Microsoft Defender for IoT

Proactively safeguard critical infrastructure while aligning with cybersecurity best practices for OT

MC2MC

—CONNECT—

John Joyner

- Senior Director of Technology, Corsica Technologies https://corsicatech.com/
- 18 x Microsoft MVP
- 2025-2026 Azure MVP & Security MVP (with specialties in Azure Management & Cloud Security)

@arkswo.bsky.social

@johnjoyner6059

https://www.amazon.com/stores/John-Joyner/author/B00J4XUH3O

https://github.com/john-joyner

https://www.linkedin.com/in/johnjoyner/

https://blog.johnjoyner.net/blog


CONNECT · COLLABORATE · CREATE
MC2MC
CONNECT


2Pint


PATCH
MY PC


robopack


wortell


INGRAM
MICRO


The Collective


bechtle


lebon.IT


ConXioN
The new style of IT


VirtualMetric


veeam


evri

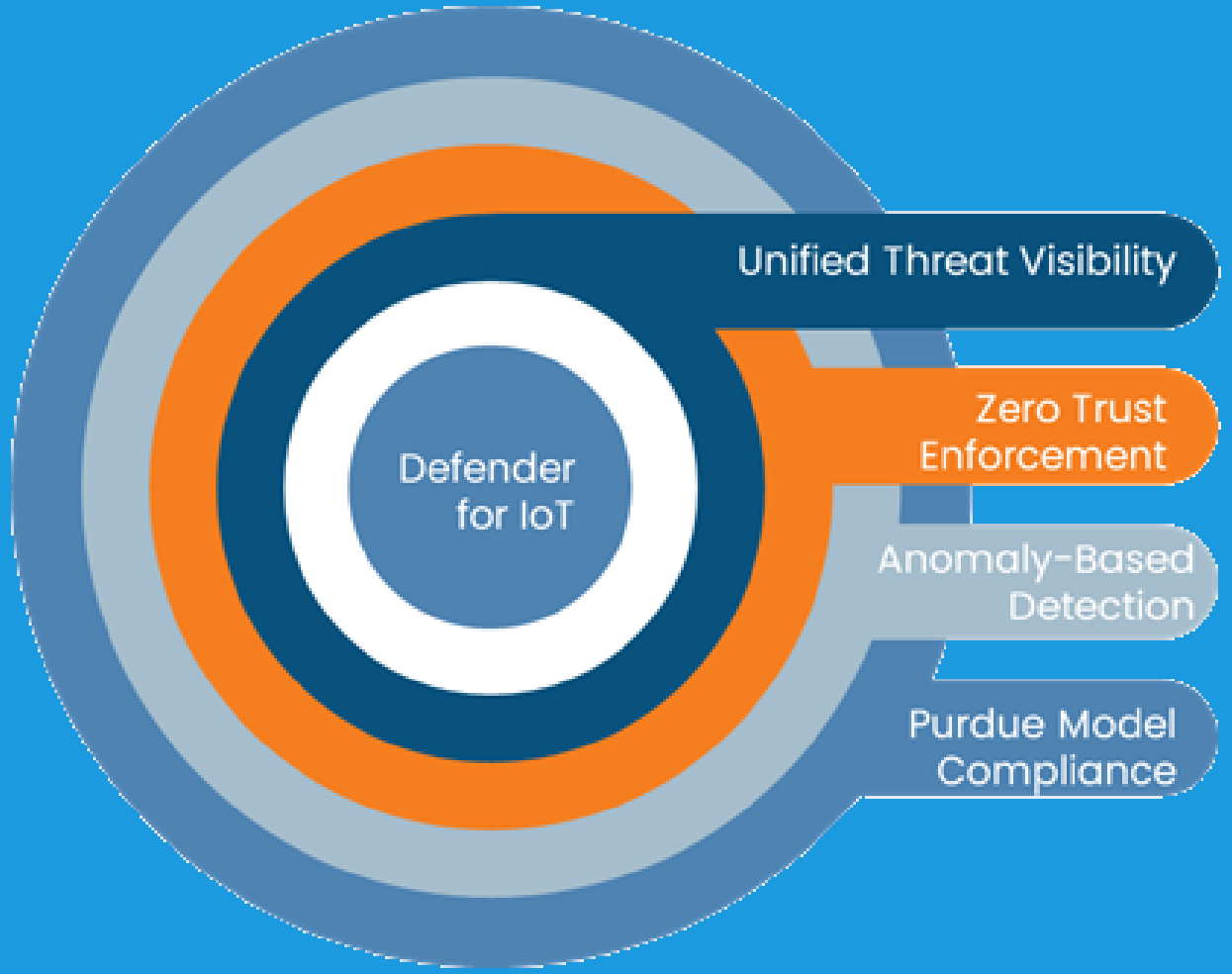
Microsoft Defender for IoT

CONNECT. COLLABORATE. CREATE

MC2MC

—CONNECT—

Microsoft Defender for IoT

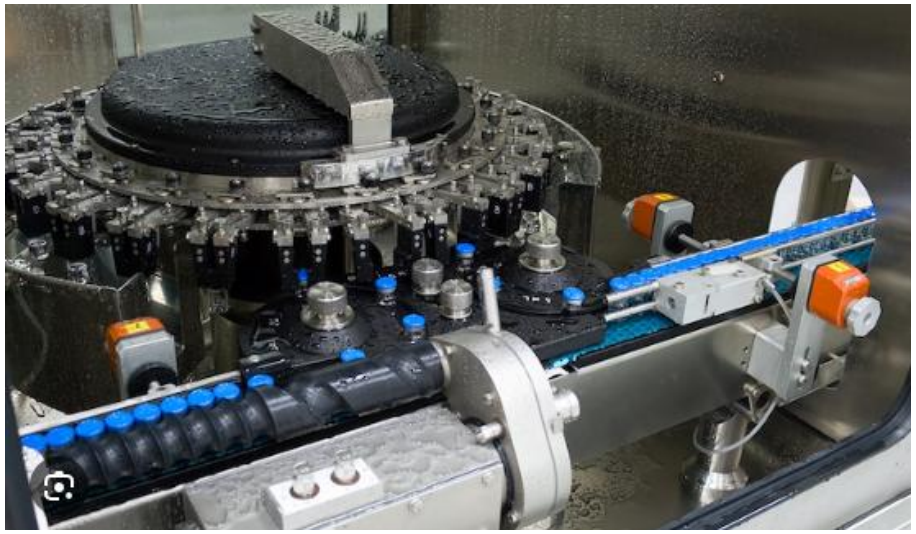


Defender for IoT is the 24x7 guardian of your OT crown jewels.

An unauthorized person connecting to the production OT network

What is Operational Technology (OT)?

Smart Factories & Distribution Centers



Pharma

Food Processing

Power Generation

Industrial Control Systems (ICS) Devices

PLC – Programmable Logic Controller

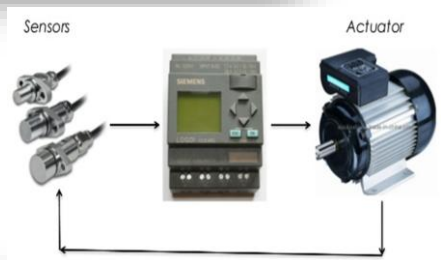
- PLC receives information from connected sensors or input devices, processes the data, and triggers outputs based on pre-programmed parameters.
  - ABB, Allen Bradley, Siemens, Mitsubishi, Honeywell, Motorola, Hitachi, General Electric,

RTU – Remote Terminal Unit

- RTU and PLCs perform similar functions, but used in wider geographical telemetry
  - ABB, GE Grid Solutions, Honeywell, Schneider Electric, Siemens Energy

HMI – Human Machine Interface

- HMI represents plant information to the operating personnel graphically in the form of diagrams
  - Mitsubishi Electric, Omron, Rockwell, Schneider Electric



Industrial Control Systems (ICS) Devices

EWS – Engineering Workstation

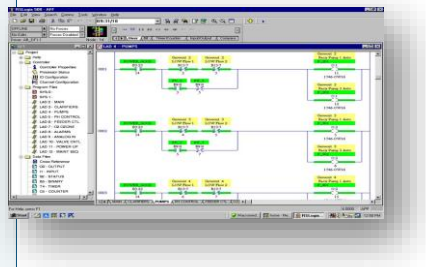
- Very reliable computer designed for configuration, maintenance and diagnostics of the Industrial Control System (ICS) applications

Historian

- Architected to pull data from a variety of systems to quickly form a complete context of the manufacturing environment.
  - Schneider Electric Wonderware, OSISoft PI, Rockwell

BMS – Building Management System

- Systems installed in buildings to control and monitor mechanical and electrical equipment, such as HVAC, lighting, energy, fire systems, and security systems.
  - Siemens, Schneider Electric, Honeywell, and Johnson Controls, Bosch, Building Logix, Delta Electronics



Comparing IT Security with OT Security

IT SECURITY	OT SECURITY
Data confidentiality & privacy	Safety & availability
High levels of connectivity	Traditionally air-gapped
Standard protocols & devices	Specialized protocols, devices & legacy OS platforms
Multiple layers of controls & telemetry	Little or no visibility into IoT/OT risk

What kind of bad actors are attacking OT?

Table: Motivation factor for bad actors

Factor	Percentage
Geo-political intent	69
Monetary considerations	15
IP/Data Theft	10
Rogue insider	03
Unknown	03

Statistics source: Global-OT-and-IoT-Threat-Landscape-Analysis-and-Assessment-Report-2023

What targets are being attacked and why?

Sector	Target	Why?
Manufacturing	Safety systems, IIoT deployments, shop floor controllers, HMIs, monitoring systems,	Data theft, ransom, large-scale disruption, geopolitical factors
Healthcare	Internet of Medical Things devices, high-value health care machines that run on legacy systems	Patient data theft, ransom, lack of adequate cybersecurity measures
Defense	Communication systems, controllers, theater and situation monitoring hardware, weapon systems	Data theft, intelligence, data on movement and use of weapon systems, injection of laterally moving malware to infect the entire chain of command structure inactive and cold combat zones
Pharmaceutical/ drug manufacturers	Assembly lines, data	Disruption of vaccination manufacture and manufacture of critical drugs
Smart cities	IoT deployments including devices and platforms, command and control centers last-mile connected devices (may or may not be part of a large IoT deployment such as standalone pollution monitoring devices)	Citizen data, long-term targeting,
Utilities	HMIs, control systems at various levels, monitoring systems	Geo-politics, ransom, data theft, manipulation of bills, and revenue diversion
Oil and gas	Upstream, midstream, and downstream assets, control systems, HMIs, LORA, and short-range connectivity-based networks	Primarily geopolitics
Maritime	Ships, navigation and communication equipment, offshore OT installations connected with cargo management	Ransom

MC2MC CONNECT

Specifically what kinds of OT devices are targeted?

Target systems

Top target systems in inbound attacks	Percent
PLCs	18
Generic IT	17
SCADA workstations	19
Firmware	04
Processes related to software	04
Safety instrumented systems	02
Thermostat	06
Mill control	04
Cyber-physical monitoring systems	09
Production management systems	05
Output control	02
Unspecified HMI systems	03
ERP	02
Unknown	05

Defender for IoT Alert reference

Supported alert categories

Each alert has one of the following categories:

- Abnormal Communication Behavior
- Abnormal HTTP Communication Behavior
- Authentication
- Backup
- Bandwidth Anomalies
- Buffer overflow
- Command Failures
- Configuration changes
- Custom Alerts
- Discovery
- Firmware change
- Illegal commands
- Internet Access
- Operation Failures
- Operational issues
- Programming
- Remote access
- Restart/Stop Commands
- Scan
- Sensor traffic
- Suspicion of malicious activity
- Suspicion of Malware
- Unauthorized Communication Behavior
- Unresponsive

https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/alert-engine-messages

Defender for IoT Alerts: Real-world alert view

Severity	Name	Site	Engine	Last detection	Status	Source device	Tactics
Medium	EtherNet/IP CIP Service Request Faile		OPERATIONAL	42 minutes ago	New	192.168.165.88	Impair process cor
Medium	EtherNet/IP CIP Service Request Faile		OPERATIONAL	42 minutes ago	New	10.92.181.170	Impair process cor
Medium	EtherNet/IP CIP Service Request Faile		OPERATIONAL	42 minutes ago	New	10.92.195.21	Impair process cor
Medium	EtherNet/IP Encapsulation Protocol C		OPERATIONAL	43 minutes ago	New	192.168.165.90	Collection
Medium	Device Failed to Receive a Dynamic IF		OPERATIONAL	an hour ago	New	10.92.248.249	Discovery
Medium	EtherNet/IP CIP Service Request Faile		OPERATIONAL	an hour ago	New	10.92.183.160	Impair process cor
Medium	Device Failed to Receive a Dynamic IF		OPERATIONAL	an hour ago	New	10.48.248.249	Discovery
Low	Suspicion of Unresponsive MODBUS		OPERATIONAL	an hour ago	New	--	Inhibit response fu
Low	Suspicion of Unresponsive MODBUS		OPERATIONAL	an hour ago	New	--	Inhibit response fu
High	Address Scan Detected		ANOMALY	an hour ago	New	logmsp522	Discovery
High	Address Scan Detected		ANOMALY	an hour ago	New	logmsp532	Discovery
High	Address Scan Detected		ANOMALY	an hour ago	New	10.90.120.151	Discovery
High	Address Scan Detected		ANOMALY	an hour ago	New	LOGPCTV025	Discovery
High	Address Scan Detected		ANOMALY	8 hours ago	New	LOGPCPS285	Discovery
High	Excessive Login Attempts		ANOMALY	15 hours ago	New	stopc814	
Medium	Firmware Change Detected		POLICY_VIOLATION	a day ago	New	192.168.165.15	
High	Port Scan Detected		ANOMALY	a day ago	New	LOGPCPS285	Discovery
Medium	Firmware Change Detected		POLICY_VIOLATION	2 days ago	New	192.168.165.14	
High	Address Scan Detected		ANOMALY	2 days ago	New	10.90.80.213	Discovery
High	Address Scan Detected		ANOMALY	2 days ago	New	logps350	Discovery
Medium	Firmware Change Detected		POLICY_VIOLATION	2 days ago	New	192.168.165.25	

Excessive Login Attempts

Alert ID: 5fff6965-15d9-45ce-8674-54415785dedc

High
Severity

New
Status

15 hours ago
Last detection

Description

A source device was seen performing excessive unsuccessful login attempts to a destination server. This may be a brute force attack. The server may be compromised by a malicious actor.

Source device

stopc814 (10.218.166.16)
Workstation

Destination device

Internet (48.222.98.0)
Unknown

MITRE ATT&CK®

Tactics

Lateral movement

The adversary is trying to move through your environment.
read more on attack.mitre.org

Impair process control

The adversary is trying to manipulate, disable, or damage physical control processes.
read more on attack.mitre.org

View full details

Alerts | Excessive Login Attempts

Refresh | Download PCAP

Excessive Login Attempts

Alert ID: 5fff6965-15d9-45ce-8674-54415785dedc

High
Severity

New
Status

15 hours ago
Last detection

Description
A source device was seen performing excessive unsuccessful login attempts to a destination server. This may be a brute force attack. The server may be compromised by a malicious actor.

Source device
stopc814 (10.218.166.16)
Workstation

Destination device
Internet (48.222.98.0)
Unknown

MITRE ATT&CK®

Tactics

Lateral movement	The adversary is trying to move through your environment. read more on attack.mitre.org
Impair process control	The adversary is trying to manipulate, disable, or damage physical control processes. read more on attack.mitre.org

Alert details | Take action

Source device stopc814	Protocol GENERIC	SiteDisplayName [redacted]
Source device address 10.218.166.16	Source (Client) Address 10.218.166.16	SensorType Ot
Destination device Internet	Destination (Server) Address 48.222.98.0	SensorZone default
Destination device address 48.222.98.0	isLearnable false	SensorVersion 25.1.1.12260320
Site [redacted]	ViolationCount 0	First detection (in the network) 12/18/2025, 12:47:07 AM
Sensor [redacted]	Login Attempts Failure Codes With Messages 403 - Forbidden.	Last detection (in the network) 2/4/2026, 6:43:27 PM
Category Authentication	Login Attempts Count 27	Last activity (manual or automated changes) 2/4/2026, 6:43:27 PM

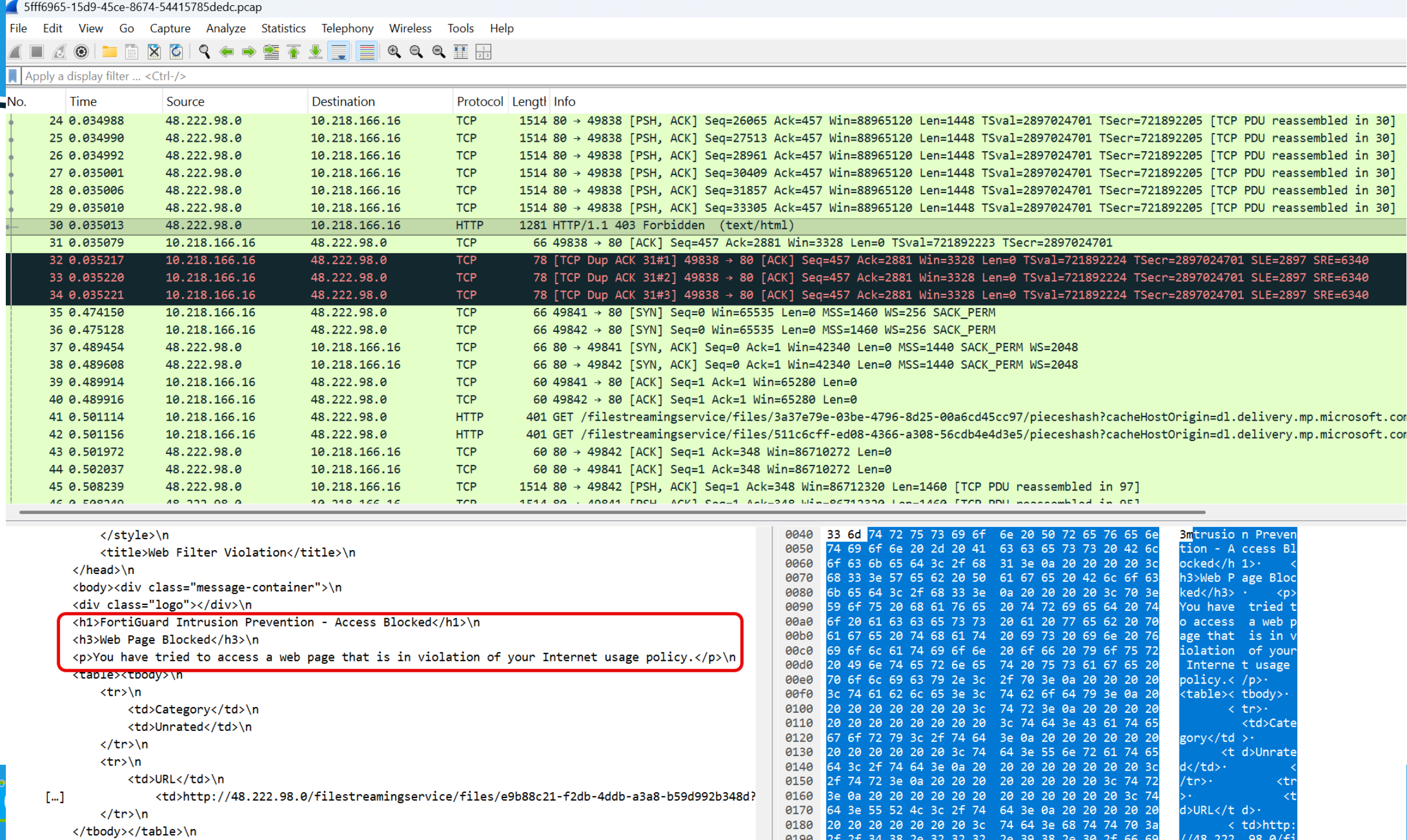
Entities

Host (1)

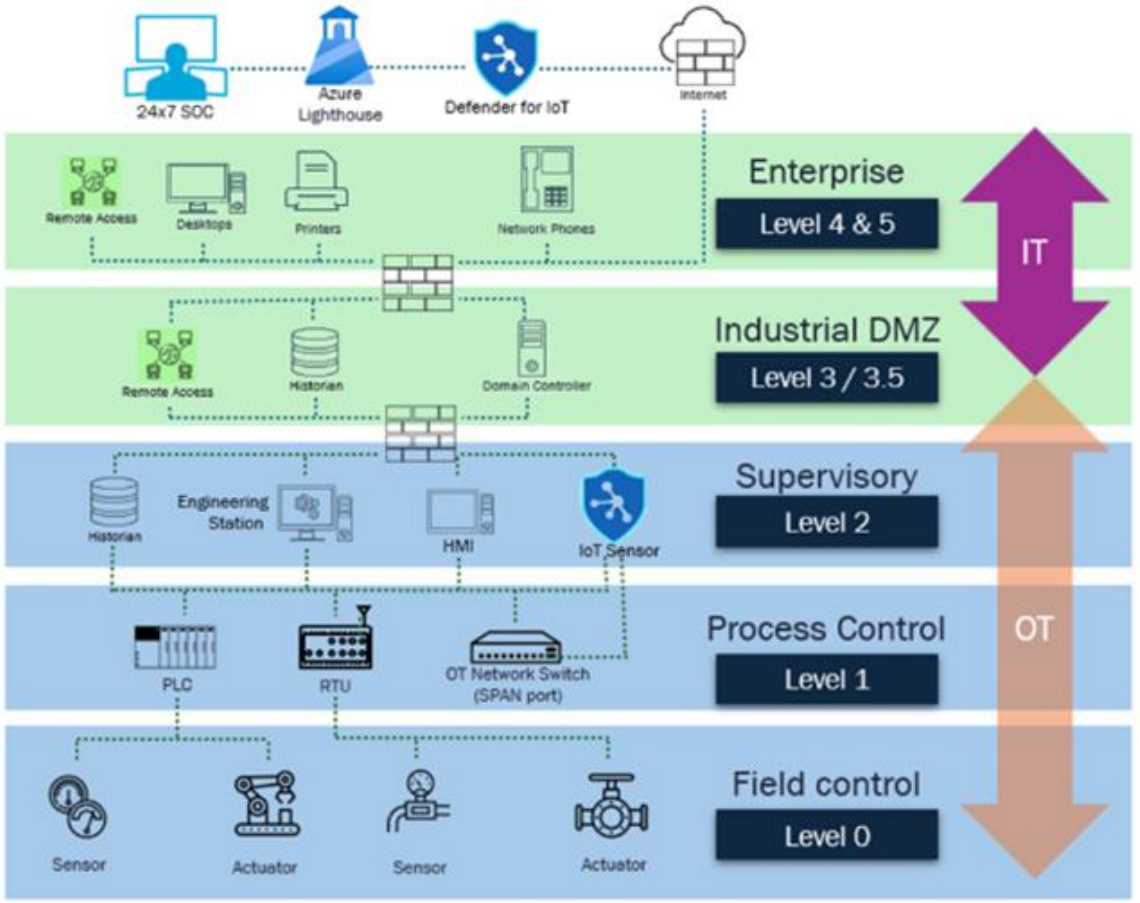
ID	Name	Subtype	Protocols	Vendor
e7f8feed-9f60-4329-af79-589ae33b01	stopc814	Workstation	LDAPS, RPC, LDAP, DNS, Netbios Name	--

IP (1)

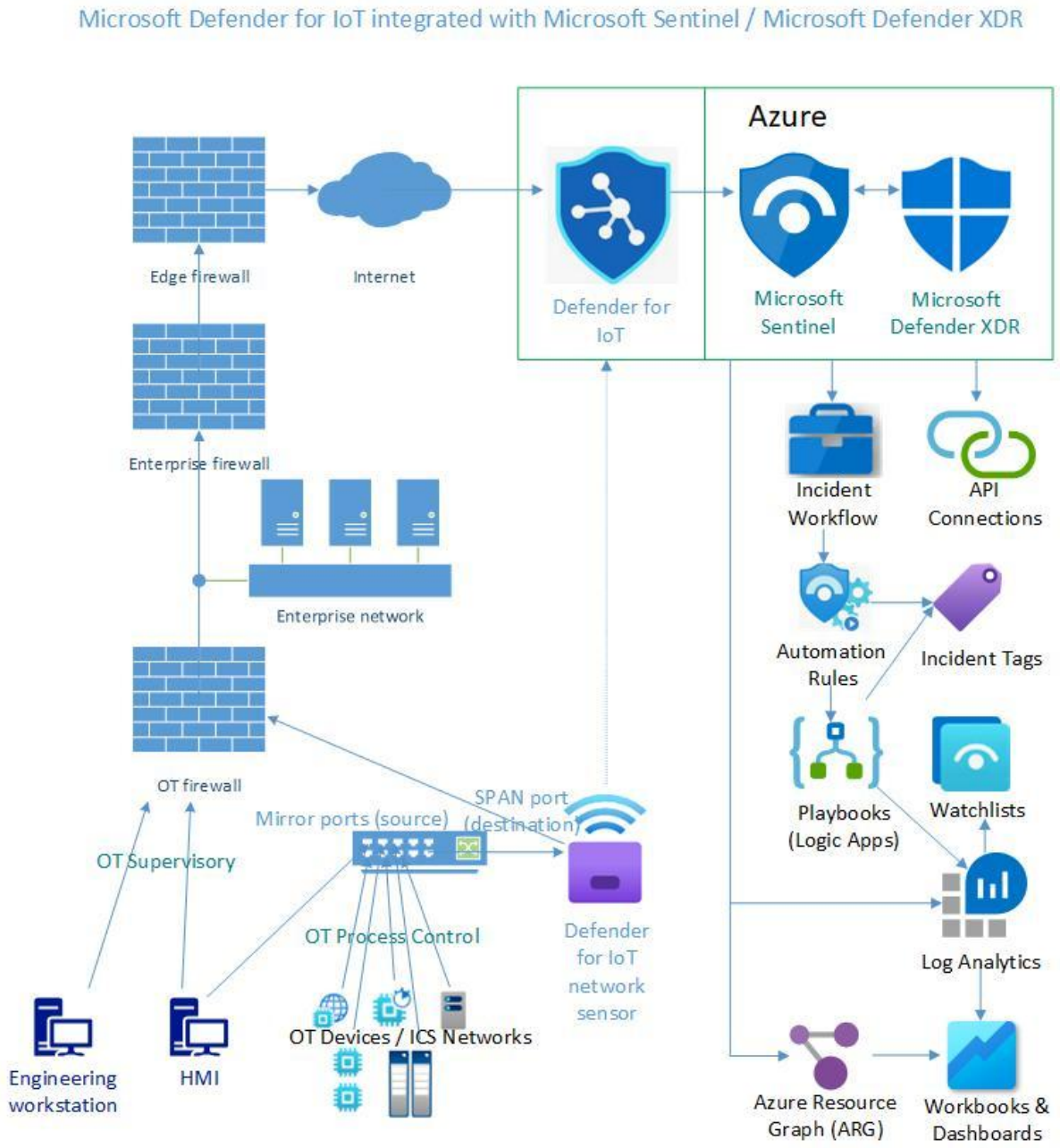
Address
48.222.98.0


5fff6965-15d9-45ce-8674-54415785dedc.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
24 0.034988 48.222.98.0 10.218.166.16 TCP 1514 80 → 49838 [PSH, ACK] Seq=26065 Ack=457 Win=88965120 Len=1448 TSval=2897024701 TSecr=721892205 [TCP PDU reassembled in 30]
25 0.034990 48.222.98.0 10.218.166.16 TCP 1514 80 → 49838 [PSH, ACK] Seq=27513 Ack=457 Win=88965120 Len=1448 TSval=2897024701 TSecr=721892205 [TCP PDU reassembled in 30]
26 0.034992 48.222.98.0 10.218.166.16 TCP 1514 80 → 49838 [PSH, ACK] Seq=28961 Ack=457 Win=88965120 Len=1448 TSval=2897024701 TSecr=721892205 [TCP PDU reassembled in 30]
27 0.035001 48.222.98.0 10.218.166.16 TCP 1514 80 → 49838 [PSH, ACK] Seq=30409 Ack=457 Win=88965120 Len=1448 TSval=2897024701 TSecr=721892205 [TCP PDU reassembled in 30]
28 0.035006 48.222.98.0 10.218.166.16 TCP 1514 80 → 49838 [PSH, ACK] Seq=31857 Ack=457 Win=88965120 Len=1448 TSval=2897024701 TSecr=721892205 [TCP PDU reassembled in 30]
29 0.035010 48.222.98.0 10.218.166.16 TCP 1514 80 → 49838 [PSH, ACK] Seq=33305 Ack=457 Win=88965120 Len=1448 TSval=2897024701 TSecr=721892205 [TCP PDU reassembled in 30]
30 0.035013 48.222.98.0 10.218.166.16 HTTP 1281 HTTP/1.1 403 Forbidden (text/html)
31 0.035079 10.218.166.16 48.222.98.0 TCP 66 49838 → 80 [ACK] Seq=457 Ack=2881 Win=3328 Len=0 TSval=721892223 TSecr=2897024701
32 0.035217 10.218.166.16 48.222.98.0 TCP 78 [TCP Dup ACK 31#1] 49838 → 80 [ACK] Seq=457 Ack=2881 Win=3328 Len=0 TSval=721892224 TSecr=2897024701 SLE=2897 SRE=6340
33 0.035220 10.218.166.16 48.222.98.0 TCP 78 [TCP Dup ACK 31#2] 49838 → 80 [ACK] Seq=457 Ack=2881 Win=3328 Len=0 TSval=721892224 TSecr=2897024701 SLE=2897 SRE=6340
34 0.035221 10.218.166.16 48.222.98.0 TCP 78 [TCP Dup ACK 31#3] 49838 → 80 [ACK] Seq=457 Ack=2881 Win=3328 Len=0 TSval=721892224 TSecr=2897024701 SLE=2897 SRE=6340
35 0.474150 10.218.166.16 48.222.98.0 TCP 66 49841 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
36 0.475128 10.218.166.16 48.222.98.0 TCP 66 49842 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
37 0.489454 48.222.98.0 10.218.166.16 TCP 66 80 → 49841 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1440 SACK_PERM WS=2048
38 0.489608 48.222.98.0 10.218.166.16 TCP 66 80 → 49842 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1440 SACK_PERM WS=2048
39 0.489914 10.218.166.16 48.222.98.0 TCP 60 49841 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
40 0.489916 10.218.166.16 48.222.98.0 TCP 60 49842 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
41 0.501114 10.218.166.16 48.222.98.0 HTTP 401 GET /filestreamingservice/files/3a37e79e-03be-4796-8d25-00a6cd45cc97/pieceshash?cacheHostOrigin=dl.delivery.mp.microsoft.com
42 0.501156 10.218.166.16 48.222.98.0 HTTP 401 GET /filestreamingservice/files/511c6cff-ed08-4366-a308-56cdb4e4d3e5/pieceshash?cacheHostOrigin=dl.delivery.mp.microsoft.com
43 0.501972 48.222.98.0 10.218.166.16 TCP 60 80 → 49842 [ACK] Seq=1 Ack=348 Win=86710272 Len=0
44 0.502037 48.222.98.0 10.218.166.16 TCP 60 80 → 49841 [ACK] Seq=1 Ack=348 Win=86710272 Len=0
45 0.508239 48.222.98.0 10.218.166.16 TCP 1514 80 → 49842 [PSH, ACK] Seq=1 Ack=348 Win=86712320 Len=1460 [TCP PDU reassembled in 97]
</style>\n
<title>Web Filter Violation</title>\n
</head>\n
<body> \n
\n
<h1>FortiGuard Intrusion Prevention - Access Blocked</h1>\n
<h3>Web Page Blocked</h3>\n
You have tried to access a web page that is in violation of your Internet usage policy. \n
<table><tbody>\n
<tr>\n
<td>Category</td>\n
<td>Unrated</td>\n
</tr>\n
<tr>\n
<td>URL</td>\n
[…] <td>http://48.222.98.0/filestreamingservice/files/e9b88c21-f2db-4ddb-a3a8-b59d992b348d?
</tr>\n
</tbody></table>\n
0040 33 6d 74 72 75 73 69 6f 6e 20 50 72 65 76 65 6e 3mtrusio n Preven
0050 74 69 6f 6e 20 2d 20 41 63 63 65 73 73 20 42 6c tion - A ccess Bl
0060 6f 63 6b 65 64 3c 2f 68 31 3e 0a 20 20 20 20 3c ocked</h 1>· <
0070 68 33 3e 57 65 62 20 50 61 67 65 20 42 6c 6f 63 h3>Web P age Bloc
0080 6b 65 64 3c 2f 68 33 3e 0a 20 20 20 20 3c 70 3e ked</h3> ·
0090 59 6f 75 20 68 61 76 65 20 74 72 69 65 64 20 74 You have tried t
00a0 6f 20 61 63 63 65 73 73 20 61 20 77 65 62 20 70 o access a web p
00b0 61 67 65 20 74 68 61 74 20 69 73 20 69 6e 20 76 age that is in v
00c0 69 6f 6c 61 74 69 6f 6e 20 6f 66 20 79 6f 75 72 iolation of your
00d0 20 49 6e 74 65 72 6e 65 74 20 75 73 61 67 65 20 Interne t usage
00e0 70 6f 6c 69 63 79 2e 3c 2f 70 3e 0a 20 20 20 20 policy.< /p>·
00f0 3c 74 61 62 6c 65 3e 3c 74 62 6f 64 79 3e 0a 20 <table>< tbody>·
0100 20 20 20 20 20 20 20 3c 74 72 3e 0a 20 20 20 20 < tr>·
0110 20 20 20 20 20 20 20 20 3c 74 64 3e 43 61 74 65 <td>Cate
0120 67 6f 72 79 3c 2f 74 64 3e 0a 20 20 20 20 20 20 gory</td >·
0130 20 20 20 20 20 20 3c 74 64 3e 55 6e 72 61 74 65 <t d>Unrate
0140 64 3c 2f 74 64 3e 0a 20 20 20 20 20 20 20 20 3c d</td>· <
0150 2f 74 72 3e 0a 20 20 20 20 20 20 20 20 3c 74 72 /tr>· <tr
0160 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 >· <t
0170 64 3e 55 52 4c 3c 2f 74 64 3e 0a 20 20 20 20 20 d>URL</t d>·
0180 20 20 20 20 20 20 20 3c 74 64 3e 68 74 74 70 3a < td>http:

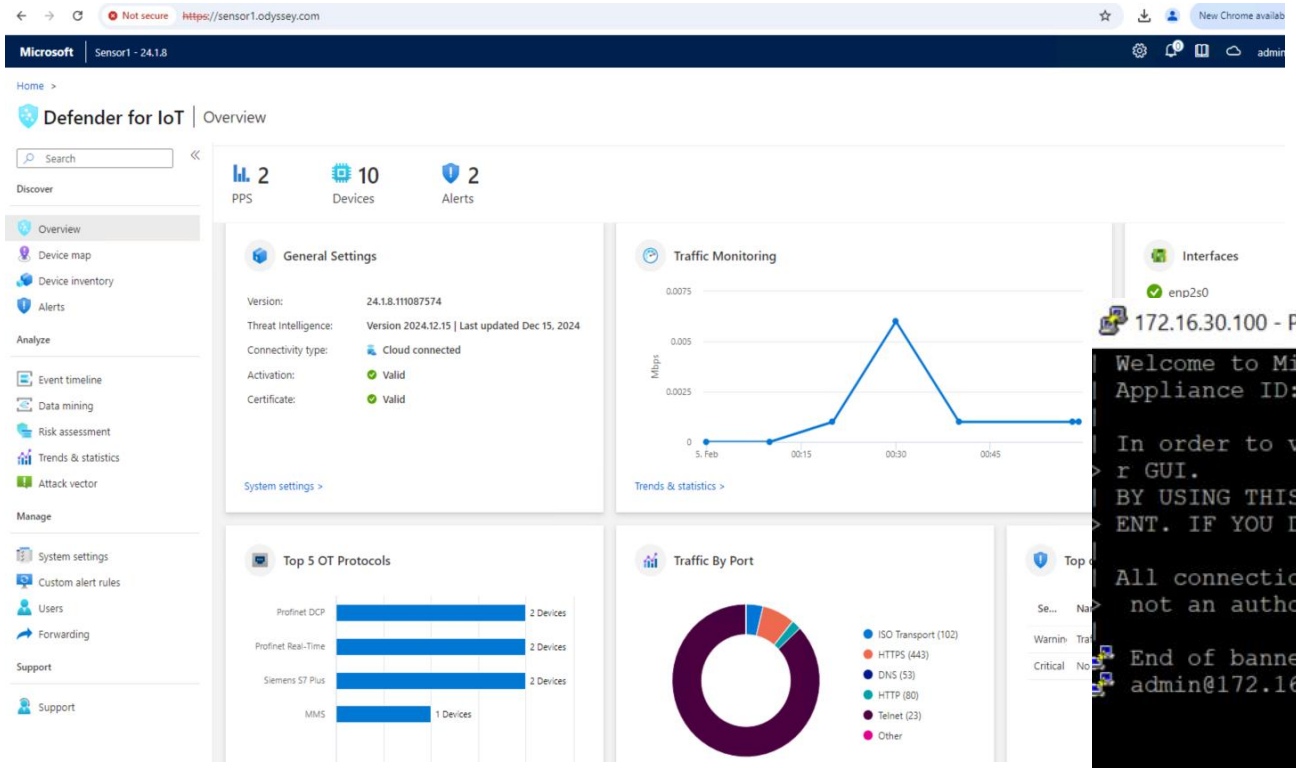
Microsoft Defender for IoT Topology

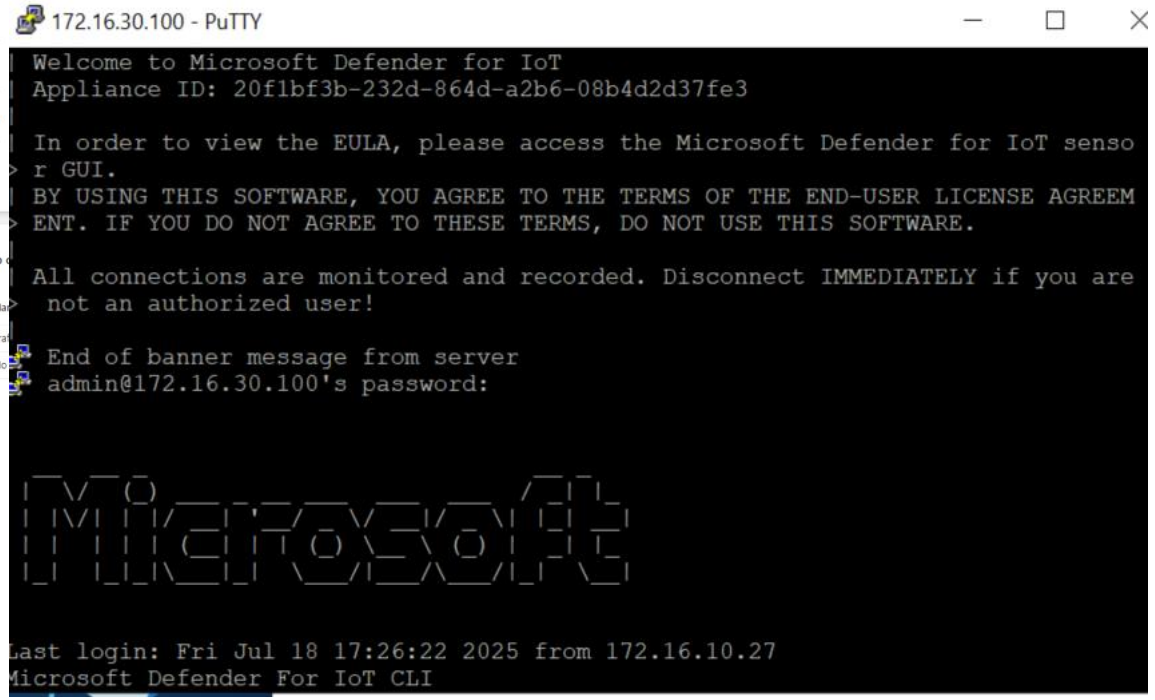


Microsoft Defender for IoT Topology: Integrated with Microsoft Sentinel/Defender XDR



Microsoft Defender for IoT Sensor Overview





Microsoft Defender for IoT

HARDWARE SENSOR

Preconfigured physical appliances for OT monitoring

Hardware profile	Appliance
C5600	HPE ProLiant DL360 Gen 11 Dell PowerEdge R660
E1800	HPE ProLiant DL20 Gen11 (4SFF) Dell PowerEdge R360
E500	Dell Edge 5200 (Rugged MIL-STD-810G)
L500	HPE ProLiant DL20 Gen11 Plus (NHP 2LFF) DELL XE4 Small Form Factor (SFF)
L100	YS-Techsystems YS-FIT2 (Rugged MIL-STD-810G) Dell Edge Gateway 3200

Hardware profile	SPAN/TAP throughput	Max monitored Assets
C5600	Up to 3 Gbps	12 K

Hardware profile	SPAN/TAP throughput	Max monitored assets
E1800	Up to 1 Gbps	10K
E1000	Up to 1 Gbps	10K
E500	Up to 1 Gbps	10K

Hardware profile	SPAN/TAP throughput	Max monitored assets
L500	Up to 200 Mbps	1,000
L100	Up to 10 Mbps	800

OT monitoring with virtual appliances

Hardware profile	Performance / Monitoring	Physical specifications
C5600	**Max bandwidth:** 2.5 Gb/sec **Max monitored assets:** 12,000	**vCPU:** 32 **Memory:** 32 GB **Storage:** 5.6 TB (600 IOPS)
E1800	**Max bandwidth:** 800 Mb/sec **Max monitored assets:** 10,000	**vCPU:** 8 **Memory:** 32 GB **Storage:** 1.8 TB (300 IOPS)
E1000	**Max bandwidth:** 800 Mb/sec **Max monitored assets:** 10,000	**vCPU:** 8 **Memory:** 32 GB **Storage:** 1 TB (300 IOPS)
E500	**Max bandwidth:** 800 Mb/sec **Max monitored assets:** 10,000	**vCPU:** 8 **Memory:** 32 GB **Storage:** 500 GB (300 IOPS)
L500	**Max bandwidth:** 160 Mb/sec **Max monitored assets:** 1,000	**vCPU:** 4 **Memory:** 8 GB **Storage:** 500 GB (150 IOPS)
L100	**Max bandwidth:** 100 Mb/sec **Max monitored assets:** 800	**vCPU:** 4 **Memory:** 8 GB **Storage:** 100 GB (150 IOPS)
L60 *	**Max bandwidth:** 10 Mb/sec **Max monitored assets:** 100	**vCPU:** 4 **Memory:** 8 GB **Storage:** 60 GB (150 IOPS)

(VM specs published by Microsoft prior to 9/18/2025 when the recommendation was changed to review corresponding physical appliance specs.)

OT site licenses

Microsoft Defender for IoT - OT site license - XS

$70.00

license/month, paid yearly

(annual commitment)

(Includes up to 100 devices per site; annual subscription—auto renews)

Microsoft Defender for IoT - OT site license - S

$150.00

license/month, paid yearly

(annual commitment)

(Includes up to 250 devices per site; annual subscription—auto renews)

Most popular

Microsoft Defender for IoT - OT site license - M

$250.00

license/month, paid yearly

(annual commitment)

(Includes up to 500 devices per site; annual subscription—auto renews)

Microsoft Defender for IoT - OT site license - L

$400.00

license/month, paid yearly

(annual commitment)

(Includes up to 1,000 devices per site; annual subscription—auto renews)

Microsoft Defender for IoT - OT site license - XL

$1,500.00

license/month, paid yearly

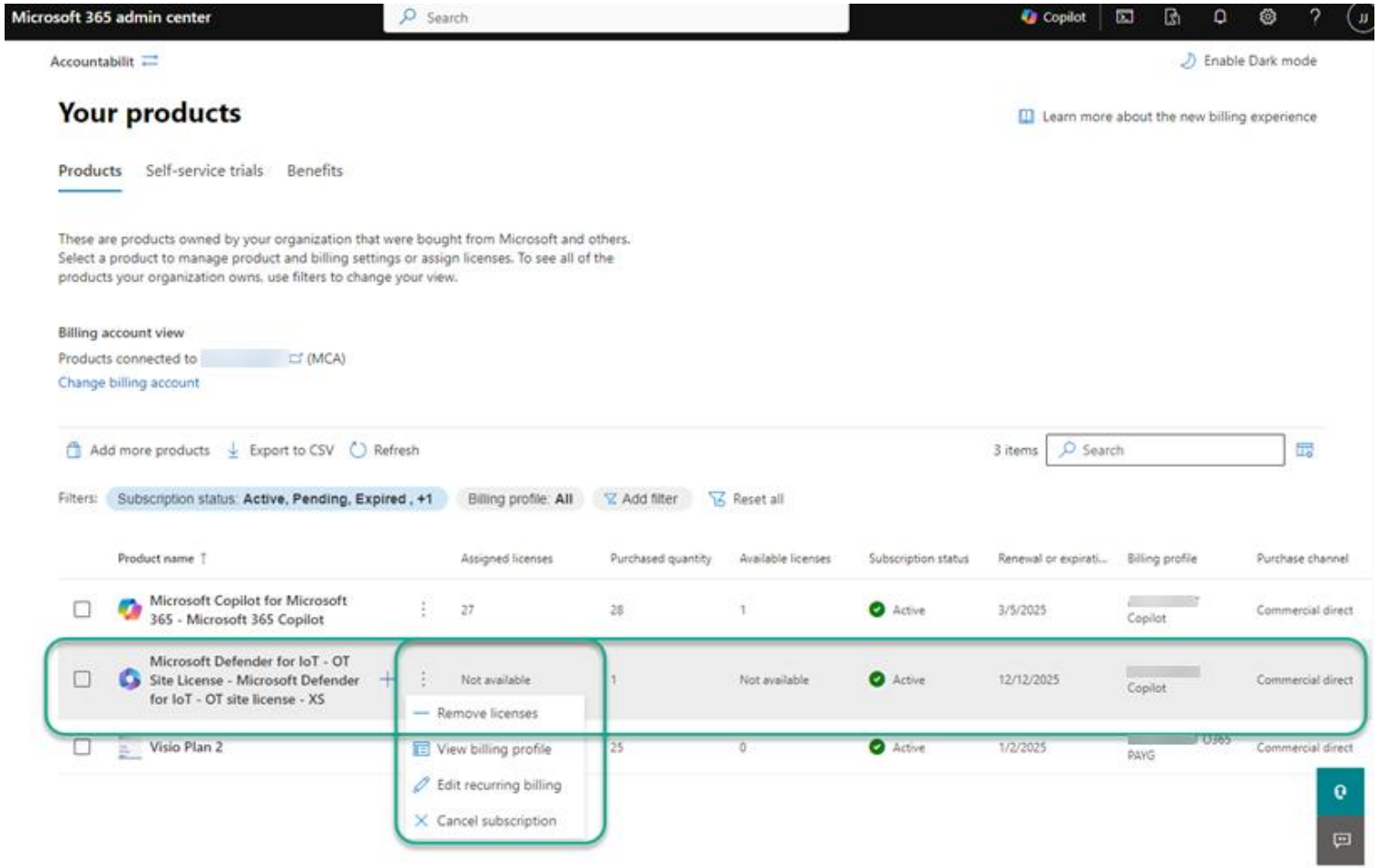
(annual commitment)

(Includes up to 5,000 devices per site; annual subscription—auto renews)

https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-iot-pricing

Microsoft Defender for IoT – OT Site License

- Purchased through M365 Admin center, then consumed from an Azure subscription
- Is an annual subscription than can not be cancelled for refund



2-Month Proof of Concept: Microsoft Defender for IoT

PHASE 1:

Defender for IoT Sensor Planning

- We begin with a collaborative gap analysis of network segmentation, firewall configurations, and sensor deployment strategies - ensuring an optimal Defender for IoT implementation aligned with industry security frameworks.
- The goal is to identify up to one hundred (100) IoT devices in one physical site that will be licensed for a production Defender for IoT deployment, leveraging best practice recommendations gathered during the gap analysis.

2-Month Proof of Concept: Microsoft Defender for IoT

PHASE 2:

IoT Sensor Deployment

- Once the target devices and networking details are agreed upon, we deploy a hardware sensor and OT Site Licensing for up to 100 IoT devices - delivering actionable insights and best-practice recommendations to enhance visibility and mitigate cyber risks across air-gapped and interconnected OT environments.

- The licensing is deployed directly into the customer tenant and the hardware sensor deployed during the POC permanently remains with the customer once the assessment is complete.

2-Month Proof of Concept: Microsoft Defender for IoT

PHASE 3:

Defender for IoT Post-Deployment

- We validate our device discovery and enable the appropriate detection engines and risk/security reporting - ensuring the operational "ready state" and effectiveness of the Defender for IoT deployment.
- Custom dashboards, alert rules, and test plans are created to enhance visibility, assess vulnerabilities, and simulate attack paths for mitigation planning.

2-Month Proof of Concept: Microsoft Defender for IoT

PHASE 4:

OT SOC Operations

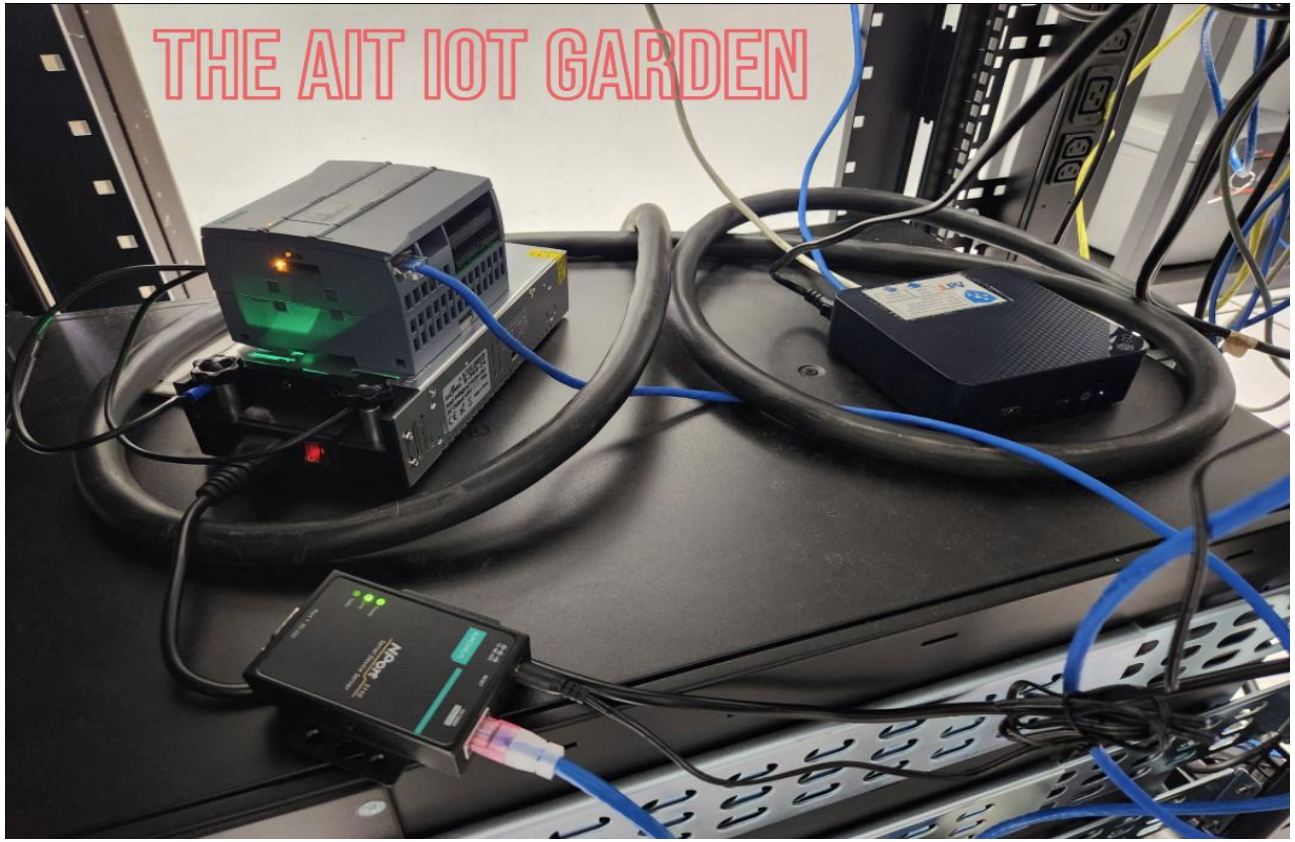
- We establish secure administration of Defender for IoT Azure resources via Azure Lighthouse and integrate Defender for IoT with a Microsoft Sentinel SIEM instance.
- The phase includes escalation, and investigation protocols between the SOC team and the customer, enabling 24x7 OT SOC services.
- This portion of the engagement initiates once Phase 3 is completed and runs through the time remaining in the POC. It includes calls with a Security Engineer and an account executive to assess risk and identify optimization opportunities.

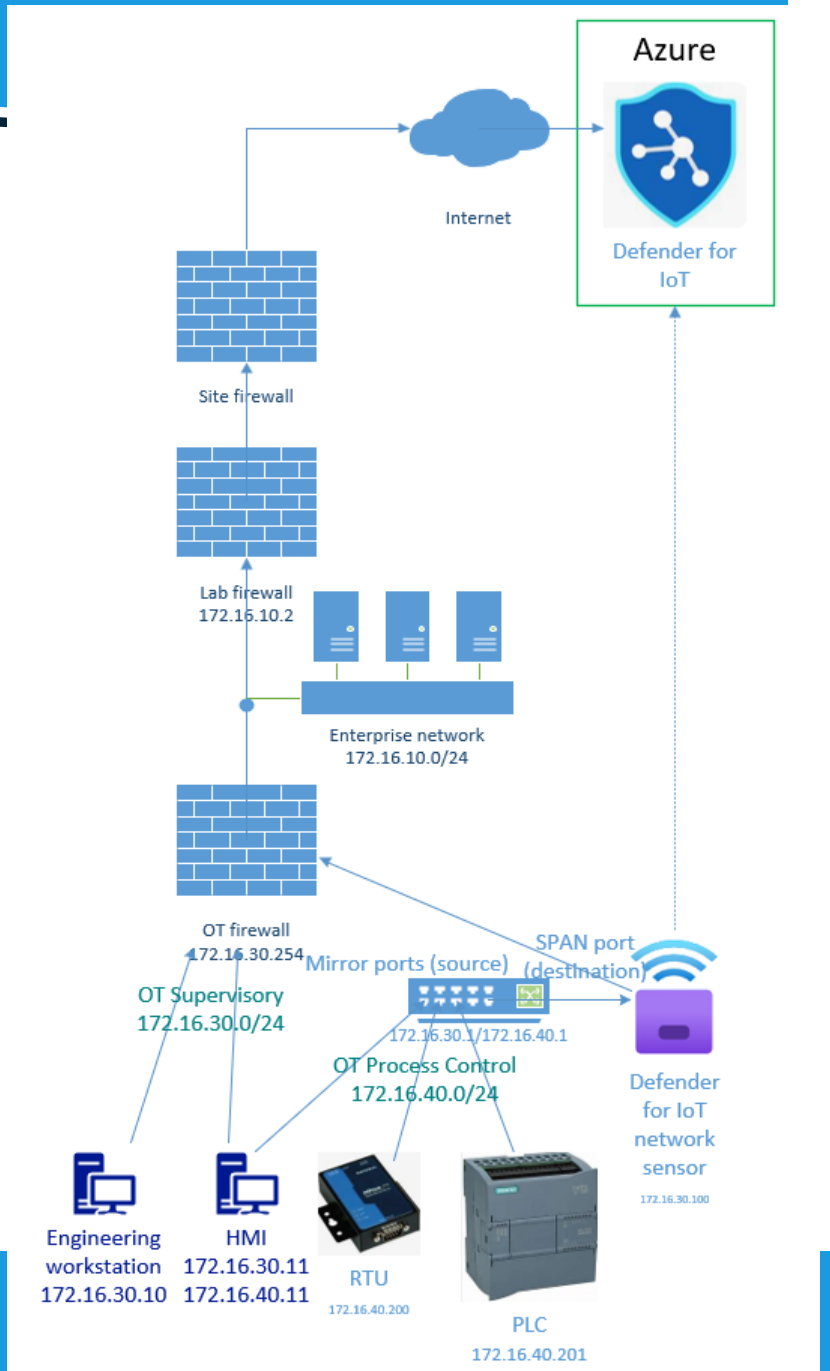
DEMO

Defender for IoT

Microsoft Defender for IoT connected to Microsoft Sentinel

Defender for IoT Demonstration Environment

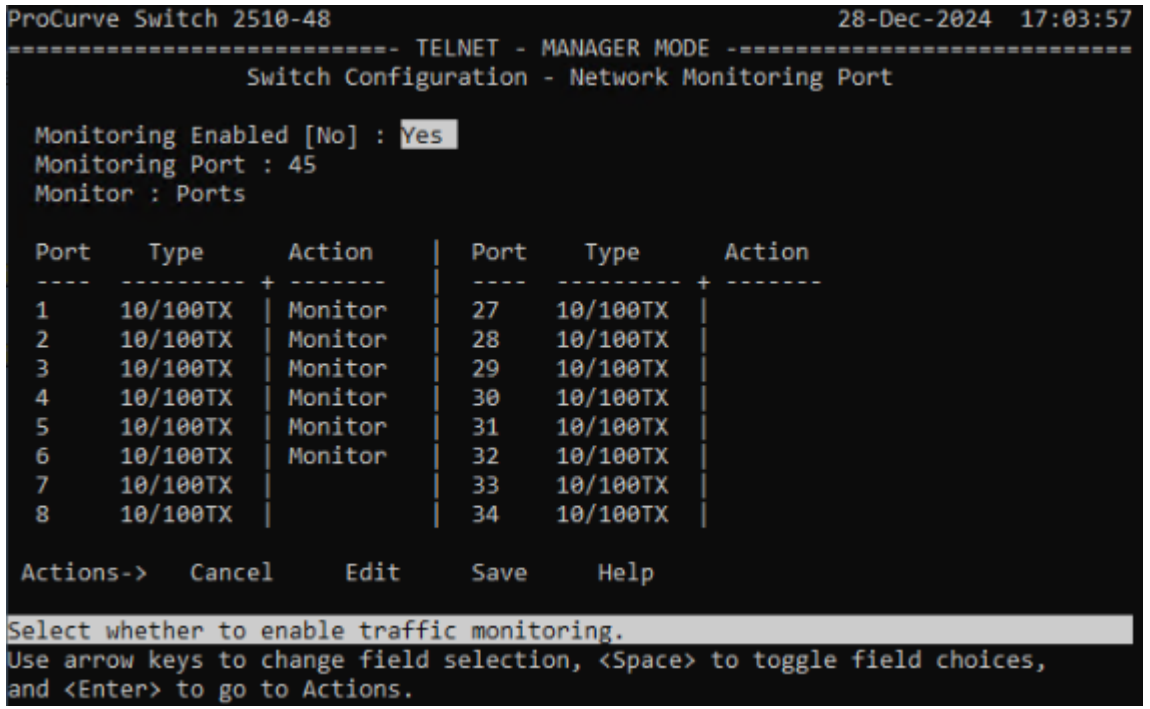




Configure mirroring with a switch SPAN port

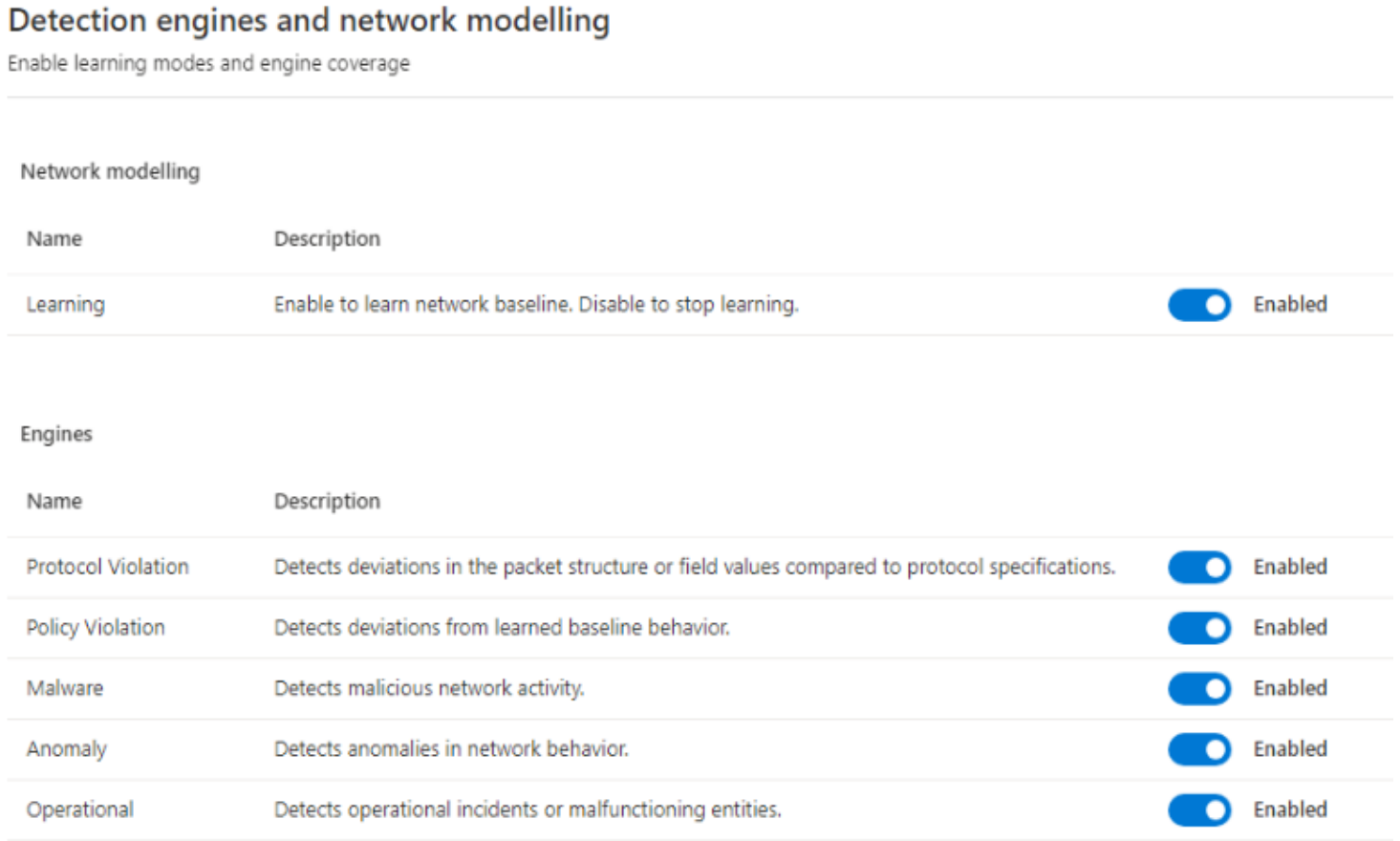
https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/traffic-mirroring/configure-mirror-span

- Ports 1-6 are mirrored to port 45
- Ports 1-6 are connected to IoT devices in the Process Control network



Configure IoT Sensor detection engines

- All on Enabled by default



Detection engines and network modelling

Enable learning modes and engine coverage

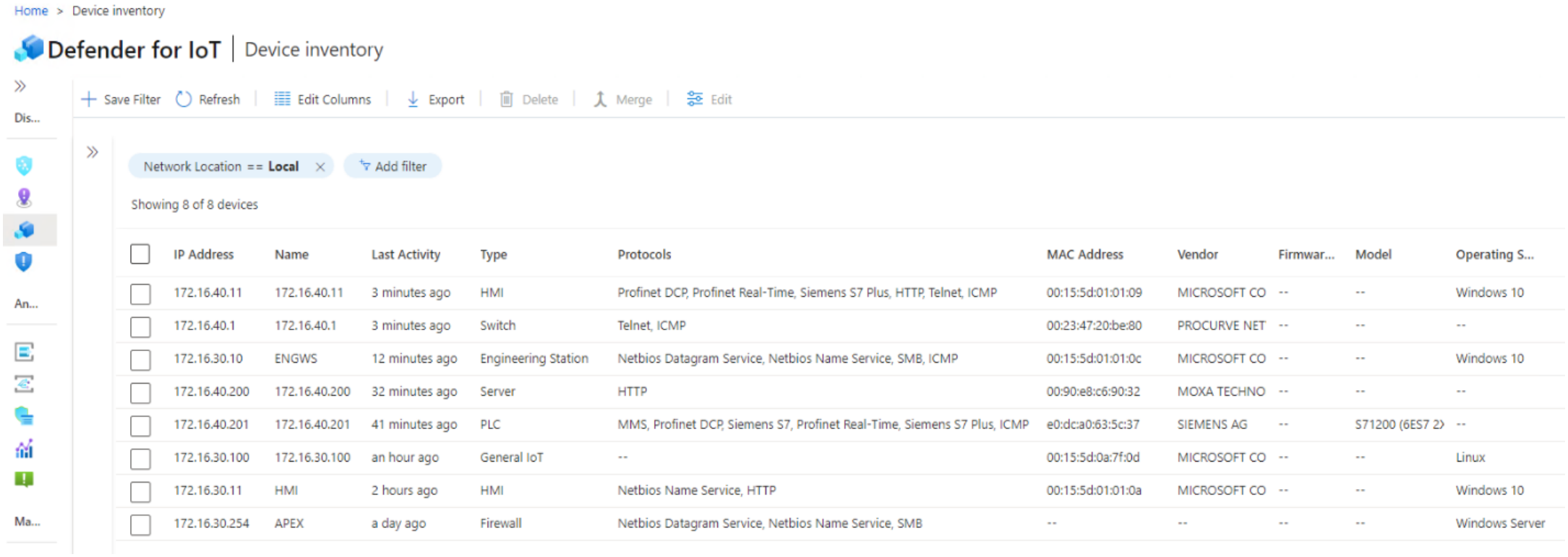
Network modelling

Name	Description	
Learning	Enable to learn network baseline. Disable to stop learning.	Enabled

Engines

Name	Description	
Protocol Violation	Detects deviations in the packet structure or field values compared to protocol specifications.	Enabled
Policy Violation	Detects deviations from learned baseline behavior.	Enabled
Malware	Detects malicious network activity.	Enabled
Anomaly	Detects anomalies in network behavior.	Enabled
Operational	Detects operational incidents or malfunctioning entities.	Enabled

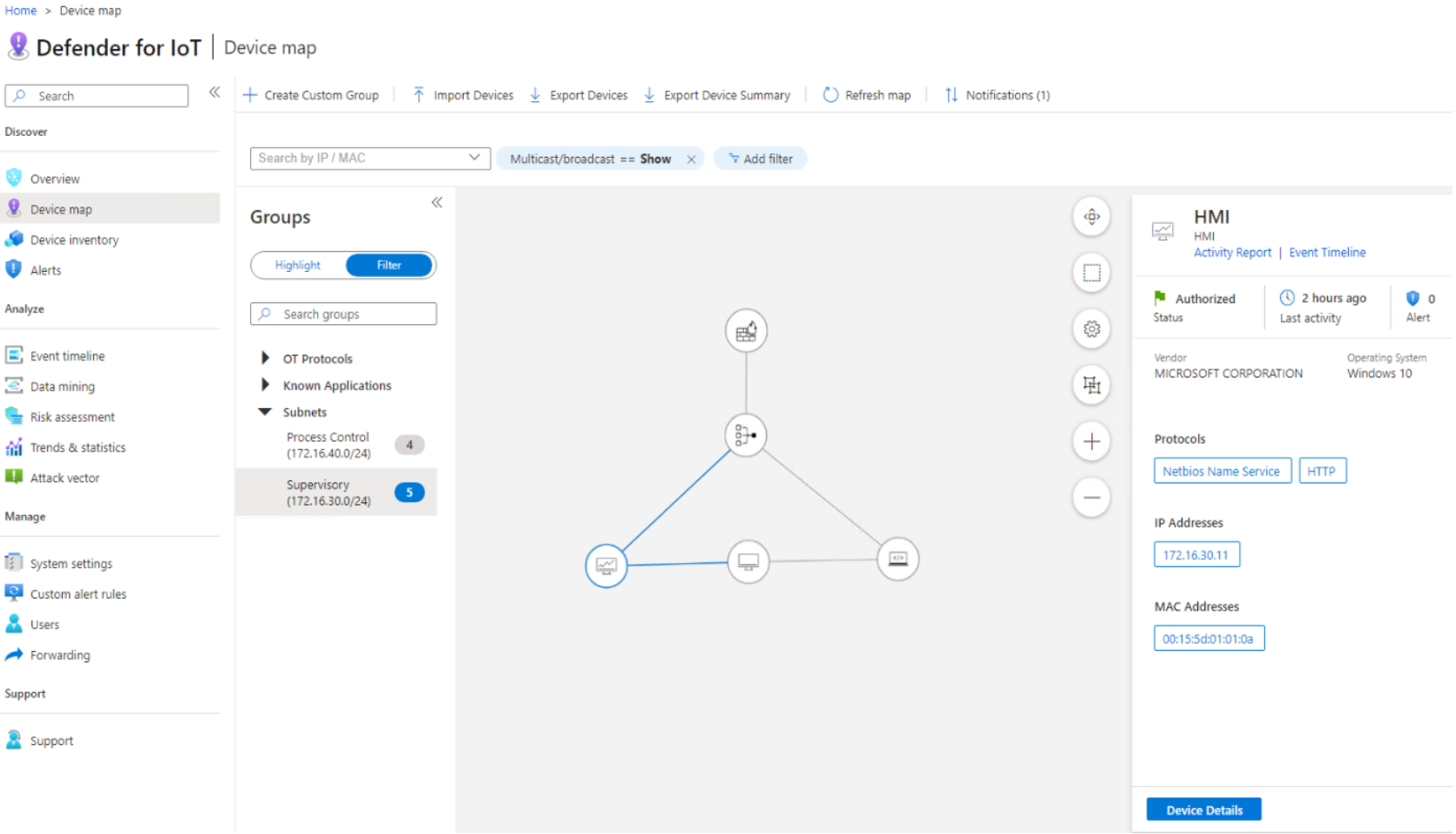
Defender for IoT: Device Inventory



IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmwar...	Model	Operating S...
172.16.40.11	172.16.40.11	3 minutes ago	HMI	Profinet DCP, Profinet Real-Time, Siemens S7 Plus, HTTP, Telnet, ICMP	00:15:5d:01:01:09	MICROSOFT CO	--	--	Windows 10
172.16.40.1	172.16.40.1	3 minutes ago	Switch	Telnet, ICMP	00:23:47:20:be:80	PROCURVE NET	--	--	--
172.16.30.10	ENGWS	12 minutes ago	Engineering Station	Netbios Datagram Service, Netbios Name Service, SMB, ICMP	00:15:5d:01:01:0c	MICROSOFT CO	--	--	Windows 10
172.16.40.200	172.16.40.200	32 minutes ago	Server	HTTP	00:90:e8:c6:90:32	MOXA TECHNO	--	--	--
172.16.40.201	172.16.40.201	41 minutes ago	PLC	MMS, Profinet DCP, Siemens S7, Profinet Real-Time, Siemens S7 Plus, ICMP	e0:dc:a0:63:5c:37	SIEMENS AG	--	S71200 (6ES7 2)	--
172.16.30.100	172.16.30.100	an hour ago	General IoT	--	00:15:5d:0a:7f:0d	MICROSOFT CO	--	--	Linux
172.16.30.11	HMI	2 hours ago	HMI	Netbios Name Service, HTTP	00:15:5d:01:01:0a	MICROSOFT CO	--	--	Windows 10
172.16.30.254	APEX	a day ago	Firewall	Netbios Datagram Service, Netbios Name Service, SMB	--	--	--	--	Windows Server

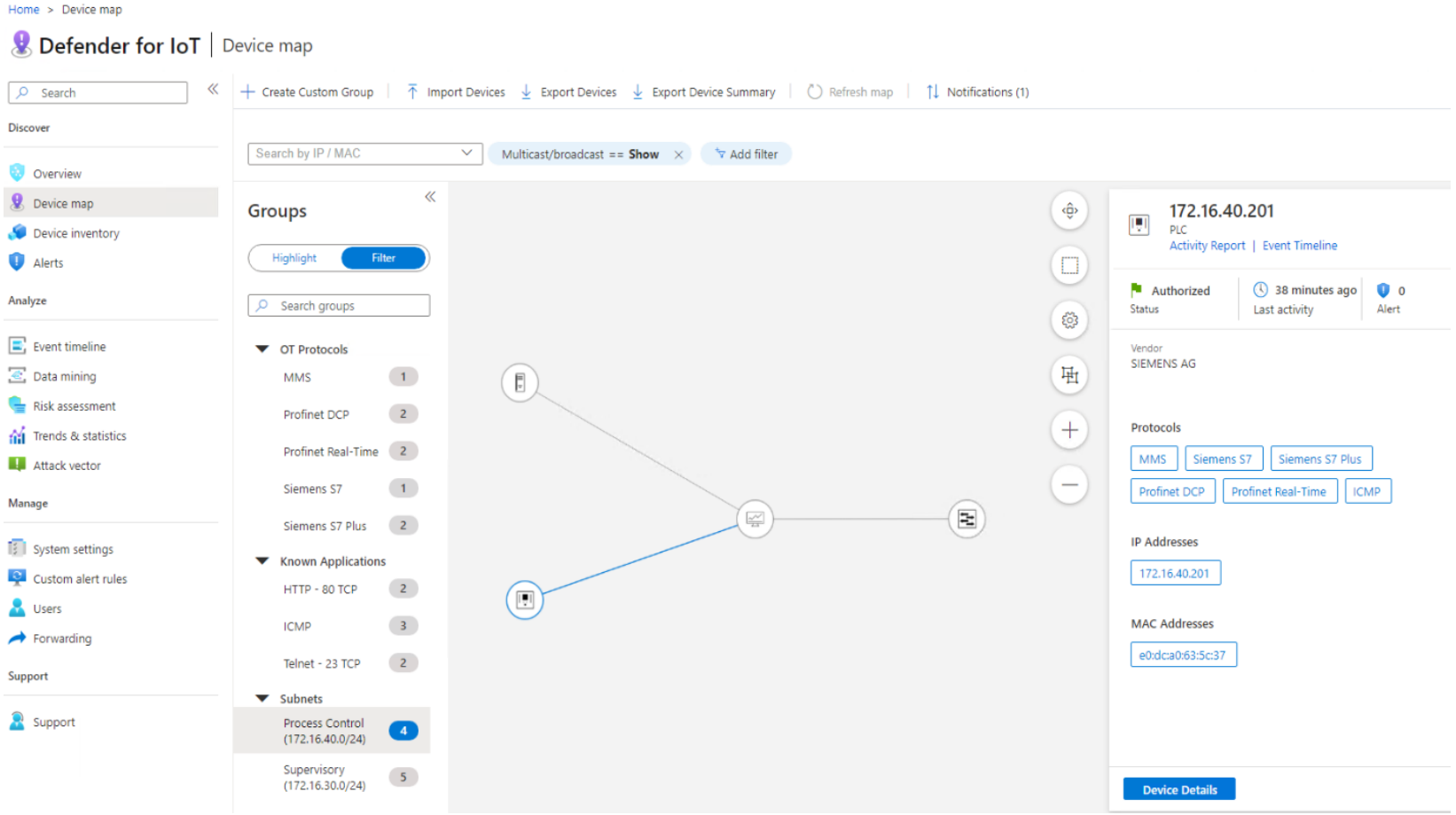
Defender for IoT Device Map

Supervisory network contains HMI, EngWs, IoT Sensor management interface, and firewall/default gateway



Defender for IoT Device Map

Process Control network contains PLC, serial server, HMI, and switch



Defender for IoT | Device map

Search

Discover

Overview
Device map
Device inventory
Alerts

Analyze

Event timeline
Data mining
Risk assessment
Trends & statistics
Attack vector

Manage

System settings
Custom alert rules
Users
Forwarding

Support

Support

+ Create Custom Group | Import Devices | Export Devices | Export Device Summary | Refresh map | Notifications (25)

Search by IP / MAC

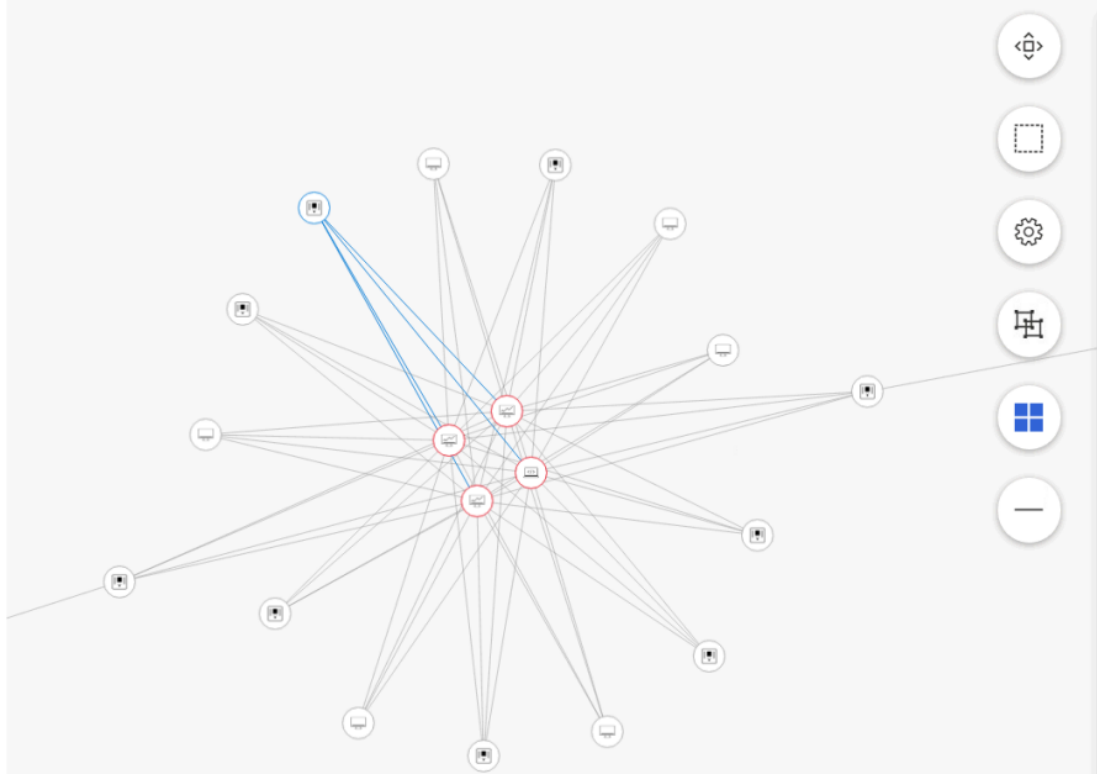
Multicast/broadcast == **Show**

Groups

Highlight | Filter

Search groups

- **OT Protocols**
  - BACNet 1
  - BACNet (NPDU) 1
  - CIP 124
  - EtherNet/IP 158
  - Honeywell Control Data Access 1
  - MODBUS 2
  - Omron FINS 1
  - Rockwell CSP2 21
- **Known Applications**
- **Subnets**
- **CDP Protocol**



[redacted]
PLC
Activity Report | Event Timeline

Authorized	4 minutes ago	0
Status	Last activity	Alert

Vendor
Rockwell Automation

Protocols

Rockwell CSP2 | ICMP

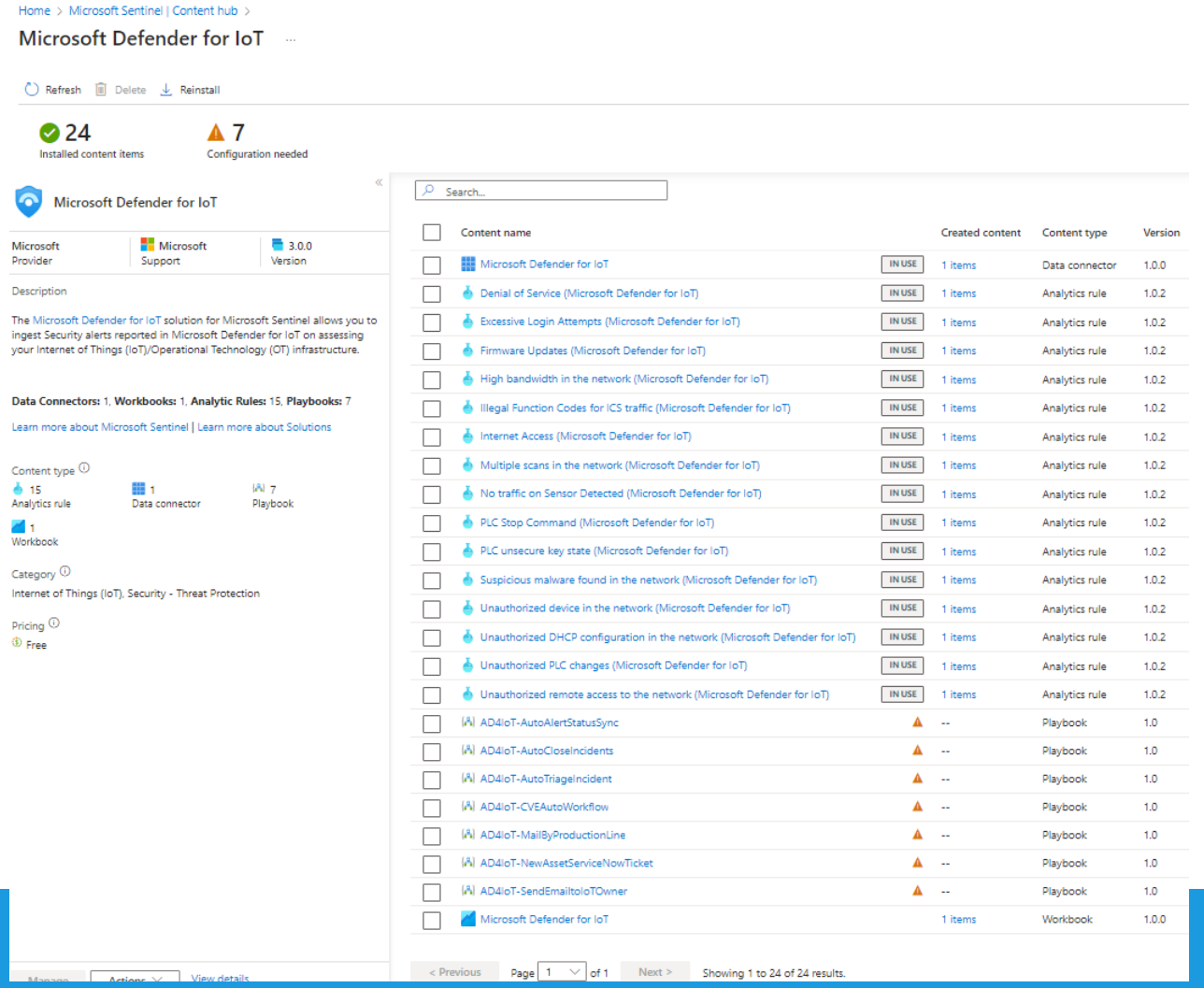
IP Addresses

[redacted]

Device Details

Microsoft Defender for IoT solution in Microsoft Sentinel Content Hub

- Data connector
- 15 analytic rules
- 7 playbooks
- 1 workbook

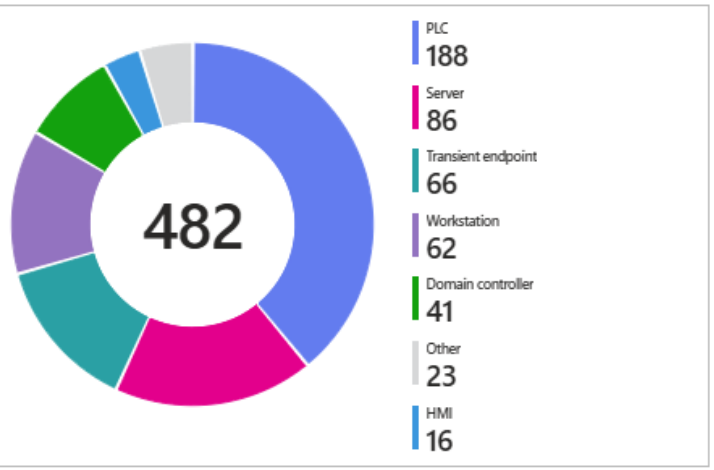


Microsoft Defender for IoT -

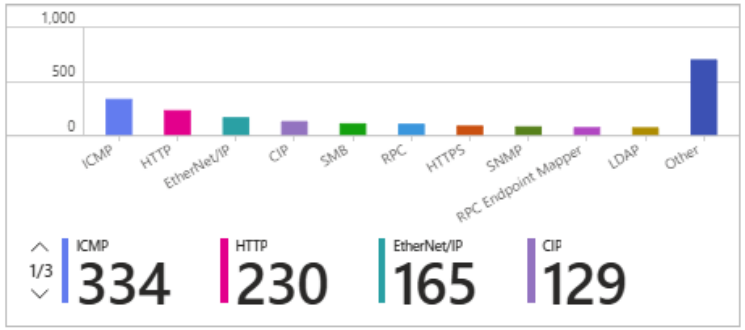
Microsoft Sentinel workbook for Defender for IoT: Overview tab

Edit Open Help Auto refresh: Off

Active Devices by Type



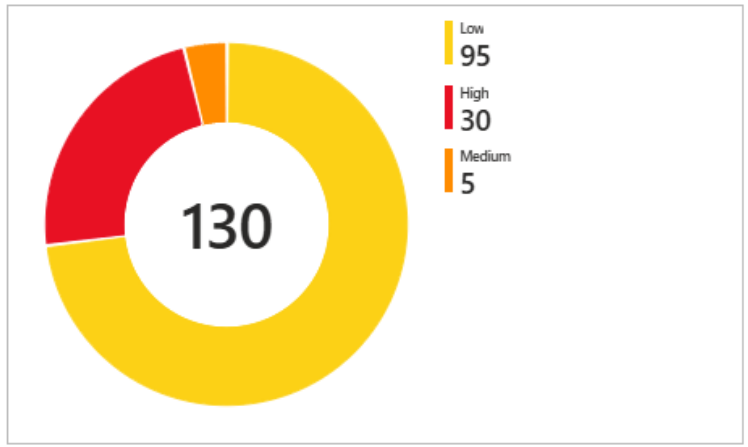
Active OT Devices by Protocol



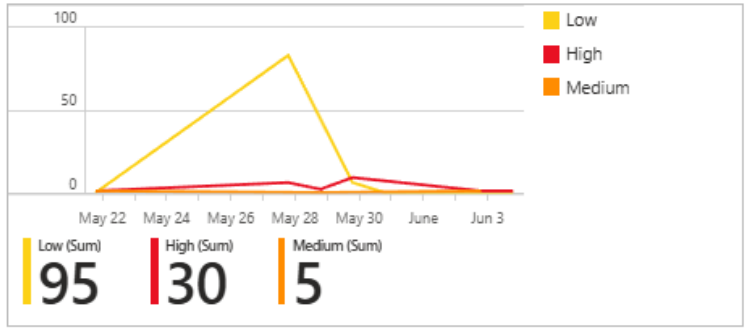
Recent Discovered Devices

Time First Seen	Device Name	Device Link	Type
6/4/2025, 9:52:09.000 AM		Device >>	
6/4/2025, 9:51:15.000 AM		Device >>	
6/4/2025, 8:58:10.000 AM		Device >>	Workstati

Incidents by Severity



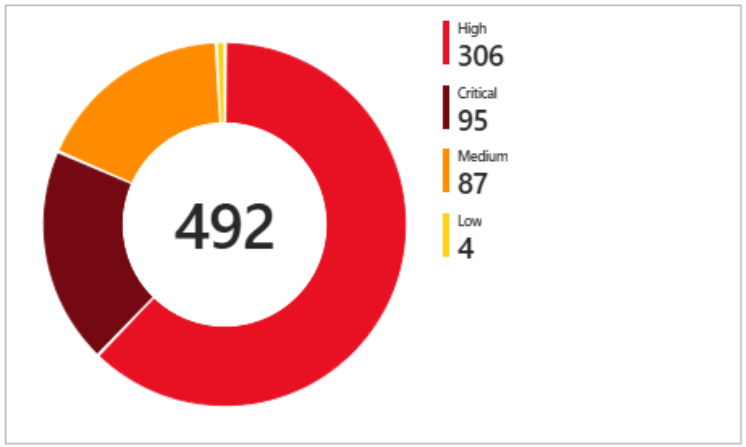
Incidents Trend Overtime



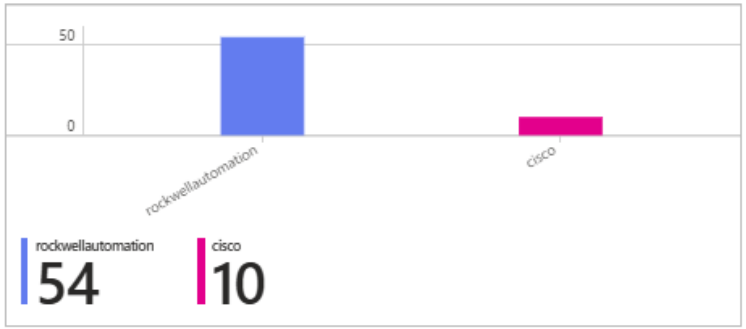
Recent Open Incidents

TimeGenerated	Incident Name	Link	Incident ID
6/4/2025, 2:23:34.223 ...	(MDIoT) Port Scan Detect...	Incident >>	
6/4/2025, 1:55:42.936 ...	(MDIoT) Port Scan Detect...	Incident >>	
6/3/2025, 7:45:45.611 ...	(MDIoT) Address Scan De...	Incident >>	

CVEs by Severity



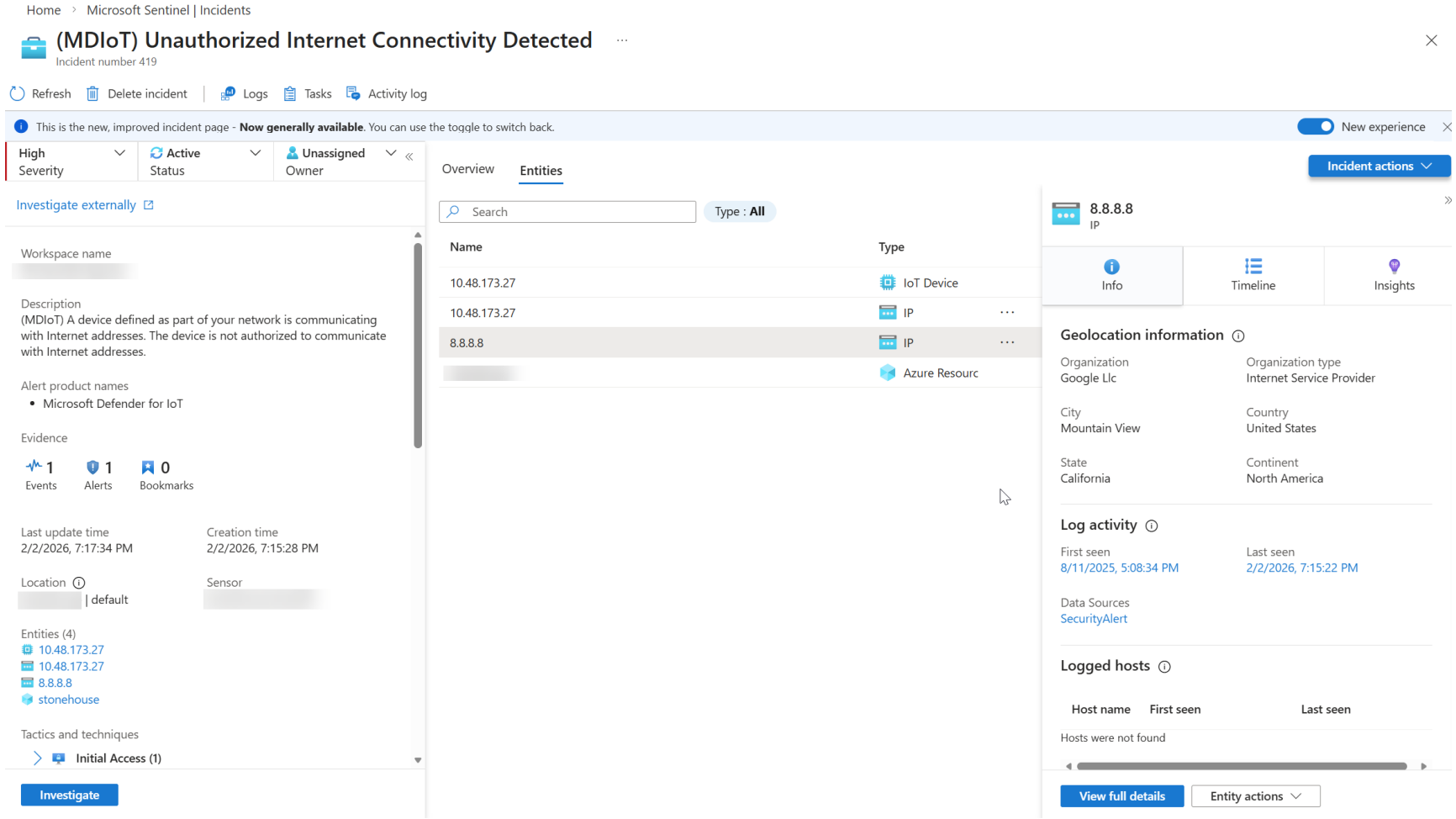
CVEs by Vendor



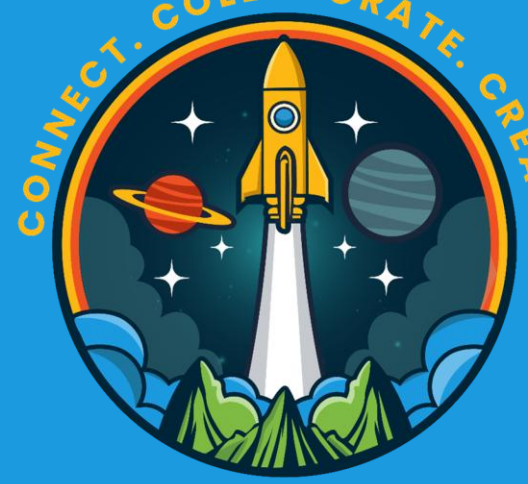
Top Vulnerable Devices

Device Name	Open Alerts	Total CVEs	Critical	High	Me
	1	24	8	12	
	1	22	8	11	
	1	19	6	9	

Microsoft Defender for IoT incidents in Microsoft Sentinel console



Session feedback available in home feed of the app after the session



MC2MC

CONNECT