



# ***OT and IIOT Security: come ridurre i rischi.***

Scenari reali di impiego

**Sergio Leoni** – Regional Sales Director **Nozomi Networks**

# Agenda

- Cosa succede intorno a noi
- Perché e cosa possiamo imparare
- Best Practices
- Panoramica sulla tecnologia
  - Visibility
  - Threats detection
  - Threats di Processo

**Cosa succede  
intorno a noi?**





# Cyberattacks are Increasing



## Ransomware Attack Hits Manufacturing – Are You Vulnerable?

Mar. 2019

Norsk Hydro, a multinational manufacturer headquartered in Norway and one of the world's largest aluminum producers, reported last week that it was hit by a ransomware that affected its production and IT systems.



## Mondelez in \$100M Court Battle with Insurer Over Cyberattack-related Damages

Jan. 2019

NotPetya malware left 1,700 servers and 24,600 laptops "permanently dysfunctional" after the attack hit Mondelez twice. Impact included loss of electronic data, software and physical damage.



## Pharmaceutical Giant Bayer Targeted by Cyberattack

April 2019

German drugmaker Bayer contained a cyberattack it believes was hatched in China, highlighting the risk of data theft and disruption faced by big business.



## Roche Confirms Cyberattack from Winnti Malware

July 2019

Roche confirmed that it experienced a cyberattack using the malware known as Winnti. "Roche has been targeted by various attackers in the past ... These attacks were detected and remediated."

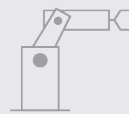




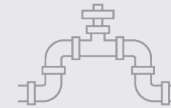
# The world around us is remote-controlled



**Electric Utilities**



**Automotive Manufacturing**



**Oil & Gas**



**Pharmaceuticals**



**Mining**



**Chemicals**



**Food & Consumer Goods**

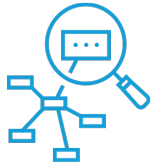


**Water/Wastewater**

The background features a complex geometric pattern of overlapping blue and white triangles and diamonds. On the right side, there is a low-angle photograph of a modern glass skyscraper with a grid of windows, partially obscured by the geometric overlay.

***Ritrovate qualcuno di  
questi temi all'interno  
delle vostre aziende?***

# Perché e cosa possiamo imparare ?



**Accurately Visualize** the Network and **Automatically Track** Industrial Assets



**Rapidly Detect** Cyber Threats/Risks and Process Anomalies



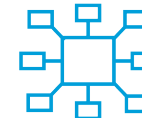
**Significantly Reduce** Troubleshooting and Forensic Efforts



**Quickly Monitor** ICS Networks and Processes with Real-time Insight



**Reliably Monitor** Multinational Installations



**Centrally or Remotely Secure** Large, Distributed Industrial Networks



# Perché e cosa possiamo imparare ?

## A Matter of Business, The High Cost of a Cybersecurity Incident

”

“Cyberattacks on critical infrastructure and strategic industrial assets are now one of the top five global risks.”

”

**World Economic Forum**  
Global Risk Report, 2018

Sources: Wired, Wall Street Journal, UK Telegraph, Threatpost

# Best Practices



## See

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



## Detect

Cyber threats, risks and  
anomalies for faster response



## Unify

Security, visibility and monitoring  
across all your assets



# **Nozomi Networks,** panoramica sulla tecnologia

# Global Leadership Footprint



## FOUNDED IN SWITZERLAND

October 2013



Global Customer Base  
2.4K Installations



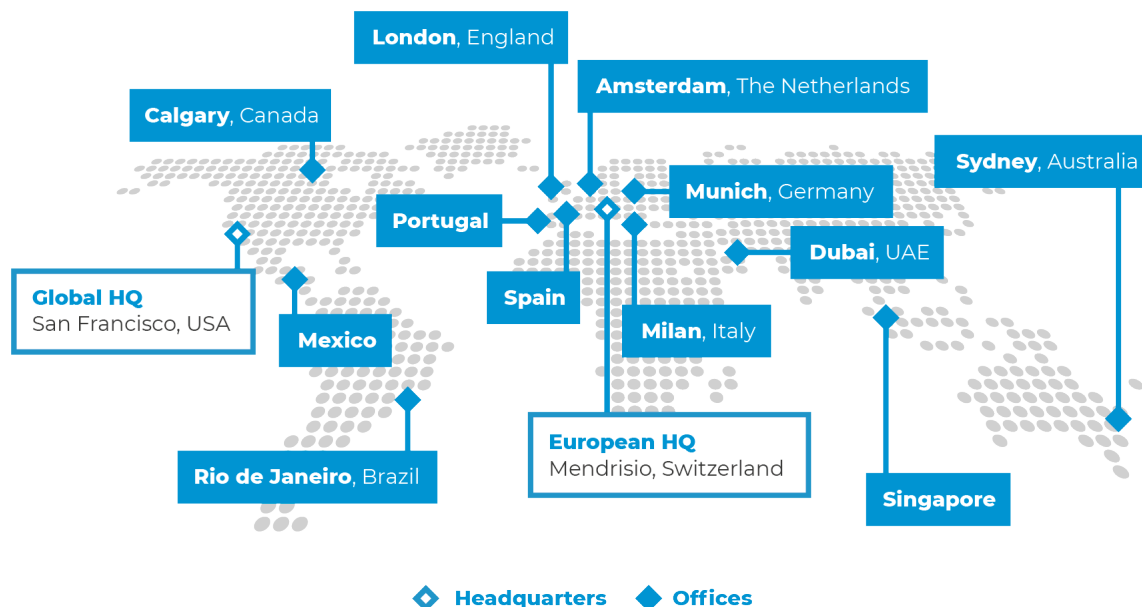
3.6M Devices Monitored  
Across Converged OT / IoT



Scalable Deployments  
Across 6 Continents

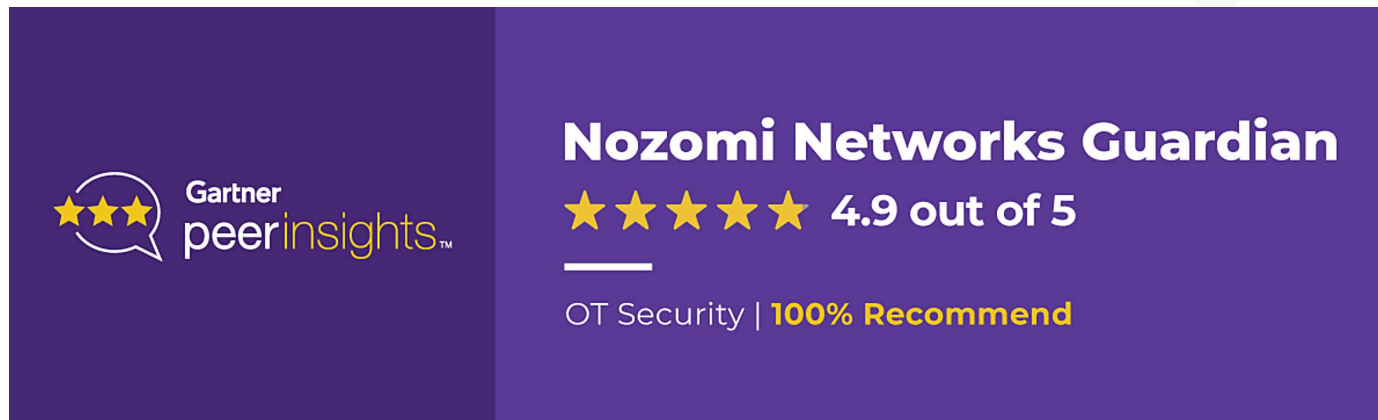


Global Expertise  
Worldwide Network of Partners  
and 700+ Certified Professionals





## We Are the Leader: Gartner, Nozomi Ranked #1



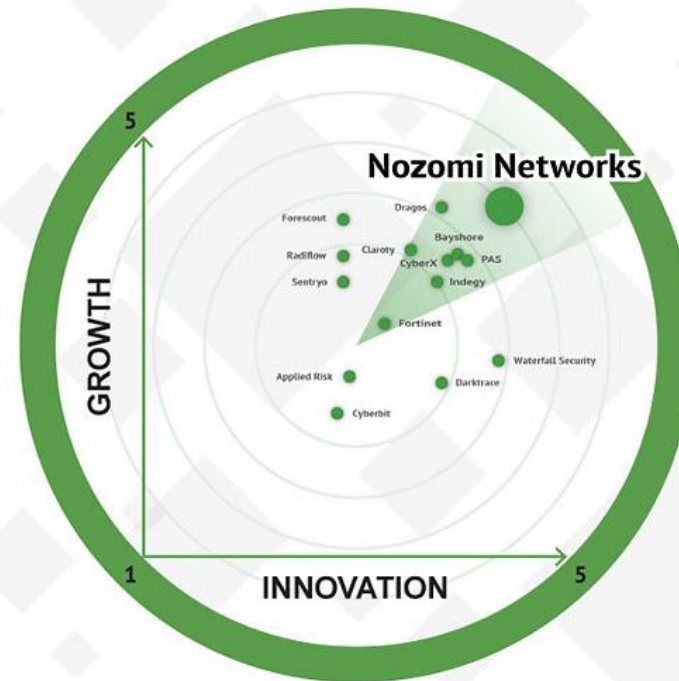
### Customers Give Nozomi Networks Top Score in Gartner Peer Reviews

This is the highest score for OT security market vendors with 10 or more reviews.  
100% say they would recommend us to others.

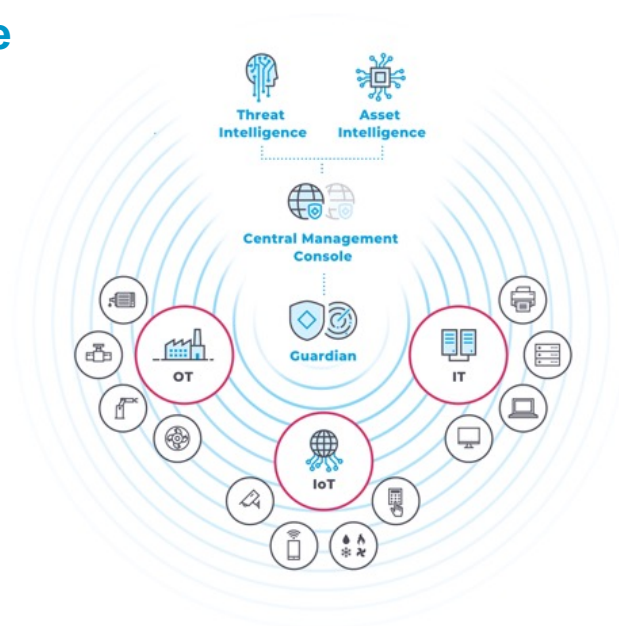
## We Are the Leader: Frost & Sullivan, Nozomi Ranked #1

FROST & SULLIVAN

FROST RADAR DECLARES  
NOZOMI NETWORKS LEADER



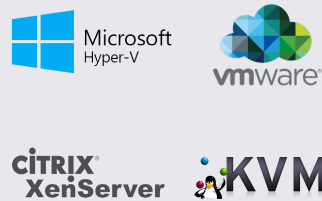
# A Comprehensive Security Solution



## One Solution. Multiple Deployment Options to Meet Your Needs.



Physical Appliances



Virtual Appliances



Containers



Embedded Offerings

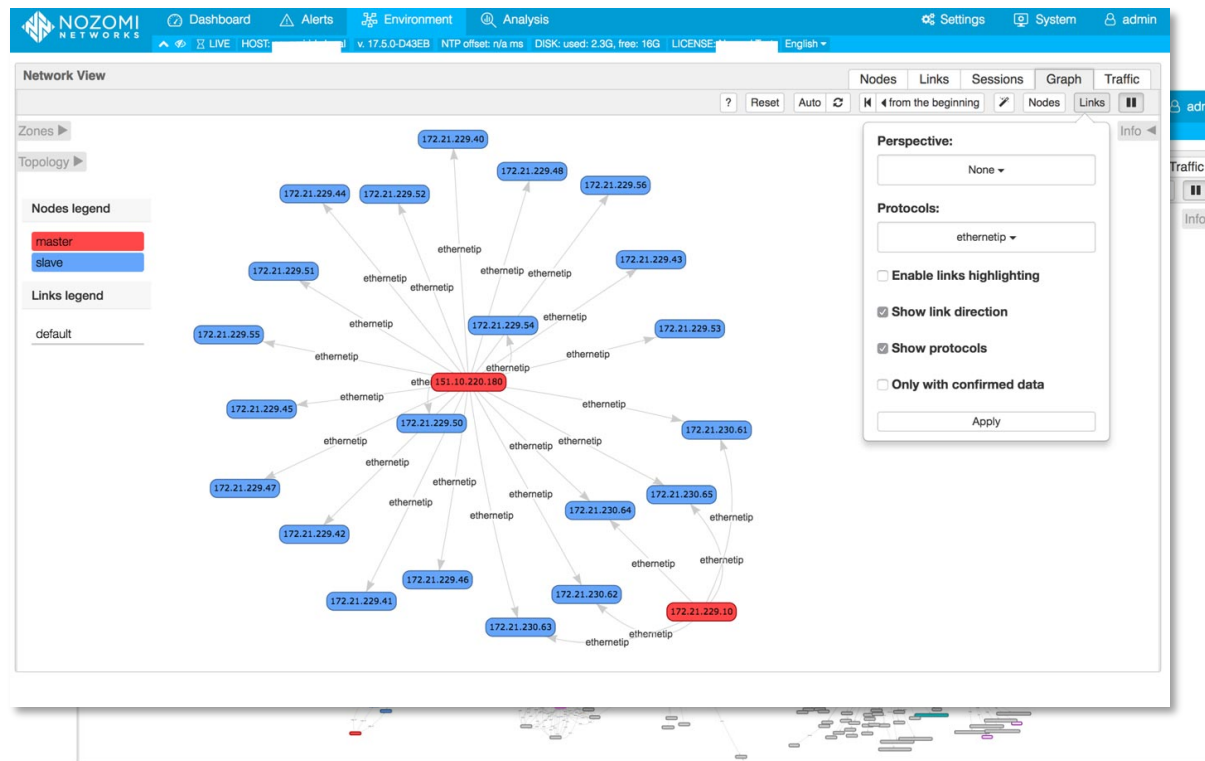




# Visibility

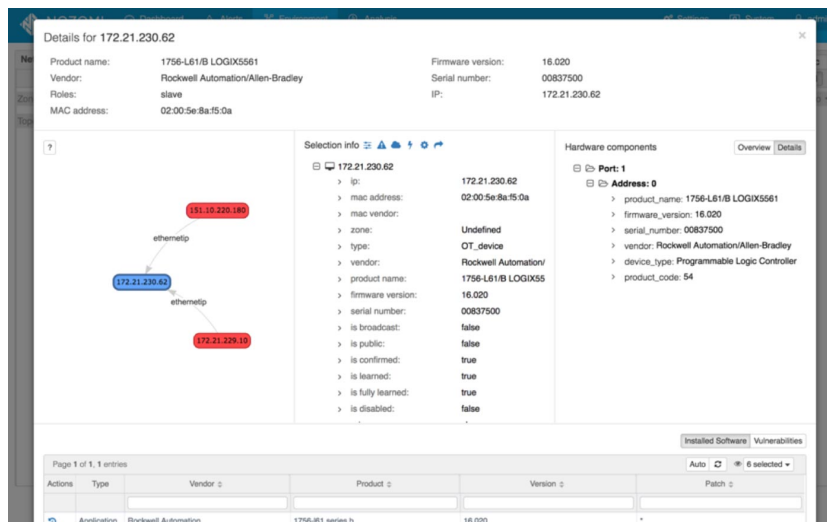
*Come si fa a proteggere quello che non si conosce?  
Che percezione si ha della vulnerabilità della propria  
rete di produzione?*

# Pain Point: Network Visualization and Monitoring

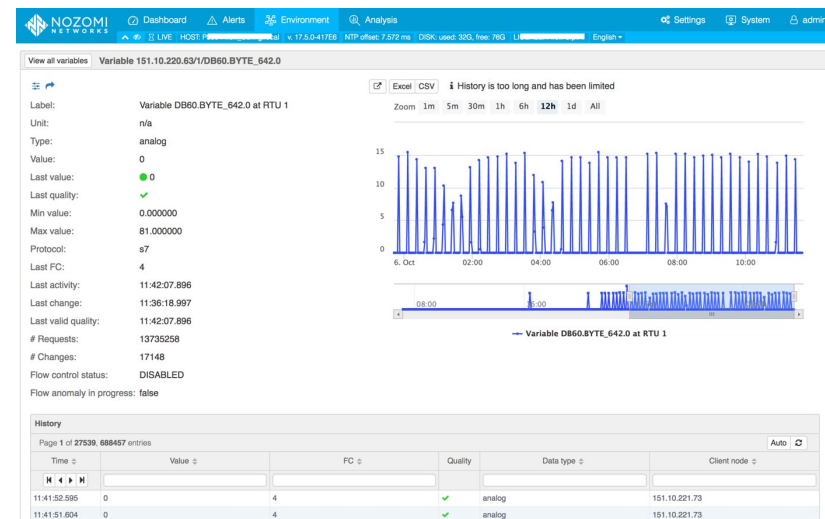


# Pain Point: Network Visualization and Monitoring

Go deep in details...



Nodes



Variables

# Pain Point: Asset Inventory

**Asset View**

Page 1 of 46, 1133 entries

Excel CSV Auto 9 selected

| Actions | Name | Type      | OS/Firmware                  | IP             | MAC address       | Vendor                           | Product name         | Serial number |
|---------|------|-----------|------------------------------|----------------|-------------------|----------------------------------|----------------------|---------------|
|         |      | computer  | Windows 7                    | 10.130.86.117  | e0:0e:da:7b:2b:ff |                                  |                      |               |
|         |      | OT_device | Firmware: 16.054             | 172.21.229.41  | 02:00:5e:8a:f5:0a | Rockwell Automation/Allen-Bradle | 1756-L61/B LOGIX5561 | 00687935      |
|         |      | computer  | Windows 8.1 / Server 2012 R2 | 151.10.221.44  | e0:0e:da:7b:2b:ff |                                  |                      |               |
|         |      | OT_device | Firmware: 16.020             | 172.21.230.62  | 02:00:5e:8a:f5:0a | Rockwell Automation/Allen-Bradle | 1756-L61/B LOGIX5561 | 00837500      |
|         |      | computer  | Windows XP SP3               | 172.21.88.47   | 00:1c:71:37:20:a5 |                                  |                      |               |
|         |      | computer  | Windows 8.1 / Server 2012 R2 | 172.21.230.150 | 02:00:5e:8a:f5:0a |                                  |                      |               |
|         |      | computer  |                              | 151.10.221.43  | 02:00:5e:0b:d4:0a |                                  |                      |               |
|         |      | computer  | Windows 8.1 / Server 2012 R2 | 172.21.229.12  | 02:00:5e:8a:f5:0a |                                  |                      |               |
|         |      | computer  | Windows XP SP3               | 172.21.88.45   | 00:1c:71:37:20:a5 |                                  |                      |               |
|         |      | computer  | Windows 7                    | 172.21.77.163  | 00:1c:71:37:20:a5 |                                  |                      |               |
|         |      | OT_device | Firmware: 16.020             | 172.21.230.61  | 02:00:5e:8a:f5:0a | Rockwell Automation/Allen-Bradle | 1756-L61/B LOGIX5561 | 00557072      |
|         |      | OT_device | Firmware: 16.054             | 172.21.229.42  | 02:00:5e:8a:f5:0a | Rockwell Automation/Allen-Bradle | 1756-L61/B LOGIX5561 | 00679184      |
|         |      | computer  | Windows XP SP3               | 10.130.86.129  | e0:0e:da:7b:2b:ff |                                  |                      |               |
|         |      | computer  | Windows XP SP3               | 151.10.220.151 | e0:0e:da:7b:2b:ff |                                  |                      |               |
|         |      | OT_device | Firmware: 16.020             | 172.21.229.47  | 02:00:5e:8a:f5:0a | Rockwell Automation/Allen-Bradle | 1756-L61/B LOGIX5561 | 00505802      |
|         |      | OT_device | Firmware: 18.011             | 172.21.229.52  | 02:00:5e:8a:f5:0a | Rockwell Automation/Allen-Bradle | 1756-L62/B LOGIX5562 | 00813A91      |
|         |      | computer  |                              | 172.21.242.137 | 02:00:5e:6a:27:0a |                                  |                      |               |
|         |      | computer  | Windows 8.1 / Server 2012 R2 | 172.21.230.134 | 02:00:5e:8a:f5:0a |                                  |                      |               |
|         |      | computer  |                              |                | 0a:f5:0a          |                                  |                      |               |

Operating System

Firmware version of the PLCs

OT Vendor, Product, Serial

# Pain Point: Asset vulnerabilities

Product Name  
Vendor

Firmware version  
of the PLCs

Hardware  
Components

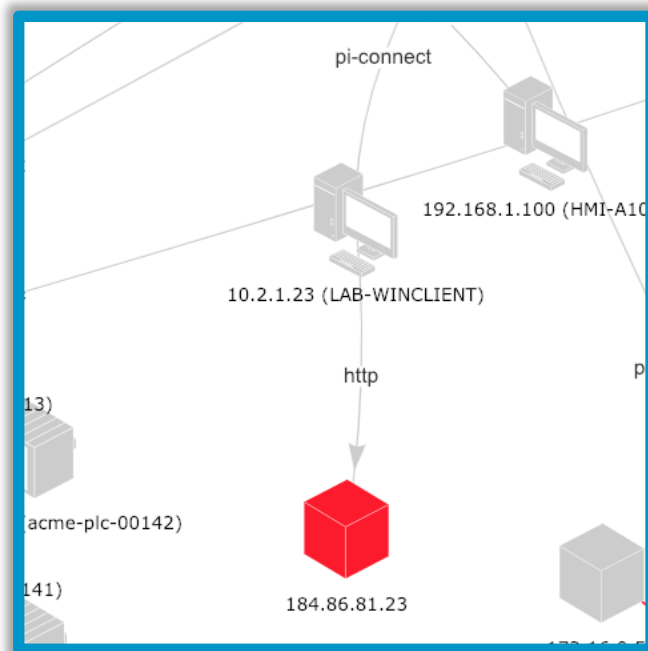
Vulnerabilities

The screenshot displays the Nozomi Networks interface for asset 172.21.230.62. The top section shows metadata: Product name (1756-L61/B LOGIX5561), Vendor (Rockwell Automation/Allen-Bradley), Roles (slave), MAC address (02:00:5e:8a:15:0a), Firmware version (16.020), Serial number (00837500), and IP (172.21.230.62). The middle section shows a network diagram with the asset highlighted. The right section shows hardware components: Port 1, Address 0, product\_name (1756-L61/B LOGIX5561), firmware\_version (16.020), serial\_number (00837500), vendor (Rockwell Automation/Allen-Bradley), device\_type (Programmable Logic Controller), and product\_code (54). The bottom section shows a table of vulnerabilities.

| CVE           | Node          | Score | CWE            | CWE name                                                                | Discovery date   | Matching CPEs                     |
|---------------|---------------|-------|----------------|-------------------------------------------------------------------------|------------------|-----------------------------------|
| CVE-2012-6442 | 172.21.229.52 | 7.6   | 119            | Improper Restriction of Operations within the Bounds of a Memory Buffer | 2017-09-13 13:10 | cpe:/h:rockwellautomation:cont... |
| CVE-2012-6441 | 172.21.229.52 | 5.0   | 200            | Information Exposure                                                    | 2017-09-13 13:10 | cpe:/h:rockwellautomation:cont... |
| CVE-2012-6440 | 172.21.229.52 | 8.3   | 287            | Improper Authentication                                                 | 2017-09-13 13:10 | cpe:/h:rockwellautomation:cont... |
| CVE-2012-6439 | 172.21.229.52 | 8.5   | [unclassified] | [unclassified]                                                          | 2017-09-13 13:10 | cpe:/h:rockwellautomation:cont... |
| CVE-2012-6438 | 172.21.229.52 | 7.6   | 119            | Improper Restriction of Operations within the Bounds of a Memory Buffer | 2017-09-13 13:10 | cpe:/h:rockwellautomation:cont... |
| CVE-2012-6437 | 172.21.229.52 | 10.0  | 287            | Improper Authentication                                                 | 2017-09-13 13:10 | cpe:/h:rockwellautomation:cont... |
| CVE-2012-6436 | 172.21.229.52 | 7.6   | 119            | Improper Restriction of Operations within the Bounds of a Memory Buffer | 2017-09-13 13:10 | cpe:/h:rockwellautomation:cont... |
| CVE-2012-6435 | 172.21.229.52 | 7.6   | 399            | Resource Management Errors                                              | 2017-09-13 13:10 | cpe:/h:rockwellautomation:cont... |



## Common Discovery: Level 1 & 2 Devices Connected to the Internet



Identifies potential threat actor access points into the network

# Common Discovery: Software Vulnerabilities

Page 1 of 1, 1 entries

Auto

6 selected

| Actions | Type        | Vendor  | Product | Version | Patch |
|---------|-------------|---------|---------|---------|-------|
|         | Application | OpenBSD | OpenSSH | 7.6     | *     |

Page 1 of 1, 2 entries

Excel

CSV

Auto

9 selected

| CVE                           | Node | Score | CWE            | CWE name                                                                | CVE creation date       | Discovery date          | Matching CPEs              | Likelihood |
|-------------------------------|------|-------|----------------|-------------------------------------------------------------------------|-------------------------|-------------------------|----------------------------|------------|
| <a href="#">CVE-2014-1692</a> |      | 7.5   | 119            | Improper Restriction of Operations within the Bounds of a Memory Buffer | 2014-01-29 06:02:05.000 | 2018-06-06 01:53:25.603 | cpe:/a:openbsd:openssh:7.6 | 0.8        |
| <a href="#">CVE-2007-2768</a> |      | 2.0   | [unclassified] | [unclassified]                                                          | 2007-05-21 12:30:00.000 | 2018-06-06 01:53:25.603 | cpe:/a:openbsd:openssh:7.6 | 0.8        |

Page 1 of 1, 12 entries

Excel

CSV

Auto

9 selected

| CVE                           | Node | Score | CWE | CWE name                     | CVE creation date       | Discovery date          | Matching CPEs                      | Likelihood |
|-------------------------------|------|-------|-----|------------------------------|-------------------------|-------------------------|------------------------------------|------------|
| <a href="#">CVE-2016-7153</a> |      | 5.0   | 200 | Information Exposure         | 2016-09-06 02:59:01.000 | 2018-06-06 01:52:56.472 | cpe:/a:google:chrome:65.0.3325.209 | 0.5        |
| <a href="#">CVE-2016-7152</a> |      | 5.0   | 200 | Information Exposure         | 2016-09-06 02:59:00.000 | 2018-06-06 01:52:56.471 | cpe:/a:google:chrome:65.0.3325.209 | 0.5        |
| <a href="#">CVE-2015-4000</a> |      | 2.0   | 310 | Cryptographic Issues         |                         |                         |                                    |            |
| <a href="#">CVE-2015-2808</a> |      | 2.0   | 310 | Cryptographic Issues         |                         |                         |                                    |            |
| <a href="#">CVE-2013-6647</a> |      | 7.5   | 416 | Use After Free               |                         |                         |                                    |            |
| <a href="#">CVE-2013-2566</a> |      | 2.0   | 310 | Cryptographic Issues         |                         |                         |                                    |            |
| <a href="#">CVE-2015-8960</a> |      | 6.8   | 310 | Cryptographic Issues         |                         |                         |                                    |            |
| <a href="#">CVE-2013-6662</a> |      | 2.0   | 295 | Improper Certificate Validat |                         |                         |                                    |            |
| <a href="#">CVE-2012-4930</a> |      | 2.0   | 310 | Cryptographic Issues         | 2012-09-15 10:55:03.000 | 2018-06-06 01:52:56.463 | cpe:/a:google:chrome:65.0.3325.209 | 0.5        |
| <a href="#">CVE-2012-4929</a> |      | 2.0   | 310 | Cryptographic Issues         | 2012-09-15 10:55:03.000 | 2018-06-06 01:52:56.461 | cpe:/a:google:chrome:65.0.3325.209 | 0.5        |

Page 1 of 1, 1 entries

Actions

Type

Vendor

Product

Version

|  |             |        |        |               |
|--|-------------|--------|--------|---------------|
|  | Application | Google | Chrome | 65.0.3325.209 |
|--|-------------|--------|--------|---------------|

Identifies high risk vulnerabilities open to exploitation

# Common Discovery: Unknown & Misconfigured Devices

| Type ID     | Status | Name              | Description                                             | Risk | Protocol  | Transport protocol |
|-------------|--------|-------------------|---------------------------------------------------------|------|-----------|--------------------|
| Vl:NEW-FUNC | open   | New SCADA fu...   | New function code 5 (Direct Operate)                    | 3.0  | dnp3      | tcp                |
| Vl:NEW-FUNC | open   | New SCADA fu...   | New function code 0 (Confirm)                           | 3.0  | dnp3      | tcp                |
| Vl:NEW-FUNC | open   | New SCADA fu...   | New function code 20 (Enable Spontaneous Msg)           | 3.0  | dnp3      | tcp                |
| Vl:NEW-NODI | open   | New node appe...  | New tcp/20000 node                                      | 2.5  | tcp/20000 | tcp                |
| Vl:NEW-FUNC | open   | New SCADA fu...   | New function code 129 (Response)                        | 3.0  | dnp3      | tcp                |
| Vl:NEW-FUNC | open   | New SCADA fu...   | New function code 1 (Read)                              | 3.0  | dnp3      | tcp                |
| Vl:NEW-FUNC | open   | New SCADA fu...   | New function code 21 (Disable Spontaneous Msg)          | 3.0  | dnp3      | tcp                |
| Vl:NEW-PROT | open   | New protocol c... | Protocol tcp/20000 between .8 and 11 has been confirmed | 2.5  | tcp/20000 | tcp                |

| Type ID    | Status | Name             | Description                                                                                                                          | Risk | Protocol | Transport protocol |
|------------|--------|------------------|--------------------------------------------------------------------------------------------------------------------------------------|------|----------|--------------------|
| SIGNPROCME | open   | Missing variable | An attempt has been made by host 13.112 to access an unexisting variable(s) on host 20 with function code 3 (Read Holding Registers) | 6.0  | modbus   | tcp                |
| SIGNPROCME | open   | Missing variable | An attempt has been made by host 3.112 to access an unexisting variable(s) on host 20 with function code 3 (Read Holding Registers)  | 6.0  | modbus   | tcp                |

Manage Learning

.2.8-2.11

Delete Learn Save Discard

Links

1.2.8 - 8.2.11

dnp3

0 (Confirm)

1 (Read)

5 (Direct Operate)

20 (Enable Spontaneous Msg)

21 (Disable Spontaneous Msg)

129 (Response)

Identifies device misconfigurations and possible indicators of compromise by threat actors

 NOZOMI NETWORKS

[www.nozominetworks.com/](http://www.nozominetworks.com/) CONFIDENTIAL

23

# Common Discovery: Unencrypted / Weak Credentials

Alerts 23:08:47.288

Page 1 of 1, 14 entries / filtered by type id: == SIGN:PASSWORD:WEAK x

| Actions | Time                    | ID                       | Type ID           | Status | Name    | Description                                                                                   |
|---------|-------------------------|--------------------------|-------------------|--------|---------|-----------------------------------------------------------------------------------------------|
|         | 2018-06-25 18:13:49.141 | <a href="#">e43ac541</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 18:10:43.961 | <a href="#">c6056bec</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 18:10:06.952 | <a href="#">b2d0ee20</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 18:07:39.162 | <a href="#">6285b76d</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 18:06:24.962 | <a href="#">7c947d87</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 18:04:33.973 | <a href="#">ecbfbf27</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 18:03:56.979 | <a href="#">0e7ad032</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 18:02:42.959 | <a href="#">edd46a5f</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 18:02:05.976 | <a href="#">70bdddea</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 17:59:00.991 | <a href="#">d36a055f</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 17:57:47.184 | <a href="#">af0529cd</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 17:55:55.973 | <a href="#">3aa1184d</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 17:54:42.019 | <a href="#">789c59f7</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |
|         | 2018-06-25 17:53:27.994 | <a href="#">3f3c2b86</a> | SIGN:PASSWORD:WEA | open   | Weak pe | Weak username/password (apc/apc) has been used to access host 10.10.200.90 with protocol http |

**Weak password used**  
14:37:00.893

**Description**  
Weak username/password (admin/admin) has been used to access host 10.10.200.90 with protocol http

**Note:**  
A weak password has been used to access a resource. To safely protect your systems, change passwords of devices and manage them in a secure manner.

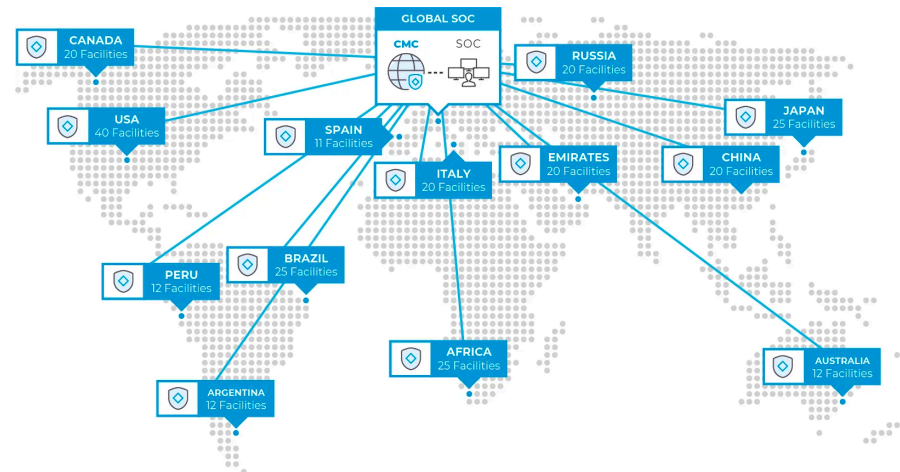
**Open details**

|                    | Src   | Dst        |
|--------------------|-------|------------|
| IP                 |       |            |
| MAC                |       |            |
| Label              |       |            |
| Port               | 52980 | 80         |
| Roles              | other | web_server |
| Is security        |       | true       |
| Protocol           |       | http       |
| Transport protocol |       | tcp        |

Detects default and easily guessed credentials, and systems open to compromise by threat actors

# Unify

## Security, Visibility and Monitoring Across All Your Assets



- Time-Saving Dashboards and Forensic Tools
- Unified Security for Thousands of Distributed Sites





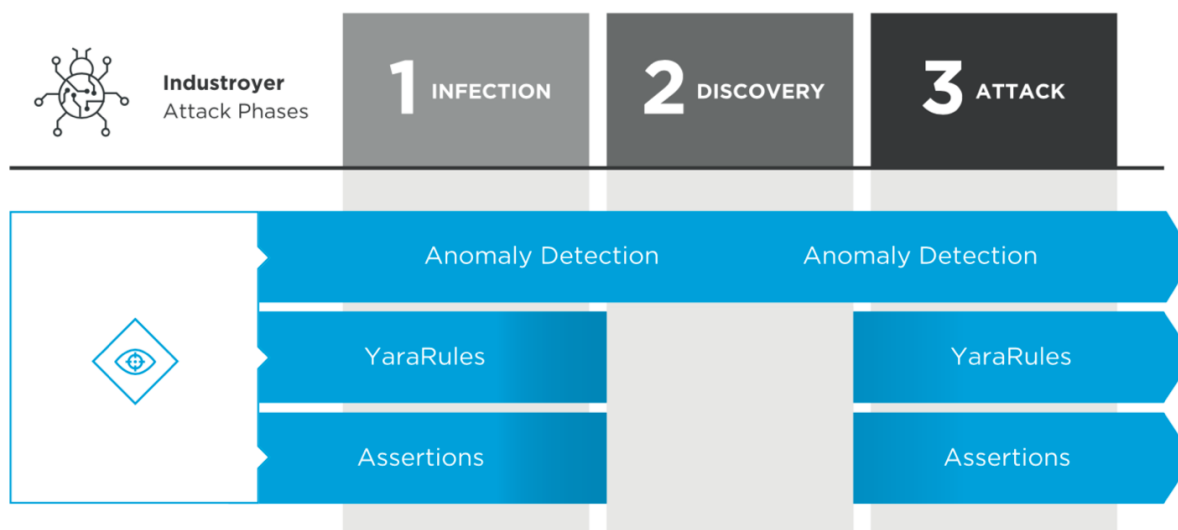
**Lesson Learned**  
**Visibility !**



## Casi d'uso

*Non si dispone di strumenti per rilevare malware o lo sfruttamento di vulnerabilità o semplicemente non si ha la percezione del rischio a cui si è esposti.*

# Pain Point: Hybrid Threat Detection



Behavior-based **anomaly detection** enriched with AI and analytics engine

**Rule-based analysis**, using (Yara, Packet, etc.) for threat hunting

**Signature assertions & queries** with out-of-box and custom functions

# Pain Point: Hybrid Threat Detection

Thanks to anomaly detection, all deviations from the baseline can be alerted at different levels

A new communication is detected

A "rogue" MAC address is identified

A new Modbus connection is detected

A Modbus Reprogram Command is detected

The screenshot displays the Nozomi Networks Alerts interface. The top navigation bar includes links for Dashboard, Alerts, Environment, Analysis, Settings, System, and admin. The Alerts section shows a table of alerts with columns for Actions, Time, ID, Type, Status, Name, and Description. A specific alert is highlighted: 'Incident New Communications [667c7336-af3b-468a-8d24-fd5419386bd]'. The alert details show that known nodes 10.2.1.24 and 172.16.0.157 have started new communications. The alert is categorized as 'NEW INCIDENT'. Below the alert details, a table lists the detected events, including 'New MAC address', 'New link with protocol', 'New protocol confirmed', 'New application detected', and 'New SCADA function code detected'. A network diagram at the bottom shows the communication between the nodes.

NEW INCIDENT

pcap traces of the attack are automatically generated

INCIDENT DETAILS

# Pain Point: Hybrid Threat Detection

Rule-based analysis allows to you identify, in real-time, known attacks and malware

The screenshot displays the NOZOMI alert interface. At the top, a navigation bar includes links for Dashboard, Alerts, Environment, Analysis, Settings, System, and admin. The main alert is titled "Alert Malware detected [b5fd231a-2269-458a-9c1f-c110f6a53d0b]" with a status of "open". The alert description states: "Suspicious transferring of malware named 'WannaCry\_Ransomware' was detected involving resource '\\192.168.1.33\\NOZOMI\_LOCALSHARE\\ed01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe' by user 'NAS\_NOZOMI\\Nozomiers' after a 'write' operation [rule author: Florian Roth (with the help of binar.ly)]".

Details (at the alert time):

- Source: 192.168.1.33 - 00:ff:9e:e0:87:77
- Destination: 192.168.2.26 - 78:4f:43:67:89:dd
- Protocol: smb [tcp]
- Ports: 445 • 61983

Note: -

Details on SIGN-MALWARE-DETECTED: A potentially malicious payload has been transferred over the network.

Involved nodes (at the current time):

A diagram shows two nodes: 192.168.1.33 and 192.168.2.26, connected by a line labeled "smb".

Selection info:

- ip: 192.168.1.33
- mac address: 00:ff:9e:e0:87:77
- mac vendor: -
- zone: ProdNet-B
- type: -
- is broadcast: false
- is public: false
- is confirmed: true
- is learned: true
- is fully learned: true
- is disabled: false
- roles: other
- links count: 1
- protocols: smb
- first activity time: 2017-11-24 14:26:18.045
- last activity time: 2017-11-24 14:27:33.357



# Pain Point: Hybrid Threat Detection

Rule-based analysis allows to you identify, in real-time, known attacks and malware

**Incident Threat LockerGoga Ransomware found [LockerGoga Ransomware] [e3b579b5-af69-4a31-9cc2-57428062978c]**

Status: open  
Created at: 09:48:00.175 (3 minutes ago)  
Last update: 09:48:00.175 (3 minutes ago)

Details on INCIDENT/MALICIOUS-FILE  
A compressed archive with some malware inside has been transferred.

Details (at the alert time)  
Source: 10.41.132.168 - a483e7b274c6 - Others  
Destination: 10.41.132.187 - 38f9d3ef2dcf - Others  
Protocol: http (tcp)  
Ports: 49614 - 8000

**Alerts** Page 1 of 2, 6 entries

| ACTIONS... | RISK | TIME         | ID       | TYPE ID               | DESCRIPTION                                | PROTOCOL | IP SRC        | IP DST        | SRC PORT | DST PORT |
|------------|------|--------------|----------|-----------------------|--------------------------------------------|----------|---------------|---------------|----------|----------|
| ***        | High | 09:48:00.175 | 8b77a975 | SIGN-MALWARE-DETECTED | Suspicious transferring of malware name... | http     | 10.41.132.168 | 10.41.132.187 | 49614    | 8000     |
| ***        | High | 09:48:00.175 | 85c8437a | SIGN-MALWARE-DETECTED | Suspicious transferring of malware name... | http     | 10.41.132.168 | 10.41.132.187 | 49614    | 8000     |
| ***        | High | 09:48:00.175 | f7798a6e | SIGN-MALWARE-DETECTED | Suspicious transfer of malware named S...  | http     | 10.41.132.168 | 10.41.132.187 | 49614    | 8000     |
| ***        | High | 09:48:00.175 | 3c8b3a49 | SIGN-MALWARE-DETECTED | Suspicious transferring of malware name... | http     | 10.41.132.168 | 10.41.132.187 | 49614    | 8000     |
| ***        | High | 09:48:00.175 | 96b7b5c4 | SIGN-MALWARE-DETECTED | Suspicious transferring of malware name... | http     | 10.41.132.168 | 10.41.132.187 | 49614    | 8000     |

**Nodes currently involved**

Selection info

- 10.41.132.168
  - appliance host: semith-5C-02
  - ip: 10.41.132.168
  - mac address: a483e7b274c6 (likely)
  - mac vendor: Apple, Inc. (likely)
  - zone: Others
  - type: computer
  - os: macOS 10.14.6
  - vendor: Apple, Inc.
  - is broadcast: false
  - is public: false
  - is confirmed: true
  - is learned: true
  - is fully learned: true
  - is disabled: false
  - roles: other



# Less-Common Discovery: An Infected Network

|                                                                                                                                                                                                                         |      |         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------|
| Suspicious transferring of malware named 'TemplateAttack_DragonFly_2.0' was detected involving resource '\\172.16.0.55\ADMIN\CVcontrolEngineer.docx' after a 'read' operation [rule author: US-CERT Code Analysis Team] | 10.0 | smb     |
| SMB Server Traffic contains NTLM-Authenticated SMBv1 Session                                                                                                                                                            | 10.0 | smb     |
| Protocol smb between 172.16.0.253 and 172.16.0.55 has been confirmed                                                                                                                                                    | 7.5  | smb     |
| New link with protocol smb between 172.16.0.253 and 172.16.0.55                                                                                                                                                         | 7.5  | smb     |
| 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  |
| OS-WINDOWS Microsoft Windows SMB remote code execution attempt                                                                                                                                                          | 10.0 | smb     |
| ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray                                                                                                                                                                     | 10.0 | smb     |
| Protocol tcp/445 between 172.16.0.55 and 172.16.0.253 has been detected as smb application protocol                                                                                                                     | 7.5  | smb     |
| Protocol tcp/445 between 172.16.0.55 and 172.16.0.253 has been confirmed                                                                                                                                                | 7.5  | tcp/445 |
| New link with protocol tcp/445 between 172.16.0.55 and 172.16.0.253                                                                                                                                                     | 7.5  | tcp/445 |
| New tcp/445 node 172.16.0.55                                                                                                                                                                                            | 7.5  | tcp/445 |
| IP 172.16.0.156 is duplicated by MACs: 00:0c:29:28:dd:c5, 00:60:78:00:6a:10                                                                                                                                             | 7.5  | arp     |
| MAC 00:0c:29:28:dd:c5 acts as a man-in-the-middle, his victims are: 172.16.0.156, 172.16.0.253                                                                                                                          | 10.0 | -       |
| IP 172.16.0.253 is duplicated by MACs: 00:04:23:e0:04:1c, 00:0c:29:28:dd:c5                                                                                                                                             | 7.5  | arp     |

9

**Malware detected**  
143656183  
[7e33ed3](#)

**Description**

Suspicious transferring of malware named 'TemplateAttack\_DragonFly\_2.0' was detected involving resource '\\172.16.0.55\ADMIN\CVcontrolEngineer.docx' after a 'read' operation [rule author: US-CERT Code Analysis Team]

**Note:**

|                    | Src               | Dst               |
|--------------------|-------------------|-------------------|
| IP                 | 172.16.0.253      | 172.16.0.55       |
| MAC                | 00:04:23:e0:04:1c | 00:0c:29:28:dd:c5 |
| Label              |                   |                   |
| Port               | 1148              | 445               |
| Roles              | other             | other             |
| Is security        |                   | true              |
| Protocol           |                   | smb               |
| Transport protocol |                   | tcp               |

A potentially malicious payload has been transferred over the network.

[Open details](#)

**Detects known malware and ransomware at all three phases of attack (infection, reconnaissance and lateral movement)**

# Built-in Reports

## Reporting for Greater Visibility

- **Vulnerability Assessment**
  - “What type of security risk are in my environment?”
- **Alerts Report**
  - “What types of Alerts are in my environment?”
  - “How many are open?”
  - “Last 7 days”
  - “Last 30 days”
  - “Total over time”
  - “Top Assets in each alert type?”





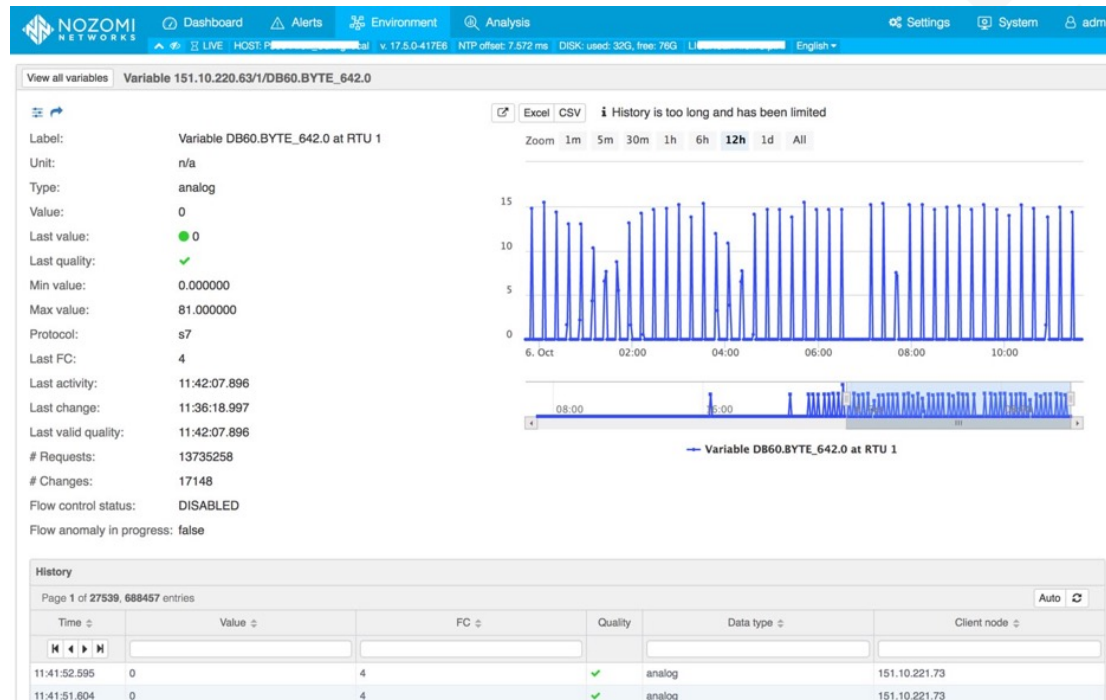
**Lesson Learned**  
**Security Detection !**



## Casi d'uso

*Dettagli sulle variabili di processo, e dialoghi dei sistemi di impianto possono essere determinanti per impedire blocchi di produzione per errori manuali (volontari o dolosi), o per rilevare in anticipo il deteriorarsi di dispositivi che, se sostituiti in manutenzione ordinaria, consentono di impedire il blocco della produzione e la conseguente perdita di denaro.*

# Common Discovery: Abnormal Device Behavior



Detects when asset and processes are deviating from normal, and moving toward states that could disrupt operations



## Common Discovery: Abnormal Device Behavior

### Alert New SCADA variable value [fc481a11-0c0e-4348-a1dc-094da343f255]

\*\*\*

New variable value (9999, expected range is [12062, 12151]) for variable 172.16.0.156/100/r45 (r45 at RTU U00)

Details (at the alert time) Note:

Source: [172.16.0.253](#) - 00:0c:29:28:dd:c5 -

Destination: [172.16.0.156](#) - 00:60:78:00:6a:10

Protocol: modbus (tcp)

Capture device: em1

Ports: 1109 > 502

Status: **open**

Created at: **15:02:35.493** (a few seconds ago)

---

Details on **ViProcNEW-VALUE**

This kind of alert occurs when a variable assumes a value never seen before. It can be an unseen behavior or a malicious attack.

#### Nodes currently involved

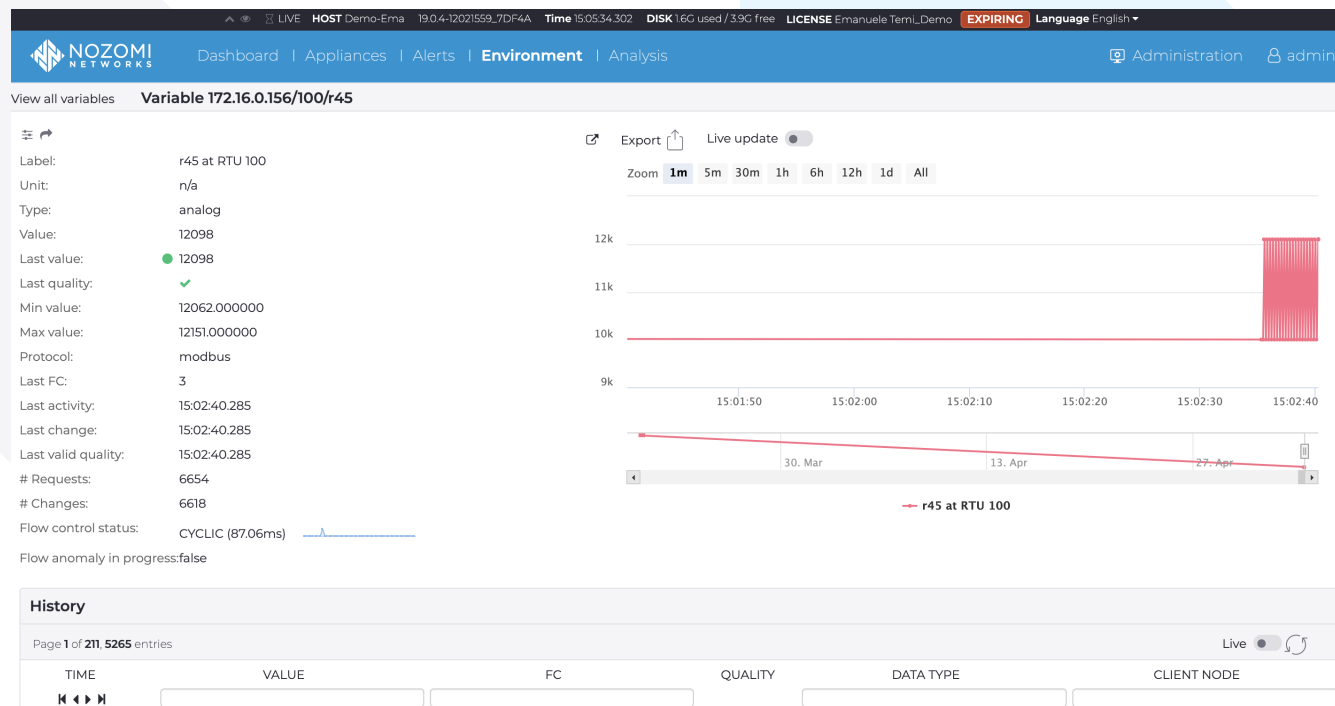
?

#### Selection info

**172.16.0.253**

- > ip: 172.16.0.253
- > mac address: 00:0c:29:28:dd:c5
- > mac vendor: VMware, Inc.
- > zone: ProdNet-A
- > type: computer
- > os: Windows XP SP3
- > vendor: Intel Corporation
- > is broadcast: false
- > is public: false
- > is confirmed: true
- > is learned: true
- > is fully learned: false
- > is disabled: false
- > roles: master
- > links count: 27
- > protocols: dns,modbus,pi-connect,smb,vnc
- > created at: 2020-03-20 10:54:06.418

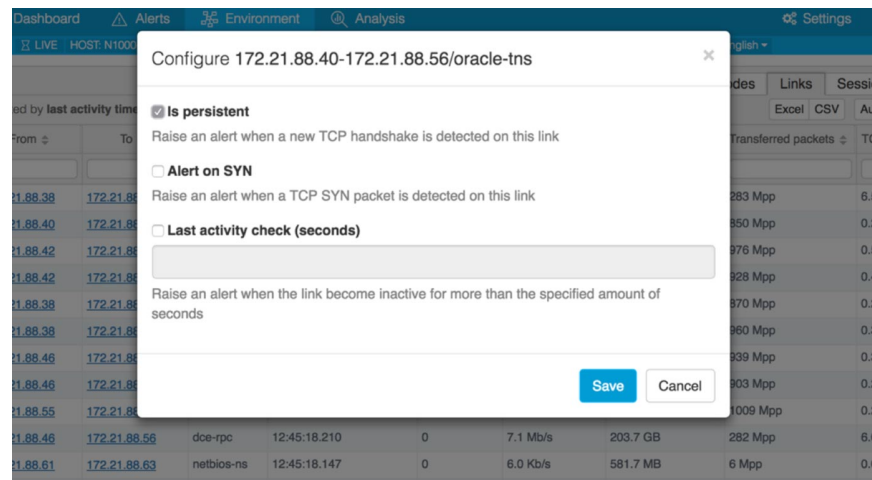
# Common Discovery: Abnormal Device Behavior



Detects when the CYCLIC communication of variable are deviating from normal

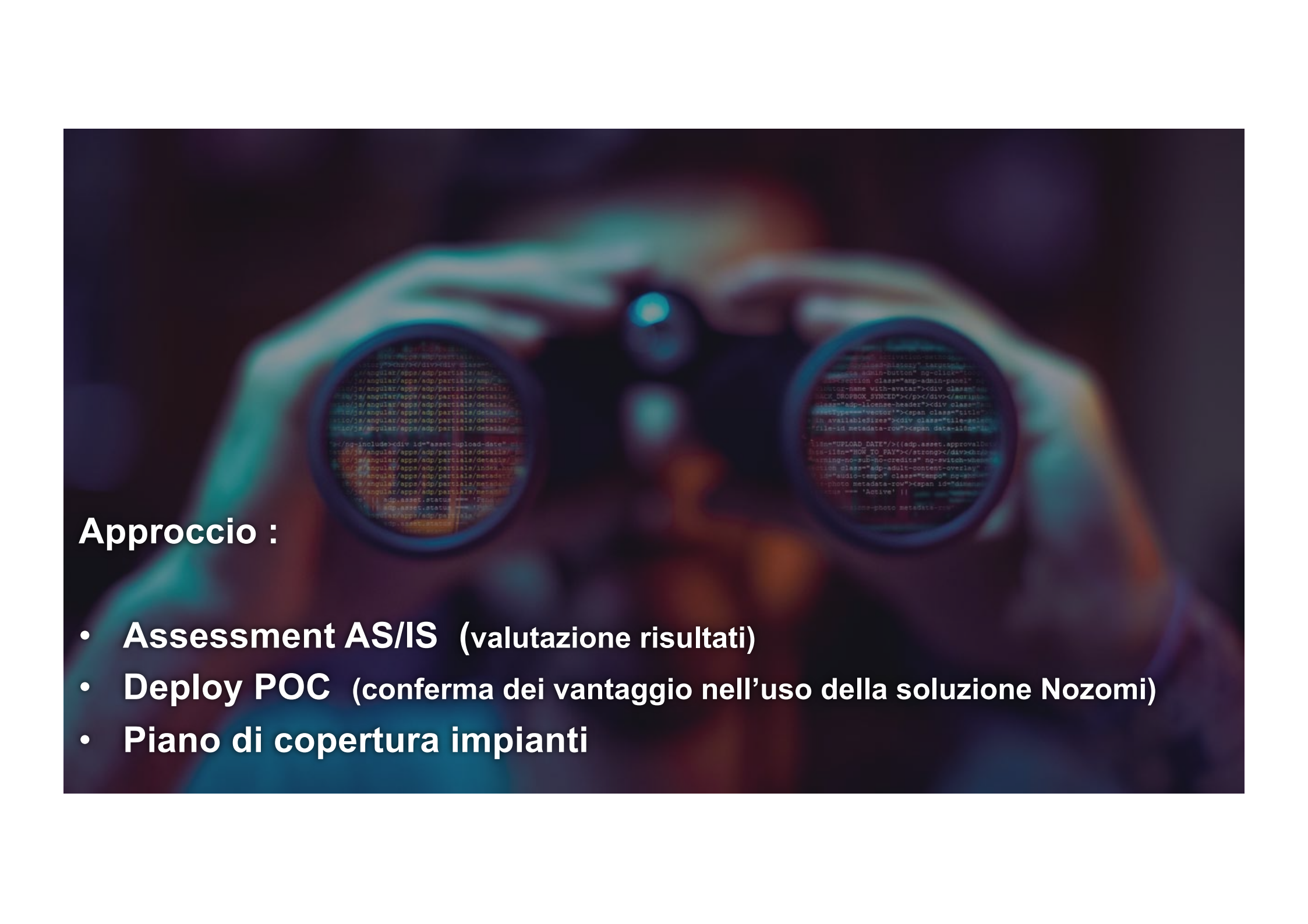
# Pain Point: Custom Alerts

... and create your own alerts, for example:





**Lesson Learned**  
**Process Monitoring !**

A person is wearing a VR headset. The lenses of the headset show snippets of code, likely HTML or JavaScript, which are slightly blurred and have a blue/cyan tint. The background is dark and out of focus.

## Approccio :

- **Assessment AS/IS** (valutazione risultati)
- **Deploy POC** (conferma dei vantaggi nell'uso della soluzione Nozomi)
- **Piano di copertura impianti**





**SINTHERA.COM**  
- KEEP MOVING FORWARD

# DOMANDE ?

Versione Free di Nozomi (Community Edition):

<https://community.nozominetworks.com>

Test Nozomi Networks Solution Live

[marketing@sinthera.com](mailto:marketing@sinthera.com)

+39 0522 621247

[www.sinthera.com](http://www.sinthera.com)



**Sergio Leoni – Regional Sales Director Nozomi Networks**

[Sergio.leoni@nozominetworks.com](mailto:Sergio.leoni@nozominetworks.com)

Mobile +39 335 7301348

# Thank You!

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

[nozominetworks.com](http://nozominetworks.com)