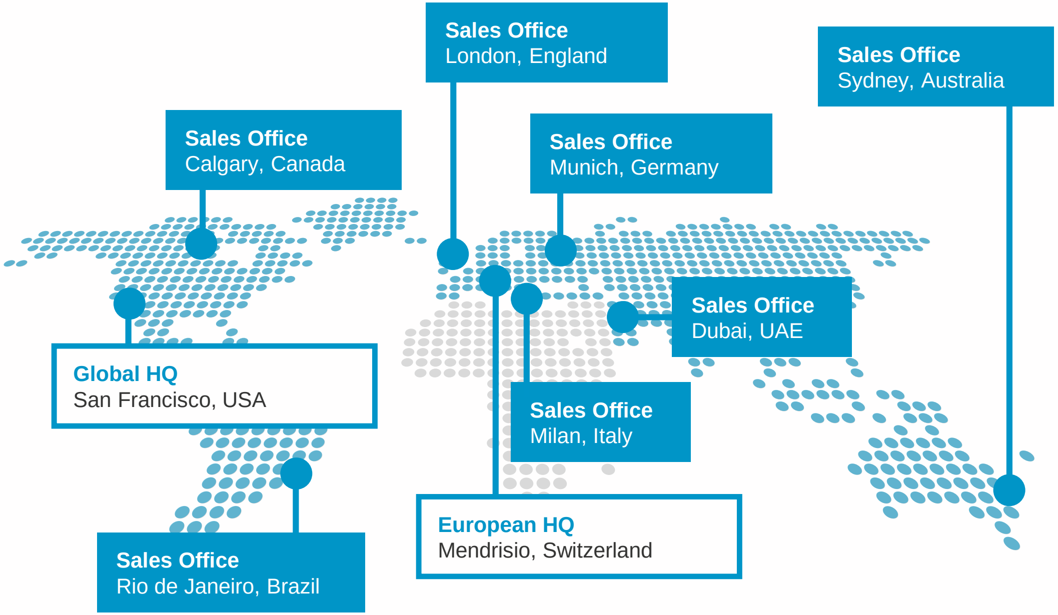
NOZOMI NETWORKS

The Leading Solution for Real-time Cyber Security and Visibility for Industrial Control Networks

Sergio Leoni

Regional Sales Director

Nozomi Networks Today: The Leader in Industrial Cybersecurity



Sales Office
London, England

Sales Office
Sydney, Australia

Sales Office
Calgary, Canada

Sales Office
Munich, Germany

Sales Office
Dubai, UAE

Global HQ
San Francisco, USA

Sales Office
Milan, Italy

European HQ
Mendrisio, Switzerland

Sales Office
Rio de Janeiro, Brazil

FOUNDED
October 2013

CUSTOMERS
+1,000 Global Installations

DEVICES
+300,000 Monitored

DEPLOYMENTS
In 5 Continents

GLOBAL REACH
Local Support

enel | VERMONT ELECTRIC | gsk | *...and more.*

NOZOMI NETWORKS

Industry Awards

NETWORK computing AWARDS 2019 WINNER BENCH TESTED PRODUCT OF THE YEAR
BloombergNEF New Energy Pioneers 2019
INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019
FROST & SULLIVAN 2019 BEST PRACTICES AWARD GLOBAL INDUSTRIAL CYBERSECURITY SOLUTIONS ENABLING TECHNOLOGY LEADERSHIP AWARD
Info Security Products Guide 2019 GLOBAL EXCELLENCE SILVER
INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2018
ASTORS AMERICAN SECURITY TODAY 2018 BRONZE AWARD WINNER
THE CHANNEL CO. CRN EMERGING VENDORS 2018
Gartner Cool Vendor 2017
2017 CUTTING EDGE ICS/SCADA SECURITY SOLUTION CDM
RED HERRING 100 WINNER N. AMERICA
CYBER SECURITY EXCELLENCE AWARDS FINALIST 2017

Market Drivers

IT/OT Convergence
Interconnectedness of non-homogenous systems, applications and platforms

Corporate Espionage
State-sponsored or independently led IP theft, corporate espionage and sabotage

Resilience & Uptime (direct loss of revenue)
Cyber-born or preventative maintenance issues that result in system failure / downtime

Reputation Risk (indirect loss of revenue)
Degradation of company reputation due to data-loss, system shutdown and safety negligence

Safety (Personnel and Environmental)
Failure of cyber-physical system maintenance and a safety systems (i.e. SIS)

National Security Responsibility
Regulatory and tort responsibility to adhere to regional and vertical standards and practice

Nozomi Networks - Our Mission

Achieve Complete Visibility into Your OT Network

Rapidly Detect Vulnerabilities, Threats & Incidents

Reduce Troubleshooting & Remediation Efforts

Successfully Deploy at Scale in the Largest Distributed Environments

Agile Development & Integrations with Rapid New Protocol Support

Centrally Monitor & **Control** Distributed Networks

One Solution. Multiple Options to Meet Your Needs.

SCADAguardian

PASSIVE

SCADAguardian Advanced

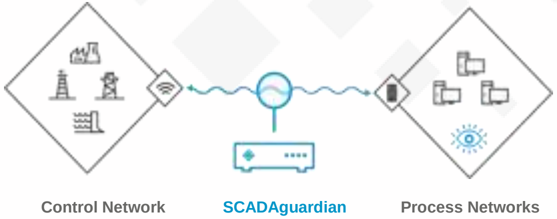
PASSIVE + ACTIVE

Central Management Console

OT ThreatFeed Service

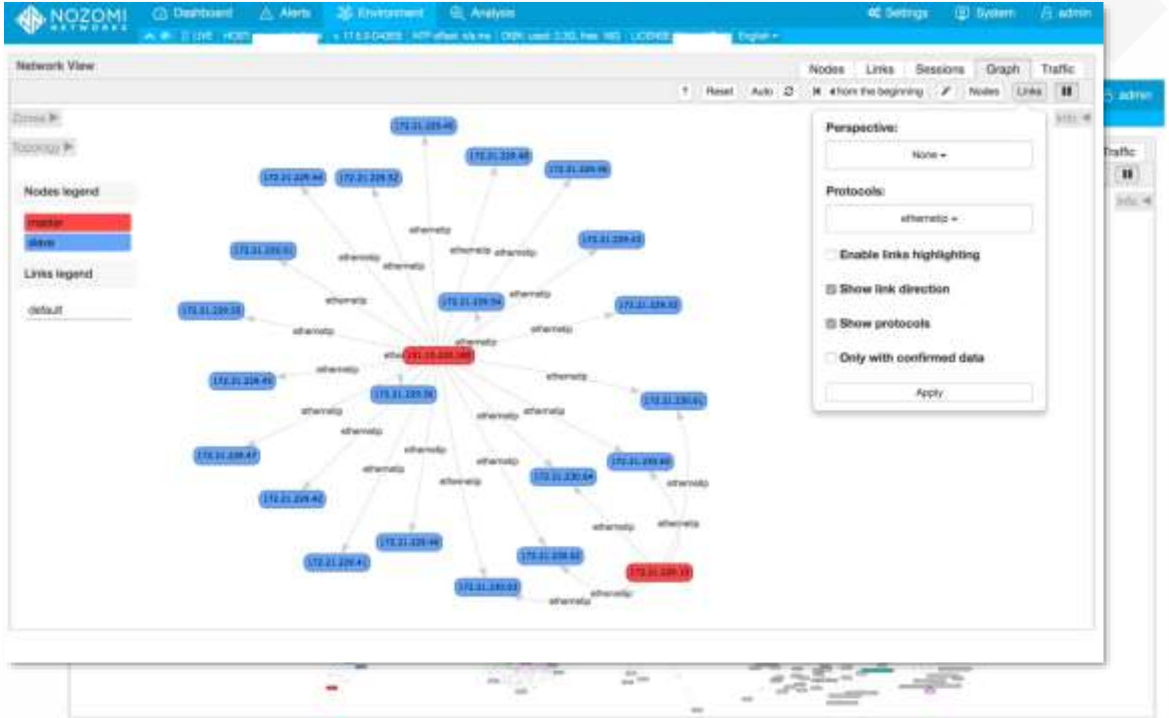
Nozomi Networks SCADAguardian

SCADAguardian protects your control networks from cyber attacks and operational disruptions by providing unprecedented visibility and rapid detection of threats and process risks – in a completely passive way.



- An appliance (physical or virtual) that passively and non-intrusively connects to the industrial network
- Listens to all traffic within the control and process networks, passively analyzing it at all levels of the OSI stack (L1 to L7)
- Uses artificial intelligence and machine learning techniques to create detailed behavior profiles for every device according to the process state to quickly detect critical state conditions
- Provides best-in-class network visualization, asset management, ICS anomaly intrusion, vulnerability assessment, as well as dashboards and reporting

Network Visualization and Monitoring



Perspective:

None ▾

Protocols:

ethernetip ▾

☐ Enable links highlighting

☑ Show link direction

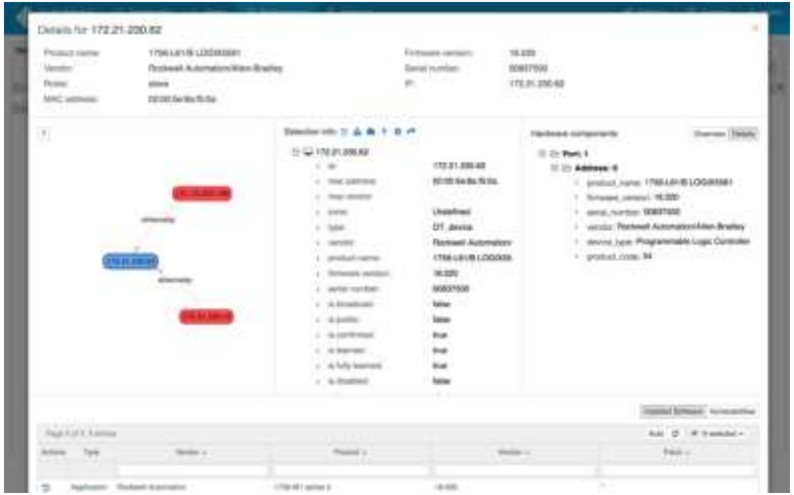
☑ Show protocols

☐ Only with confirmed data

Apply

Network Visualization and Monitoring

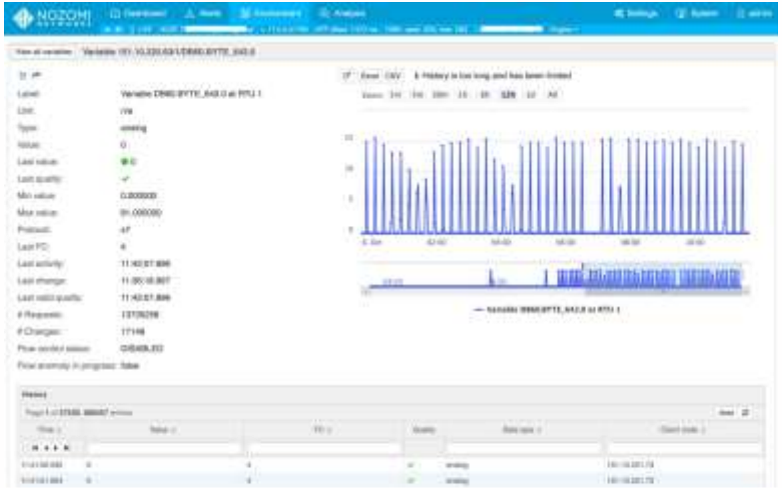
Go deep in details…



Details for 172.21.200.82

Product name:	1756-L61/B LOGIX5561	Firmware version:	16.020
Vendor:	Rockwell Automation/Allen-Bradley	Serial number:	00837500
Role:	slave	IP:	172.21.200.82
MAC address:	[illegible]		

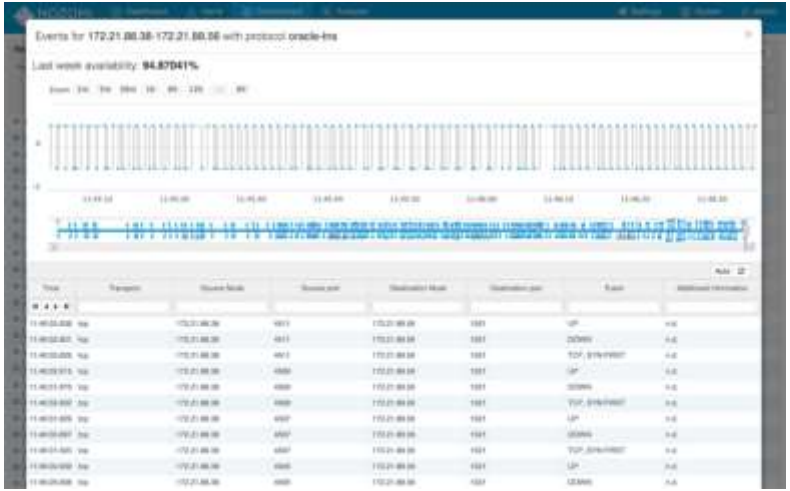
Nodes



Variables

Network Visualization and Monitoring

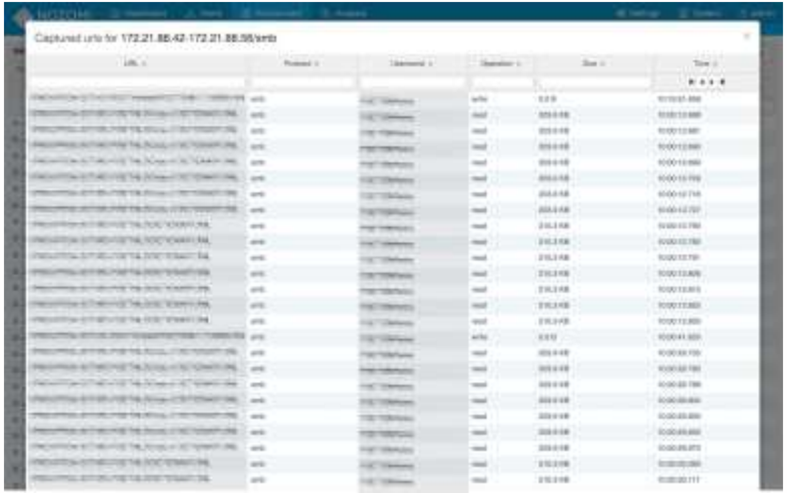
Go deep in details…



Events for 172.21.88.38-172.21.88.98 with protocol oracle-tns

Last week availability: 94.87041%

Links



Captured urls for 172.21.88.42-172.21.88.98/smb

Contents

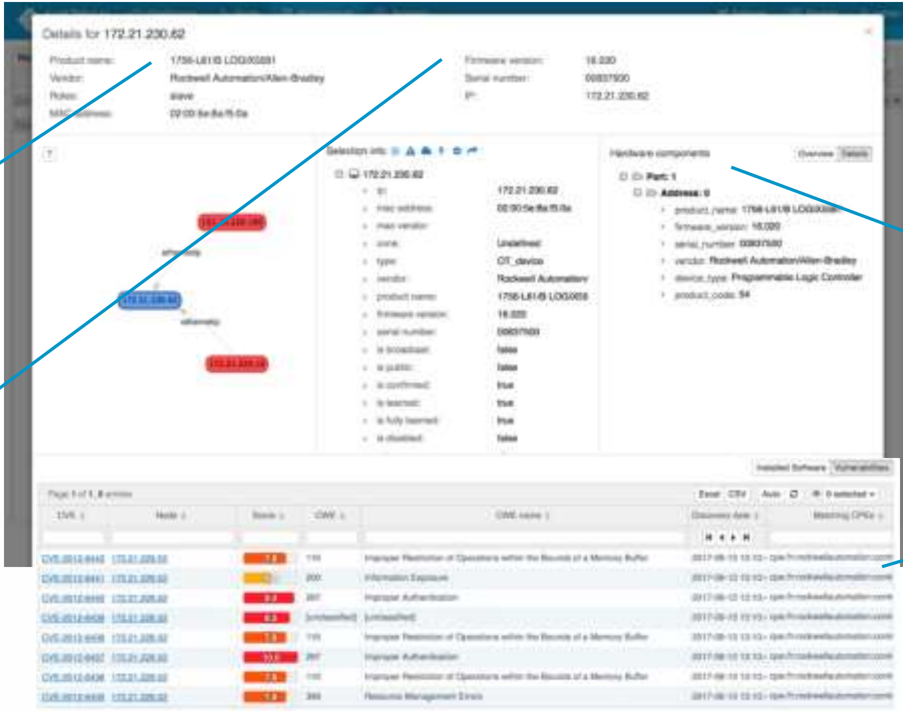
Asset Inventory

Product Name Vendor

Firmware version of the PLCs

Hardware Components

Vulnerabilities



Details for 172.21.230.62

Product name:	1756-L61/B LOGIX5561	Firmware version:	16.020
Vendor:	Rockwell Automation/Allen-Bradley	Serial number:	00837500
Roles:	slave	IP:	172.21.230.62
MAC address:	00:00:5e:8a:f5:0a		

Selection info:

□ 172.21.230.62

id:	172.21.230.62
mac address:	00:00:5e:8a:f5:0a
mac vendor:	
zone:	Undefined
type:	OT_device
vendor:	Rockwell Automation/
product name:	1756-L61/B LOGIX556
firmware version:	16.020
serial number:	00837500
is broadcast:	false
is public:	false
is confirmed:	true
is learned:	true
is fully learned:	true
is disabled:	false

Hardware components

Overview Details

□ Part: 1

□ Address: 0

- product_name: 1756-L61/B LOGIX556
- firmware_version: 16.020
- serial_number: 00837500
- vendor: Rockwell Automation/Allen-Bradley
- device_type: Programmable Logic Controller
- product_code: 54

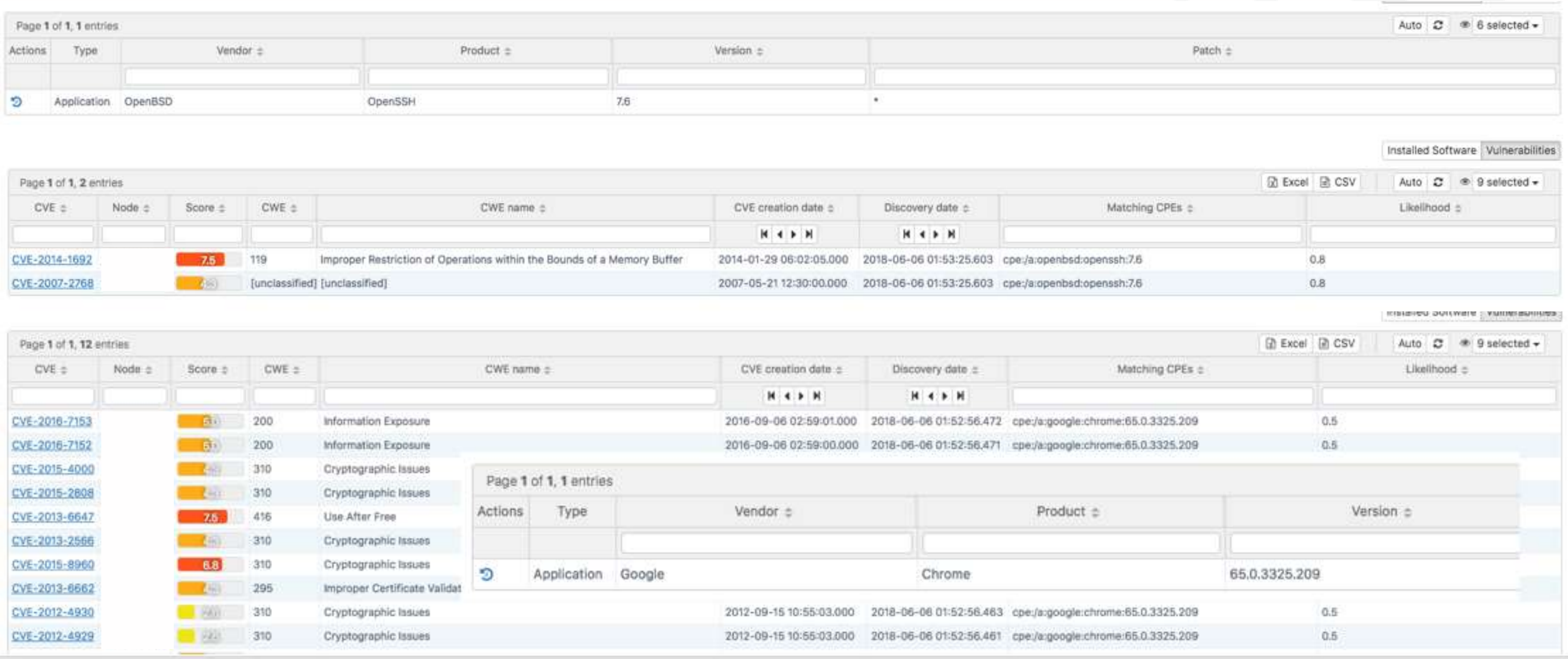
Installed Software Vulnerabilities

Page 1 of 1, 8 entries

Excel CSV Auto 0 selected

CVE	Node	Score	CWE	CWE name	Discovery date	Matching CPEs
CVE-2012-6442	172.21.226.32	7.8	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-08-13 13:13	cpe:/h:rockwellautomation:contr
CVE-2012-6441	172.21.226.32	[illegible]	200	Information Exposure	2017-08-13 13:13	cpe:/h:rockwellautomation:contr
CVE-2012-6440	172.21.226.32	9.4	287	Improper Authentication	2017-08-13 13:13	cpe:/h:rockwellautomation:contr
CVE-2012-6439	172.21.226.32	8.3	(unclassified)	(unclassified)	2017-08-13 13:13	cpe:/h:rockwellautomation:contr
CVE-2012-6438	172.21.226.32	7.8	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-08-13 13:13	cpe:/h:rockwellautomation:contr
CVE-2012-6437	172.21.226.32	10.0	287	Improper Authentication	2017-08-13 13:13	cpe:/h:rockwellautomation:contr
CVE-2012-6436	172.21.226.32	7.8	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-08-13 13:13	cpe:/h:rockwellautomation:contr
CVE-2012-6435	172.21.226.32	7.8	399	Resource Management Errors	2017-08-13 13:13	cpe:/h:rockwellautomation:contr

Common Discovery: Software Vulnerabilities



Page 1 of 1, 1 entries

Actions	Type	Vendor	Product	Version	Patch
⟲	Application	OpenBSD	OpenSSH	7.6	*

Page 1 of 1, 2 entries

CVE	Node	Score	CWE	CWE name	CVE creation date	Discovery date	Matching CPEs	Likelihood
CVE-2014-1692		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
CVE-2007-2768		[illegible]	[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

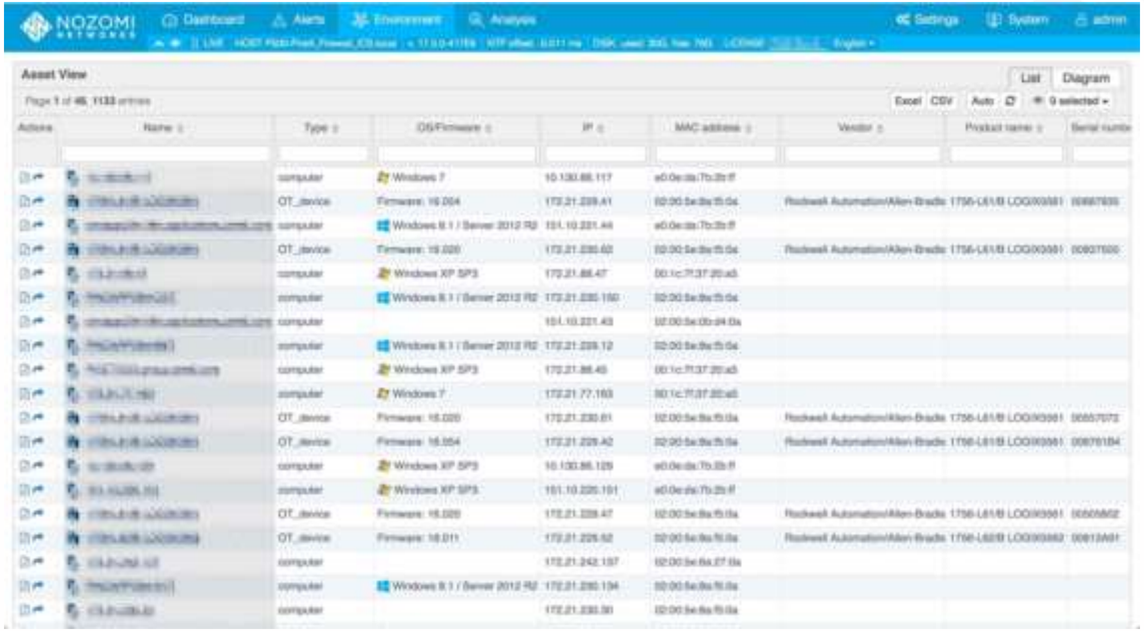
CVE	Node	Score	CWE	CWE name	CVE creation date	Discovery date	Matching CPEs	Likelihood
CVE-2016-7153		[illegible]	200	Information Exposure	2016-09-06 02:59:01.000	2018-06-06 01:52:56.472	cpe:/a:google:chrome:65.0.3325.209	0.5
CVE-2016-7152		[illegible]	200	Information Exposure	2016-09-06 02:59:00.000	2018-06-06 01:52:56.471	cpe:/a:google:chrome:65.0.3325.209	0.5
CVE-2015-4000		[illegible]	310	Cryptographic Issues				
CVE-2015-2808		[illegible]	310	Cryptographic Issues				
CVE-2013-6647		7.6	416	Use After Free				
CVE-2013-2566		[illegible]	310	Cryptographic Issues				
CVE-2015-8960		6.8	310	Cryptographic Issues				
CVE-2013-6662		[illegible]	295	Improper Certificate Validat				
CVE-2012-4930		[illegible]	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
CVE-2012-4929		[illegible]	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: Multiple OS/Firmware Versions



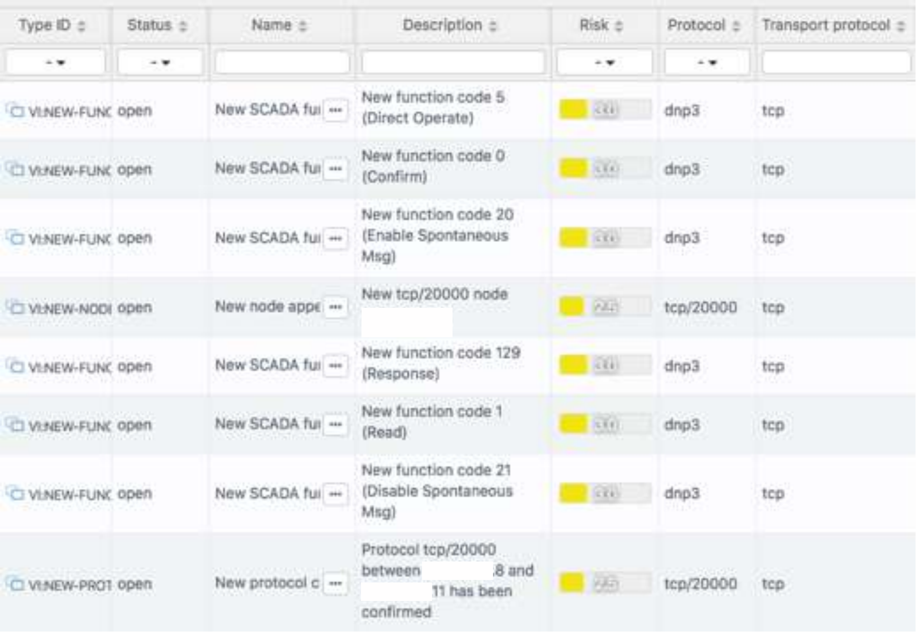
Asset View

Page 1 of 46, 1133 entries

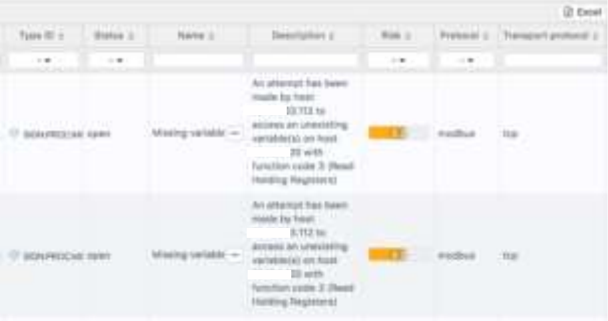
Actions	Name	Type	OS/Firmware	IP	MAC address	Vendor	Product name	Serial number
	[redacted]	computer	Windows 7	10.130.88.117	a0:0e:da:7b:2b:ff			
	[redacted]	OT_device	Firmware: 16.004	172.21.229.41	02:00:5e:8a:f5:0a	Rockwell Automation/Allen-Bradle	1756-L61/B LOGIX5561	00687835
	[redacted]	computer	Windows 8.1 / Server 2012 R2	151.10.221.44	a0:0e:da:7b:2b:ff			
	[redacted]	OT_device	Firmware: 16.020	172.21.230.60	02:00:5e:8a:f5:0a	Rockwell Automation/Allen-Bradle	1756-L61/B LOGIX5561	00607500
	[redacted]	computer	Windows XP SP3	172.21.88.47	00:1c:7f:37:20:a5			
	[redacted]	computer	Windows 8.1 / Server 2012 R2	172.21.230.150	02:00:5e:8a:f5:0a			
	[redacted]	computer		151.10.221.43	02:00:5e:0b:d4:0a			
	[redacted]	computer	Windows 8.1 / Server 2012 R2	172.21.229.12	02:00:5e:8a:f5:0a			
	[redacted]	computer	Windows XP SP3	172.21.88.45	00:1c:7f:37:20:a5			
	[redacted]	computer	Windows 7	172.21.77.163	00:1c:7f:37:20:a5			
	[redacted]	OT_device	Firmware: 16.020	172.21.230.61	02:00:5e:8a:f5:0a	Rockwell Automation/Allen-Bradle	1756-L61/B LOGIX5561	00557072
	[redacted]	OT_device	Firmware: 16.054	172.21.229.42	02:00:5e:8a:f5:0a	Rockwell Automation/Allen-Bradle	1756-L61/B LOGIX5561	00676184
	[redacted]	computer	Windows XP SP3	10.130.86.129	a0:0e:da:7b:2b:ff			
	[redacted]	computer	Windows XP SP3	151.10.226.101	a0:0e:da:7b:2b:ff			
	[redacted]	OT_device	Firmware: 16.020	172.21.229.47	02:00:5e:8a:f5:0a	Rockwell Automation/Allen-Bradle	1756-L61/B LOGIX5561	00605802
	[redacted]	OT_device	Firmware: 18.011	172.21.225.52	02:00:5e:8a:f5:0a	Rockwell Automation/Allen-Bradle	1756-L62/B LOGIX5562	00613A01
	[redacted]	computer		172.21.242.137	02:00:5e:6a:27:0a			
	[redacted]	computer	Windows 8.1 / Server 2012 R2	172.21.230.134	02:00:5e:8a:f5:0a			
	[redacted]	computer		172.21.230.30	02:00:5e:8a:f5:0a			

Identifies opportunities to reduce operational risk by closing vulnerability gaps

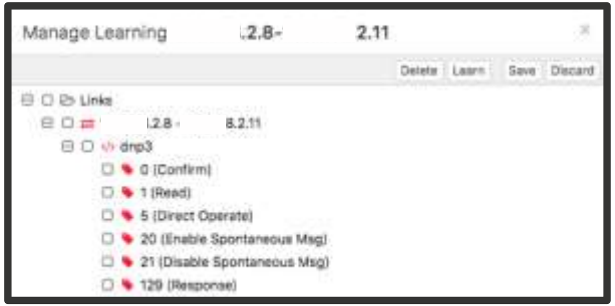
Common Discovery: Unknown & Misconfigured Devices



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



Type ID	Status	Name	Description	Risk	Protocol	Transport protocol
SIGN:PROC:[illegible]	open	Missing variable	An attempt has been made by host 10.112 to access an unexisting variable(s) on host 20 with function code 3 (Read Holding Registers)	[illegible]	modbus	tcp
SIGN:PROC:[illegible]	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)	[illegible]	modbus	tcp

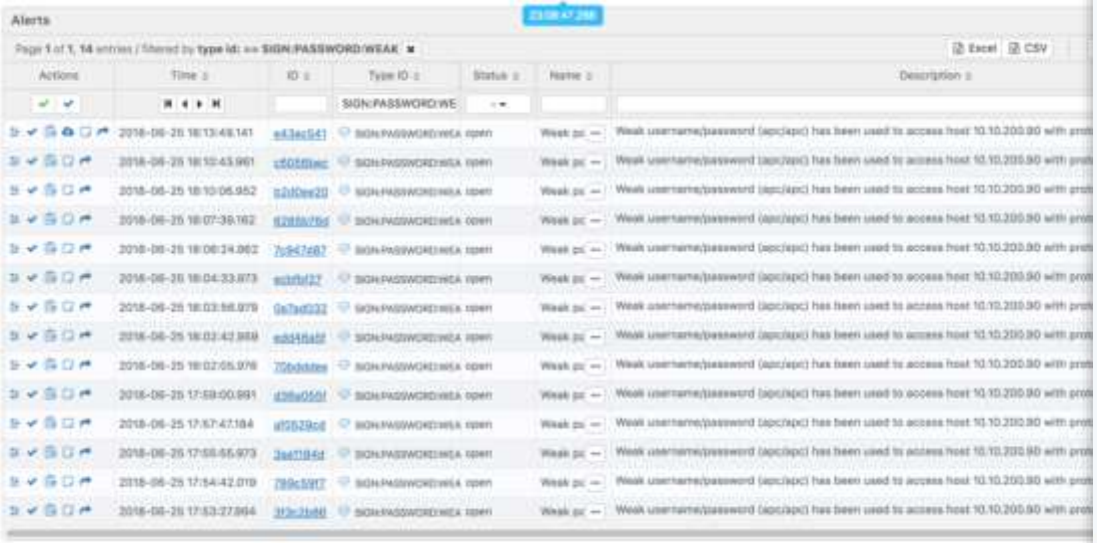


Manage Learning .2.8- 2.11

- ⊟ □ Links
  - ⊟ □ .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

Common Discovery: Unencrypted / Weak Credentials

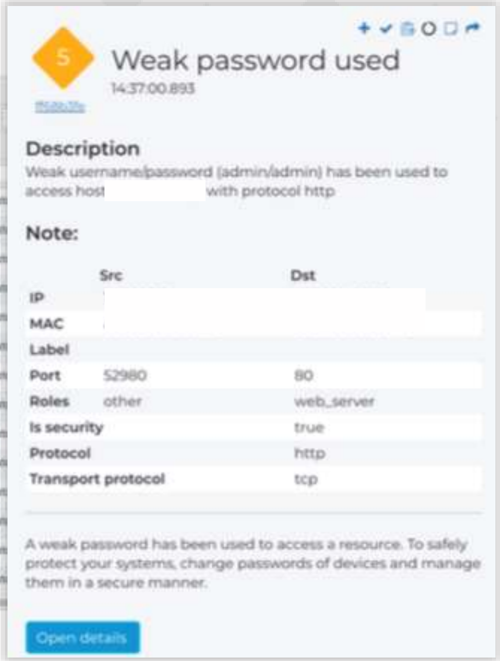


Alerts

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

Excel CSV

Actions	Time	ID	Type ID	Status	Name	Description
✓ ✓	⏮ ◀ ▶ ⏭		SIGN:PASSWORD:WE	- ▾		
	2018-06-25 18:13:48.141	e43ac541	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 18:10:43.961	c6058bac	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 18:10:06.952	82d0ee20	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 18:07:39.162	8288b76d	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 18:06:24.062	7c947e87	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 18:04:33.873	ecbfbf27	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 18:03:56.979	0a7ad032	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 18:02:43.988	edd4fa8f	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 18:02:05.976	70bddbee	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 17:59:00.991	d36a056f	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 17:57:47.184	af5529cd	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 17:55:55.973	3a47184d	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 17:54:42.019	789c5917	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot
	2018-06-25 17:53:27.964	3f3c2b80	SIGN:PASSWORD:WEA	open	Weak pa	Weak username/password (apc/apc) has been used to access host 10.10.200.90 with prot



5

Weak password used

14:37:00.893

Description

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

Note:

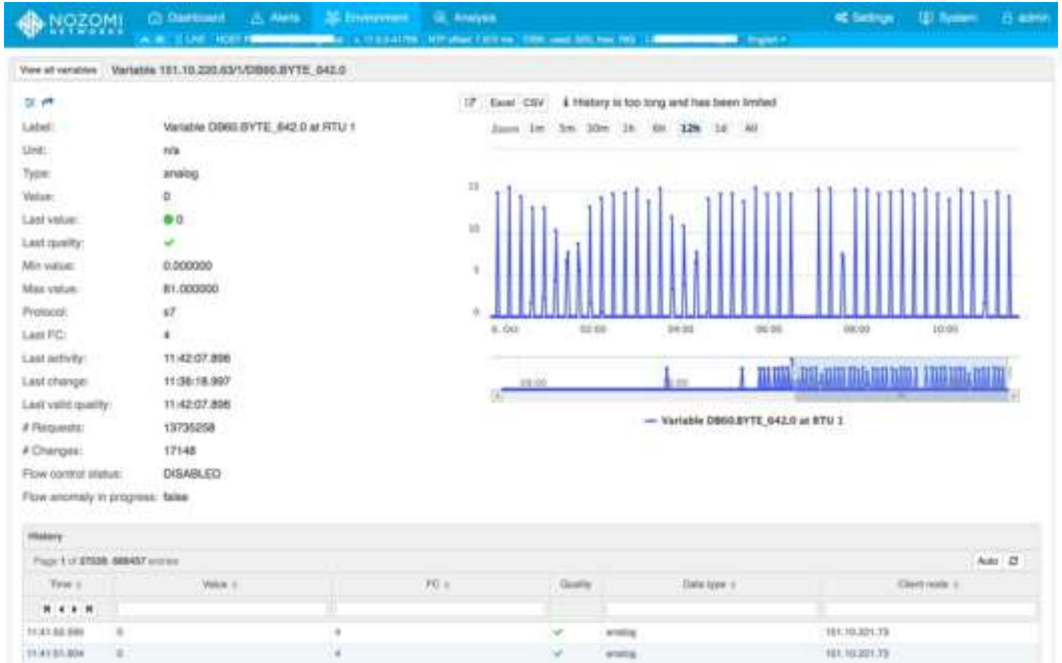
	Src	Dst
IP		
MAC		
Label		
Port	52980	80
Roles	other	web_server
Is security		true
Protocol		http
Transport protocol		tcp

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

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

Common Discovery: Abnormal Device Behavior



Variable 151.10.220.63/1/DB60.BYTE_642.0

History is too long and has been limited

Label:	Variable DB60.BYTE_642.0 at RTU 1
Unit:	n/a
Type:	analog
Value:	0
Last value:	● 0
Last quality:	✓
Min value:	0.000000
Max value:	81.000000
Protocol:	s7
Last FC:	4
Last activity:	11:42:07.898
Last change:	11:38:18.997
Last valid quality:	11:42:07.898
# Requests:	13735258
# Changes:	17148
Flow control status:	DISABLED
Flow anomaly in progress:	false

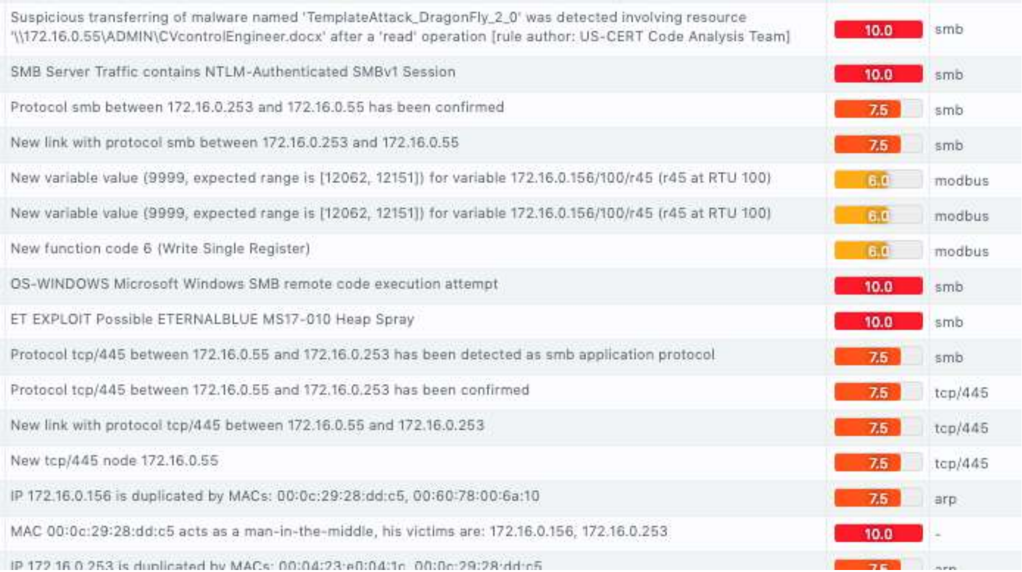
History

Page 1 of 27538, 688457 entries

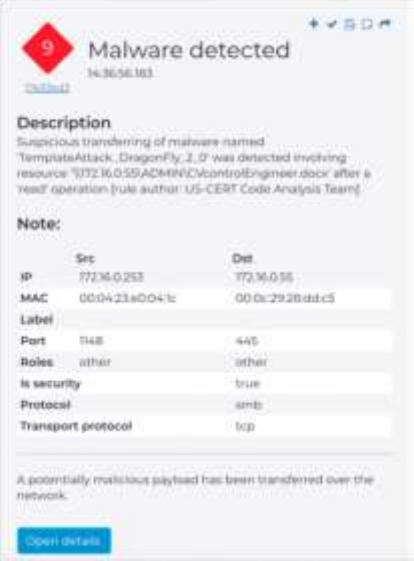
Time	Value	FC	Quality	Data type	Client node
11:41:52.580	0	4	✓	analog	151.10.221.73
11:41:51.804	0	4	✓	analog	151.10.221.73

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

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



Malware detected

14:36:56.183

[illegible]

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

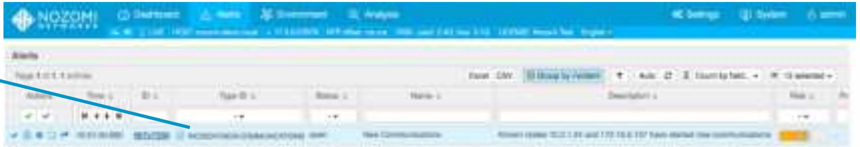
A potentially malicious payload has been transferred over the network.

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

Hybrid ICS Threat Detection

Thanks to Anomaly Detection, all deviations from the baseline can be alerted at different levels

A new communication is detected

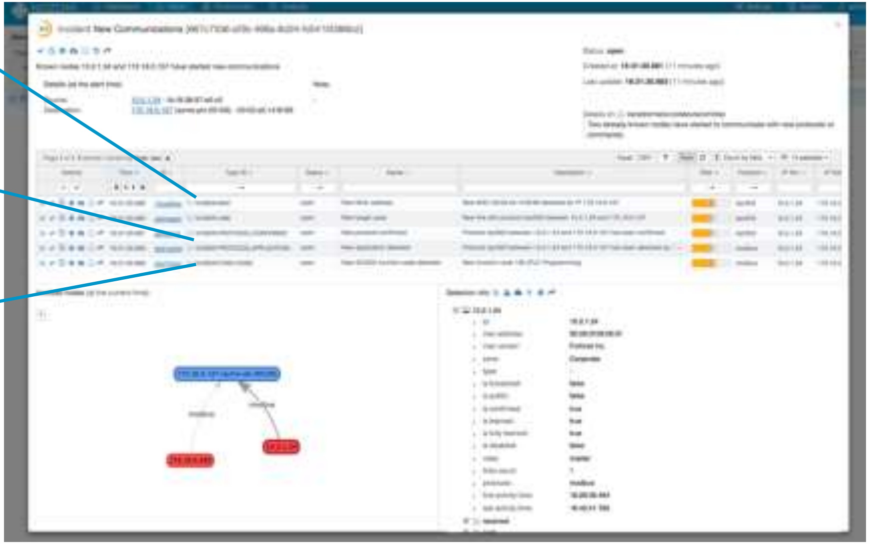


NEW INCIDENT

A ”rogue” MAC address is identified

A new Modbus connection is detected

A Modbus Reprogram Command is detected

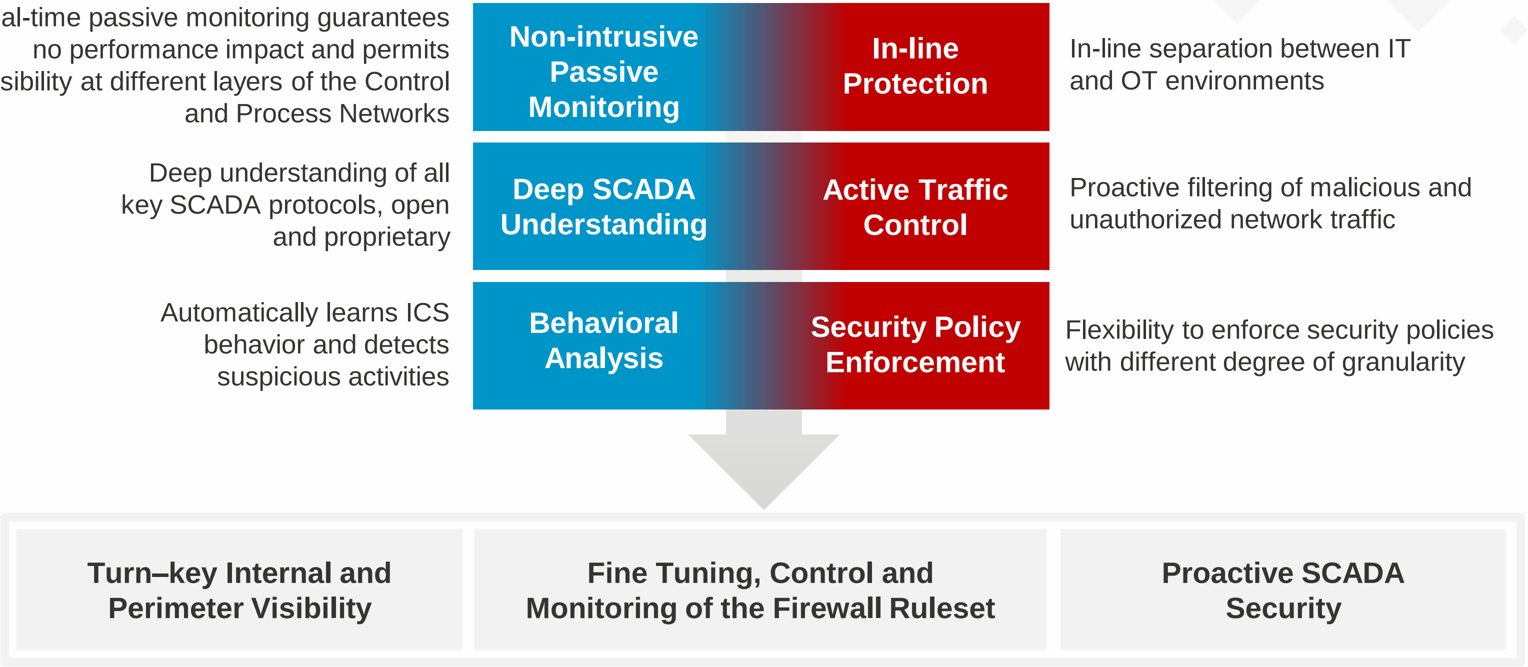


pcap traces of the attack are automatically generated

INCIDENT DETAILS

The Fortinet / Nozomi Networks Capabilities

NOZOMI NETWORKS FORTINET



Real-time passive monitoring guarantees no performance impact and permits visibility at different layers of the Control and Process Networks

Non-intrusive Passive Monitoring

In-line Protection

In-line separation between IT and OT environments

Deep understanding of all key SCADA protocols, open and proprietary

Deep SCADA Understanding

Active Traffic Control

Proactive filtering of malicious and unauthorized network traffic

Automatically learns ICS behavior and detects suspicious activities

Behavioral Analysis

Security Policy Enforcement

Flexibility to enforce security policies with different degree of granularity

Turn–key Internal and Perimeter Visibility

Fine Tuning, Control and Monitoring of the Firewall Ruleset

Proactive SCADA Security

Grazie

Sergio Leoni

Regional Sales Director

sergio.leoni@nozominetworks.com