweb.com/industry-best-practices/what-industrial-cybersecurity-planning-maturity-model

OT Is Everywhere



Transportation Fleet Management

Lower costs and reduce maintenance disruptions by monitoring fuel efficiency and engine performance; Improve safety record by monitoring driver behavior.

Airport

Improve passenger experience by monitoring security queue and baggage handling; Reduce operational costs by optimizing fleet, power grid and building management.

Pharma

Reduce manufacturing disruptions by monitoring production and distribution supply chain.

Agriculture

Increase productivity by measuring ground humidity, precipitation, and amount of sunlight.

Building Automation Management

Reduce costs by optimizing energy consumption and maintenance operations.

Oil & Gas

Reduce unplanned disruptions through improved monitoring of pumps and pipelines.

Maritime/Ports

Improve flow of containers by monitoring location of vehicles and goods, status of cargo, local terminal parking and traffic congestion.

Energy

Reduce disruptions by monitoring every stage in transmission and consumption of electricity, from substation to individual meter.

Mining

Improve the accuracy of ore data during drilling to increase production efficiency; Automate fleet operations with driverless trucks to haul ore.

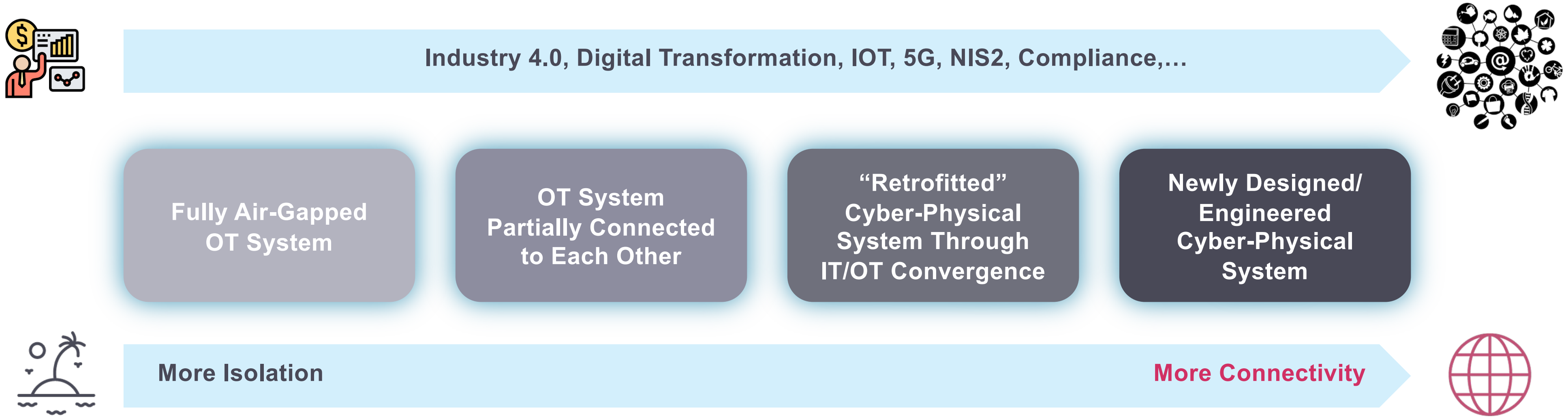
Manufacturing

Reduce downtime by monitoring raw material supply chains; Reduce maintenance-related disruptions by measuring equipment performance in production processes.

IT vs. OT – Commonalities and Differences

IT	OT
Security – Protection from Cyber Threats	Safety – Protection of life and limb
Availability: 99.8%	“No disruption, never down”
Hardware-Lifetime: ~ 5 years	Lifetime of production assets: > 20 years
Regular system patches	Windows XP Systems
Loss of information – TCP is taking over	Realtime protocols
Anti-Virus protection + EDR	Closed systems from Vendors
Encrypted connections	Cleartext protocols
Password-complexity + MFA	Simple access to systems (Safety!)
Active monitoring	Monitoring capabilities limited
Central visibility	“Sneaker-Work”

OT Systems Evolution



Industry 4.0, Digital Transformation, IOT, 5G, NIS2, Compliance,…

Fully Air-Gapped OT System

OT System Partially Connected to Each Other

“Retrofitted” Cyber-Physical System Through IT/OT Convergence

Newly Designed/ Engineered Cyber-Physical System

More Isolation

More Connectivity

Examples of Traditional OT Systems

- Supervisory Control and Data Acquisition (SCADA)
- Industrial Control Systems (ICS)
- Programmable Logic Control (PLC)
- Process Control Networks (PCN) – Including Safety Instrumented Systems (SIS), Engineer Workstation and Human Machine Interface (HMI)
- Distributed Control Systems (DCS)
- Computer Numerical Control (CNC)

Examples of OT-Related Cyber-Physical Systems

- Industrial Robots
- Virtual Reality Manufacturing Simulation Systems
- Self-Optimizing Press-Bending and Roll-Forming Machine
- Adaptable Production Systems
- Energy-Efficient Intralogistics Systems
- Connected 3D Printers
- Smart Grids
- IIoT

Digitalization…not without cybersecurity

14 sec

a ransomware attack occurs

5 min

the average time it takes for an IoT device to be attacked after going online

3.8

Mio USD – average cost of a breach

67%

is the increase in security breaches over last year

70%

of the employees don`t understand cybersecurity

50 days

typically pass between breach discovery and reporting dates

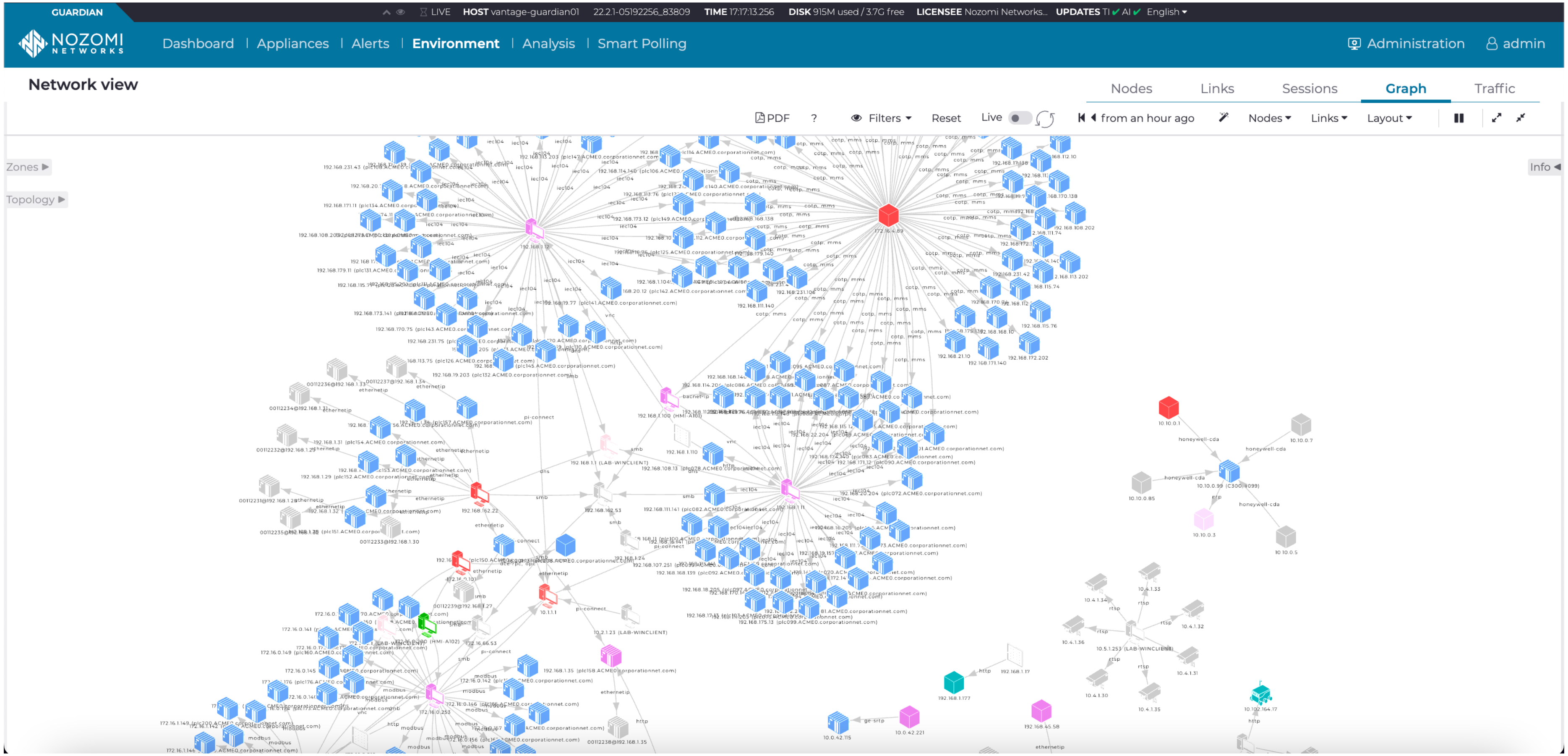
Challenges

- Responsibility
- Speak the same language
- Limited ressources
- Pressure from the Business
    - Digital transformation
    - IOT / 5G
    - Regulatory compliance

We need transparency

- “We can’t protect what we cannot see”
- Setting the baseline
  - How does my landscape look like?
  - Which assets are communicating?
  - How do they communicate?
  - Are there any anomalies in this communication?
  - How is my process configured?

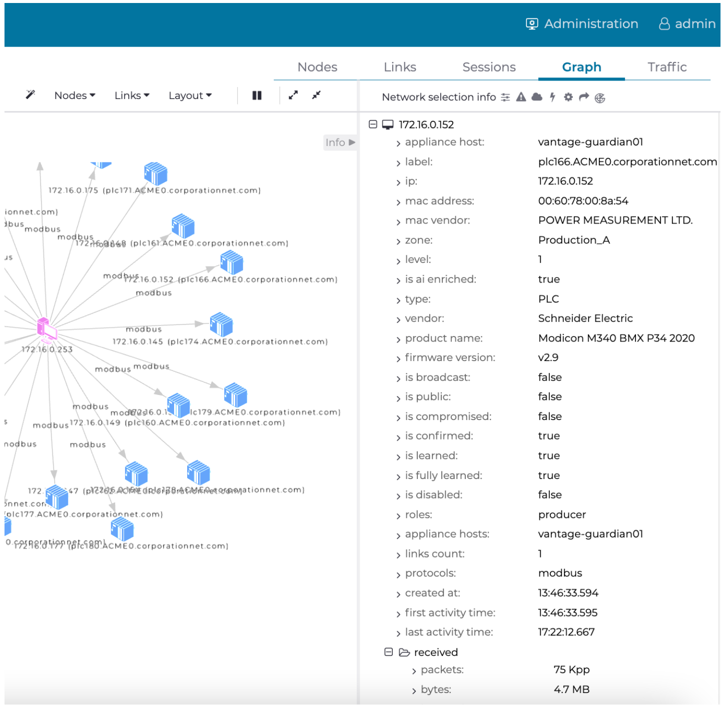
Goal: Network visualization - Transparency!



GUARDIAN LIVE HOST vantage-guardian01 22.2.1-05192256_83809 TIME 17:17:13.256 DISK 915M used / 3.7G free LICENSEE Nozomi Networks... UPDATES TI ✓ AI ✓ English

Pain Point: Network visualization and monitoring

Go deep in details …



Administration
admin
Nodes
Links
Sessions
Graph
Traffic
Nodes ▾
Links ▾
Layout ▾
Info ▶
modbus
172.16.0.175 (plc171.ACME0.corporationnet.com)
172.16.0.152 (plc166.ACME0.corporationnet.com)
172.16.0.145 (plc174.ACME0.corporationnet.com)
172.16.0.149 (plc160.ACME0.corporationnet.com)
172.16.0.253
plc179.ACME0.corporationnet.com
plc161.ACME0.corporationnet.com
plc177.ACME0.corporationnet.com
plc180.ACME0.corporationnet.com

Network selection info

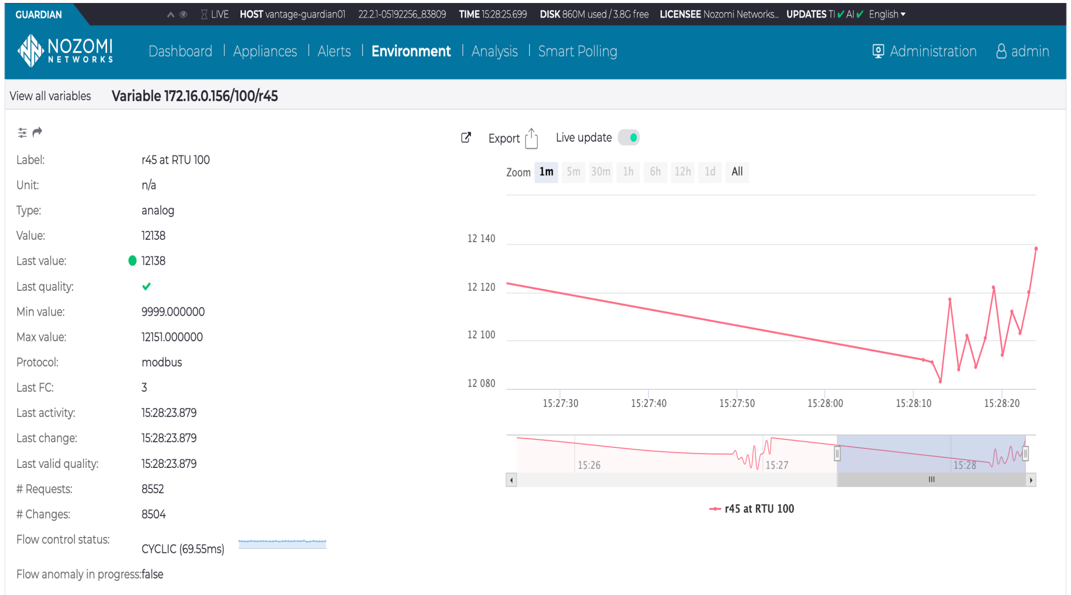
172.16.0.152

appliance host:	vantage-guardian01
label:	plc166.ACME0.corporationnet.com
ip:	172.16.0.152
mac address:	00:60:78:00:8a:54
mac vendor:	POWER MEASUREMENT LTD.
zone:	Production_A
level:	1
is ai enriched:	true
type:	PLC
vendor:	Schneider Electric
product name:	Modicon M340 BMX P34 2020
firmware version:	v2.9
is broadcast:	false
is public:	false
is compromised:	false
is confirmed:	true
is learned:	true
is fully learned:	true
is disabled:	false
roles:	producer
appliance hosts:	vantage-guardian01
links count:	1
protocols:	modbus
created at:	13:46:33.594
first activity time:	13:46:33.595
last activity time:	17:22:12.667

received

packets:	75 Kpp
bytes:	4.7 MB

Nodes

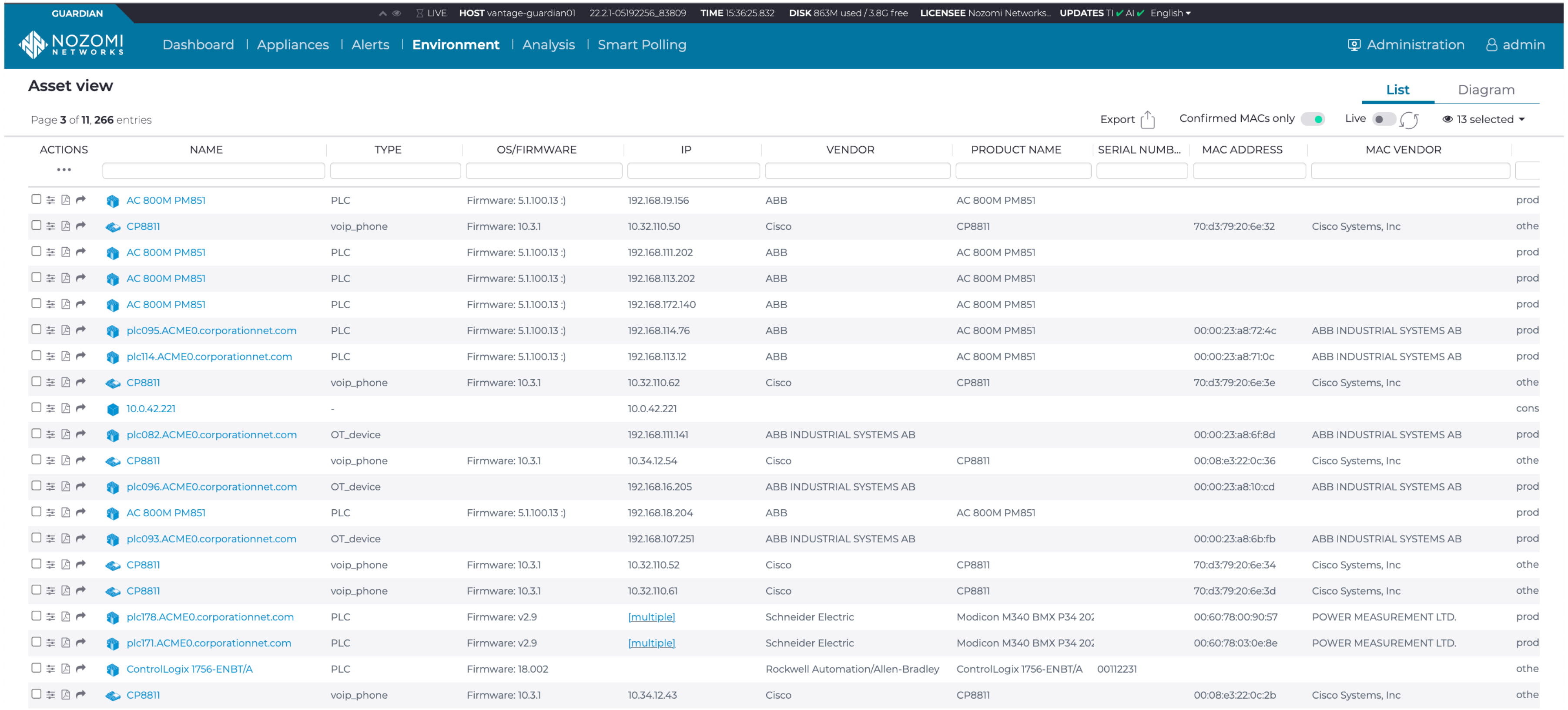


View all variables Variable 172.16.0.156/100/r45

Label:	r45 at RTU 100
Unit:	n/a
Type:	analog
Value:	12138
Last value:	● 12138
Last quality:	✓
Min value:	9999.000000
Max value:	12151.000000
Protocol:	modbus
Last FC:	3
Last activity:	15:28:23.879
Last change:	15:28:23.879
Last valid quality:	15:28:23.879
# Requests:	8552
# Changes:	8504
Flow control status:	CYCLIC (69.55ms)
Flow anomaly in progress:	false

Variables

#1 – Asset Discovery



GUARDIAN LIVE **HOST** vantage-guardian01 22.2.1-05192256_83809 **TIME** 15:36:25.832 **DISK** 863M used / 3.8G free **LICENSEE** Nozomi Networks... **UPDATES** TI ✓ AI ✓ English ▾

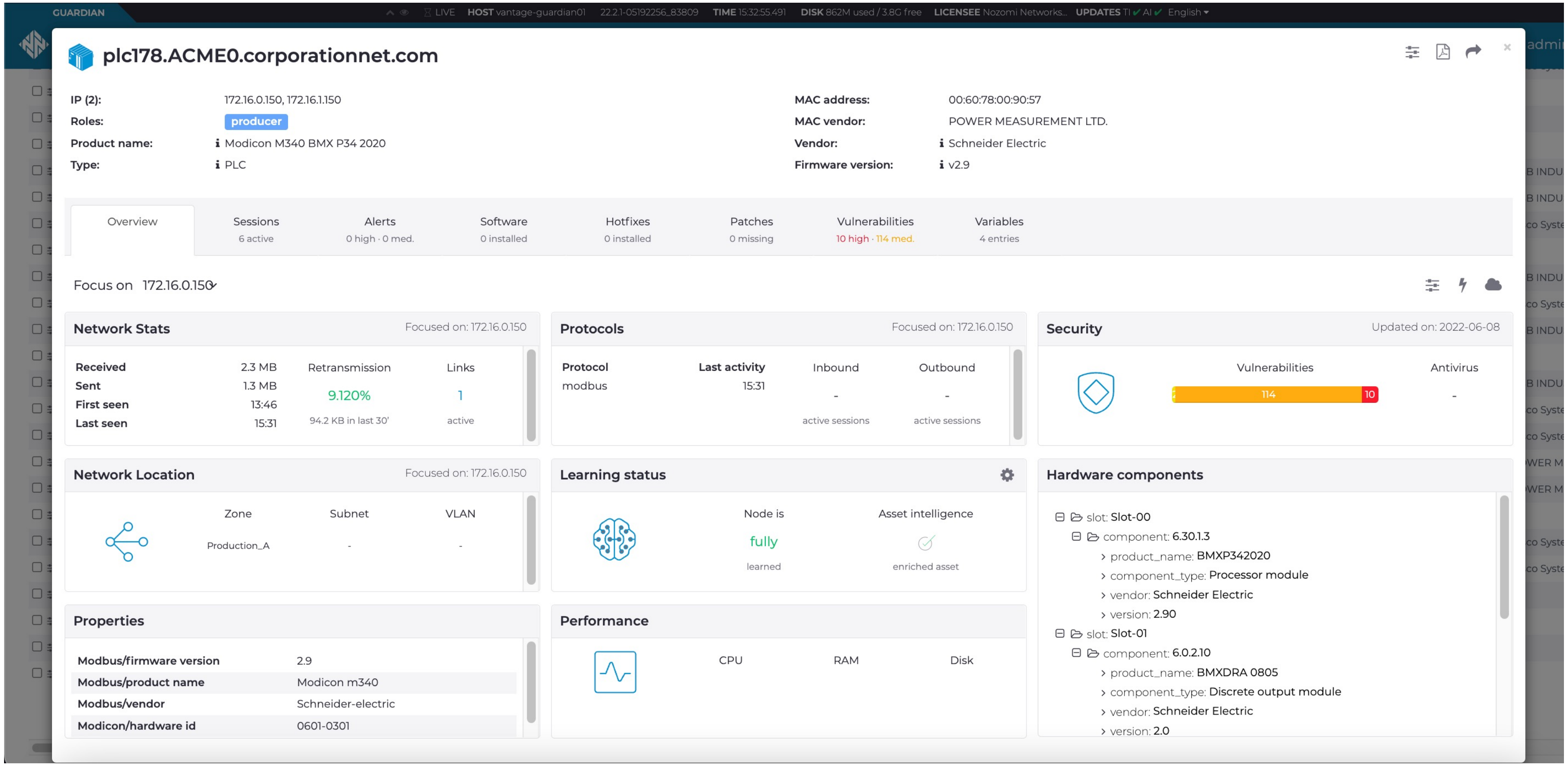
NOZOMI NETWORKS
Dashboard | Appliances | Alerts | **Environment** | Analysis | Smart Polling
Administration
admin

Asset view

Page **3** of **11**, **266** entries

ACTIONS	NAME	TYPE	OS/FIRMWARE	IP	VENDOR	PRODUCT NAME	SERIAL NUMB...	MAC ADDRESS	MAC VENDOR	
•••										
□	AC 800M PM851	PLC	Firmware: 5.1.100.13 :)	192.168.19.156	ABB	AC 800M PM851				prod
□	CP8811	voip_phone	Firmware: 10.3.1	10.32.110.50	Cisco	CP8811		70:d3:79:20:6e:32	Cisco Systems, Inc	othe
□	AC 800M PM851	PLC	Firmware: 5.1.100.13 :)	192.168.111.202	ABB	AC 800M PM851				prod
□	AC 800M PM851	PLC	Firmware: 5.1.100.13 :)	192.168.113.202	ABB	AC 800M PM851				prod
□	AC 800M PM851	PLC	Firmware: 5.1.100.13 :)	192.168.172.140	ABB	AC 800M PM851				prod
□	plc095.ACME0.corporationnet.com	PLC	Firmware: 5.1.100.13 :)	192.168.114.76	ABB	AC 800M PM851		00:00:23:a8:72:4c	ABB INDUSTRIAL SYSTEMS AB	prod
□	plc114.ACME0.corporationnet.com	PLC	Firmware: 5.1.100.13 :)	192.168.113.12	ABB	AC 800M PM851		00:00:23:a8:71:0c	ABB INDUSTRIAL SYSTEMS AB	prod
□	CP8811	voip_phone	Firmware: 10.3.1	10.32.110.62	Cisco	CP8811		70:d3:79:20:6e:3e	Cisco Systems, Inc	othe
□	10.0.42.221	-		10.0.42.221						cons
□	plc082.ACME0.corporationnet.com	OT_device		192.168.111.141	ABB INDUSTRIAL SYSTEMS AB			00:00:23:a8:6f:8d	ABB INDUSTRIAL SYSTEMS AB	prod
□	CP8811	voip_phone	Firmware: 10.3.1	10.34.12.54	Cisco	CP8811		00:08:e3:22:0c:36	Cisco Systems, Inc	othe
□	plc096.ACME0.corporationnet.com	OT_device		192.168.16.205	ABB INDUSTRIAL SYSTEMS AB			00:00:23:a8:10:cd	ABB INDUSTRIAL SYSTEMS AB	prod
□	AC 800M PM851	PLC	Firmware: 5.1.100.13 :)	192.168.18.204	ABB	AC 800M PM851				prod
□	plc093.ACME0.corporationnet.com	OT_device		192.168.107.251	ABB INDUSTRIAL SYSTEMS AB			00:00:23:a8:6b:fb	ABB INDUSTRIAL SYSTEMS AB	prod
□	CP8811	voip_phone	Firmware: 10.3.1	10.32.110.52	Cisco	CP8811		70:d3:79:20:6e:34	Cisco Systems, Inc	othe
□	CP8811	voip_phone	Firmware: 10.3.1	10.32.110.61	Cisco	CP8811		70:d3:79:20:6e:3d	Cisco Systems, Inc	othe
□	plc178.ACME0.corporationnet.com	PLC	Firmware: v2.9	[multiple]	Schneider Electric	Modicon M340 BMX P34 202		00:60:78:00:90:57	POWER MEASUREMENT LTD.	prod
□	plc171.ACME0.corporationnet.com	PLC	Firmware: v2.9	[multiple]	Schneider Electric	Modicon M340 BMX P34 202		00:60:78:03:0e:8e	POWER MEASUREMENT LTD.	prod
□	ControlLogix 1756-ENBT/A	PLC	Firmware: 18.002		Rockwell Automation/Allen-Bradley	ControlLogix 1756-ENBT/A	00112231			othe
□	CP8811	voip_phone	Firmware: 10.3.1	10.34.12.43	Cisco	CP8811		00:08:e3:22:0c:2b	Cisco Systems, Inc	othe

#2 – Asset Details



GUARDIAN LIVE **HOST** vantage-guardian01 22.2.1-05192256_83809 **TIME** 15:32:55.491 **DISK** 862M used / 3.8G free **LICENSEE** Nozomi Networks... **UPDATES** TI ✓ AI ✓ English

plc178.ACME0.corporationnet.com

IP (2):	172.16.0.150, 172.16.1.150	**MAC address:**	00:60:78:00:90:57
Roles:	producer	**MAC vendor:**	POWER MEASUREMENT LTD.
Product name:	ℹ Modicon M340 BMX P34 2020	**Vendor:**	ℹ Schneider Electric
Type:	ℹ PLC	**Firmware version:**	ℹ v2.9

Focus on 172.16.0.150

Network Stats

Focused on: 172.16.0.150

		Retransmission	Links
Received	2.3 MB	9.120%	1
Sent	1.3 MB	94.2 KB in last 30'	active
First seen	13:46		
Last seen	15:31		

Protocols

Focused on: 172.16.0.150

Protocol	**Last activity**	Inbound	Outbound
modbus	15:31	- active sessions	- active sessions

Security

Updated on: 2022-06-08

Vulnerabilities	Antivirus
114 10	-

Network Location

Focused on: 172.16.0.150

Zone	Subnet	VLAN
Production_A	-	-

Learning status

Node is	Asset intelligence
fully learned	enriched asset

Hardware components

- slot: Slot-00
  - component: 6.30.1.3
    - product_name: BMXP342020
    - component_type: Processor module
    - vendor: Schneider Electric
    - version: 2.90
- slot: Slot-01
  - component: 6.0.2.10
    - product_name: BMXDRA 0805
    - component_type: Discrete output module
    - vendor: Schneider Electric
    - version: 2.0

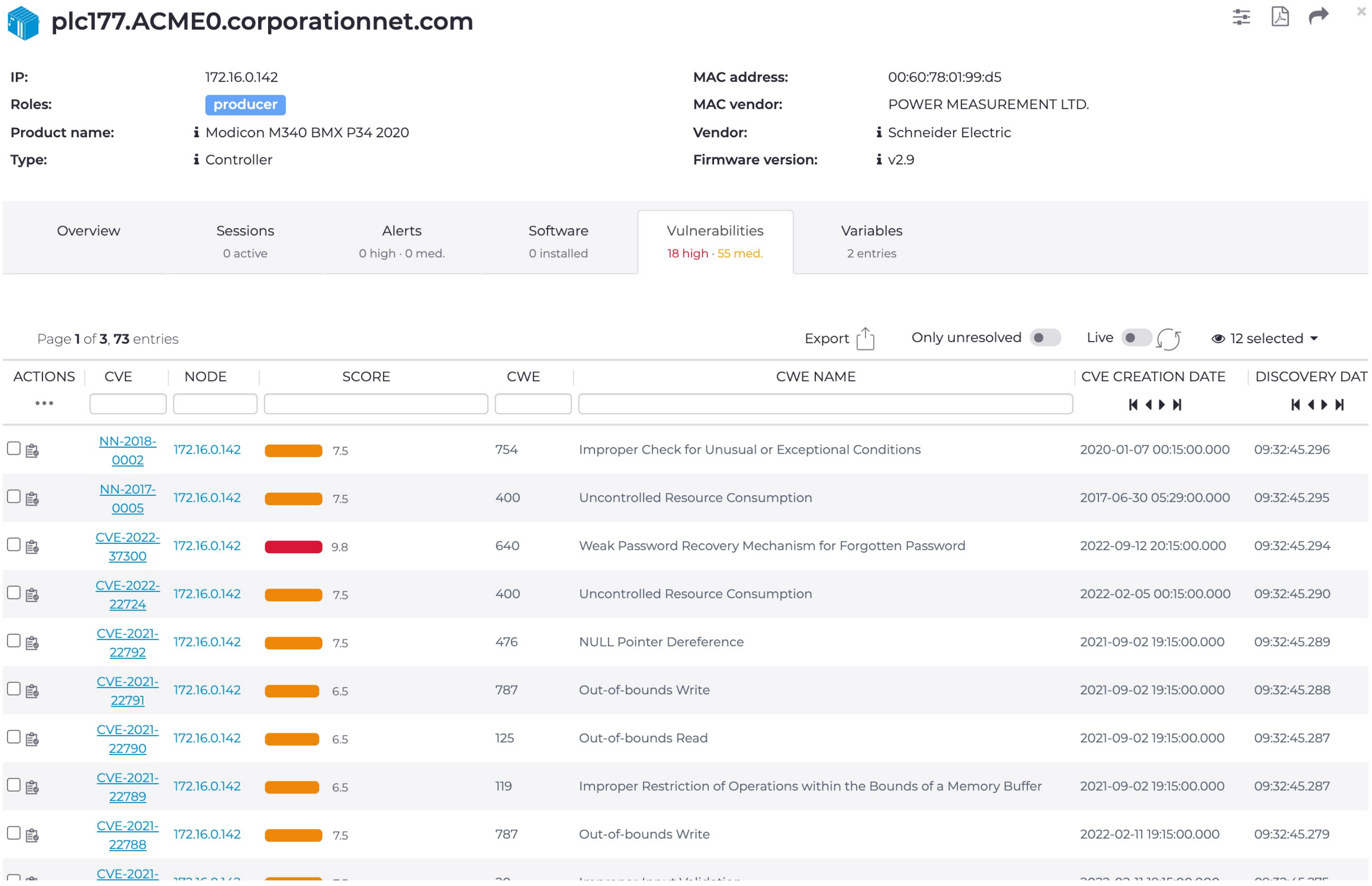
Properties

Modbus/firmware version	2.9
Modbus/product name	Modicon m340
Modbus/vendor	Schneider-electric
Modicon/hardware id	0601-0301

Performance

CPU	RAM	Disk

#3 – Vulnerability Information



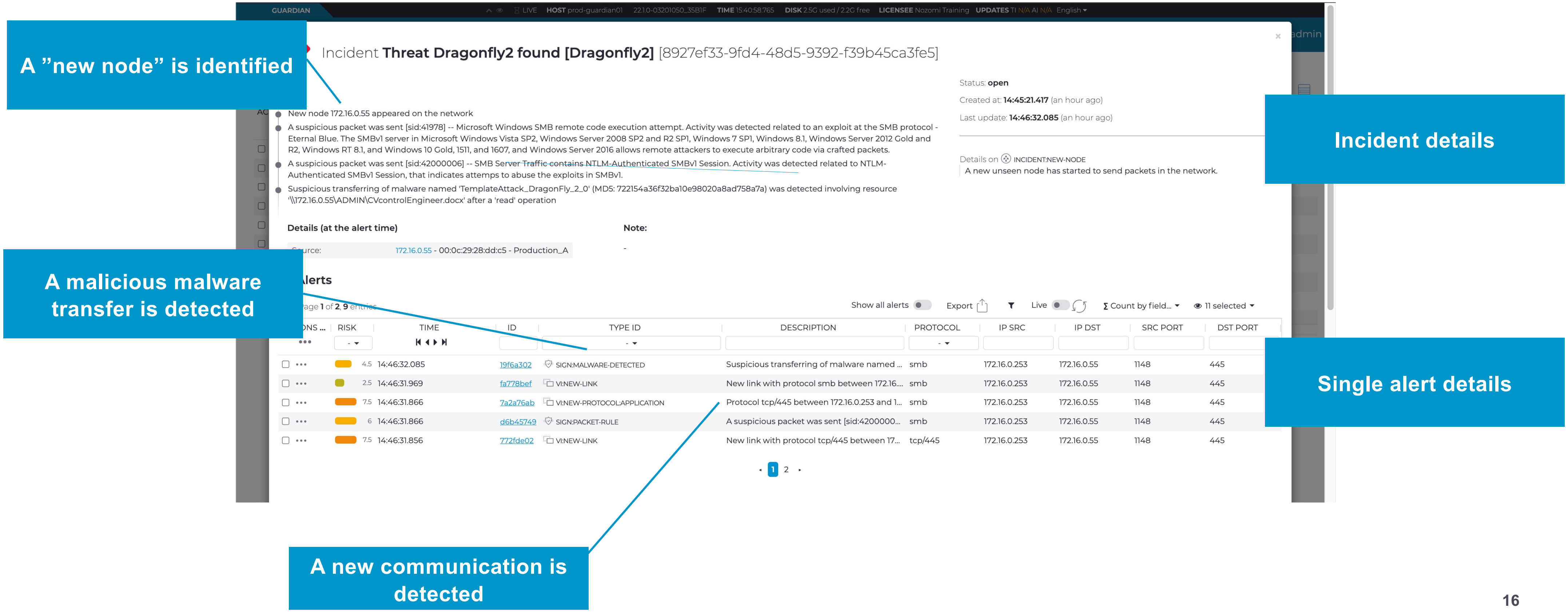
plc177.ACME0.corporationnet.com

IP:	172.16.0.142	**MAC address:**	00:60:78:01:99:d5
Roles:	producer	**MAC vendor:**	POWER MEASUREMENT LTD.
Product name:	ℹ Modicon M340 BMX P34 2020	**Vendor:**	ℹ Schneider Electric
Type:	ℹ Controller	**Firmware version:**	ℹ v2.9

Page **1** of **3**, **73** entries

ACTIONS	CVE	NODE	SCORE	CWE	CWE NAME	CVE CREATION DATE	DISCOVERY DAT
□	NN-2018-0002	172.16.0.142	7.5	754	Improper Check for Unusual or Exceptional Conditions	2020-01-07 00:15:00.000	09:32:45.296
□	NN-2017-0005	172.16.0.142	7.5	400	Uncontrolled Resource Consumption	2017-06-30 05:29:00.000	09:32:45.295
□	CVE-2022-37300	172.16.0.142	9.8	640	Weak Password Recovery Mechanism for Forgotten Password	2022-09-12 20:15:00.000	09:32:45.294
□	CVE-2022-22724	172.16.0.142	7.5	400	Uncontrolled Resource Consumption	2022-02-05 00:15:00.000	09:32:45.290
□	CVE-2021-22792	172.16.0.142	7.5	476	NULL Pointer Dereference	2021-09-02 19:15:00.000	09:32:45.289
□	CVE-2021-22791	172.16.0.142	6.5	787	Out-of-bounds Write	2021-09-02 19:15:00.000	09:32:45.288
□	CVE-2021-22790	172.16.0.142	6.5	125	Out-of-bounds Read	2021-09-02 19:15:00.000	09:32:45.287
□	CVE-2021-22789	172.16.0.142	6.5	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	2021-09-02 19:15:00.000	09:32:45.287
□	CVE-2021-22788	172.16.0.142	7.5	787	Out-of-bounds Write	2022-02-11 19:15:00.000	09:32:45.279
□	CVE-2021-	172.16.0.142	7.5	20	Improper Input Validation	2022-02-11 19:15:00.000	09:32:45.275

#4 – Anomaly Detection



GUARDIAN LIVE **HOST** prod-guardian01 22.1.0-03201050_35B1F **TIME** 15:40:58.765 **DISK** 2.5G used / 2.2G free **LICENSEE** Nozomi Training **UPDATES** TI N/A AI N/A English

Incident **Threat Dragonfly2 found [Dragonfly2]** [8927ef33-9fd4-48d5-9392-f39b45ca3fe5]

- New node 172.16.0.55 appeared on the network
- 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 R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets.
- A suspicious packet was sent [sid:42000006] -- SMB Server Traffic contains NTLM-Authenticated SMBv1 Session. Activity was detected related to NTLM-Authenticated SMBv1 Session, that indicates attemps to abuse the exploits in SMBv1.
- Suspicious transferring of malware named 'TemplateAttack_DragonFly_2_0' (MD5: 722154a36f32ba10e98020a8ad758a7a) was detected involving resource '\\172.16.0.55\ADMIN\CVcontrolEngineer.docx' after a 'read' operation

Status: **open**

Created at: **14:45:21.417** (an hour ago)

Last update: **14:46:32.085** (an hour ago)

Details on INCIDENT:NEW-NODE

A new unseen node has started to send packets in the network.

Details (at the alert time)

Source: 172.16.0.55 - 00:0c:29:28:dd:c5 - Production_A

Note:

-

Alerts

Page **1** of **2**, **9** entries

Show all alerts Export Live ∑ Count by field... 11 selected

	ONS ...	RISK	TIME	ID	TYPE ID	DESCRIPTION	PROTOCOL	IP SRC	IP DST	SRC PORT	DST PORT
□	•••	4.5	14:46:32.085	19f6a302	SIGN:MALWARE-DETECTED	Suspicious transferring of malware named ...	smb	172.16.0.253	172.16.0.55	1148	445
□	•••	2.5	14:46:31.969	fa778bef	VI:NEW-LINK	New link with protocol smb between 172.16....	smb	172.16.0.253	172.16.0.55	1148	445
□	•••	7.5	14:46:31.866	7a2a76ab	VI:NEW-PROTOCOL:APPLICATION	Protocol tcp/445 between 172.16.0.253 and 1...	smb	172.16.0.253	172.16.0.55	1148	445
□	•••	6	14:46:31.866	d6b45749	SIGN:PACKET-RULE	A suspicious packet was sent [sid:4200000...	smb	172.16.0.253	172.16.0.55	1148	445
□	•••	7.5	14:46:31.856	772fde02	VI:NEW-LINK	New link with protocol tcp/445 between 17...	tcp/445	172.16.0.253	172.16.0.55	1148	445

1 2

A ”new node” is identified

Incident details

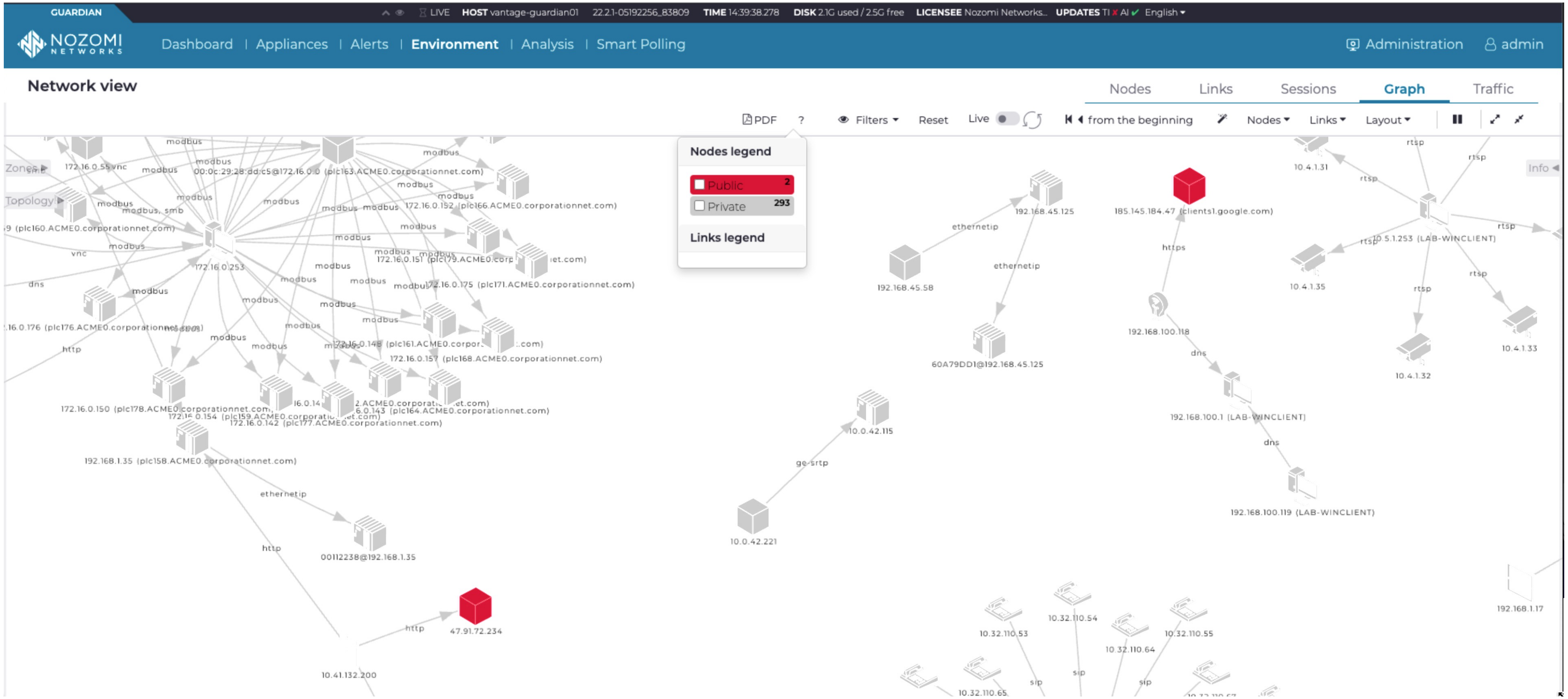
A malicious malware transfer is detected

Single alert details

A new communication is detected

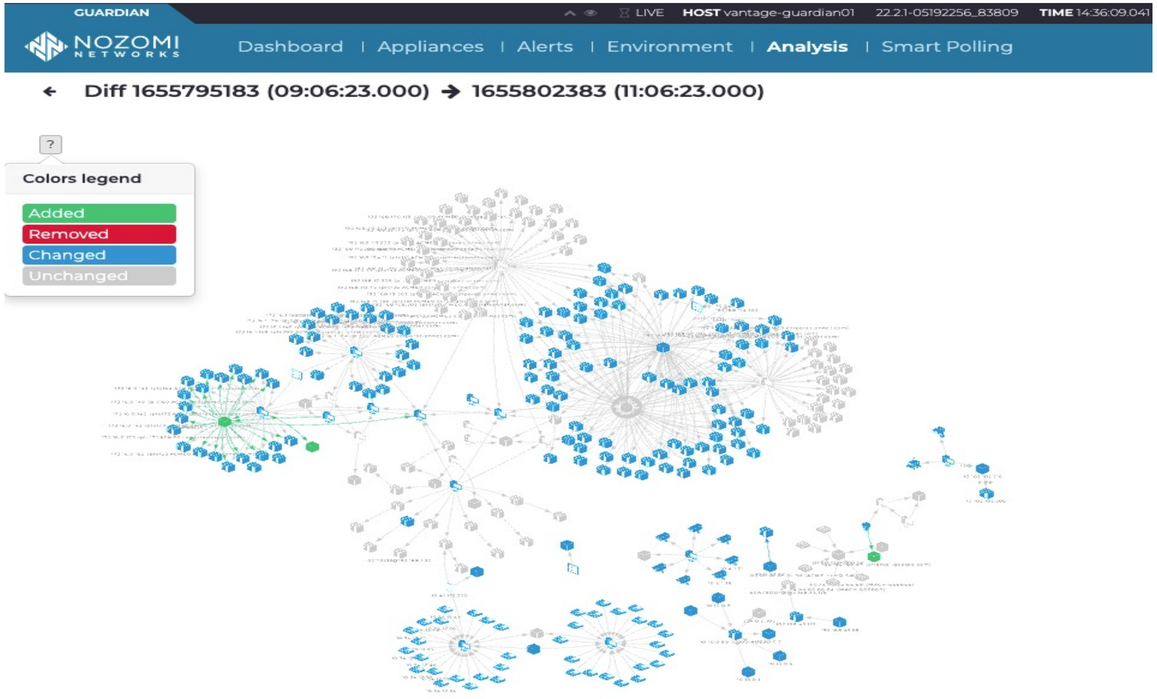
Pain Point: Network visualization and monitoring

… find connection attempts to public internet …


GUARDIAN
LIVE
HOST vantage-guardian01
22.2.1-05192256_83809
TIME 14:39:38.278
DISK 2.1G used / 2.5G free
LICENSEE Nozomi Networks...
UPDATES TI AI
English
NOZOMI NETWORKS
Dashboard
Appliances
Alerts
Environment
Analysis
Smart Polling
Administration
admin
Network view
Nodes
Links
Sessions
Graph
Traffic
PDF
?
Filters
Reset
Live
from the beginning
Nodes
Links
Layout
Zones
Topology
Info
Nodes legend
Public 2
Private 293
Links legend
modbus
vnc
dns
http
smb
ethernetip
https
rtsp
sip
ge-srtp
172.16.0.55
172.16.0.253
00:0c:29:28:dd:c5@172.16.0.0 (plc163.ACME0.corporationnet.com)
172.16.0.152 (plc166.ACME0.corporationnet.com)
172.16.0.151 (plc179.ACME0.corporationnet.com)
172.16.0.175 (plc171.ACME0.corporationnet.com)
172.16.0.176 (plc176.ACME0.corporationnet.com)
172.16.0.148 (plc161.ACME0.corporationnet.com)
172.16.0.157 (plc168.ACME0.corporationnet.com)
172.16.0.150 (plc178.ACME0.corporationnet.com)
172.16.0.154 (plc159.ACME0.corporationnet.com)
172.16.0.143 (plc164.ACME0.corporationnet.com)
172.16.0.142 (plc177.ACME0.corporationnet.com)
192.168.1.35 (plc158.ACME0.corporationnet.com)
00112238@192.168.1.35
47.91.72.234
10.41.132.200
10.0.42.115
10.0.42.221
192.168.45.125
192.168.45.58
60A79DD1@192.168.45.125
185.145.184.47 (clients1.google.com)
192.168.100.118
192.168.100.1 (LAB-WINCLIENT)
192.168.100.119 (LAB-WINCLIENT)
10.4.1.31
10.4.1.35
10.5.1.253 (LAB-WINCLIENT)
10.4.1.32
10.4.1.33
192.168.1.17
10.32.110.53
10.32.110.54
10.32.110.55
10.32.110.64
10.32.110.65

Pain Point: Network visualization and monitoring

… look back into the past



GUARDIAN

LIVE HOST vantage-guardian01 22.2.1-05192256_83809 TIME 14:36:09.041

NOZOMI NETWORKS
Dashboard | Appliances | Alerts | Environment | Analysis | Smart Polling

Diff 1655795183 (09:06:23.000) → 1655802383 (11:06:23.000)

Colors legend

- 🟩 Added
- 🟥 Removed
- 🟦 Changed
- ⬜ Unchanged

Result after we have achieved transparency

- Complete Asset Inventory (-> Integration into CMDB?)
- Cyber Threat Protection in realtime
- Integrations with existing systems, automated remediation
  - E. g. Firewall- or SIEM systems
- Vulnerability Management

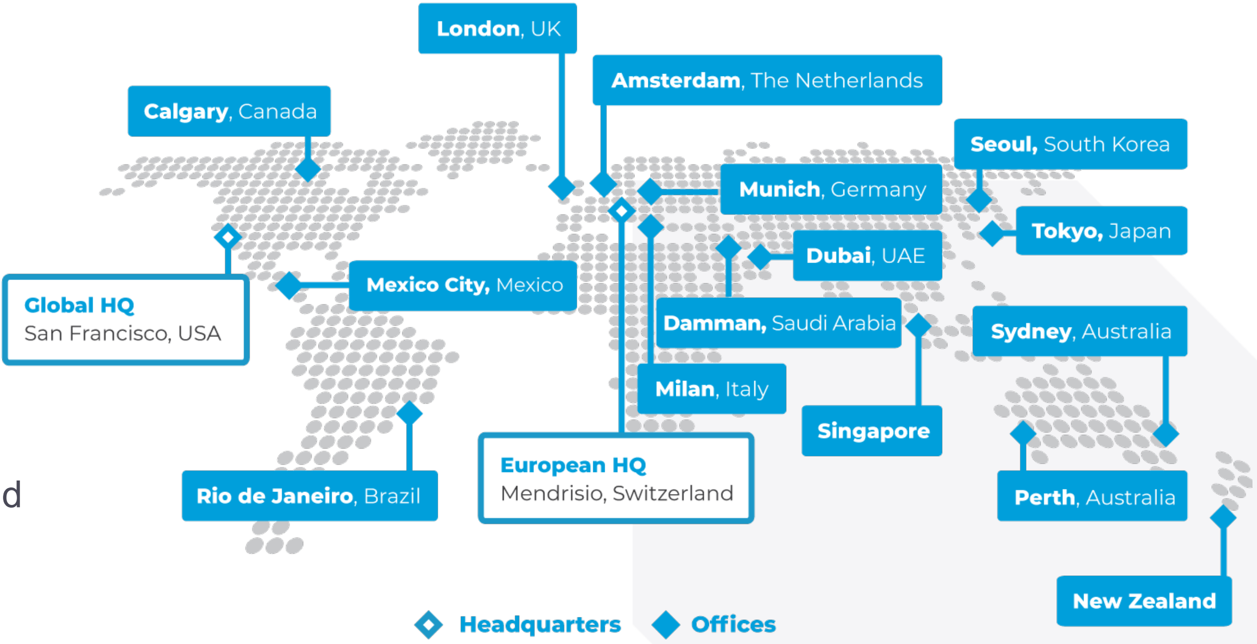
Global Leadership Footprint

Global Customer Base
11K+ Installations

102M Devices Monitored
Across Converged OT/IoT

Scalable Deployments
Across **6 Continents**

Global Expertise
Worldwide Network of Partners and
1,800+ 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

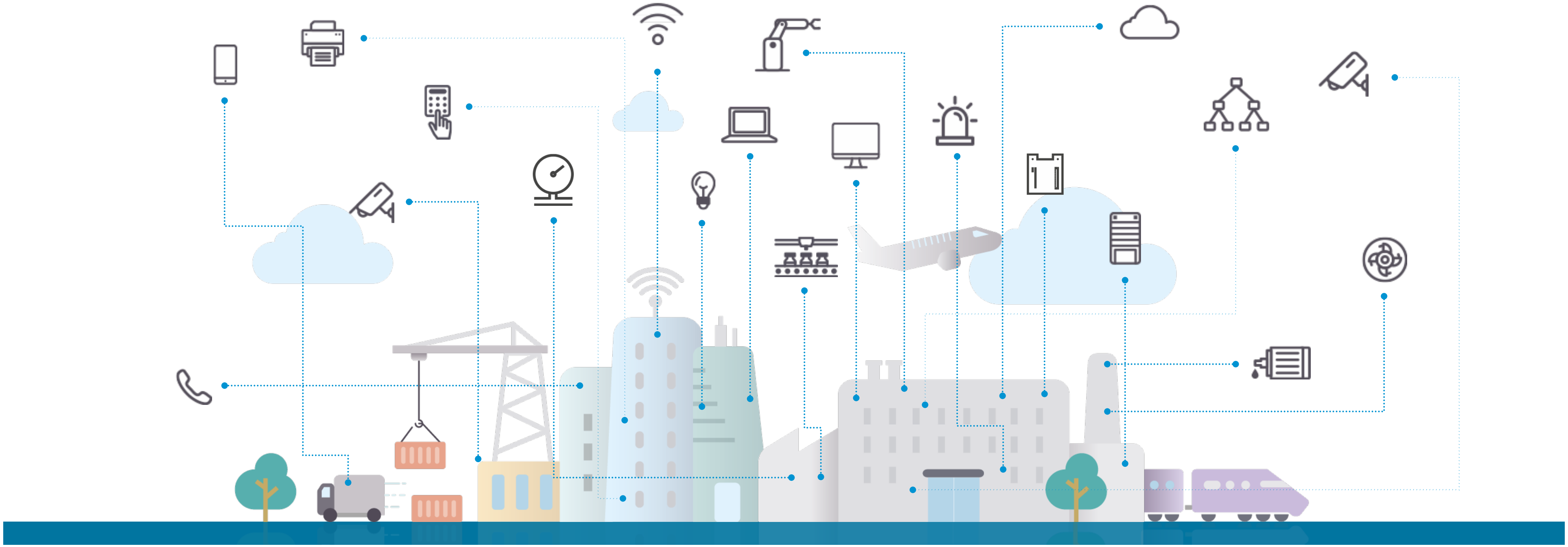
Logistics

Smart Cities

Transportation

Security and Visibility for Any Device, Anywhere

Accelerating digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats.



Nozomi Networks Solution Portfolio

MANAGEMENT OPTIONS

VANTAGE

- *SaaS*
- *FIPS-compliant*

CENTRAL MANAGEMENT CONSOLE

- *On-Premises*
- *FIPS-compliant*

SENSORS

GUARDIAN

- *ANSSI-certified*
- *FIPS-compliant*

GUARDIAN AIR

ARC SENSOR

- *Windows*
- *Apple*
- *Linux*

REMOTE COLLECTOR

ENHANCED CAPABILITIES

VANTAGE IQ

SMART POLLING

THREAT INTELLIGENCE

ASSET INTELLIGENCE

SERVICE OFFERINGS

Certified Engineer Training

Professional Services

Customer Support

OnePass/ HWaaS

Nozomi Networks Strengths

Proven Scalability

Central Management & Analysis
Manage any number of sites & assets

Cloud Multi-tier Architecture
SaaS platform monitors any number of assets and locations from anywhere

Agentless Protection
Single Guardian sensor can monitor over 500K assets

Faster Deployment

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

Cloud Architecture
SaaS platform speeds onboarding, eliminates sizing issues

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

Always-On Monitoring

Continuous Monitoring of All Supported Protocols: OT, IoT and IT
No critical blind spots

Unmatched Detection & Visibility
Prevents operational disruptions

Audit-ready Default Configuration
Avoids findings due to misconfiguration

Full Stack Solution

No Reliance on Other Vendors
Avoids EOL impacts or waiting for patches

Rigorous QA Ensures Interoperability and Stability
Improves hardening, scalability, rollback, data analysis

Integrated Development
Extracts the best performance from hardware and software

Successful customers: Gartner Peer Insights

Gartner peerinsights™

★★★★★

ROLE: RAIL OT CYBERSECURITY
INDUSTRY: TRANSPORTATION
COMPANY SIZE: 10B – 30B USD

Great Ride for a Major Rail Operator

Nozomi supported us from the beginning of our initiative for improving the visibility of the network activity on our Critical OT Infrastructure. Their solution has been chosen after a long process, including evaluation of multiple options over a long period of time. The sales, presales and delivery team were a big part of the reason why we chose Nozomi in addition to the technology itself. We are currently rolling out the technology over a large rail network, and before we took the decision we made a thorough Proof of Concept/Value process.

★★★★★

ROLE: INFRASTRUCTURE AND OPERATIONS
INDUSTRY: ENERGY PRODUCTION
COMPANY SIZE: 1B – 3B USD

Nozomi Is Very Easy to Use and Its Information Can Be Integrated Easily Into SIEMs

We use Nozomi for analysis of our OT network and we appreciate a lot feedback from system and the fact that is very powerful system.

★★★★★

ROLE: SECURITY AND RISK MANAGEMENT
INDUSTRY: PROVIDER
COMPANY SIZE: 250M – 500M USD

A CISO Must Have for OT Environment

Nozomi Networks is the leader in this field. It's not just a security technology, it's simple a eye wide open into the darkness world of the Operation Technology. For me as Security Manager it's really a must have!!

More Reviews from Nozomi Networks Customers

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.

nozominetworks.com