CLAROTY
Clarity for OT Networks

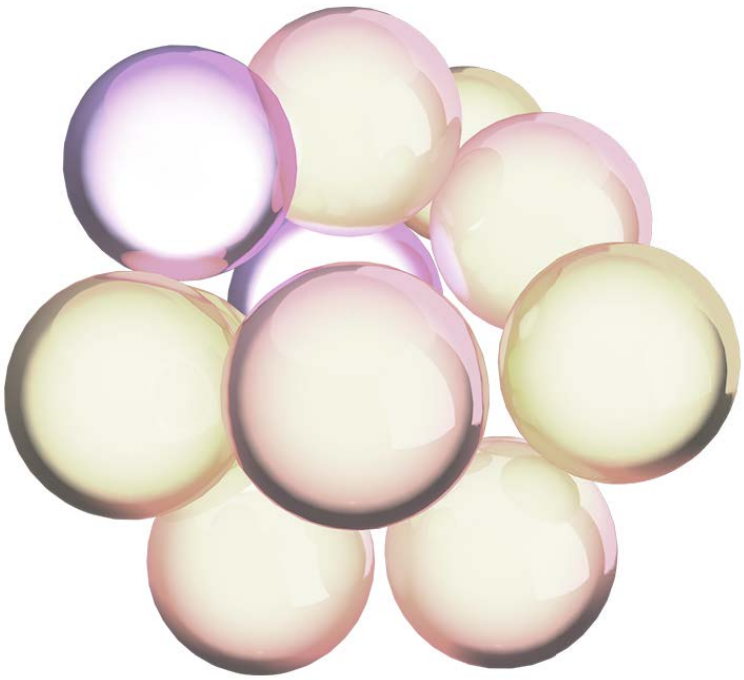
Data Sheet

Claroty Security Posture Assessment

Overview

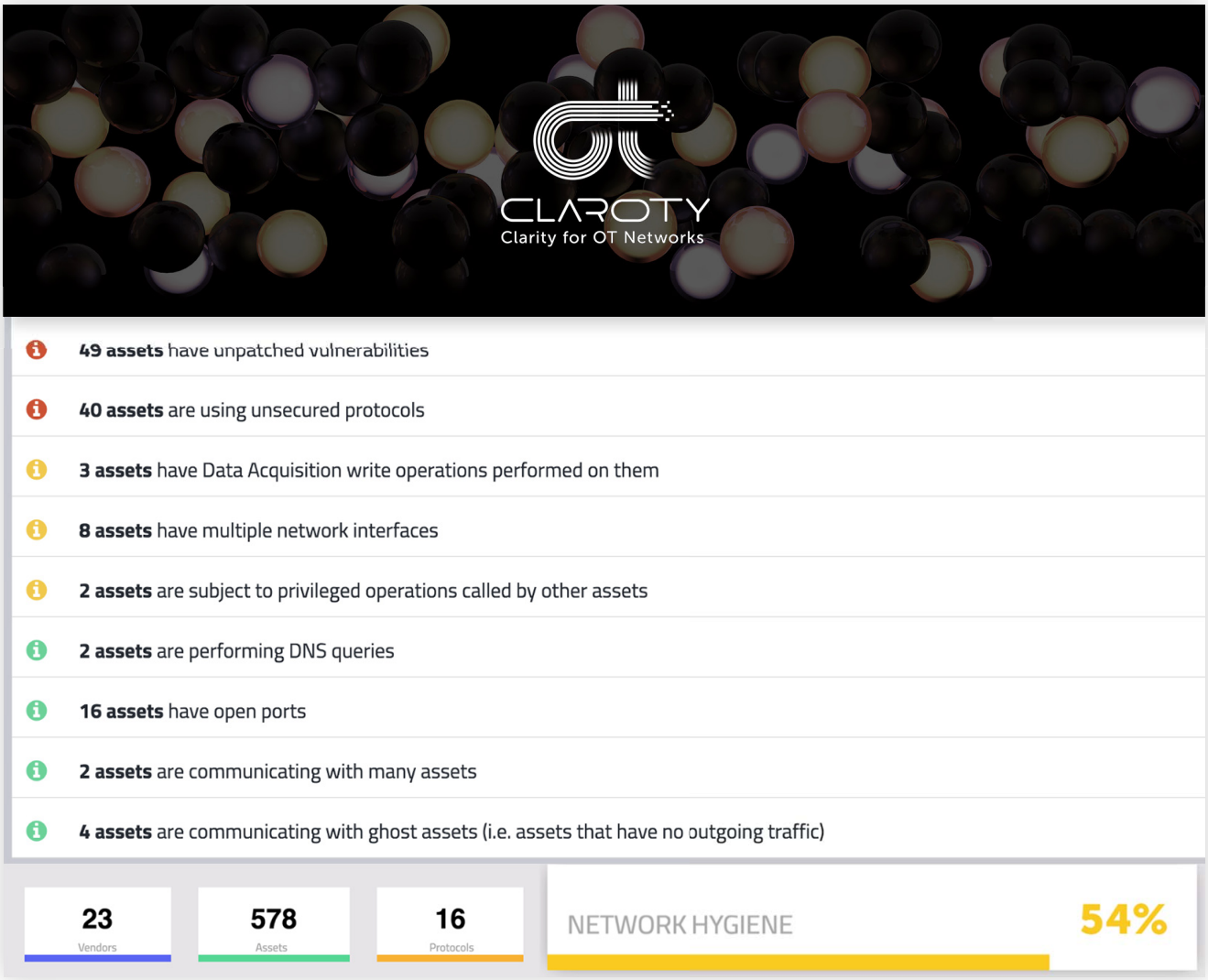
The Claroty Security Posture Analysis is an offline assessment product that provides security teams with visibility and insights into the OT network's security risk posture. The tool consumes a PCAP (packet capture) data file, collected from a network switch, and produces a comprehensive analysis of the ICS network. The report provides a summary and detailed analysis of the assets and communications discovered on the industrial network, pinpoints vulnerable assets and resolutions, and uncovers network configuration and other "network hygiene" issues that can provide attackers a pathway or impact critical processes.

As part of the report generation process, intelligence extracted from the OT protocols provides situational insights into existing vulnerabilities, network hygiene issues and possible misconfigurations, weak passwords, and unsecured connections or remote connections. The Security Posture Analysis operates in a fully passive manner, does not require the installation of an agent on protected endpoint devices, and has zero impact on the OT network.



Summary of Findings

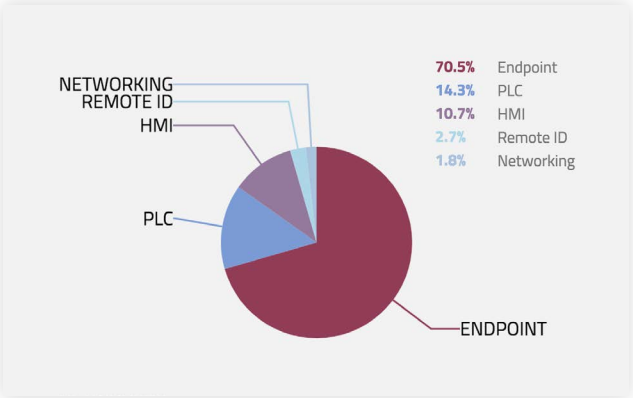
Claroty's Security Posture Analysis provides a snapshot with detailed threat and vulnerability information along with risk-prioritized insights and recommended mitigation steps. Using this information, security teams and SOC managers can dramatically reduce their network attack surface effectively helping to strengthen their ICS risk posture.



Asset Discovery & Communication

The Security Posture Analysis automatically identifies assets across the entire ICS network including assigned IP, nested assets, and assets that communicate over serial connections. Leveraging real-time visibility allows creating a logical map of devices within the network to be utilized for asset inventory and management tasks as well as addressing various regulatory and internal audit requirements.

ICS Network Assets and Protocols Breakdown

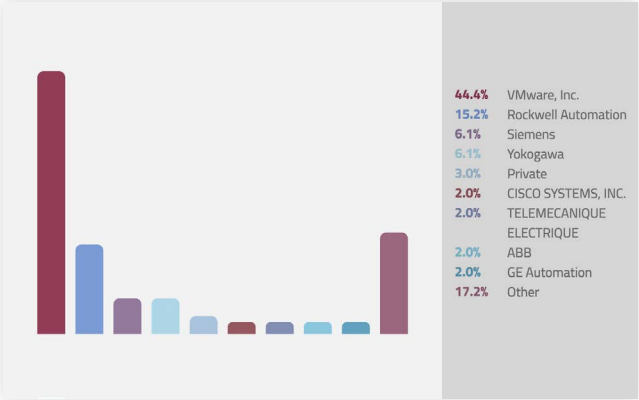


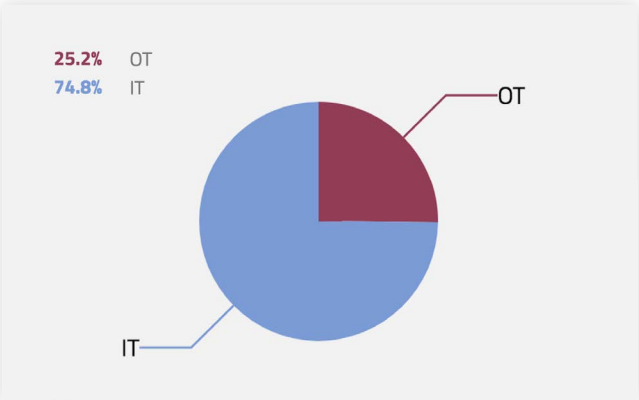
Asset Breakdown by Type

Breakdown of the various assets as found in the network

Asset Breakdown by Vendor

Snapshot of the various vendors as found in the network



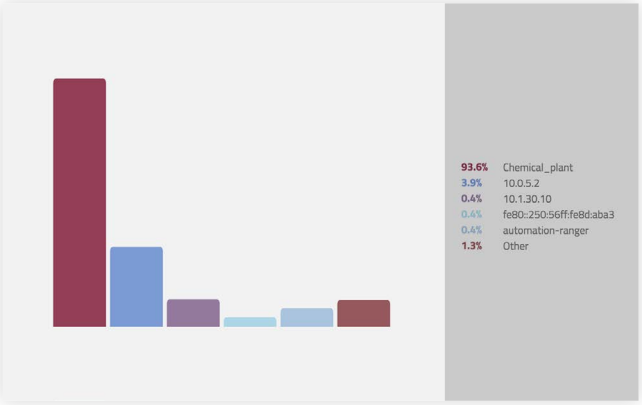


IT vs. OT Assets

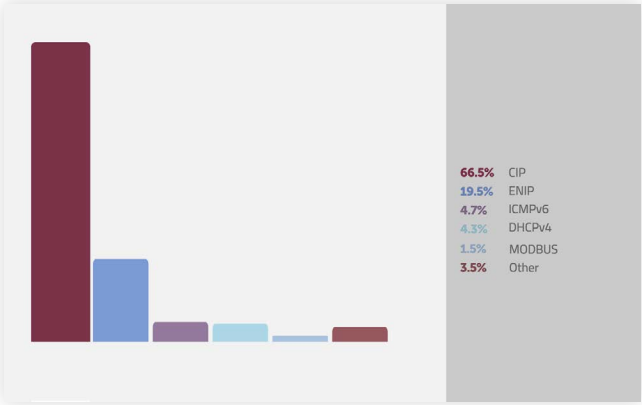
Side by side comparison of IT vs. OT assets as found on the network

Top Volume Assets Communication

A snapshot of the top communicating asset on the network



Detailed Assets and Protocols Information

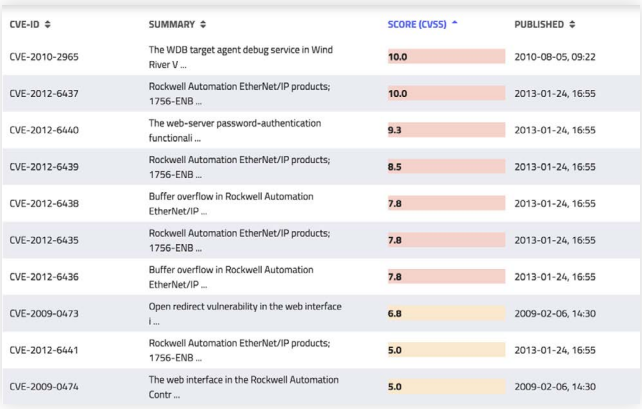


Protocol Traffic

A snapshot of the most prominent protocols used on the Network

Granular Asset Information

Provides additional visibility and insight on specific assets including their device IP, used protocols, device type, and vendor. Additionally, and assuming the device is communicating via a rack slot, the report provides granular information (enumerate and display) on the specific slots, respective model, internal serial number, vendor, and firmware version.



CVE-ID	SUMMARY	SCORE (CVSS)	PUBLISHED
CVE-2010-2965	The WDB target agent debug service in Wind River V ...	10.0	2010-08-05, 09:22
CVE-2012-6437	Rockwell Automation EtherNet/IP products; 1756-ENB ...	10.0	2013-01-24, 16:55
CVE-2012-6440	The web-server password-authentication functionali ...	9.3	2013-01-24, 16:55
CVE-2012-6439	Rockwell Automation EtherNet/IP products; 1756-ENB ...	8.5	2013-01-24, 16:55
CVE-2012-6438	Buffer overflow in Rockwell Automation EtherNet/IP ...	7.8	2013-01-24, 16:55
CVE-2012-6435	Rockwell Automation EtherNet/IP products; 1756-ENB ...	7.8	2013-01-24, 16:55
CVE-2012-6436	Buffer overflow in Rockwell Automation EtherNet/IP ...	7.8	2013-01-24, 16:55
CVE-2009-0473	Open redirect vulnerability in the web interface i ...	6.8	2009-02-06, 14:30
CVE-2012-6441	Rockwell Automation EtherNet/IP products; 1756-ENB ...	5.0	2013-01-24, 16:55
CVE-2009-0474	The web interface in the Rockwell Automation Contr ...	5.0	2009-02-06, 14:30

Unsecured Protocols

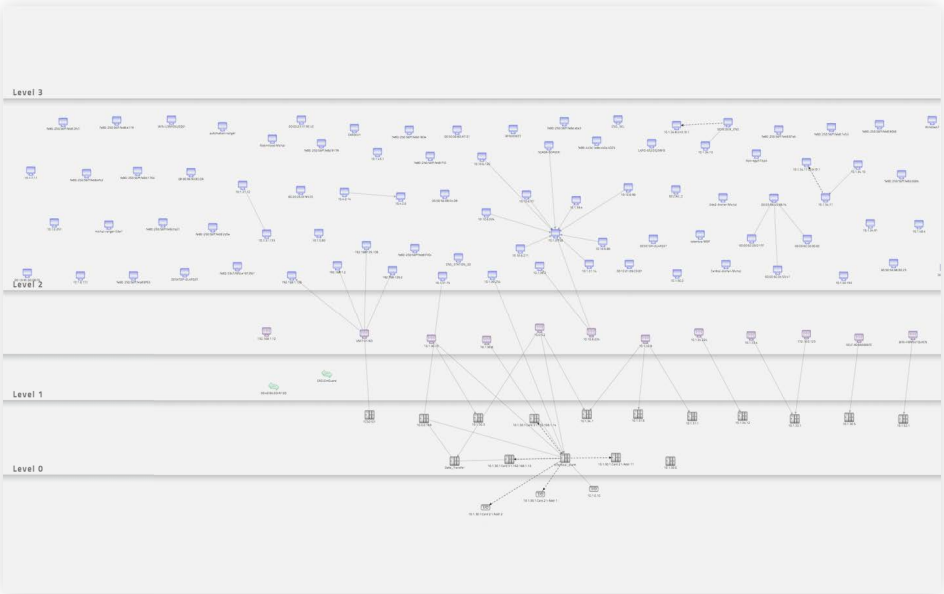
The relevant security weaknesses that attackers can leverage to compromise the network's security.

PROTOCOL	REASON PROTOCOL IS UNSECURED
NETBIOS-NAME	Unsecured protocol
LANMAN	Unsecured protocol
SMB	Unsecured protocol version. SMB versions 1/...

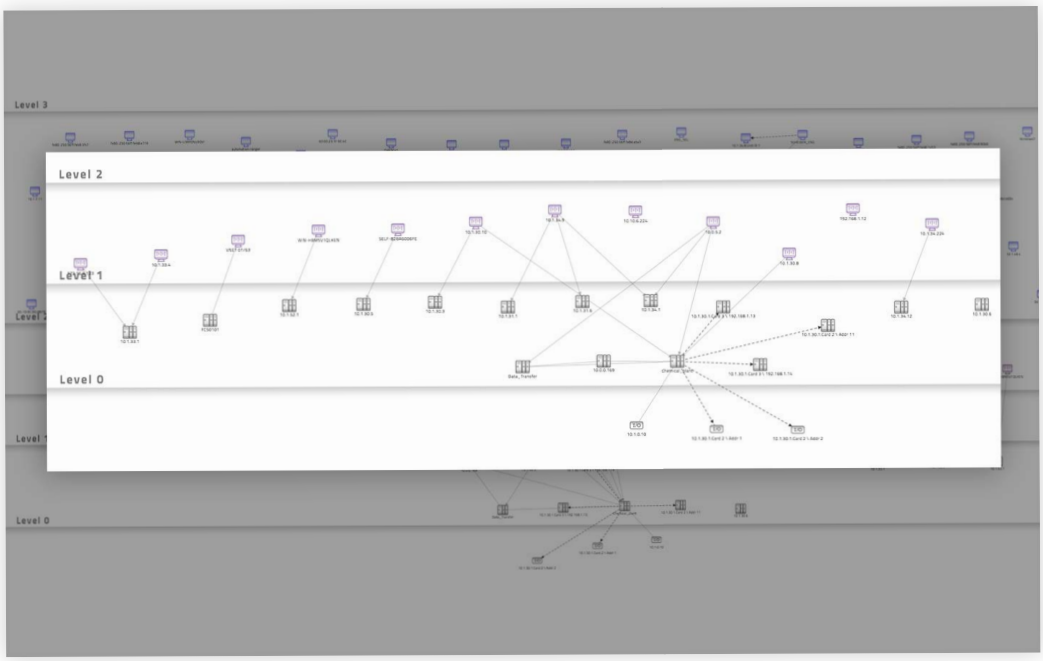
Network Analysis

The Security Posture Analysis provides a detailed report on the various control process devices and how they communicate across the network, including specific visibility on their communication paths and associated devices.

- **Layered Communication Mapping:** An automatic asset discovery capability provides a network topology and logical connectivity of the various devices based on their respective communication level (layer). Each element within the network includes all the data required for inventory management, including: IP, Type, Protocols identified, status and more.
- **OT Network Graph:** This view provides a detailed topology of OT elements and how they communicate with one another and across the network – based on their respective communication level (layer).



Detailed Network Topology



OT Network Topology

- **Network Anomalies:** The Security Posture Analysis highlights various network anomalies that are instantly generated following the upload of your network data (PCAPs). The report then provides, amongst other things, a risk score for the entire ICS network as well as a score for each discovered device, specific CVEs for each device, and other network threats and vulnerabilities.

Type	Description	Detected Date	Category
New Asset	A new asset has been detected **10.1.31.133**.	Wed Dec 13 2017	Integrity
Login	Failed login attempt to controller **10.1.0.80** from **10.1.0.171**	Wed Dec 13 2017	Security
Configuration Upload	Configuration uploaded from controller **10.1.34.1** by **SCHEIDER_ENG**	Wed Dec 13 2017	Integrity
Asset Information Change	Information has been changed for asset **10.1.34.1**	Wed Dec 13 2017	Integrity
Configuration Download	Configuration downloaded to controller **10.1.34.1** by **SCHEIDER_ENG**	Wed Dec 13 2017	Integrity

Network Anomalies

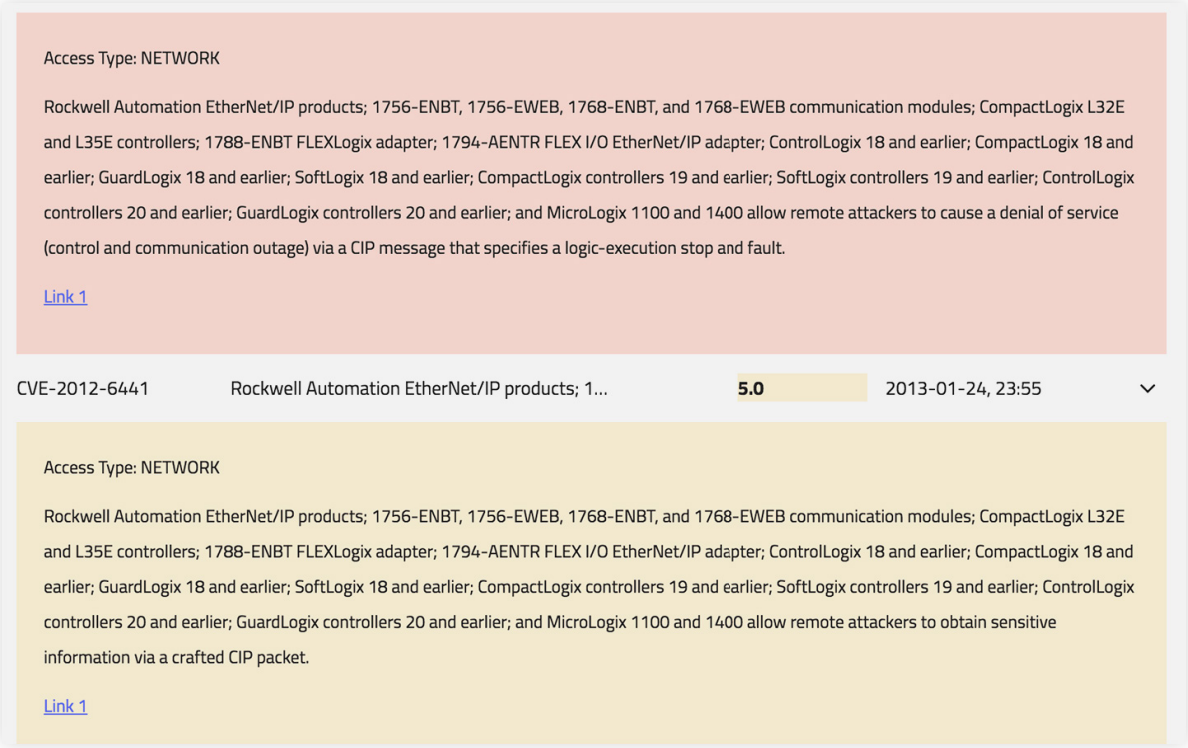
Comprehensive Insights

The Security Posture Analysis provides a detailed network posture as well as an overall network hygiene score calculated based on device security levels along with additional vulnerabilities, misconfiguration issues, and other threats.

The report provides a summary and detailed analysis of the assets and communications discovered on the industrial network, pinpointing vulnerable assets and resolutions, and uncovering network configuration and other "network hygiene" issues that can provide attackers a pathway in or impact critical processes.

Common Vulnerabilities & Exposures (CVE's)

A standard that provides a reference method for publicly known information security vulnerabilities and exposures. The report highlights relevant assets that run software versions that can be leveraged by attackers for various malicious purposes such as remote code execution, DDOS, etc. The following example shows a list of Common Vulnerabilities and Exposures (CVE's) highlighting the specific CVE, its score, publish date, a Common Vulnerability Scoring System (CVSS), and external links to additional information and recommended mitigation actions.



CVE Table

WRITING ASSET	PROTOCOL	OPERATED ON
172.16.30.253	MODBUS	41 affected PLCs - click to filter
P1SPOSRV2	MODBUS	36 affected PLCs - click to filter
P1SPOSRV1	MODBUS	30 affected PLCs - click to filter
172.16.30.7	MODBUS	2 affected PLCs - click to filter
172.16.30.28	MODBUS	2 affected PLCs - click to filter
172.16.30.35	MODBUS	2 affected PLCs - click to filter
172.16.30.27	MODBUS	1 affected PLC - click to filter
172.16.30.14	MODBUS	1 affected PLC - click to filter
172.16.30.17	MODBUS	1 affected PLC - click to filter
172.16.30.39	MODBUS	1 affected PLC - click to filter

Data Acquisition Write Operations

Assets performing Data Acquisition Write actions pose potential risks as they can change process values on PLCs.

Privileged Commands

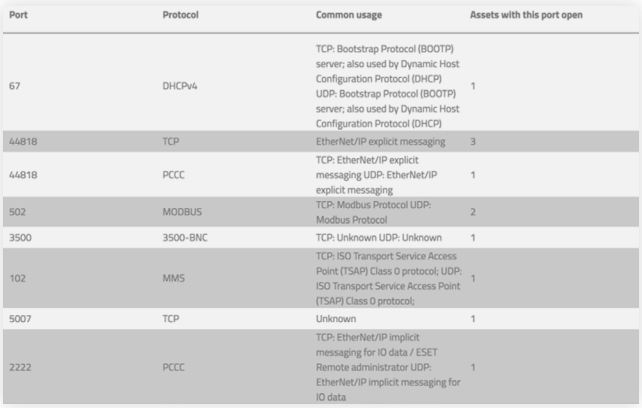
Privileged commands are usually performed by engineering stations. This insight gives an indication of rogue assets sending privileged commands to PLCs.

Engineering Station	Protocol	Operated on
10.1.30.8	CIP	1 affected PLC
SCHEIDER_ENG	MODBUS	1 affected PLC
WIN-HBMSV1QLKEN	3500-BNC	1 affected PLC
10.0.5.2	CIP	2 affected PLCs
10.1.30.10	CIP	1 affected PLC

DNS Server	Protocol	Query	Total assets
10.0.0.169	DNS	teredo.ipv6.microsoft.com.	1
10.0.0.169	DNS	armmf.adobe.com.	1

DNS Queries

Examination of DNS queries can reveal if an asset features any anomalous outbound communication that may indicate malicious presence.



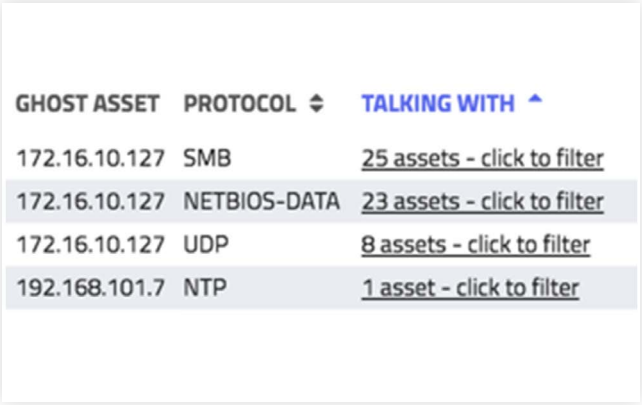
Port	Protocol	Common usage	Assets with this port open
67	DHCPv4	TCP: Bootstrap Protocol (BOOTP) server; also used by Dynamic Host Configuration Protocol (DHCP) UDP: Bootstrap Protocol (BOOTP) server; also used by Dynamic Host Configuration Protocol (DHCP)	1
44818	TCP	EtherNet/IP explicit messaging	3
44818	PCCC	TCP: EtherNet/IP explicit messaging UDP: EtherNet/IP explicit messaging	1
502	MODBUS	TCP: Modbus Protocol UDP: Modbus Protocol	2
3500	3500-BNC	TCP: Unknown UDP: Unknown	1
102	MMS	TCP: ISO Transport Service Access Point (TSAP) Class 0 protocol; UDP: ISO Transport Service Access Point (TSAP) Class 0 protocol;	1
5007	TCP	Unknown	1
2222	PCCC	TCP: EtherNet/IP implicit messaging for IO data / ESET Remote administrator UDP: EtherNet/IP implicit messaging for IO data	1

Open Port Vulnerabilities

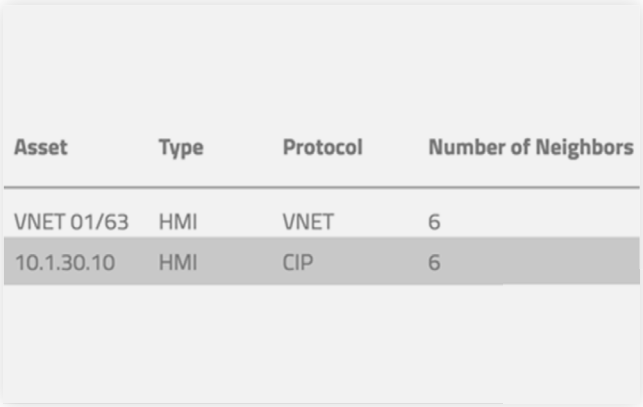
Misconfigured open ports may be taken advantage of for purposes other than intended. The report leverages a variety of port filters to display vulnerability information in multiple ways – allowing to identify any potential risk associated with open ports and services.

Communication with Ghost Assets

Ghost assets are network entities that may have been misconfiguration and can be leveraged as an attack entry points into the network. The report highlights those specific assets along with the specific communication protocol used.



GHOST ASSET	PROTOCOL	TALKING WITH
172.16.10.127	SMB	25 assets - click to filter
172.16.10.127	NETBIOS-DATA	23 assets - click to filter
172.16.10.127	UDP	8 assets - click to filter
192.168.101.7	NTP	1 asset - click to filter



Asset	Type	Protocol	Number of Neighbors
VNET 01/63	HMI	VNET	6
10.1.30.10	HMI	CIP	6

Popular Assets

These assets are high ranked in terms of the amount of network connections they initiate. In some cases, this indicates key elements in the network - data collection services, monitor servers, or possibly an adversary performing broad reconnaissance.