

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/B00J4XUH30>



<https://github.com/john-joyner>



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



<https://blog.johnjoyner.net/blog>

2Pint



robopack

wortell

INGRAM
MICRO®



The Collective



bechtle



lebon.IT



VirtualMetric



veeam



evri

Microsoft Defender for IoT



OT Overview

OT Security Market Drivers

IT vs. OT Security

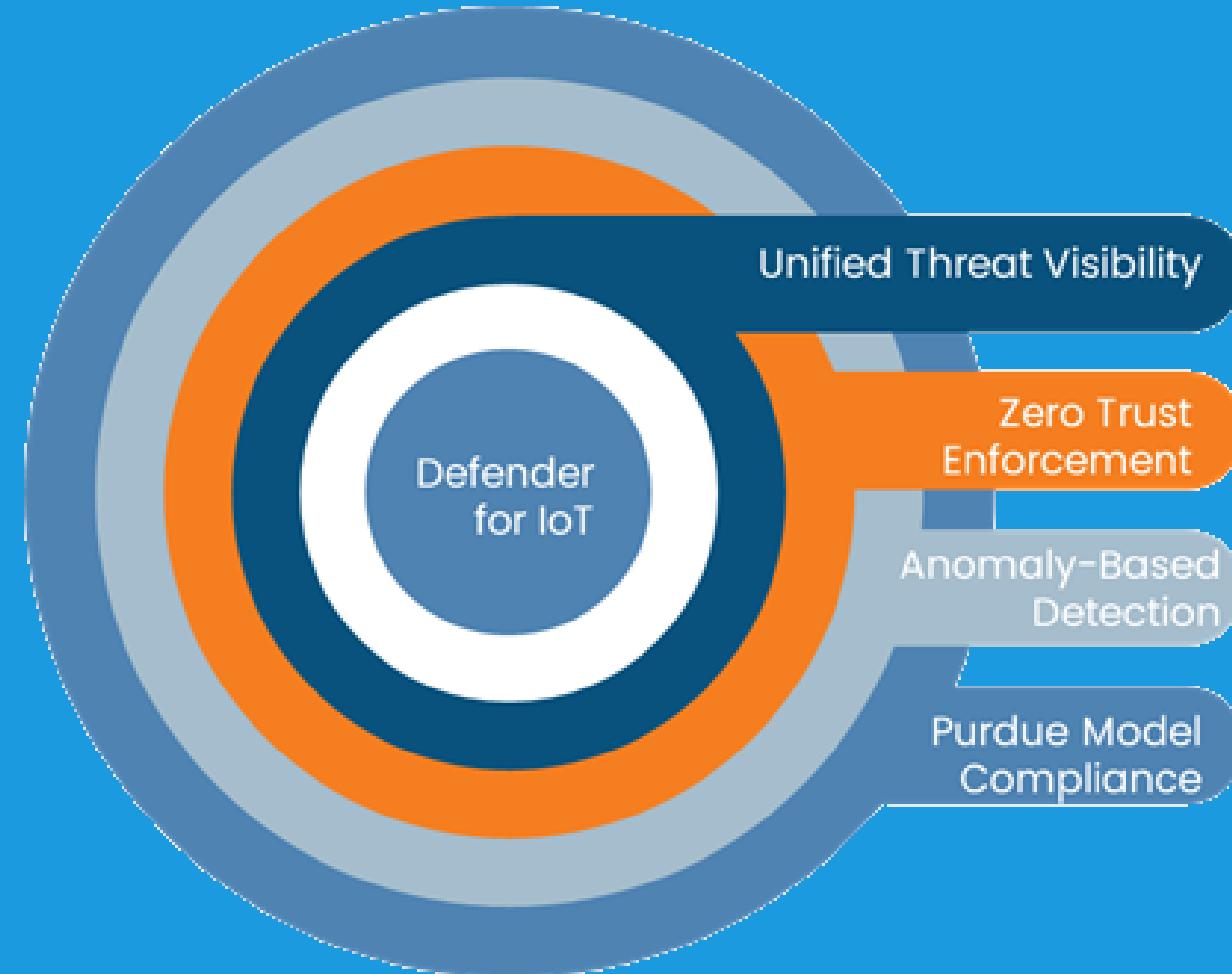
Defender for IoT Architecture

OT Customer Challenges

Microsoft Defender XDR Integration

TODAY'S
AGENDA

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

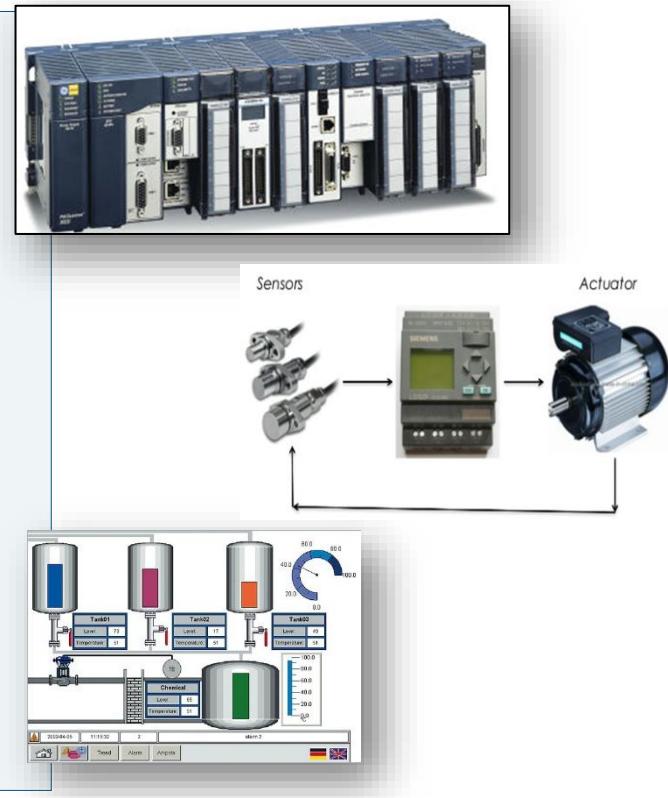
- ▶ PLC receives information from connected sensors or input devices, processes the data, and triggers outputs based on pre-programmed parameters.
 - ABB, Allen Bradley, Siemens, Mitsubishi, Honeywell, Motorola, Hitachi, General Electric,

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

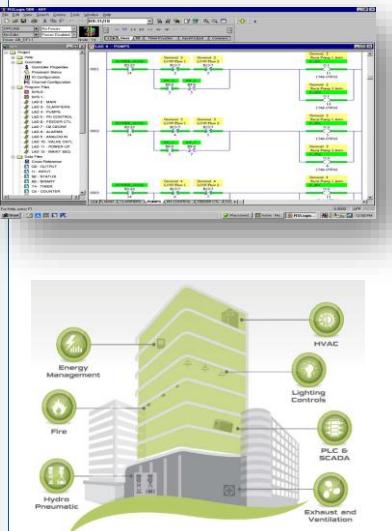
- ▶ Very reliable computer designed for configuration, maintenance and diagnostics of the Industrial Control System (ICS) applications

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

- Data confidentiality & privacy
- High levels of connectivity
- Standard protocols & devices
- Multiple layers of controls & telemetry

OT SECURITY

- Safety & availability
- Traditionally air-gapped
- Specialized protocols, devices & legacy OS platforms
- 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

Specifically what kinds of OT devices are targeted?

II 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 Failed		OPERATIONAL	42 minutes ago	New	192.168.165.88	Impair process control
Medium	EtherNet/IP CIP Service Request Failed		OPERATIONAL	42 minutes ago	New	10.92.181.170	Impair process control
Medium	EtherNet/IP CIP Service Request Failed		OPERATIONAL	42 minutes ago	New	10.92.195.21	Impair process control
Medium	EtherNet/IP Encapsulation Protocol Configuration Change		OPERATIONAL	43 minutes ago	New	192.168.165.90	Collection
Medium	Device Failed to Receive a Dynamic IP		OPERATIONAL	an hour ago	New	10.92.248.249	Discovery
Medium	EtherNet/IP CIP Service Request Failed		OPERATIONAL	an hour ago	New	10.92.183.160	Impair process control
Medium	Device Failed to Receive a Dynamic IP		OPERATIONAL	an hour ago	New	10.48.248.249	Discovery
Low	Suspicion of Unresponsive MODBUS		OPERATIONAL	an hour ago	New	--	Inhibit response function
Low	Suspicion of Unresponsive MODBUS		OPERATIONAL	an hour ago	New	--	Inhibit response function
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	Address Scan Detected		ANOMALY	15 hours ago	New	stopc814	Discovery
High	Excessive Login Attempts		POLICY_VIOLATION	a day ago	New	192.168.165.15	Discovery
Medium	Firmware Change Detected		ANOMALY	a day ago	New	LOGPCPS285	Discovery
High	Port Scan Detected		POLICY_VIOLATION	2 days ago	New	192.168.165.14	Discovery
Medium	Firmware Change Detected		ANOMALY	2 days ago	New	10.90.80.213	Discovery
High	Address Scan Detected		ANOMALY	2 days ago	New	logps350	Discovery
High	Address Scan Detected		POLICY_VIOLATION	2 days ago	New	192.168.165.25	Discovery
Medium	Firmware Change Detected						

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

Severity: High | **Status:** New | **Last detection:** 15 hours ago

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) → **Destination device:** Internet (48.222.98.0)

MITRE ATT&CK®

Tactics: Lateral movement, Impair process control

The adversary is trying to move through your environment. [read more on attack.mitre.org](#)

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: 5ffff6965-15d9-45ce-8674-54415785dedc

⚠ High

💡 New

🕒 15 hours ago

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

Source device address

10.218.166.16

Destination device

Internet

Destination device address

48.222.98.0

Site

Sensor

Category

Authentication

PROTOCOL

GENERIC

Source (Client) Address

10.218.166.16

Destination (Server) Address

48.222.98.0

isLearnable

false

ViolationCount

0

Login Attempts Failure Codes

With Messages

403 - Forbidden.

Login Attempts Count

27

SiteDisplayName

SensorType

Ot

SensorZone

default

SensorVersion

25.1.1.12260320

First detection (in the network)

12/18/2025, 12:47:07 AM

Last detection (in the network)

2/4/2026, 6:43:27 PM

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



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=d1.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=d1.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]
46	0.508240	48.222.98.0	10.218.166.16	TCP	1514	80 → 49841 [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><div class="message-container">\n
<div class="logo"></div>\n
<h1>FortiGuard Intrusion Prevention - Access Blocked</h1>\n
<h3>Web Page Blocked</h3>\n
<p>You have tried to access a web page that is in violation of your Internet usage policy.</p>\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?</td>\n
    </tr>\n
</tbody></table>\n

```

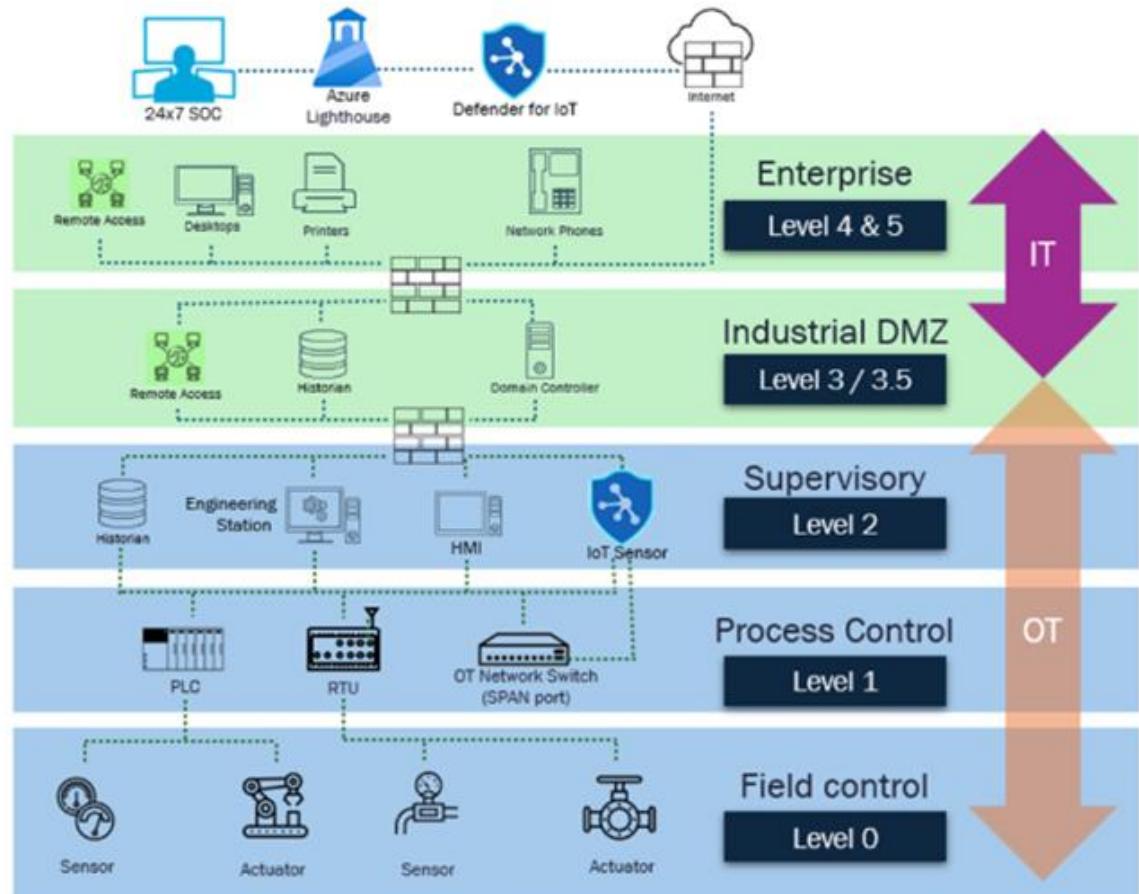
```

0040 33 6d 74 72 75 73 69 6f 6e 20 50 72 65 76 65 6e\n
0050 74 69 6f 6e 20 2d 20 41 63 63 65 73 73 20 42 6c\n
0060 6f 63 6b 65 64 3c 2f 68 31 3e 0a 20 20 20 20 3c\n
0070 68 33 3e 57 65 62 20 50 61 67 65 20 42 6c 6f 63\n
0080 6b 65 64 3c 2f 68 33 3e 0a 20 20 20 3c 70 3e\n
0090 59 6f 75 20 68 61 76 65 20 74 72 69 65 64 20 74\n
00a0 6f 20 61 63 63 65 73 73 20 61 20 77 65 62 20 70\n
00b0 61 67 65 20 74 68 61 74 20 69 73 20 69 6e 20 76\n
00c0 69 6f 6c 61 74 69 6f 6e 20 6f 66 20 79 6f 75 72\n
00d0 20 49 6e 74 65 72 6e 65 74 20 75 73 61 67 65 20\n
00e0 70 6f 6c 69 63 79 2e 3c 2f 70 3e 0a 20 20 20 20\n
00f0 3c 74 61 62 6c 65 3e 3c 74 62 6f 64 79 3e 0a 20\n
0100 20 20 20 20 20 20 3c 74 72 3e 0a 20 20 20 20\n
0110 20 20 20 20 20 20 20 3c 74 64 3e 43 61 74 65\n
0120 67 6f 72 79 3c 2f 74 64 3e 0a 20 20 20 20 20\n
0130 20 20 20 20 20 20 3c 74 64 3e 55 6e 72 61 74 65\n
0140 64 3c 2f 74 64 3e 0a 20 20 20 20 20 20 3c 74 72\n
0150 2f 74 72 3e 0a 20 20 20 20 20 20 20 3c 74 72\n
0160 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 74 72\n
0170 64 3e 55 52 4c 3c 2f 74 64 3e 0a 20 20 20 20 20\n
0180 20 20 20 20 20 20 20 3c 74 64 3e 68 74 74 70 3a\n
0190 2f 2f 34 38 2e 32 32 32 2e 39 38 2e 30 2f 66 69\n

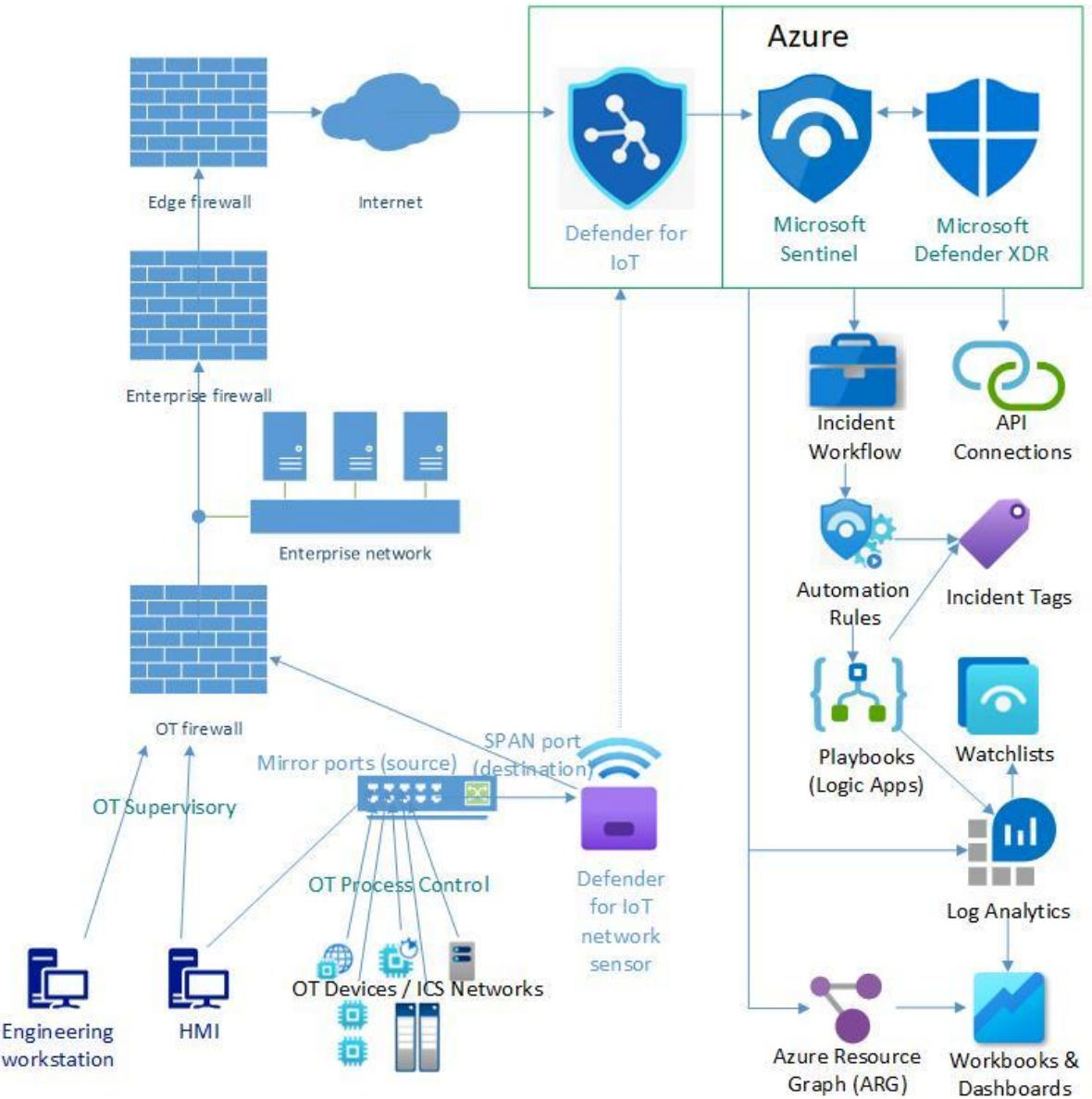
```

3mtrusio n Preven
tion - A ccess Bl
ocked</h1> . <
h3>Web P age Bloc
ked</h3> . <p>
You have tried t
o access a web p
age that is in v
iolation of your
Interne t usage
policy.</p>
<table><tbody>
 <tr>
 <td>Category</td>
 <td>Unrate
d</td>.
 </tr>
 <tr>
 <td>URL</td>
 <td>http://48.222.98.0/fi
/

Microsoft Defender for IoT Topology



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



Microsoft Defender for IoT Sensor Overview

Not secure <https://sensor1.odyssey.com>

Sensor1 - 24.1.8

Home > **Defender for IoT | Overview**

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

2 PPS

10 Devices

2 Alerts

General Settings

Version: 24.1.8.111087574 Threat Intelligence: Version 2024.12.15 | Last updated Dec 15, 2024 Connectivity type: Cloud connected Activation: Valid Certificate: Valid

System settings >

Top 5 OT Protocols

Protocol	Devices
Profinet DCP	2 Devices
Profinet Real-Time	2 Devices
Siemens S7 Plus	2 Devices
MMS	1 Device

Traffic Monitoring

Trends & statistics >

Traffic By Port

Interfaces

enp2s0

172.16.30.100 - PuTTY

Welcome to Microsoft Defender for IoT
Appliance ID: 20f1bf3b-232d-864d-a2b6-08b4d2d37fe3

In order to view the EULA, please access the Microsoft Defender for IoT sensor GUI.

BY USING THIS SOFTWARE, YOU AGREE TO THE TERMS OF THE END-USER LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THIS SOFTWARE.

All connections are monitored and recorded. Disconnect IMMEDIATELY if you are not an authorized user!

End of banner message from server admin@172.16.30.100's password:

Last login: Fri Jul 18 17:26:22 2025 from 172.16.10.27
Microsoft Defender For IoT CLI

Microsoft Defender for IoT

HARDWARE SENSOR



Preconfigured physical appliances for OT monitoring

Hardware profile	Appliance	Hardware profile	SPAN/TAP throughput	Max monitored Assets
C5600	HPE ProLiant DL360 Gen 11	C5600	Up to 3 Gbps	12 K
	Dell PowerEdge R660			
E1800	HPE ProLiant DL20 Gen11 (4SFF)	E1800	Up to 1 Gbps	10K
	Dell PowerEdge R360	E1000	Up to 1 Gbps	10K
E500	Dell Edge 5200 (Rugged MIL-STD-810G)	E500	Up to 1 Gbps	10K
L500	HPE ProLiant DL20 Gen11 Plus (NHP 2LFF)	L500	Up to 200 Mbps	1,000
	DELL XE4 Small Form Factor (SFF)	L100	Up to 10 Mbps	800
L100	YS-Techsystems YS-FIT2 (Rugged MIL-STD-810G)			
	Dell Edge Gateway 3200			

OT monitoring with virtual appliances

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

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)

OT site licenses

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

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)

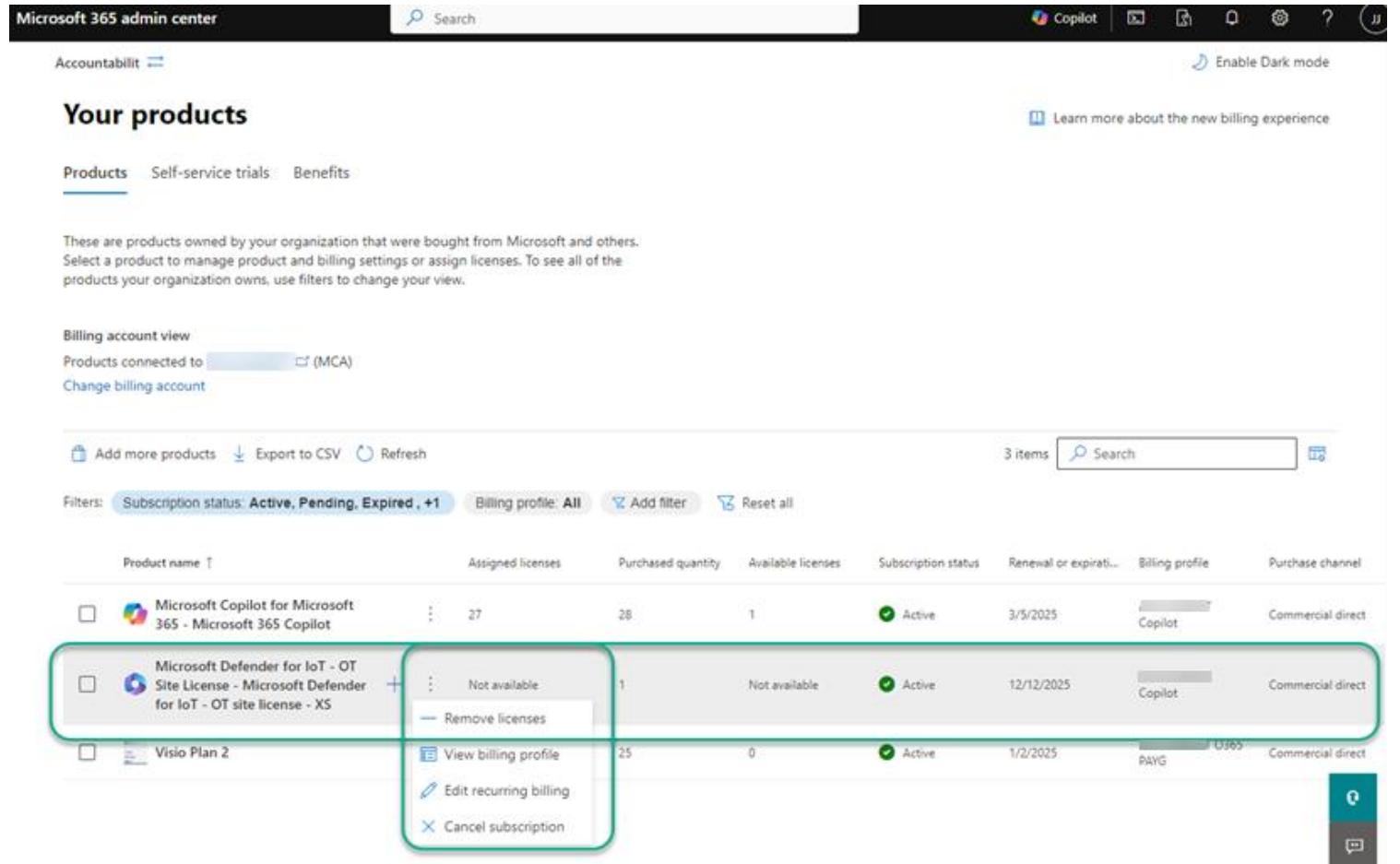
Microsoft Defender for IoT - OT site license - XL

\$1,500.00

license/month, paid yearly
(annual commitment)
(Includes up to 5,000 devices per site; annual subscription—auto renews)

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



Your products

Products Self-service trials Benefits

These are products owned by your organization that were bought from Microsoft and others. Select a product to manage product and billing settings or assign licenses. To see all of the products your organization owns, use filters to change your view.

Billing account view
Products connected to

Product name	Assigned licenses	Purchased quantity	Available licenses	Subscription status	Renewal or expiration date	Billing profile	Purchase channel
Microsoft Copilot for Microsoft 365 - Microsoft 365 Copilot	27	28	1	Active	3/5/2025	Copilot	Commercial direct
Microsoft Defender for IoT - OT Site License - Microsoft Defender for IoT - OT site license - XS	Not available	1	Not available	Active	12/12/2025	Copilot	Commercial direct
Visio Plan 2	25	0	0	Active	1/2/2025	PAYG	Commercial direct

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

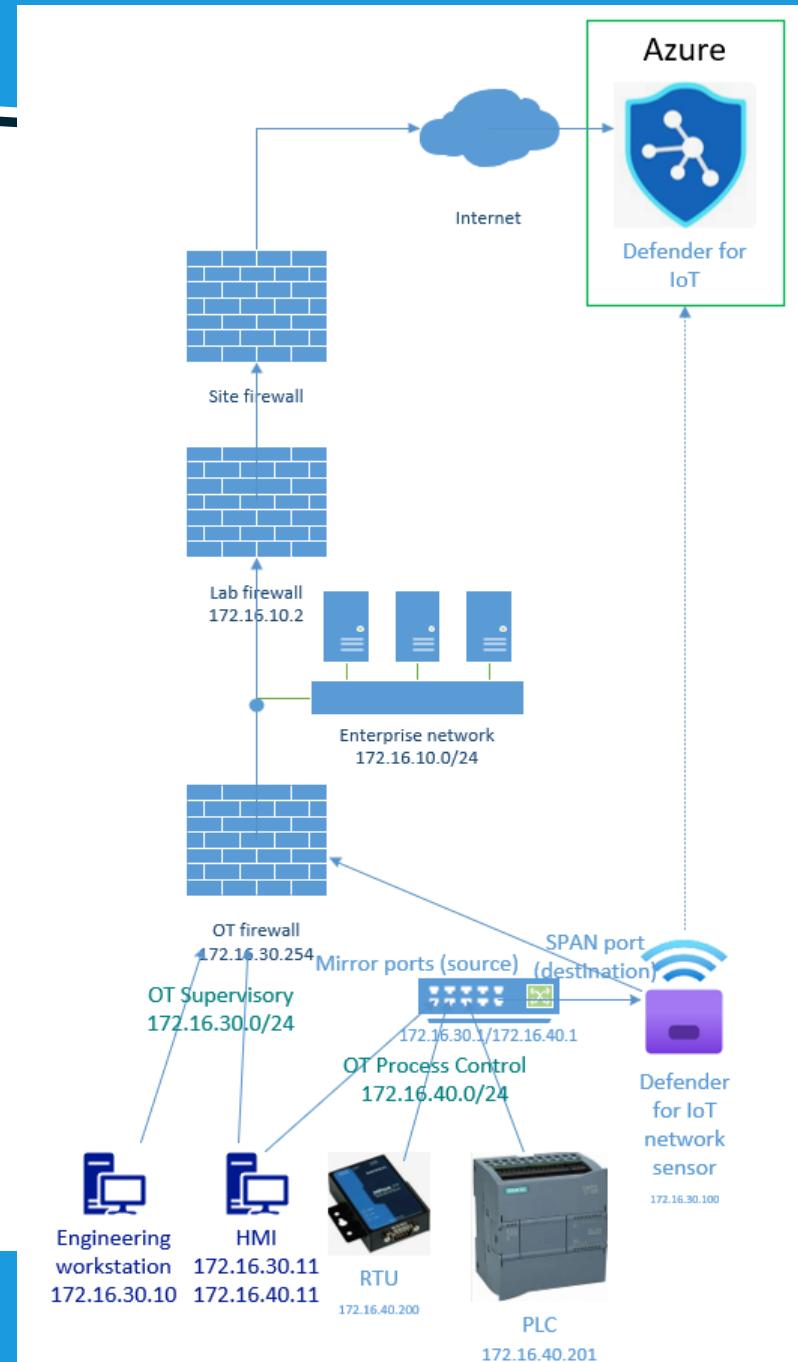
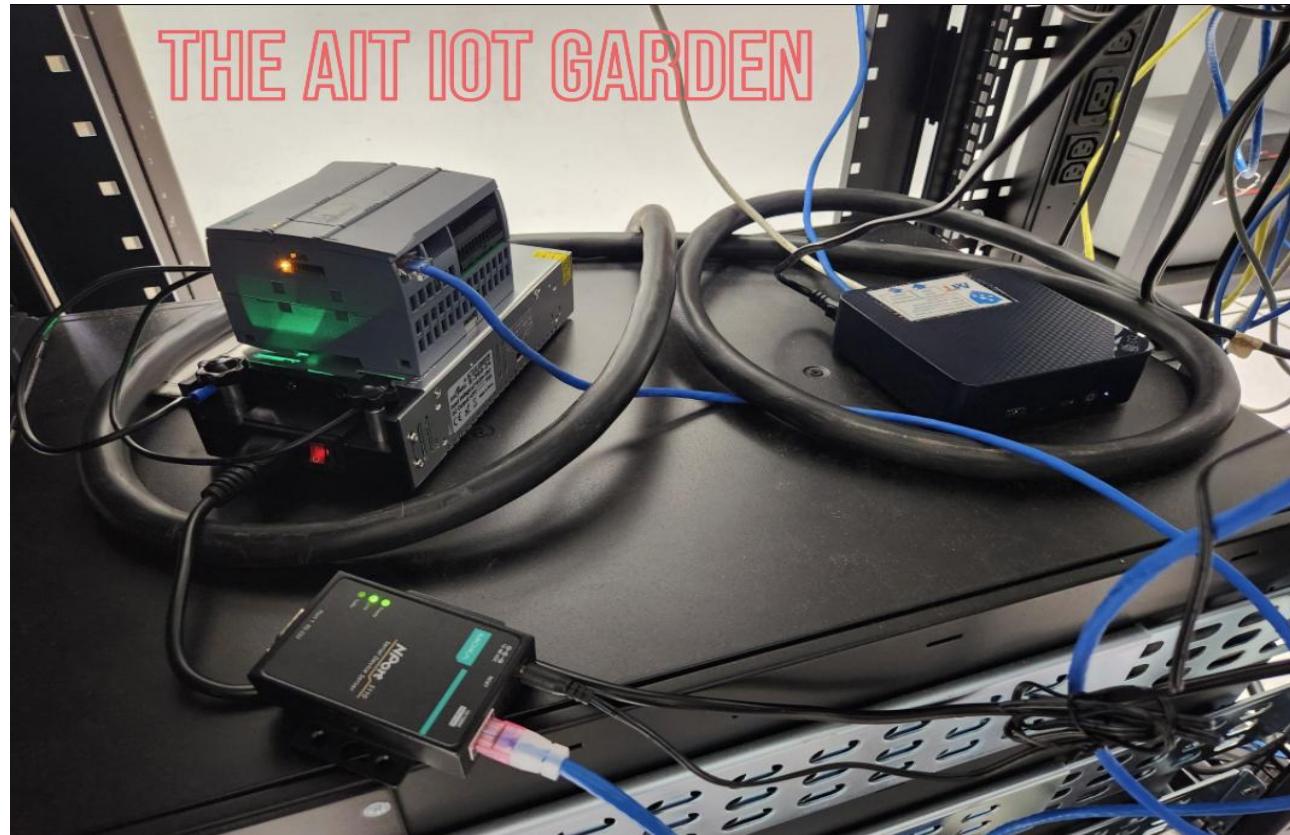
- ▶ We establish secure administration of Defender for IoT Azure resources via Azure Lighthouse and integrate Defender for IoT with a Microsoft Sentinel SIEM instance.
- ▶ The phase includes escalation, and investigation protocols between the SOC team and the customer, enabling 24x7 OT SOC services.
- ▶ 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

```
ProCurve Switch 2510-48                               28-Dec-2024 17:03:57
----- TELNET - MANAGER MODE -----
Switch Configuration - Network Monitoring Port

Monitoring Enabled [No] : Yes
Monitoring Port : 45
Monitor : Ports

Port   Type      Action    Port   Type      Action
-----+-----+-----+-----+-----+-----+
 1    10/100TX | Monitor | 27   10/100TX |
 2    10/100TX | Monitor | 28   10/100TX |
 3    10/100TX | Monitor | 29   10/100TX |
 4    10/100TX | Monitor | 30   10/100TX |
 5    10/100TX | Monitor | 31   10/100TX |
 6    10/100TX | Monitor | 32   10/100TX |
 7    10/100TX | Monitor | 33   10/100TX |
 8    10/100TX | Monitor | 34   10/100TX |

Actions->   Cancel   Edit   Save   Help

Select whether to enable traffic monitoring.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

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.	<input checked="" type="button"/> Enabled

Engines

Name	Description	
Protocol Violation	Detects deviations in the packet structure or field values compared to protocol specifications.	<input checked="" type="button"/> Enabled
Policy Violation	Detects deviations from learned baseline behavior.	<input checked="" type="button"/> Enabled
Malware	Detects malicious network activity.	<input checked="" type="button"/> Enabled
Anomaly	Detects anomalies in network behavior.	<input checked="" type="button"/> Enabled
Operational	Detects operational incidents or malfunctioning entities.	<input checked="" type="button"/> Enabled

Defender for IoT: Device Inventory

Home > Device inventory

 Defender for IoT | Device inventory

Save Filter Refresh Edit Columns Export Delete Merge Edit

Network Location == Local Add filter

Showing 8 of 8 devices

	IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmware...	Model	Operating S...
<input type="checkbox"/>	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
<input type="checkbox"/>	172.16.40.1	172.16.40.1	3 minutes ago	Switch	Telnet, ICMP	00:23:47:20:be:80	PROCURVE NET	--	--	--
<input type="checkbox"/>	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
<input type="checkbox"/>	172.16.40.200	172.16.40.200	32 minutes ago	Server	HTTP	00:90:e8:c6:90:32	MOXA TECHNO	--	--	--
<input type="checkbox"/>	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:dca0:63:5c:37	SIEMENS AG	--	S71200 (6ES7 2)	--
<input type="checkbox"/>	172.16.30.100	172.16.30.100	an hour ago	General IoT	--	00:15:5d:0a:7f:0d	MICROSOFT CO	--	--	Linux
<input type="checkbox"/>	172.16.30.11	HMI	2 hours ago	HMI	Netbios Name Service, HTTP	00:15:5d:01:01:0a	MICROSOFT CO	--	--	Windows 10
<input type="checkbox"/>	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

Home > Device map

Defender for IoT | Device map

Search | Create Custom Group | Import Devices | Export Devices | Export Device Summary | Refresh map | Notifications (1)

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

Groups

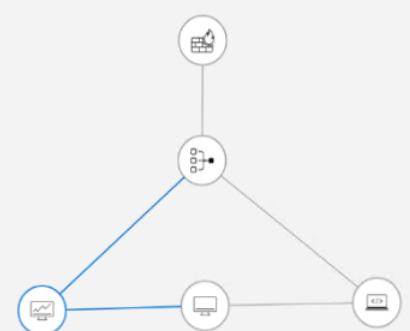
Highlight Filter

Search groups

- OT Protocols
- Known Applications
- Subnets

Process Control (172.16.40.0/24) 4

Supervisory (172.16.30.0/24) 5



HMI
HMI
Activity Report | Event Timeline

Authorized Status
2 hours ago
Last activity
0 Alert

Vendor
MICROSOFT CORPORATION
Operating System
Windows 10

Protocols
Netbios Name Service | HTTP

IP Addresses
172.16.30.11

MAC Addresses
00:15:5d:01:01:0a

Device Details

Defender for IoT Device Map

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

Home > Device map

Defender for IoT | Device map

Search: Create Custom Group Import Devices Export Devices Export Device Summary Refresh map Notifications (1)

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

Groups

Highlight Filter

Search groups

OT Protocols

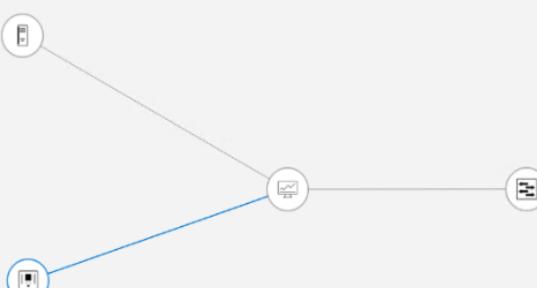
- MMS 1
- Profinet DCP 2
- Profinet Real-Time 2
- Siemens S7 1
- Siemens S7 Plus 2

Known Applications

- HTTP - 80 TCP 2
- ICMP 3
- Telnet - 23 TCP 2

Subnets

- Process Control (172.16.40.0/24) 4
- Supervisory (172.16.30.0/24) 5



172.16.40.201
PLC
Activity Report | Event Timeline

Authorized Status 38 minutes ago Last activity 0 Alerts

Vendor SIEMENS AG

Protocols MMS Siemens S7 Siemens S7 Plus Profinet DCP Profinet Real-Time ICMP

IP Addresses 172.16.40.201

MAC Addresses e0:dca:06:35:c3:37

Device Details

Defender for IoT | Device map

 Search

+ Create Custom Group

Import Devices

Export Devices

Export Device Summary

Refresh map

Notifications (25)

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

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

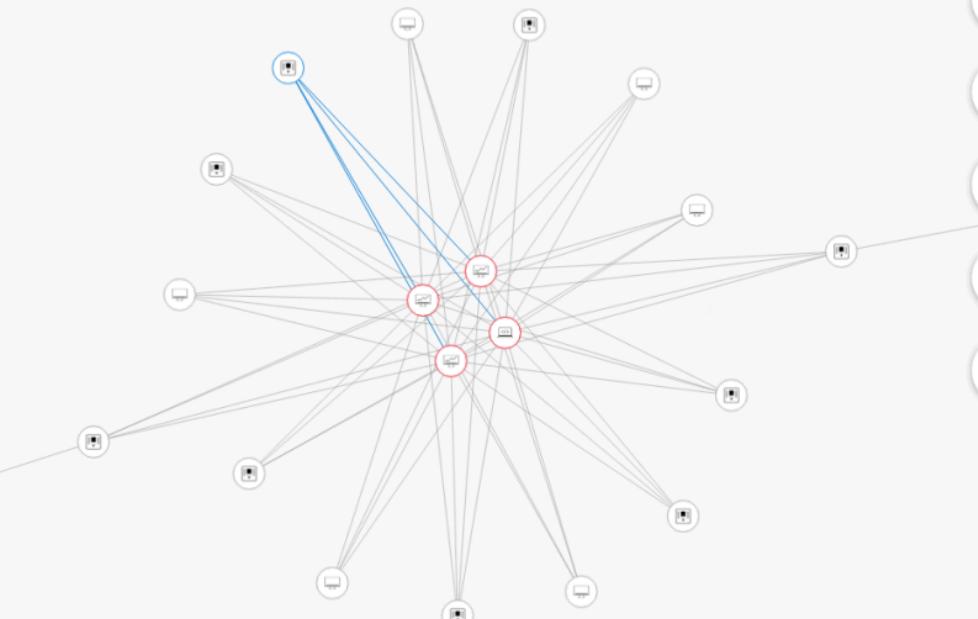
Rockwell CSP2

21

▶ Known Applications

▶ Subnets

▶ CDP Protocol



PLC

Activity Report | Event Timeline

Authorized

Status

4 minutes ago

Last activity

0 Alert

Vendor
Rockwell Automation

Protocols

Rockwell CSP2

ICMP

IP Addresses

Device Details

Microsoft Defender for IoT solution in Microsoft Sentinel Content Hub

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

Home > Microsoft Sentinel | Content hub > Microsoft Defender for IoT ...

Refresh Delete Reinstall

24 Installed content items **7** Configuration needed

Microsoft Defender for IoT

Content name	Created content	Content type	Version
Microsoft Defender for IoT	1 items	Data connector	1.0.0
Denial of Service (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Excessive Login Attempts (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Firmware Updates (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
High bandwidth in the network (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Illegal Function Codes for ICS traffic (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Internet Access (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Multiple scans in the network (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
No traffic on Sensor Detected (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
PLC Stop Command (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
PLC unsecure key state (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Suspicious malware found in the network (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Unauthorized device in the network (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Unauthorized DHCP configuration in the network (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Unauthorized PLC changes (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
Unauthorized remote access to the network (Microsoft Defender for IoT)	1 items	Analytics rule	1.0.2
[AD4IoT-AutoAlertStatusSync]	--	Playbook	1.0
[AD4IoT-AutoCloseIncidents]	--	Playbook	1.0
[AD4IoT-AutoTriageIncident]	--	Playbook	1.0
[AD4IoT-CVEAutoWorkflow]	--	Playbook	1.0
[AD4IoT-MailByProductionLine]	--	Playbook	1.0
[AD4IoT-NewAssetServiceNowTicket]	--	Playbook	1.0
[AD4IoT-SendEmailtoIoTOwner]	--	Playbook	1.0
Microsoft Defender for IoT	1 items	Workbook	1.0.0

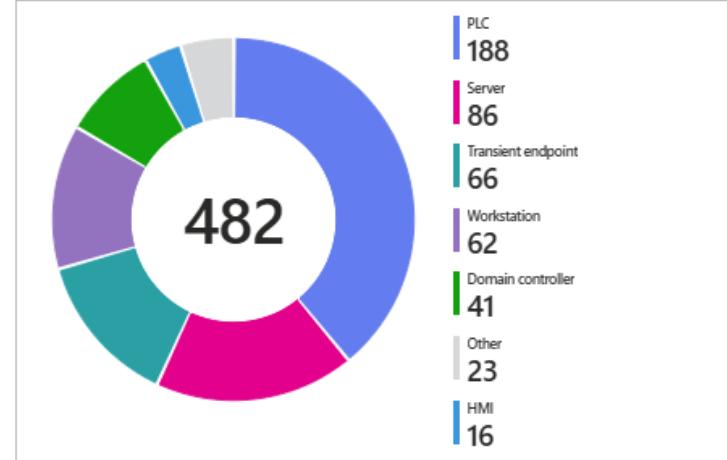
< Previous Page 1 of 1 Next > Showing 1 to 24 of 24 results.

Microsoft Defender for IoT -

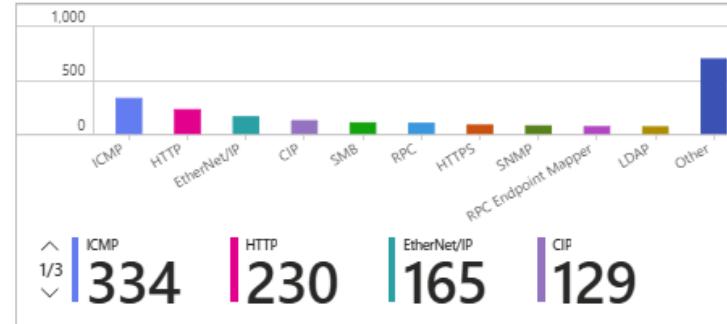
Microsoft Sentinel workbook for Defender for IoT: Overview tab

Edit Open Help Auto refresh: Off

Active Devices by Type



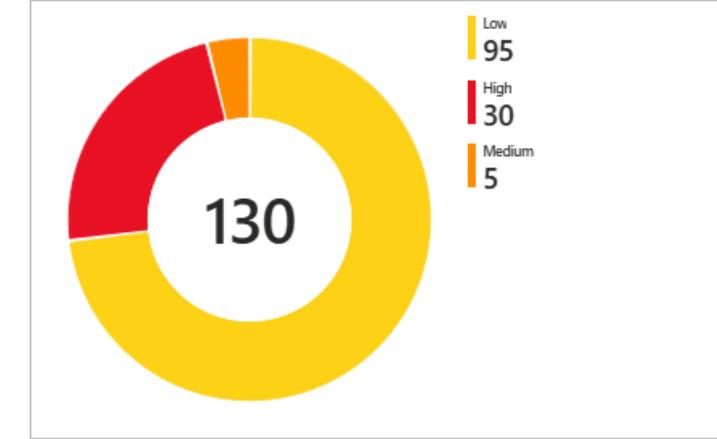
Active OT Devices by Protocol



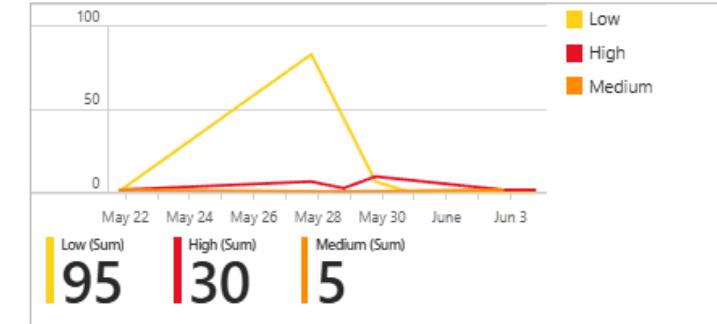
Recent Discovered Devices

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 >>	Workstation

Incidents by Severity



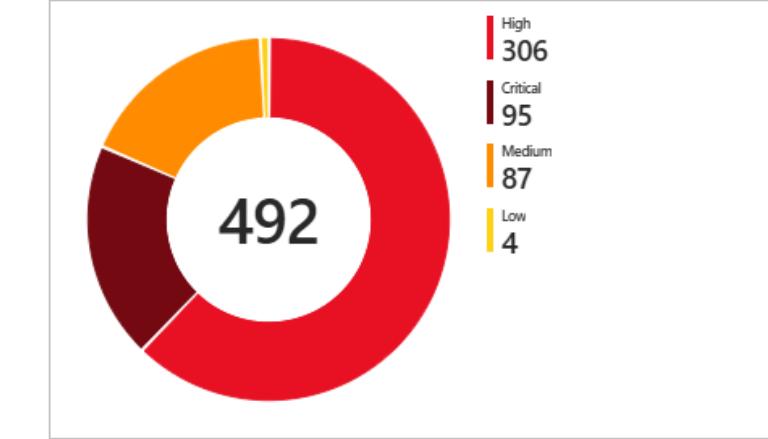
Incidents Trend Overtime



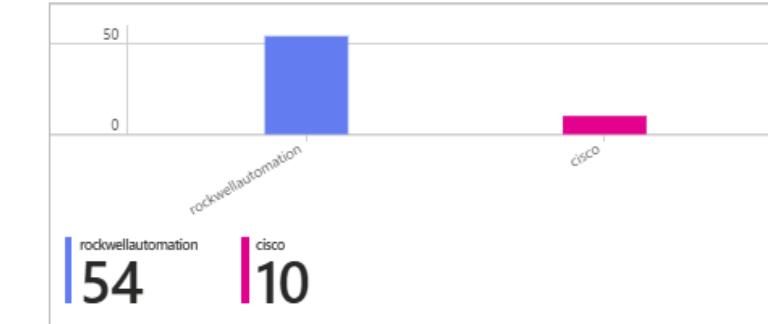
Recent Open Incidents

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
[REDACTED]				1		24	8	12		
[REDACTED]				1		22	8	11		
[REDACTED]				1		19	6	9		

M C Z

Microsoft Defender for IoT incidents in Microsoft Sentinel console

Home > Microsoft Sentinel | Incidents

(MDIoT) Unauthorized Internet Connectivity Detected Incident number 419

Refresh Delete incident Logs Tasks Activity log

This is the new, improved incident page - Now generally available. You can use the toggle to switch back.

New experience

Investigate externally

Entities

Name	Type
10.48.173.27	IoT Device
10.48.173.27	IP
8.8.8.8	Azure Resource

8.8.8.8 IP

Info Timeline Insights

Geolocation information

Organization: Google LLC	Organization type: Internet Service Provider
City: Mountain View	Country: United States
State: California	Continent: North America

Last update time: 2/2/2026, 7:17:34 PM Creation time: 2/2/2026, 7:15:28 PM

Location: default Sensor:

Entities (4): 10.48.173.27, 10.48.173.27, 8.8.8.8, stonehouse

Tactics and techniques: Initial Access (1)

Investigate

View full details Entity actions

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





MC2MC
—CONNECT—