NOZOMI NETWORKS

Cybersecurity Audit for Critical Infrastructure

<Client Name>

Ausit Report

Prepared by <SE name>

<date>

Content

- Executive Summary
- Architecture and Methodology
- Network Visibility & Asset Inventory
- Findings
- OT Risks & Implications

Executive Summary

Objectives

- Minimize potential business disruptions to <client>'s operational industrial environments
- Ensure the highest possible resiliency of <client>'s Industrial environment
- Gain full centralized visibility of their industrial network environments
- Monitor the security posture of those environments
- Enable swift response and remediation actions when a security incident or potential disruption of the production environment occurs

Results

Nozomi Networks Guardian solution has been proven to provide the key Operational Technology Cyber Security functionality required by <client>, including:

- Network asset discovery and inventory management
- Continuous real-time network monitoring
- Reporting and risk analysis
- <client> required technical integrations
- Ability to effectively roll-out the solution globally (Scalability)

Long-term Commitment: Nozomi Networks will evolve its solution is looking forward to working with <client> to bolster Operational Technology, Cyber Security and reduce risk.

Executive Summary of Findings

Cyber Security	• Clear text passwords, weak passwords being used, multiple unsuccessful logins • Frequent network scanning • BoT (Network already infected) found and destroyed during PoC • Excessively high number of vulnerabilities
Networking	• Good use of Cisco standards for SIP phones • Some hosts communicating on protocols that shouldn't be in high risk networks SMBv1 • Potential Exfiltration of data from CoD networks
Operational	• High levels of upload traffic from many sources • ICMP scans from At&t that need validated as useful or necessary

Architecture & Methodology

Architecture and Methodology

Appliances at two sites::

- <Site1> 1x N1000
- <Site2> 1x R50
- Central Management Console (CMC) in <client datacenter>

- Networks Monitored:
- Start Date:
- End Date
- Guardian Version:
- Learning Strategy:
- Learining Time (days):
- Zones Configured (Yes/No)
- Integrations Tested:
  - Active Directory
  - SIEM (Splunk)

Guardian Summary Dashboards

Environment information

Assets	Nodes	Links	Protocols	Sessions	Variables
91	232	294	27	0	50
	232 active	294 active	27 active 25 IT and 2 OT	0 active	50 active

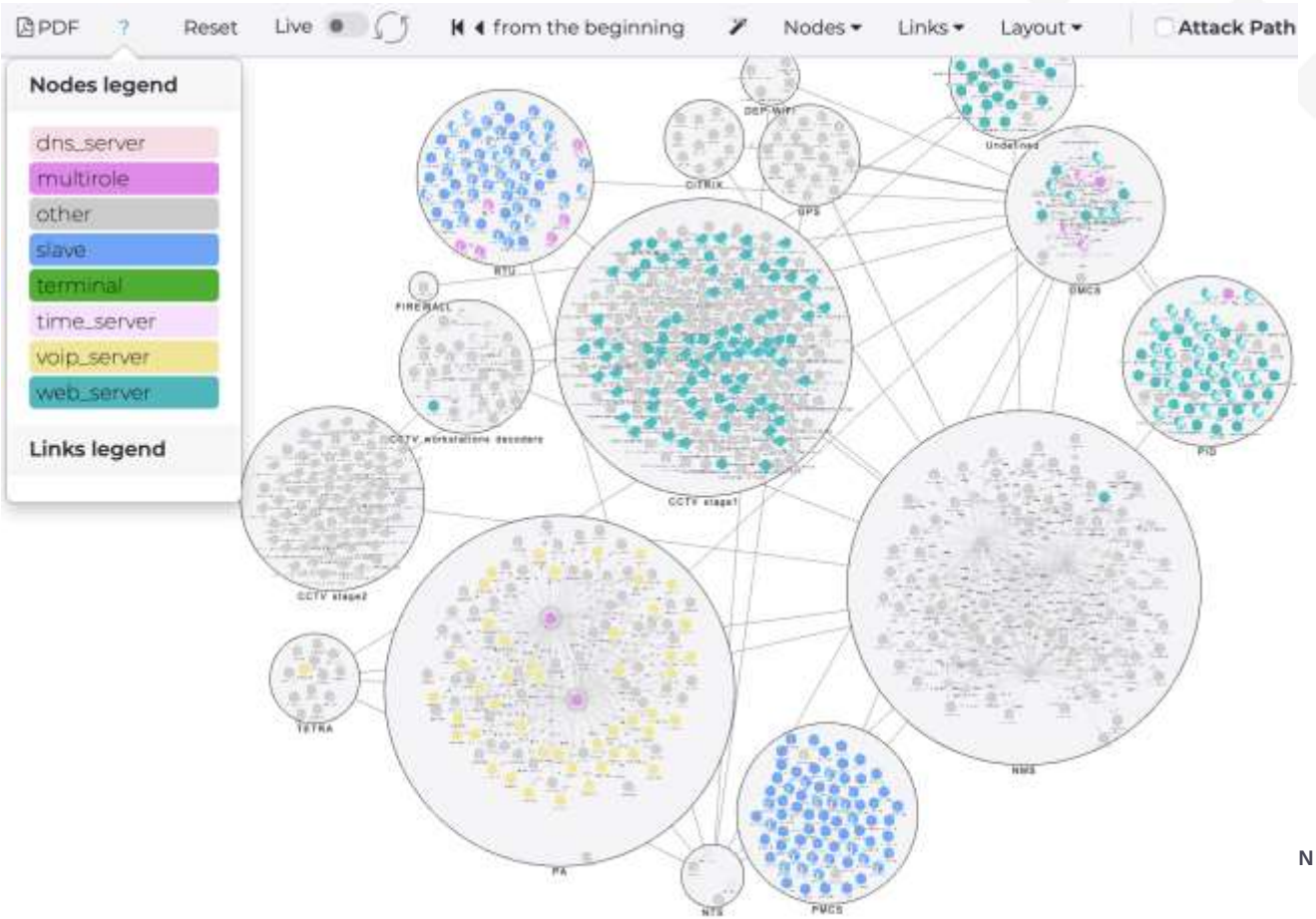
Level 1			
	1 Computer	10 PLCs	7 OT Devices
	8 HMIs	46 <unknown>	

Situational awareness

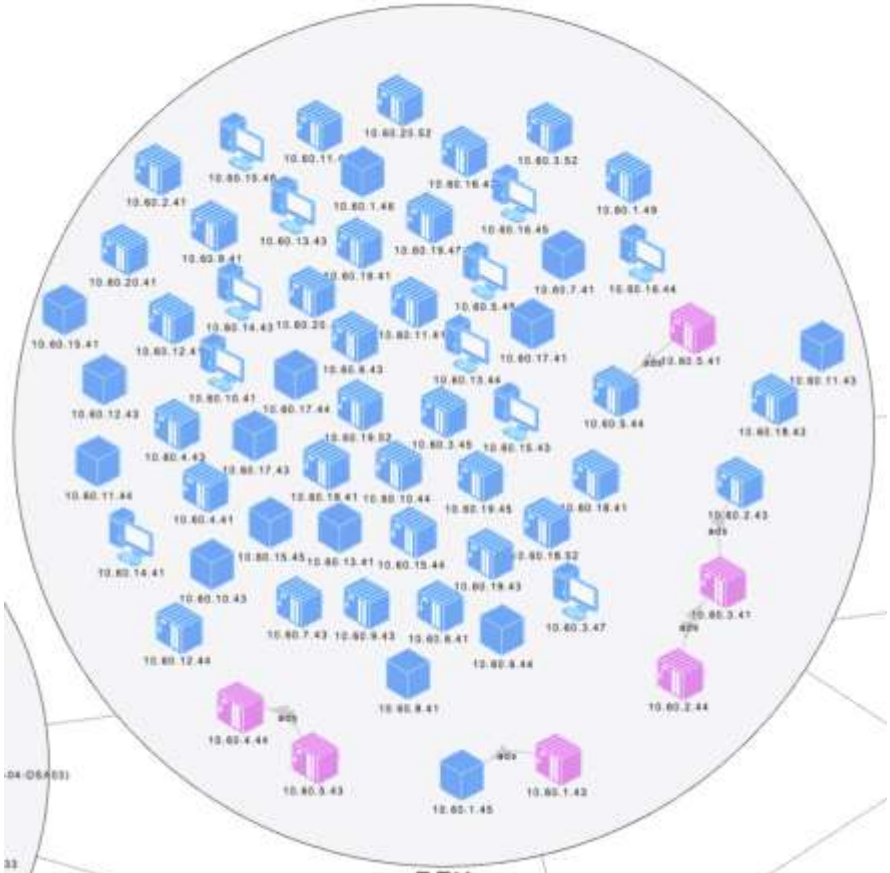
- There are **12** Unidentified Assets.
- **1** attempted links to Public Internet.
- There are **49** open Vulnerabilities.
- There are **9** different types of technology.
- **13** Assets are governing the process.
- There are **1** Engineering stations.
- There are **2** different Operating Systems.

Network Visibility
&
Asset Inventory

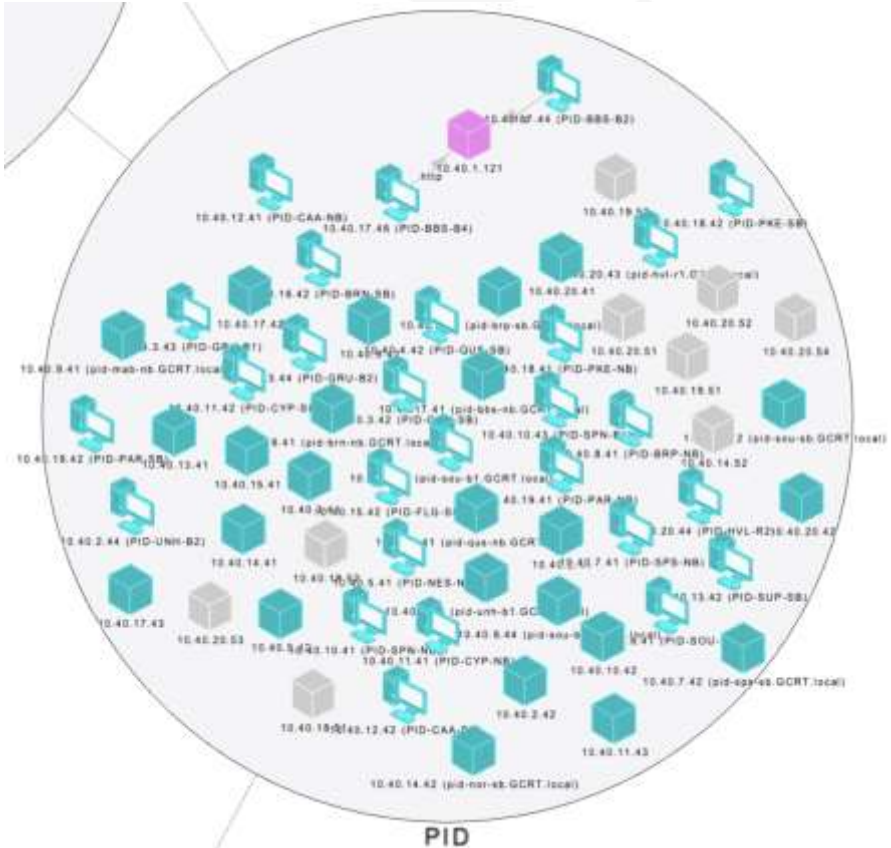
Network Graph View - Overall Network (Grouped by Zones)



Network Graph View - Overall Network (RTU and PID Zones Example)

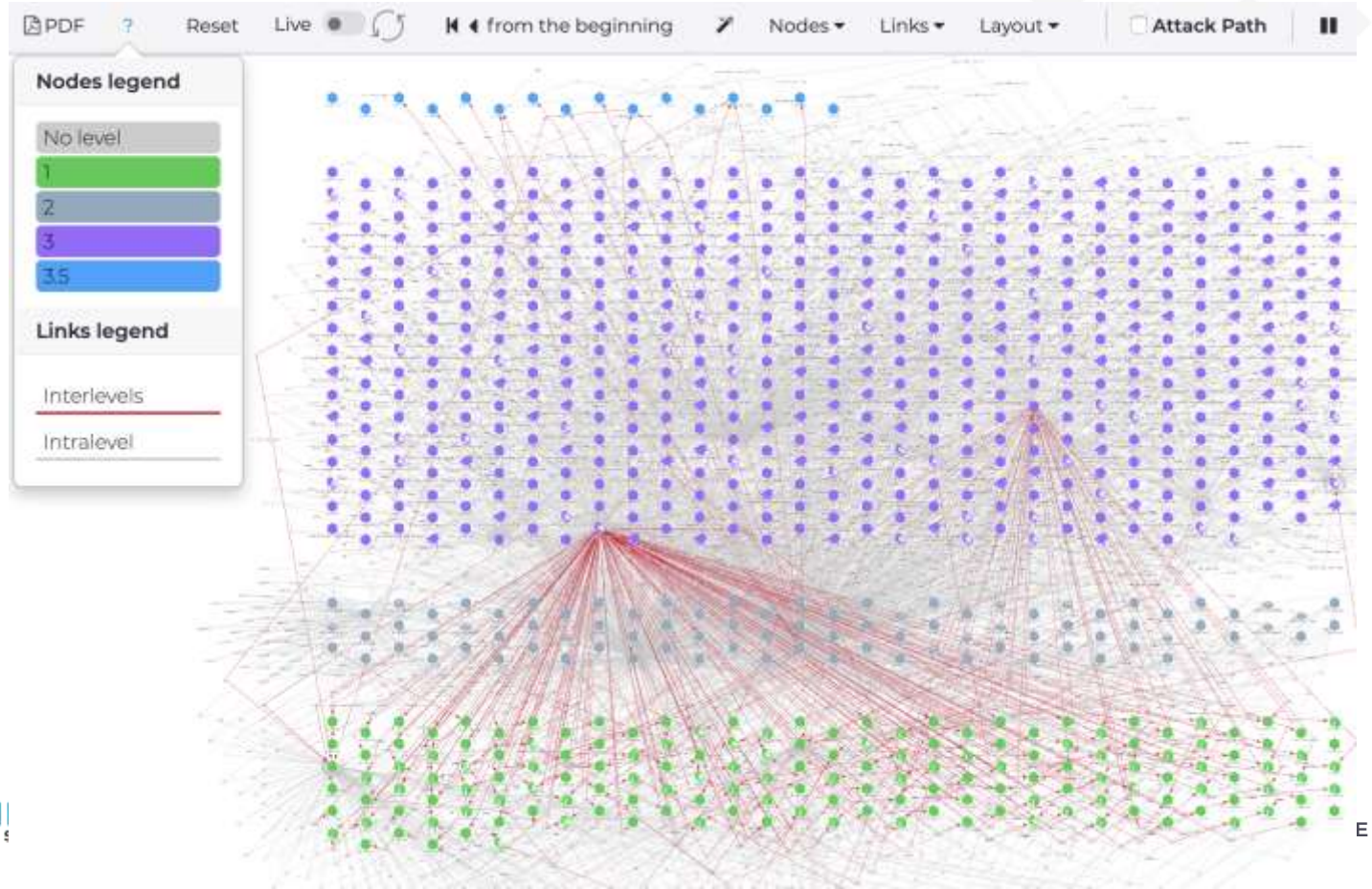


RTU

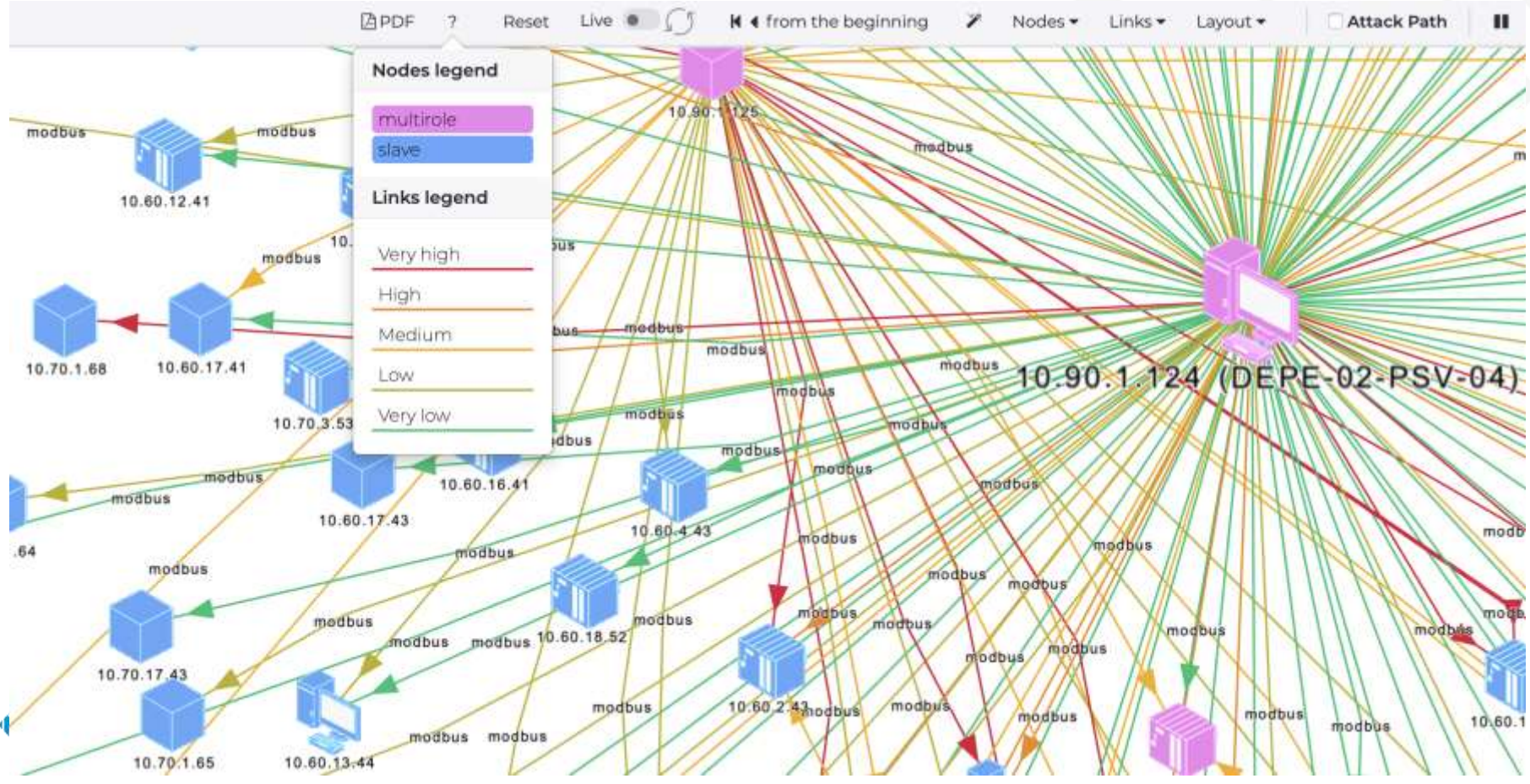


PID

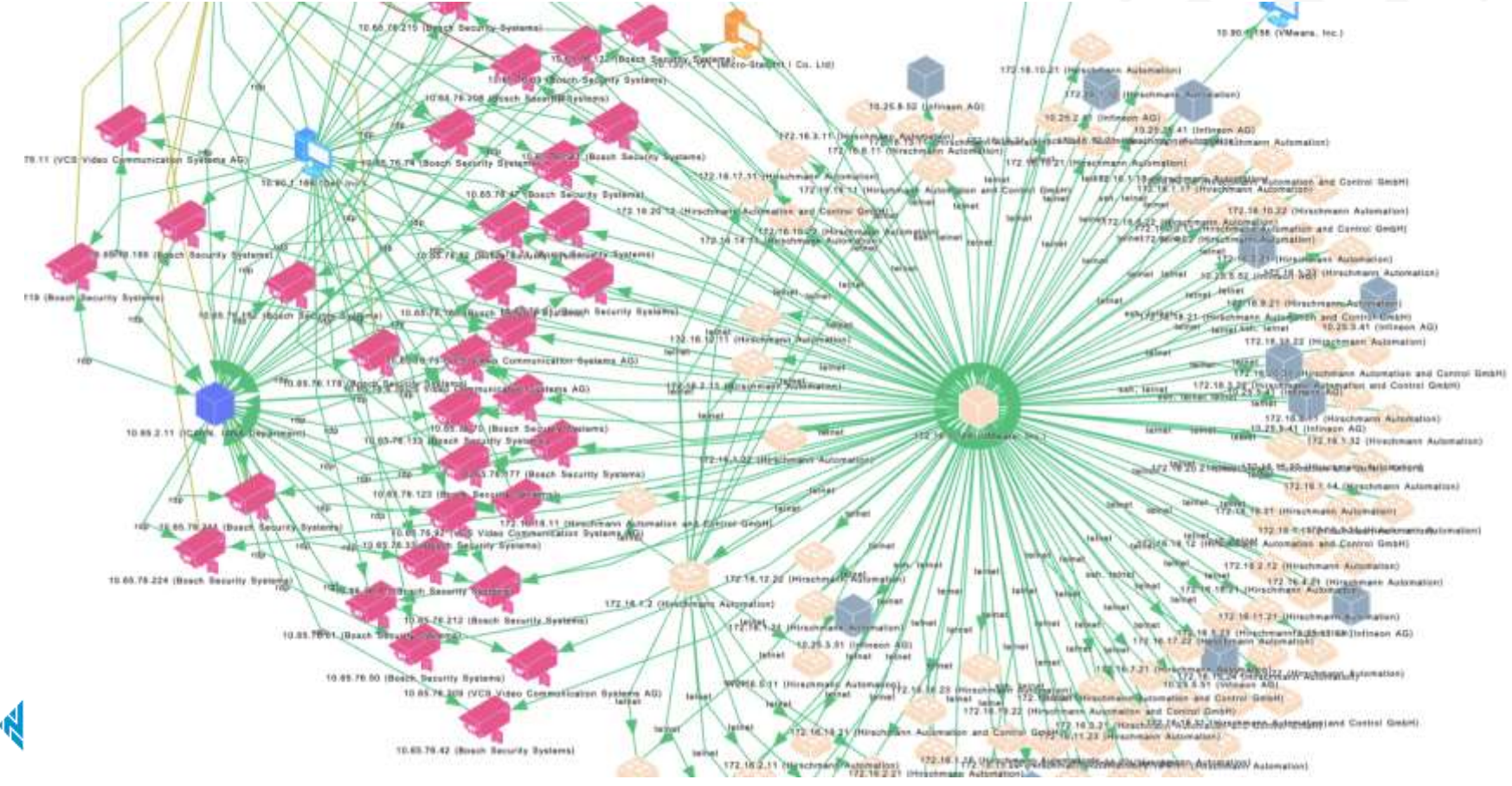
Network Graph View - Overall Network (Purdue Model)



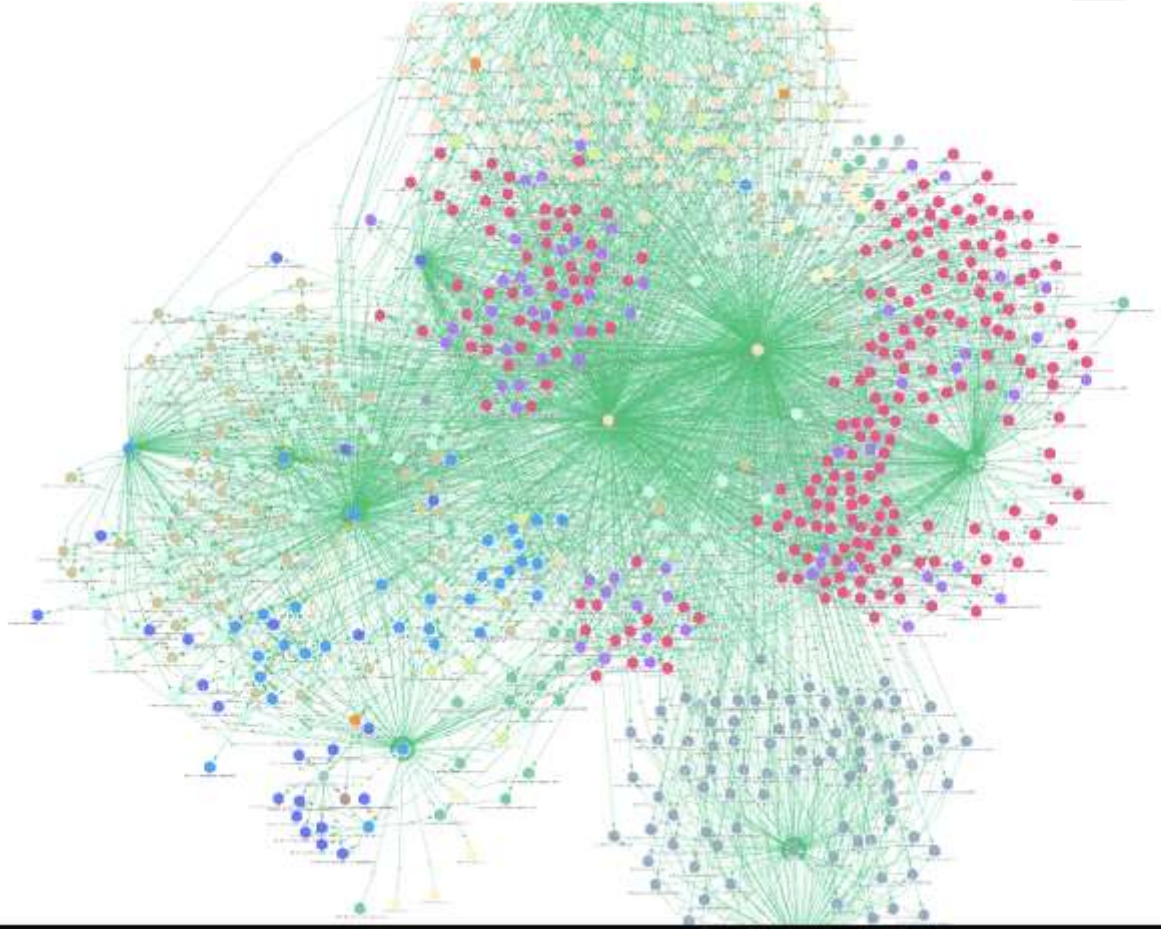
Network Graph View – Close Up (Modbus Links)



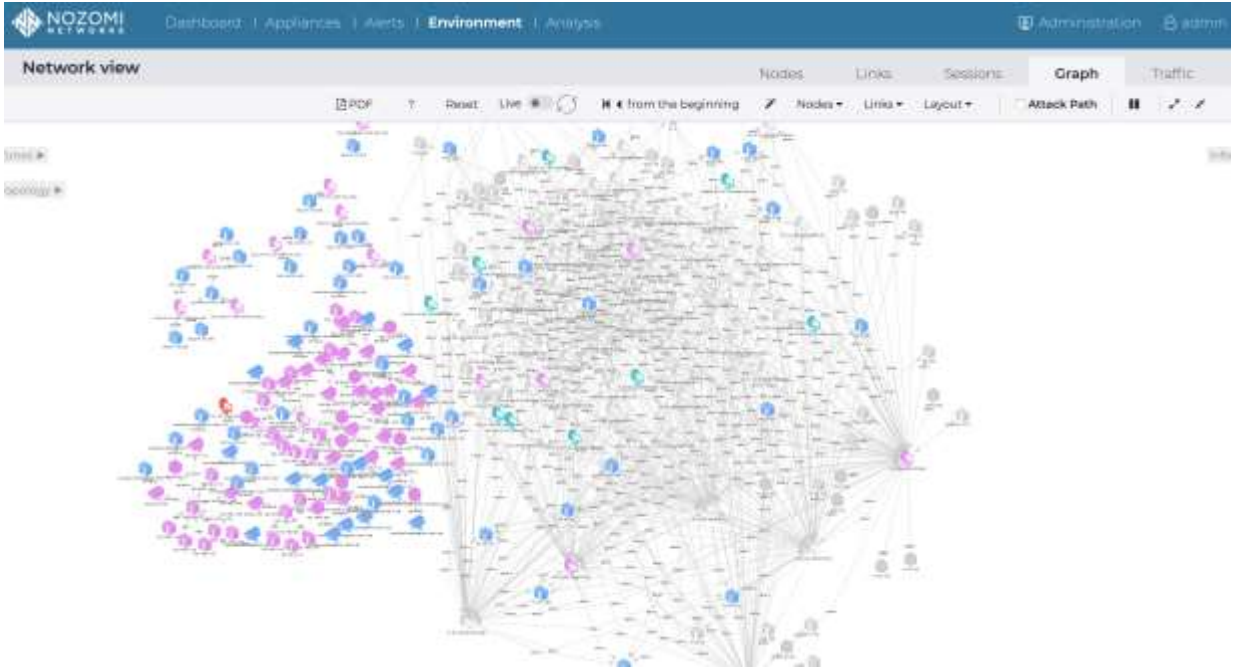
Network Graph View – Remote Access



Network Graph View – Plain Text Protocols



OT Protocols discovered in <client>’s Network



- Ethernetip
- Ethernetip-implicit
- Rockwell-cps2
- DeltaV
- Dlms-cosem
- Ge-strp
- Melsoft
- Modbus-rtu
- Sel-serial
- slmp

Protocols and Links Retransmissions greater than 20%

ads
bacnet-ip
browser
dce-rpc
dhcpv6
dlms-cosem
dns
ftp
ge-egd
gvcp
http
https
iec104
igmp
kerberos
kms
ldap
lldp
llmnr
mdns
modbus
mqtt
netbios-ns
ntp
oracle-tns
other
rdp
roc
rtcp
rtsp
s8000
sel-serial
sip
smb
snmp
ssdp
ssh
stp
syslog
tcp/20000
tcp/44818
telnet

from	to	protocol	
172.16.1.121	10.90.1.122	other	22.6%
172.16.1.121	13.107.4.50	http	39.9%
10.40.19.41	10.90.1.122	dce-rpc	29.0%
10.90.1.154	10.90.1.121	dce-rpc	23.4%
10.0.0.59	10.90.1.121	smb	30.5%
10.40.17.46	10.90.1.125	http	28.8%
10.40.2.44	10.90.1.122	dce-rpc	25.4%
10.40.20.41	10.90.1.122	dce-rpc	20.9%
10.40.20.44	10.90.1.122	dce-rpc	27.6%
172.16.1.125	10.40.1.121	http	30.4%
10.65.76.131	10.10.1.128	other	21.4%
10.40.2.41	10.90.1.121	dce-rpc	20.3%
10.40.19.42	10.90.1.122	dce-rpc	24.8%
10.40.20.42	10.90.1.122	dce-rpc	26.0%
10.40.18.41	10.90.1.122	dce-rpc	21.5%
10.40.18.42	10.90.1.122	dce-rpc	25.4%

Asset Inventory (Sample)

NAME	TYPE	OS/FIRMWARE	IP	MAC ADDRESS	MAC VENDOR	ROLES	LEVEL	VENDOR...	PR
EN100_E+ TPS_BK02/SIPB15A	OT_device		10.70.19.49	b4:b1:5a:00:aa:cc	Siemens AG Energy Managemen	slave	1	Siemens AG	
I6__-02-RTU01	OT_device	Windows CE 6.0	10.60.4.43	00:01:05:44:14:fe	Beckhoff Automation GmbH	slave	1	Beckhoff Aut	
SPN_-02-RTU01	OT_device	Windows CE 6.0	10.60.10.41	00:01:05:11:40:2c	Beckhoff Automation GmbH	master, slave	1	Beckhoff Aut	
I8__-02-RTU01	OT_device	Windows CE 6.0	10.60.5.43	00:01:05:12:1a:4e	Beckhoff Automation GmbH	master, slave	1	Beckhoff Aut	
BBS_-02-RTU01	OT_device	Windows CE 6.0	10.60.17.41	00:01:05:11:a5:e4	Beckhoff Automation GmbH	master, slave	1	Beckhoff Aut	
DEPJ-02-RTU01	OT_device	Windows CE 6.0	10.60.1.43	00:01:05:11:40:1e	Beckhoff Automation GmbH	master, slave	1	Beckhoff Aut	
SOUJ-02-RTU01	OT_device	Windows CE 6.0	10.60.6.43	00:01:05:45:b5:ce	Beckhoff Automation GmbH	slave	1	Beckhoff Aut	
UNHE-02-RTU01	OT_device	Windows CE 6.0	10.60.2.41	00:01:05:11:41:2e	Beckhoff Automation GmbH	master, slave	1	Beckhoff Aut	
FLG_-02-RTU01	OT_device	Windows CE 6.0	10.60.15.41	00:01:05:21:84:d8	Beckhoff Automation GmbH	master, slave	1	Beckhoff Aut	
10.70.19.51	OT_device		10.70.19.51	28:63:36:ab:6b:b6	Siemens AG	slave	1	Siemens AG	
I28_-02-RTU01	OT_device	Windows CE 6.0	10.60.11.44	00:01:05:12:1a:76	Beckhoff Automation GmbH	slave	1	Beckhoff Aut	

Asset Details (OT Device)

Asset Details (Windows)

Asset Details (IP Camera Controller)

Process View (Sample)

HOST	HOST LABEL	LABEL	TYPE	VALUE	LAST VALUE	PROTOC...	# CHANGES
10.70.1.71		r114 at RTU 0	analog	nan	0	modbus	2064973
10.60.6.41	SOU_-02-RTU01	ir30062 at RTU 0	analog	nan	260	modbus	673720
10.70.5.49		r114 at RTU 0	analog	nan	32768	modbus	645150
10.60.13.41	SUP_-02-RTU01	ir30062 at RTU 0	analog	nan	327	modbus	589497
10.60.4.41	QUS_-02-RTU01	ir30062 at RTU 0	analog	nan	305	modbus	586058
10.70.1.41		r5 at RTU 0	analog	nan	792	modbus	574057
10.70.1.41		r4 at RTU 0	analog	nan	794	modbus	565796
10.70.3.53		r54 at RTU 0	analog	nan	538	modbus	561490
10.70.17.49		r114 at RTU 0	analog	nan	0	modbus	554156
10.60.4.41	QUS_-02-RTU01	ir30063 at RTU 0	analog	nan	300	modbus	550757
10.70.1.49		r114 at RTU 0	analog	nan	0	modbus	545297
10.70.18.52		r44 at RTU 0	analog	nan	15	modbus	515147
10.70.3.53		r25 at RTU 0	analog	nan	798	modbus	511045
10.70.1.63		r5 at RTU 0	analog	nan	789	modbus	504351
10.70.1.63		r4 at RTU 0	analog	nan	791	modbus	503811
10.70.15.49		r114 at RTU 0	analog	nan	0	modbus	496824
10.70.1.62		r4 at RTU 0	analog	nan	790	modbus	484771
10.70.1.62		r5 at RTU 0	analog	nan	790	modbus	483200
10.70.3.53		r15 at RTU 0	analog	nan	793	modbus	479093
10.70.3.50	EN100_E+ TPS_7K02/SIPB	ir9 at RTU 1	analog	nan	1101	modbus	470555
10.70.3.50	EN100_E+ TPS_7K02/SIPB	ir8 at RTU 1	analog	nan	1107	modbus	470405

Process View (Sample - Modbus)

View all variables **Variable 10.70.1.41/0/r5**

Label:	r5 at RTU 0
Unit:	n/a
Type:	analog
Value:	nan
Last value:	792
Last quality:	✓
Min value:	0.000000
Max value:	1000.000000
Protocol:	modbus
Last FC:	3
Last activity:	2020-02-26 09:19:25.299
Last change:	2020-02-26 09:19:25.299
Last valid quality:	2020-02-26 09:19:25.299
# Requests:	653669
# Changes:	574057
Flow control status:	DISABLED

Findings

Vulnerabilities Summary

Vulnerability Average Score

Number of hosts with vulnerabilities

0

Number of vulnerabilities

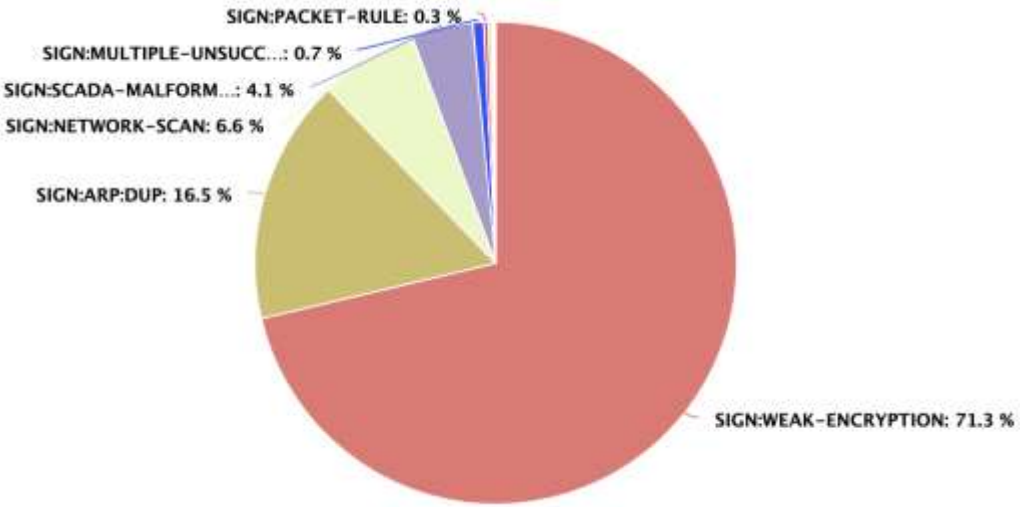
0

Vulnerability Total Score

0.0

ASSET	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS
		Firmware			
DEP2W2	switch	Firmware: 09.0.16	5		5
I4_W1	switch	Firmware: 09.0.16	5		5
DEPWT1	switch	Firmware: 09.0.16	5		5
DEPEV2	switch	Firmware: 09.0.16	5		5

Alerts Summary



PROC:WRONG-TIME

SIGN:ARP:DUP

SIGN:MULTIPLE-UNSUCCESSFUL-LOGINS

SIGN:NETWORK-SCAN

SIGN:PACKET-RULE

SIGN:PROC:MISSING-VAR

SIGN:PROC:UNKNOWN-RTU

SIGN:SCADA-MALFORMED

SIGN:TCP-SYN-FLOOD

SIGN:UNSUPPORTED-FUNC

Main alerts and types

GROUP	RISK AVG	COUNT
INCIDENT:NEW-NODE	7.33	200
INCIDENT:NEW-COMMUNICATIONS	4	164
INCIDENT:INTERNET-NAVIGATION	5.95	41
SIGN:ARP:DUP	3	17
SIGN:INVALID-IP	7.0	5
VI:NEW-ARP	6.0	4
VI:NEW-FUNC-CODE	6.0	1
VI:NEW-PROTOCOL:CONFIRMED	3	1
VI:NEW-PROTOCOL	6.0	1
INCIDENT:PORT-SCAN	7.5	1

These are the main alerts picked up by Guardian during the PoC.
We will focus the analysis on the most relevant in terms of risk.

New nodes on the network

Findings

Guardian picked up lots of new nodes (200) added to the network.

Level of Risk

This is quite uncommon for industrial networks where the environment is pretty static. An unknown node added to the network could introduce problems to the process especially if the people taking care of the process are not aware of it.

High

Medium

Low

Suggested Action

Check if these devices should be on the network or not and remove the accordingly.

New function code / non existent function code alerts

ACTIONS ...	RISK	TIME	ID	TYPE ID	STATUS	NAME	DESCRIPTION
•••	-			VI:NEW-FUNC-CODE	-		
•••	6	2019-10-22 18:01:51.411	22da5852	VI:NEW-FUNC-CODE	open	New SCADA function code detected	New function code Unregister_Session

Alert New SCADA function code detected [22da5852-255c-4280-8307-8e3d

New function code Unregister_Session

Details (at the alert time)

Source: 10.236.50.224 - 00:04:E:00:99:00
Destination: 10.236.50.61 - 00:0f:73:01:79:80
Protocol: ethernetip (tcp)
Capture device: port2
Ports: 53442 → 44818

Note:

Nodes currently involved

10.236.50.61

ip:	10.236.50.61
mac address:	00:0f:73:01:79:80
mac vendor:	RS Automation Co., Ltd
zone:	Undefined
level:	1
type:	PLC
vendor:	Rockwell Automation/Allen-Bradley
product name:	MicroLogix 1763-L16BWA B/7.00

Findings

Guardian picked up a new function code requested.

Level of Risk

These attempts are typically basic misconfigurations or part of the process to setting up a new connection over an industrial process, but could also be indicative of a compromised machine and a threat actor trying to determine possibilities for how to interact with a compromised network.

High

Medium

Low

Suggested Action

Request operations team to investigate for misconfiguration or to explain cause of these scans.

Internet Connections to public IPs

RISK	TIME	ID	TYPE ID	DESCRIPTION
			INCIDENT:INTERNET-NAVIGATION	
	2020-02-26 08:56:49.300	A658aad1	INCIDENT:INTERNET-NAVIGATION	The host 172.16.1.124 is attempting to start public Internet activity
	2020-02-11 00:23:33.587	6D9923a6	INCIDENT:INTERNET-NAVIGATION	The host 10.90.1.156 is attempting to start public Internet activity
	2020-02-07 13:58:03.062	E5ae5ec5	INCIDENT:INTERNET-NAVIGATION	The host 172.16.1.124@500 is attempting to start public Internet activity
	2020-01-13 12:59:42.103	Ebbf826e	INCIDENT:INTERNET-NAVIGATION	The host 172.16.1.124 is attempting to start public Internet activity

Findings

Guardian picked up several alerts for attempted access to external IP addresses over a variety of protocols.
Refer to attached list of connection attempts and successful connections for more information

2785 attempted links to Public Internet.

Level of Risk

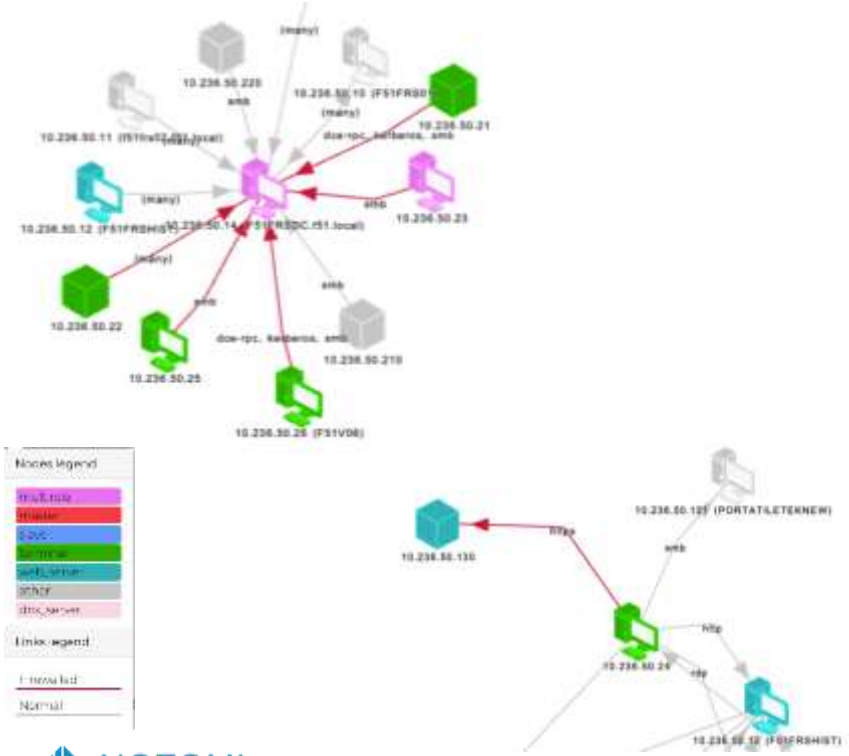
Connectivity to and from the internet in control networks greatly increases likelihood of threat actors' access to the network, and increases possibility that user error or negligence makes a network vulnerable.

High
Medium
Low

Suggested Action

Restrict as much as possible access to/from the internet, and isolate hosts and networks that require internet access from critical control networks.

Links blocked by firewalls



Findings

Guardian picked up some links blocked by firewalls.

Level of Risk

This could be a symptom of a misconfiguration of the firewall or of the host trying to connect to a specific devices.

High

Medium

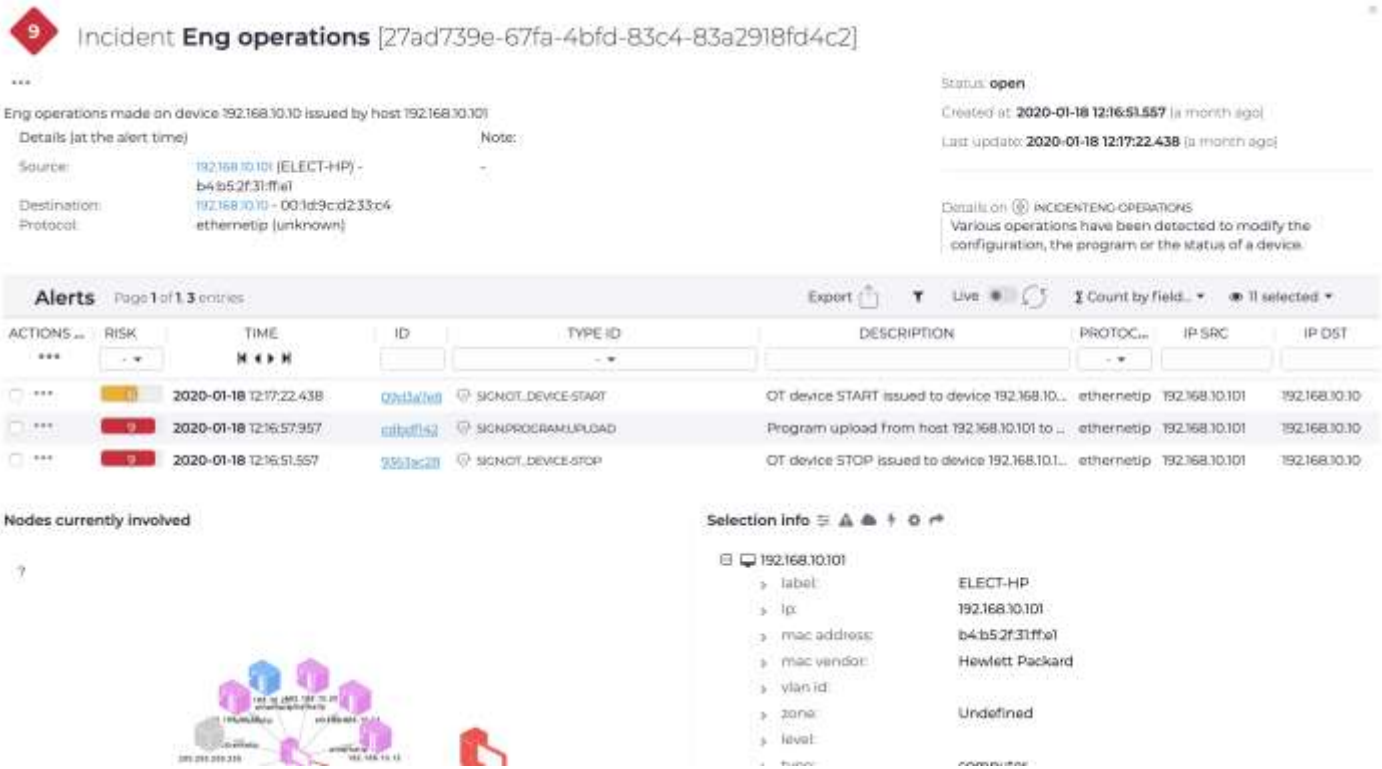
Low

Suggested Action

Check if such connections are allowed or not and configure the firewall accordingly.

Engineering Operations

Guardian has to ability to track Engineering operations such as Starts, Stops and program uploads being sent to the PLC's



DeltaV DCS Workstation Vulnerability

(This vulnerability was discovered and disclosed by Nozomi Networks August 16, 2018)

Details for **CVE-2018-14793**

Node:	10.5.0.214
Score:	
CWE name:	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE:	119
Matching CPEs:	cpe:/a:emerson:deltav:13.3.1:-:-
CVE creation date:	2018-08-21 04:29:00.000
CVE update date:	2019-10-09 13:35:00.000
Discovery date:	2019-11-14 09:28:43.705

Summary:

DeltaV Versions 11.3.1, 12.3.1, 13.3.0, 13.3.1, and R5 is vulnerable to a buffer overflow exploit through an open communication port to allow arbitrary code execution.

References:
Source "BID", Type "VENDOR_ADVISORY"
105105
Source "MISC", Type "VENDOR_ADVISORY"
https://ics-cert.us-cert.gov/advisories/ICSA-18-228-01

Findings

There are a variety of vulnerabilities present in the Emerson DeltaV DCS Workstations.

Level of Risk

Successful exploitation of these vulnerabilities could allow arbitrary code execution, malware injection, or malware to spread to other workstations.

- **High**
- Medium
- Low

Suggested Action

Emerson recommends users patch the affected products listed below:
DeltaV DCS Versions 11.3.1, 12.3.1, 13.3.0, 13.3.1, and R5: Apply patch from vendor.

Weak passwords and default credentials

5

Weak password used

2020-02-19 05:33:21.880 | Status: open

Weak username/password (machine/machine) has been used to access host 10.5.124.30 with protocol http

	Source	Destination
IP	192.219.137.31	10.5.124.30
MAC	80:ee:73:cb:4d:40	70:69:5a:9c:d2:bd
Label		pcppacsw01.cppdv.cariboopulp.local
Port	63689	80
Roles	web_server	web_server
Is security	true	
Protocol	http (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 >

Weak Password Alert

Findings

Multiple instances of weak and default credentials in use and passing in clear text in the environment.

Level of Risk

Default or easily guessed credentials are one of the most common means of compromise, especially in networking equipment and applications.

High

Medium

Low

Suggested Action

Change all default credentials, and avoid easily guessed or cracked passwords on all systems and applications.

New Function Codes Detected

6

New function code detected

2020-02-16 10:51:04.656 | **Status:** open

New function code ReadProperty

	Source	Destination
IP	10.8.0.114	10.8.0.230
MAC	00:0a:f7:4b:43:9a	18:66:da:f8:3b:39
Label	DVOWS-STM-13	DVAPP-002
Port	18507	18507
Roles	other	dns_server, time_server
Is security	true	
Protocol	delta-v (udp)	

This kind of alert occurs when a known protocol between two nodes starts using a new function code or command. For example if a client A uses a function code 'read' when talking to server B, this alert is raised if client A begins to use function code 'write'. This alert should be checked carefully because the unexpected behavior can damage the involved nodes.

Open details >

Findings

Guardian picked up frequent instances of new function codes detected once it entered Protected mode. The reason for the alert is indicating that this is a function code not seen while in learning mode.

Level of Risk

These attempts could be basic misconfigurations or part of the process to setting up a new connection over an industrial process but could also be indicative of a compromised machine and a threat actor trying to determine possibilities for how to interact with a compromised network.

High

Medium

Low

Suggested Action

Request operations team to investigate and explain cause of these function cods detected..

New Network Device Detected

1.5

New network device detected

2019-12-28 06:54:20.786 | **Status:** open

A new switch or router with MAC address aa:aa:03:00:00:00 appeared

	Source	Destination
MAC	aa:aa:03:00:00:00	00:60:00:00:00:00
Roles	other	other
Is security	true	
Protocol	cdp (ethernet)	

A new network device (switch or router) appeared on the network.

Open details >

Guardian detected the installation of a new network device (switch or router).

Malformed Network Traffic Detected

Malformed Network packet

2019-11-15 12:39:51.914 | **Status:** open

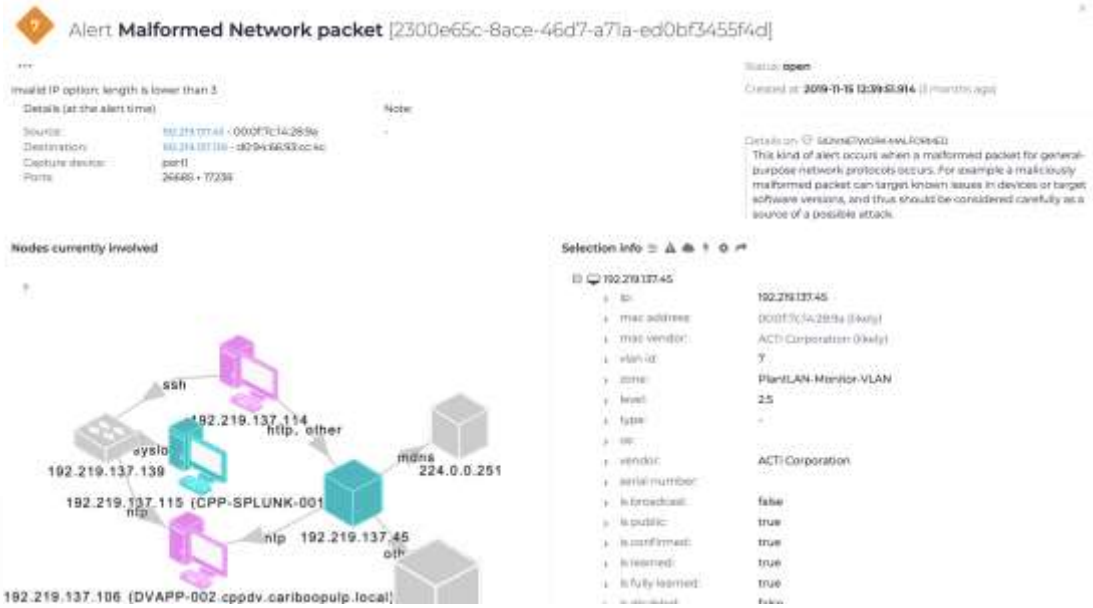
Invalid IP option: length is lower than 3

	Source	Destination
IP	192.219.137.45	192.219.137.139
MAC	00:0f:7c:14:28:9a	d0:94:66:93:cc:4c
Port	26685	17238
Roles	other	other
Is security	true	
Protocol	udp	

This kind of alert occurs when a malformed packet for general-purpose network protocols occurs. For example a maliciously malformed packet can target known issues in devices or target software versions, and thus should be considered carefully as a source of a possible attack.

Open details >

This kind of alert occurs when a malformed packet for general-purpose network protocols occurs. For example a maliciously malformed packet can target known issues in devices or target software versions, and thus should be considered carefully as a source of a possible attack.



Issues Discovered/Feature Requests

1. Issue with graphic change causing multiple program upload alerts

- Multiple alerts generated whenever a graphic is changed and replicated to all DeltaV workstations. PCAPS were sent of legitimate uploads vs. graphics changes. AN issue was identified in how Guardian handled the graphic change and will be fixed in the release slated for mid April. YouTrack Issue # N2OS-6803.

2. More in depth mapping of fields for DeltaV

- Additional alarm types that Guardian is not currently mapping in DeltaV were discovered. There will be enhanced DeltaV mapping by leveraging a project Apache is currently working on with DeltaV protocol slated for the Mid April release

3. Additional Type ID

- Add Wireless-AP to the list of Type ID's for categorization – will be in version 20 being released Mid March.

Conclusion and Next Steps

- Nozomi detected a likely network misconfiguration due to links blocked by firewalls and retransmissions. Further investigation needed.
- A host running Win XP has been found. Its presence could pose a significant risk and should be carefully evaluated.
- The alerts show a big number of connections to internet, mainly to Microsoft (probably for updates). Nevertheless, internet connections should not be present in ICS environment because they pose a significant risk of external intrusions.
- Large number of nodes appeared on the network. This is uncommon for ICS where networks are usually stable. It should be investigated if all the added nodes where legitimate or not
- An invalid ip and a port scan have been found. Further investigation is needed.
- Lastly, besides the detection, Nozomi Guardian can also offer a proactive protection integrating with firewall technologies deployed to segment the networks. Nozomi can also integrate with Security Incident and Event Management systems (SIEMs) such as Splunk or QRadar, along with other methods of remote logging.

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