nedscaper

Demystifying

Microsoft Defender for IoT

nedscaper

Demystifying Microsoft Defender for OT

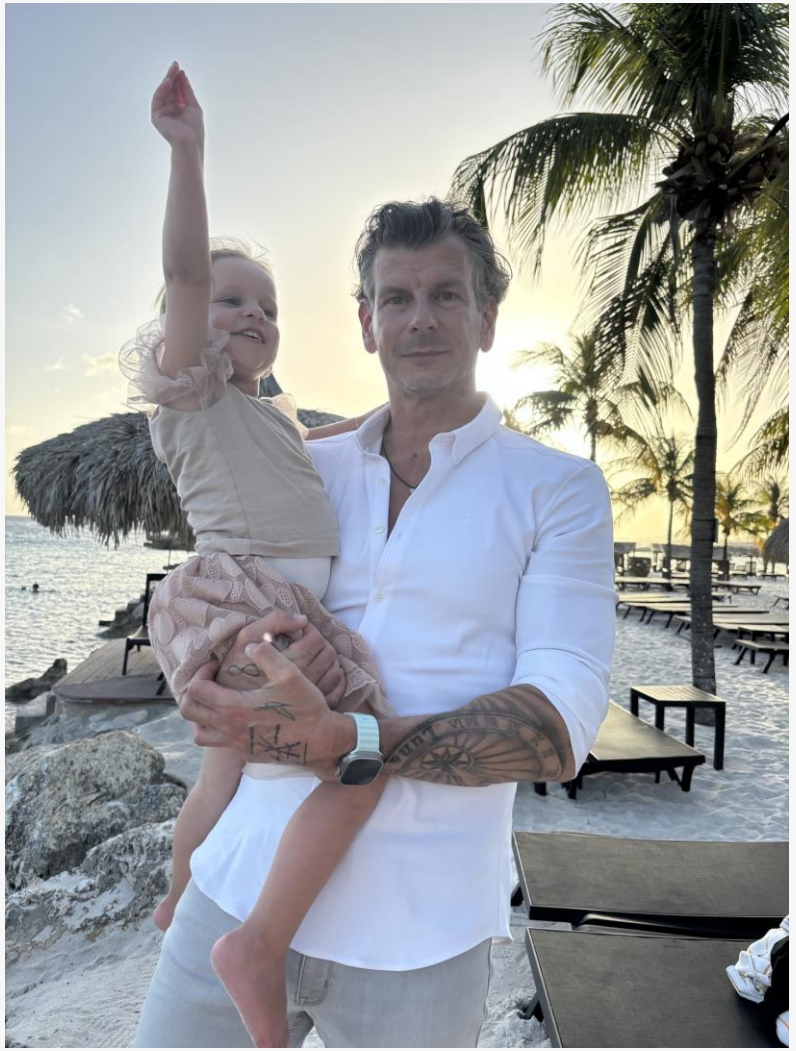
Welcome

MICROSOFT SECURITY

Derk van der Woude
CTO Nedscaper
Microsoft Security **MVP**
Microsoft **CCP** Discussion Leader | **Defender for IoT**

What keeps me Awake at Night?

What keeps me Awake at Night?



What keeps me Awake at Night?

Cyber Attack on Kudankulam Nuclear Power Plant

A Wake Up Call

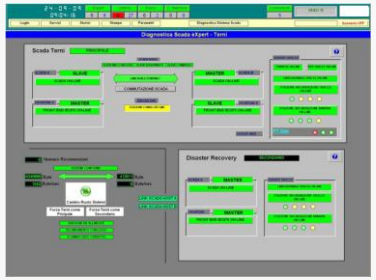
Stuxnet

1981 Operation Opera

- bombing of **Iraq** nuclear plant in development

2005 Operation Olympic games

- Stuxnet development for **Iran** (Natanz) nuclear plant **30m underground**
- **150.000** lines of code *(~10x average malware lines of code*)
- **2007** initial access via USB / equipment (**AIVD**)
- **2010** Stuxnet Detected (*VirusBlokAda*)
- **Malware** for Windows & Siemens PLCs (Mossad & CIA)
- **4 zero-days**
- Destroyed ~20% by spinning the Centrifuges over their limit but show all operator consoles set back development many years



2025 Operation Rising Lion …

- Bombing of **Iran** (Natanz) nuclear plant …

PRESENTATION NEDSCAPER

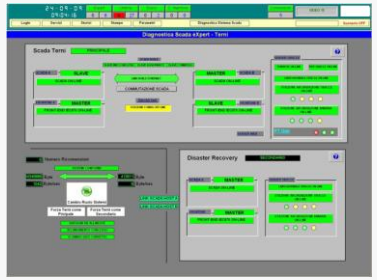
Stuxnet

1981 Operation Opera

- bombing of **Iraq** nuclear plant in development

2005 Operation Olympic games

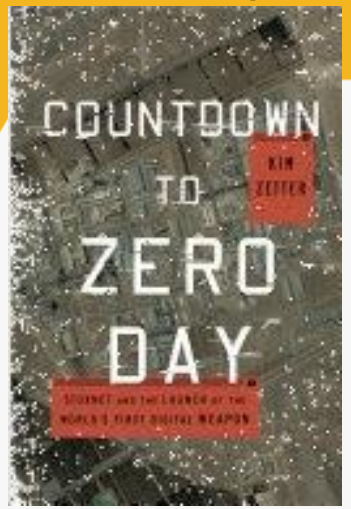
- Stuxnet development for **Iran** (Natanz) nuclear plant **30m underground**
- **150.000** lines of code *(~10x average malware lines of code*)
- **2007** initial access via USB / equipment (**AIVD**)
- **2010** Stuxnet Detected (*VirusBlokAda*)
- **Malware** for Windows & Siemens PLCs (Mossad & CIA)
- **4 zero-days**
- Destroyed ~20% by spinning the Centrifuges over their limit but show all operator consoles set back development many years



2025 Operation Rising Lion …

- Bombing of **Iran** (Natanz) nuclear plant …

Booktip



PRESENTATION NEDSCAPER

Abbreviations

OT Operational technology

EIoT Enterprise IoT
IIoT *Industrial IoT*
MIoT *Medical IoT*

BMS Building Management System

Abbreviations

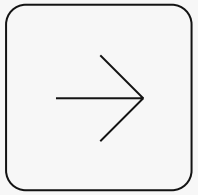
OT Operational technology

EIoT Enterprise IoT

IIoT *Industrial IoT*

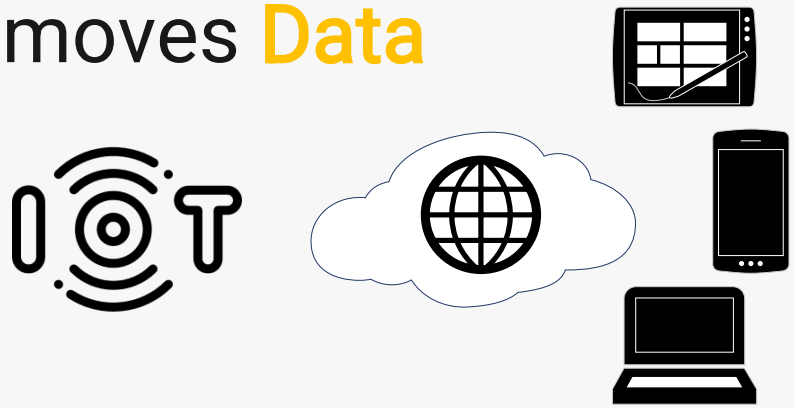
MIoT *Medical IoT*

BMS Building Management System

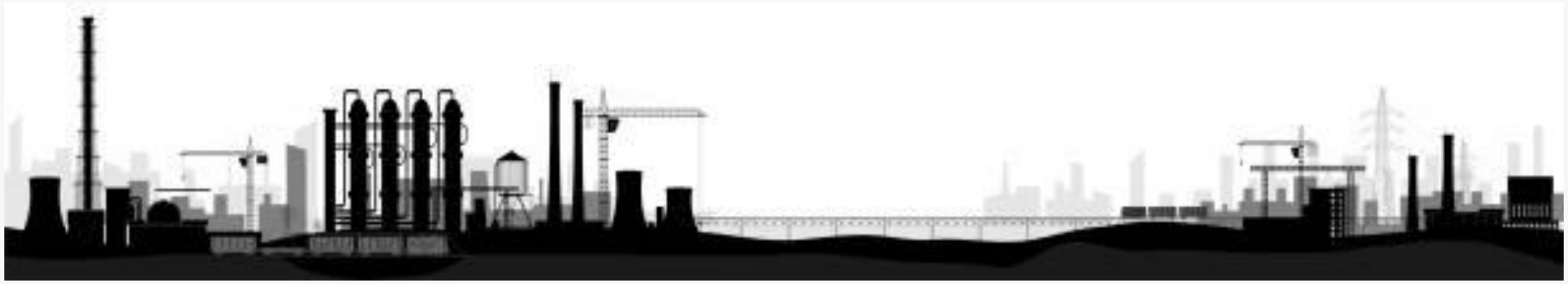


Difference in use-case(s)

- EIoT moves Data



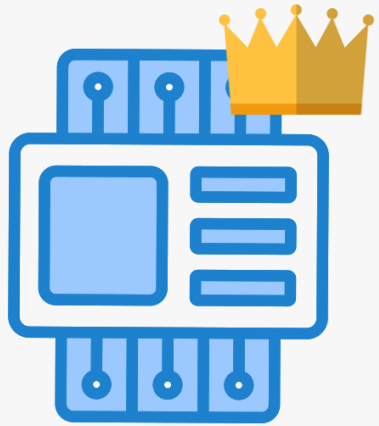
- OT (BMS) moves Physical Systems



An Attacker perspective

Rule of thumb

EIoT devices are LMPs [Lateral Movement Paths]



OT devices are **Crown Jewels / Critical Assets**

Example of IoT as entry-point

BUSINESS INSIDER

Subscribe

DOW JONES +0.75% NASDAQ +0.61% S&P 500 +0.58% AAPL -0.29% NVDA -1.98% MSFT +0.05% AMZN -0.52% META -1.04% TSLA -1.4%

FINANCE

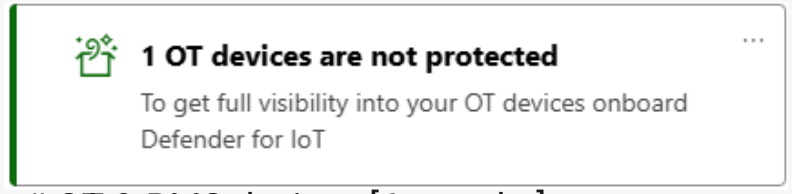
Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank

ATTACKERS EXFILTRATED A CASINO'S HIGH-ROLLER LIST THROUGH A CONNECTED FISH TANK

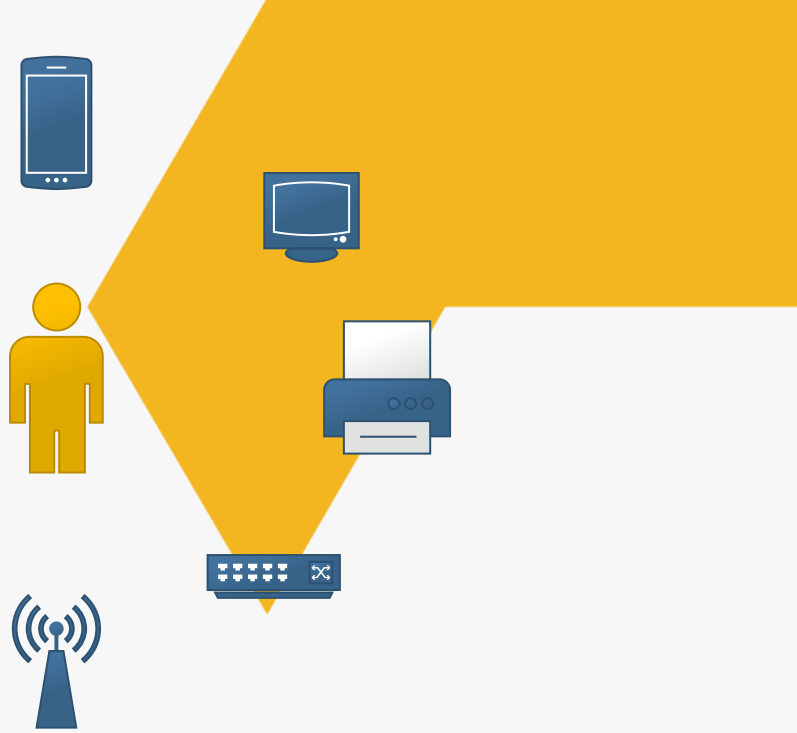
Pierluigi Paganini April 16, 2018

Microsoft License(s) – part I

- **Microsoft 365 E5 | E5** Security [1:5]
  - **Risk** Level & **Exposure** Level for **EIoT** devices
  - **MDE P2** requires EIoT add-on per device
  - OT Device Discovery



OT & BMS devices [6 months]



Microsoft License(s) – part II

- **Microsoft Defender for IoT** [Site-based - **#** of devices]
  - **Risk-, Exposure- & Critical** Level for **OT** devices [Defender XDR]
  - **Set criticality** for OT Devices
  - Operational Technology | **Site security** [Defender XDR]

    OR
  - Defender for IoT | Azure Portal

Topics to discuss

NIST Cybersecurity Framework

Device Discovery ⟸ Identity

Vulnerability Management ⟸ Protect

Threat Detection ⟸ Detect & Respond

- The Future of Microsoft OT

Solution Type(s)

- Defender XDR | MDE | Enterprise IoT
- Defender XDR | MDE | D4IOT
- Azure | Sensor | D4IOT

Microsoft Defender for IoT

Device Discovery

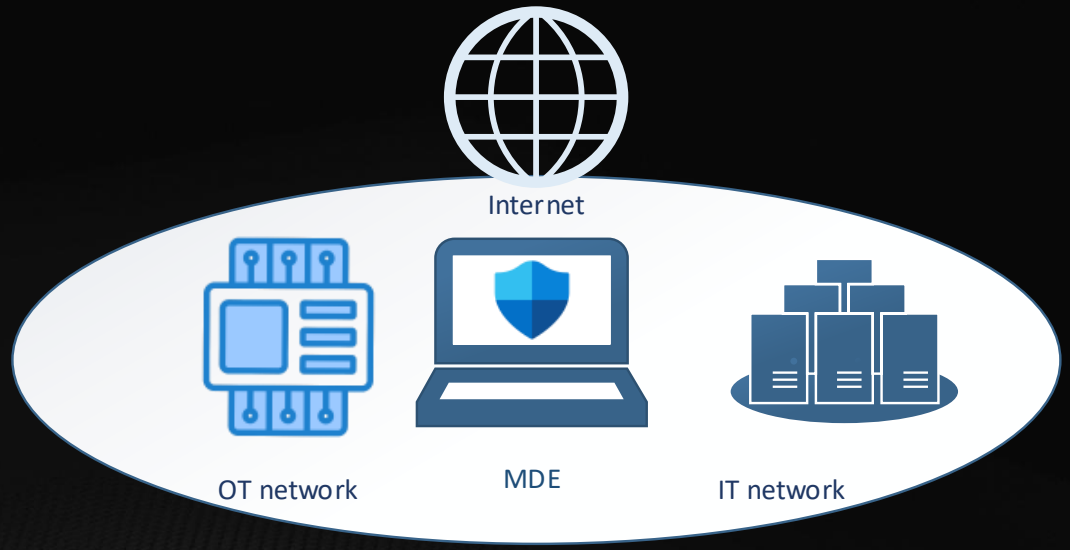
nedscaper

You cannot Protect what you don’t know

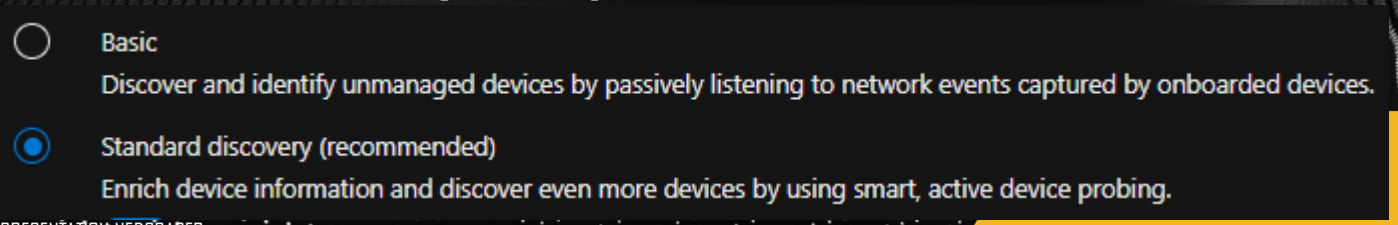
nedscaper

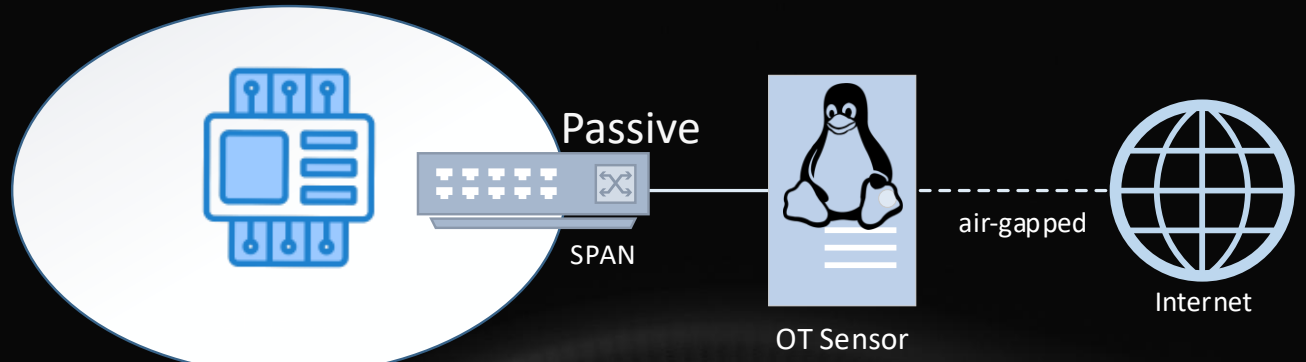
Device Discovery Overview

(E)IoT & OT Device Discovery via Defender for Endpoint



Active [default] or Passive





OT Device Discovery via OT Sensor [SPAN/TAP]

nedscaper

Enterprise IoT Device discovery settings

Settings

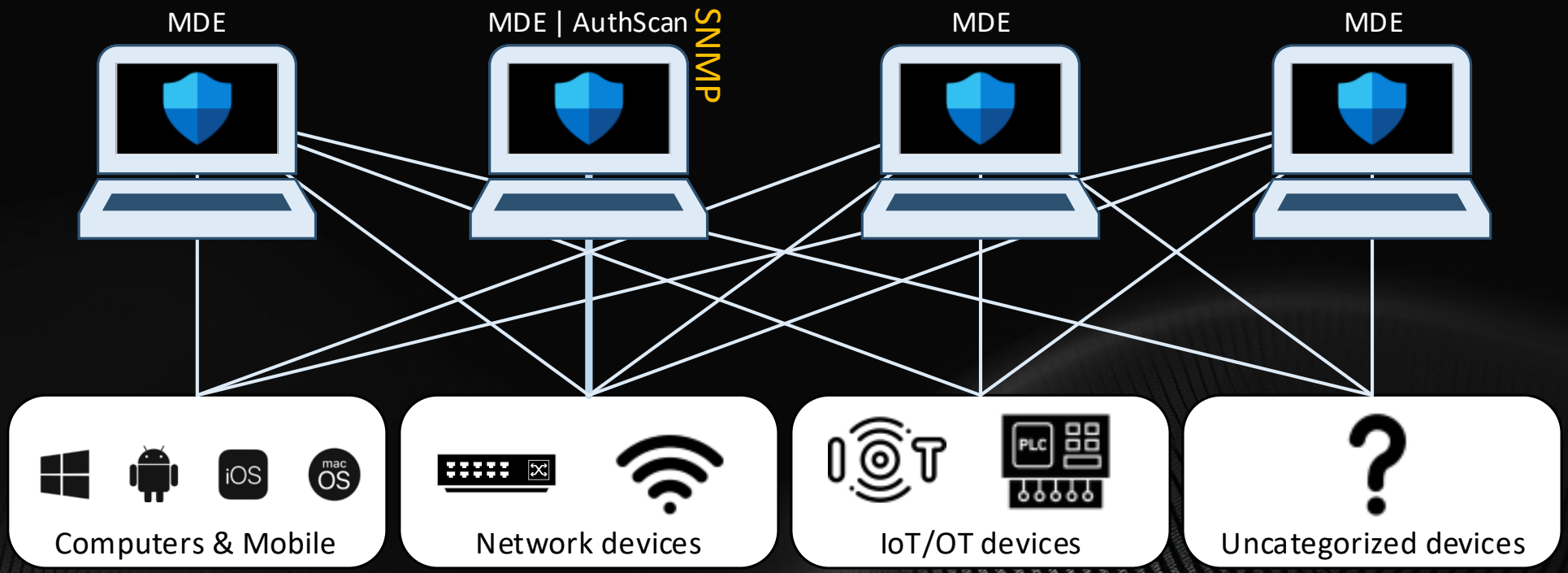
8 items

	Name	Description
	Microsoft Defender portal	General settings for the Microsoft Defender portal
	Microsoft Defender XDR	General settings for Microsoft Defender XDR
	Endpoints	General settings for endpoints
	Email & collaboration	General settings for email & collaboration
	Identities	General settings for identities
	Device discovery	Select your device discovery mode and customize standard discovery settings
	Cloud Apps	General settings for cloud apps
	Microsoft Sentinel	General settings for Microsoft Sentinel

Disabled by default

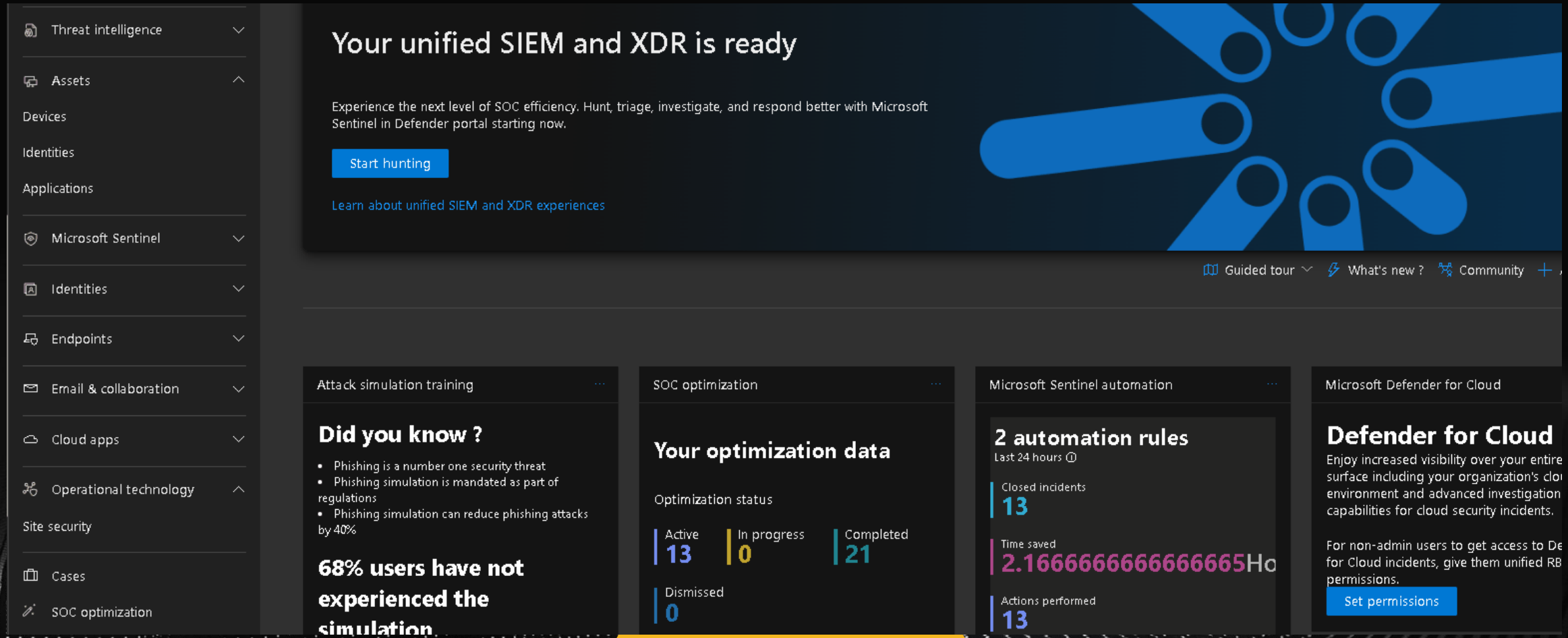
nedscaper

Device Discovery via MDE



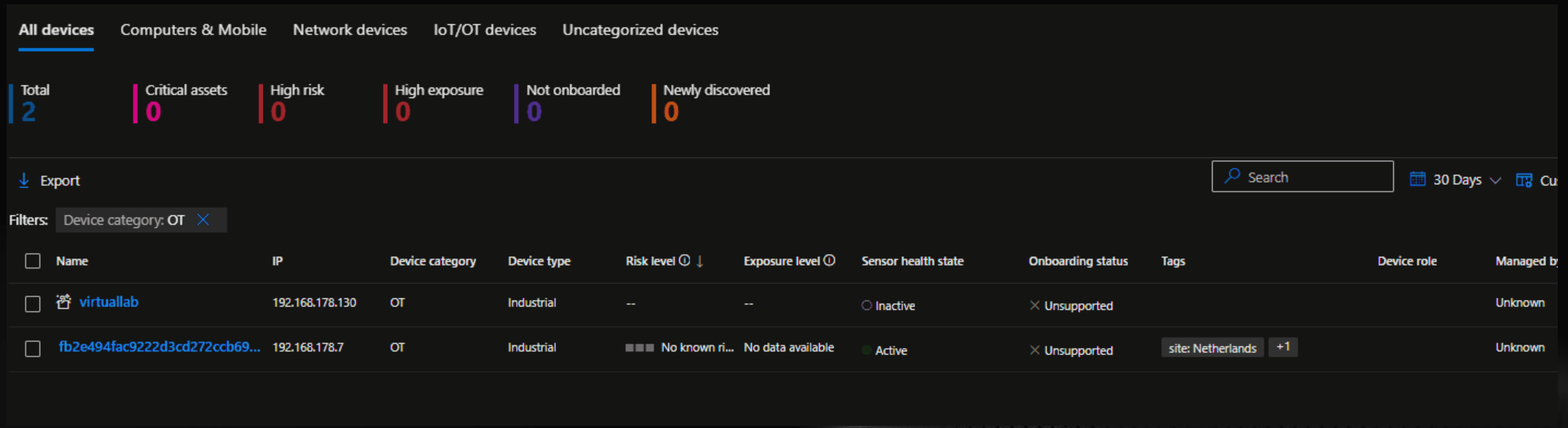
nedscaper

Defender XDR | Assets | Devices [OT]



nedscaper

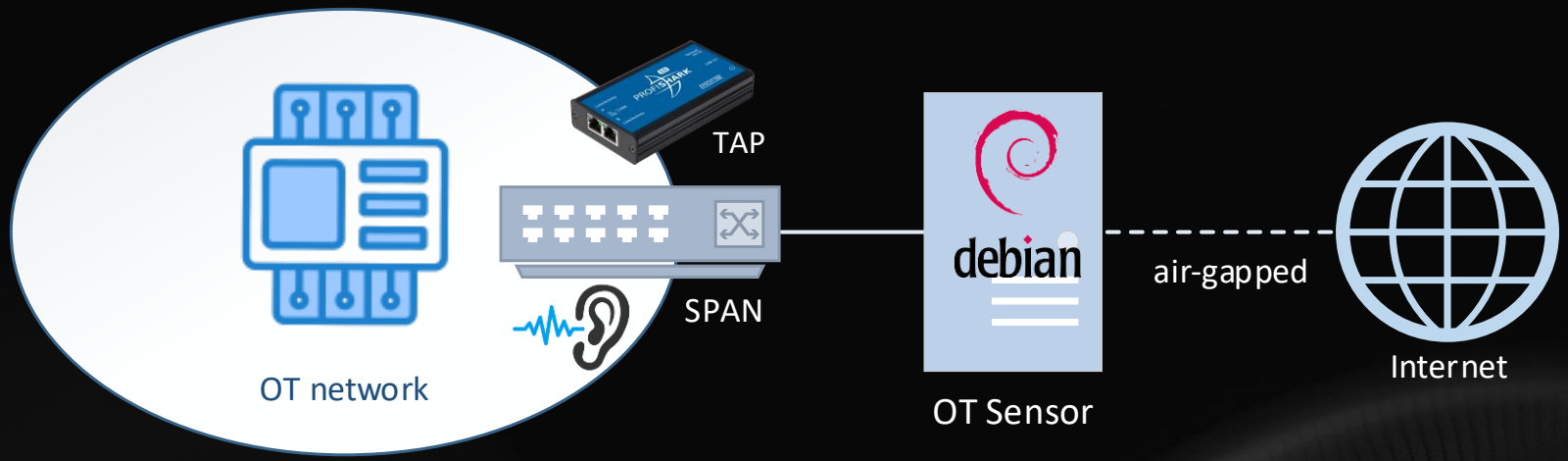
Assets | Devices | Set criticality

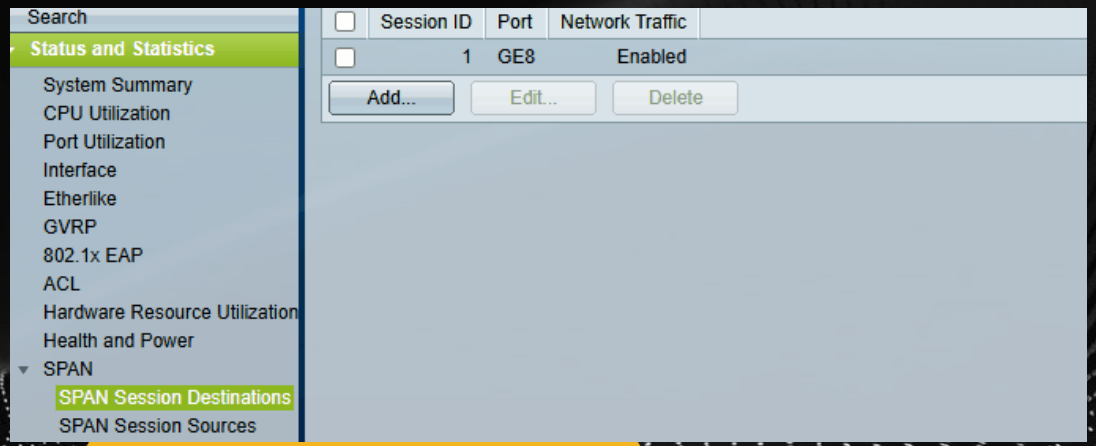


Requires the Defender for IoT – Site license
used in MSEM | Attack Paths

nedscaper

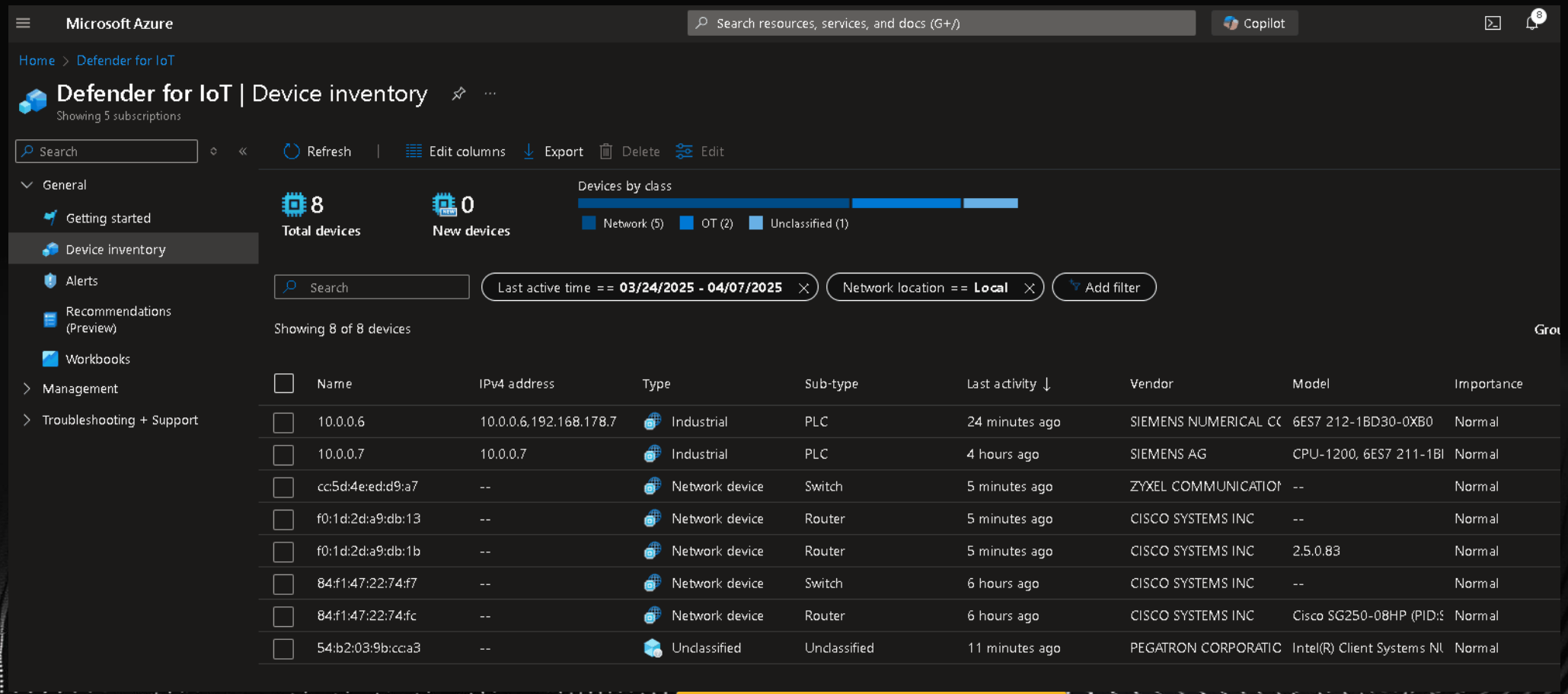
Azure | D4IOT | Device inventory [SPAN]





nedscaper

Azure | D4IOT | Device inventory



nedscaper

User Asset security ✅ #ZeroTrust

ZERO TRUST

nedscaper

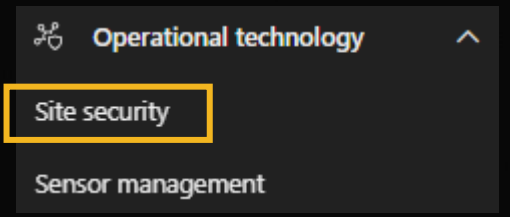
XDR | OT Physical Site security

nedscaper

XDR | Operational technology | Site security

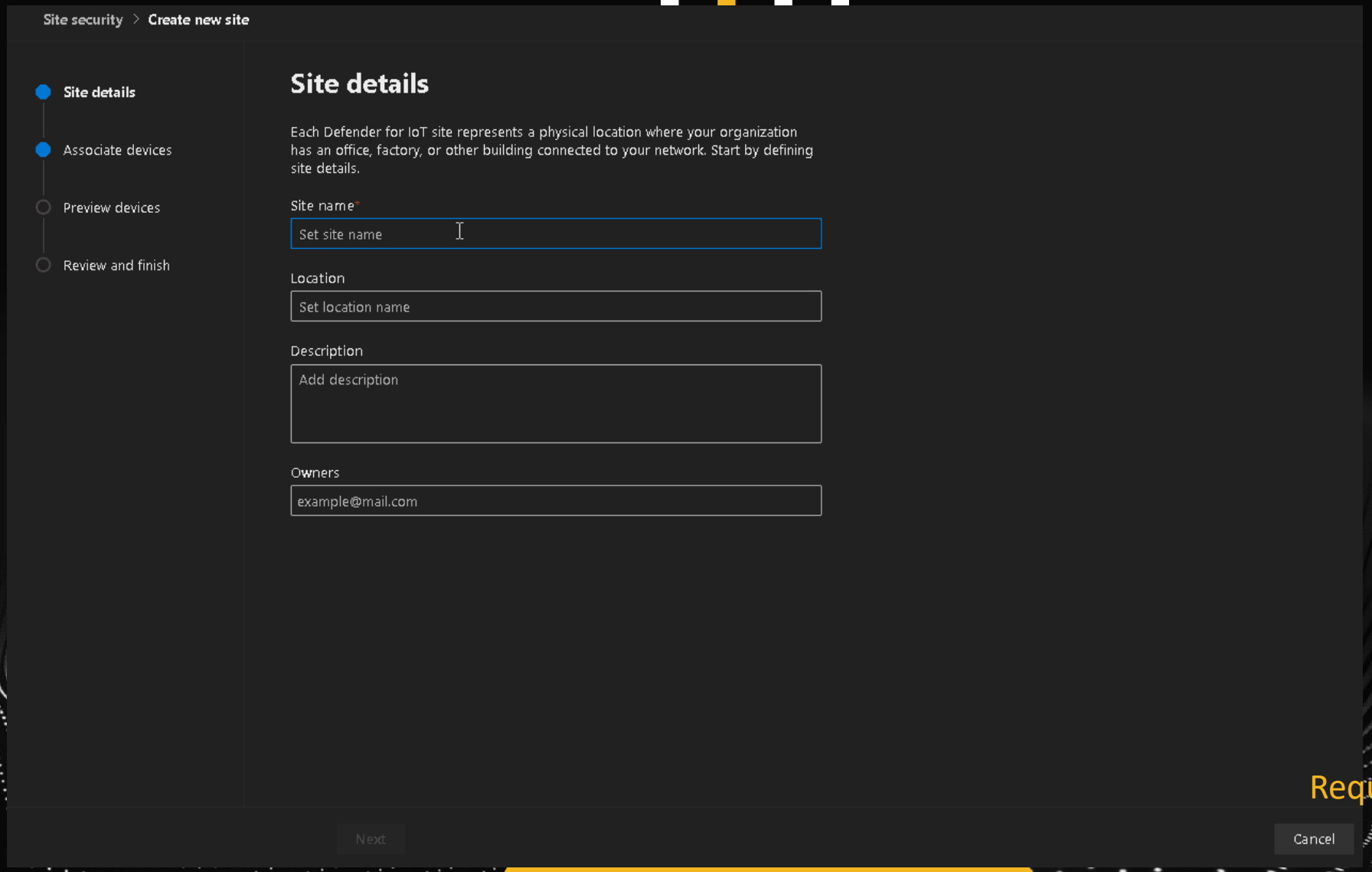
Overview of **physical** locations with OT devices

- Connected computer, network & IoT devices
- # of compromised devices | ■■■ Risk Level
- # of vulnerable devices | ■■■ Exposure Level
- # of Critical devices | ■■■ Device Criticality
- Top vendors



nedscaper

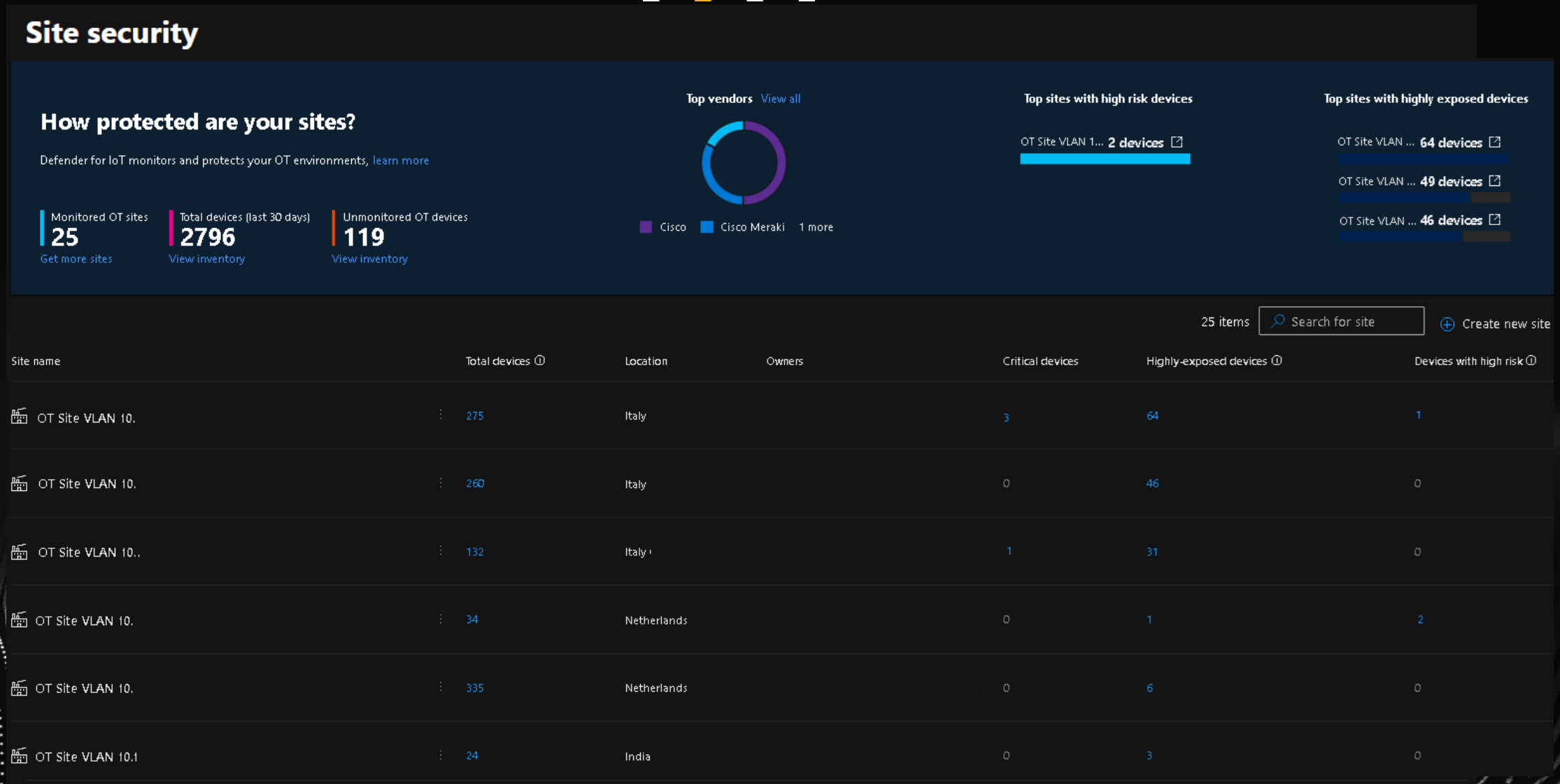
OT | Site security | Create new site



Requires active OT device(s)

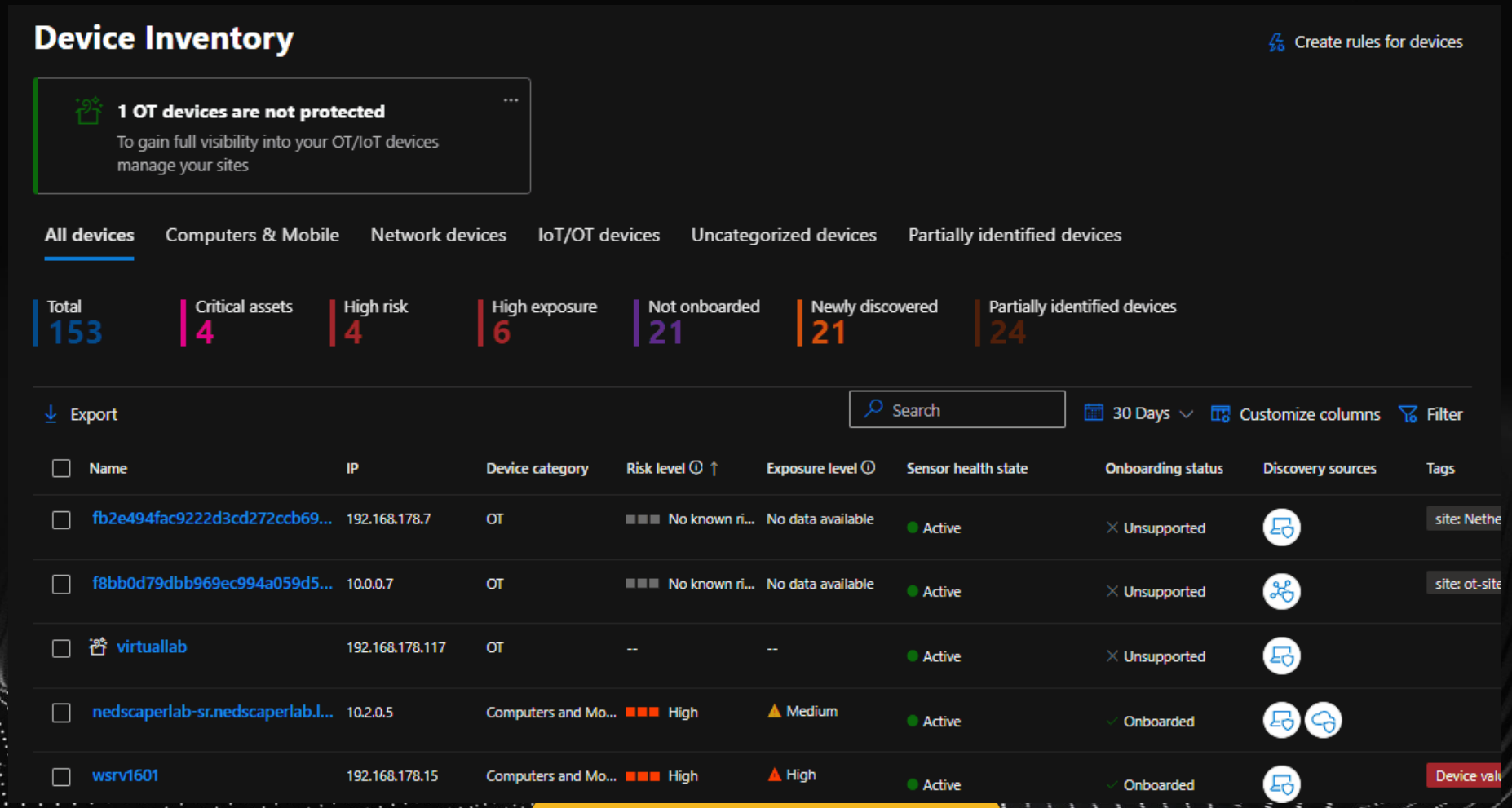
nedscaper

OT | Site security | Overview



nedscaper

XDR | Devices | Discovery sources



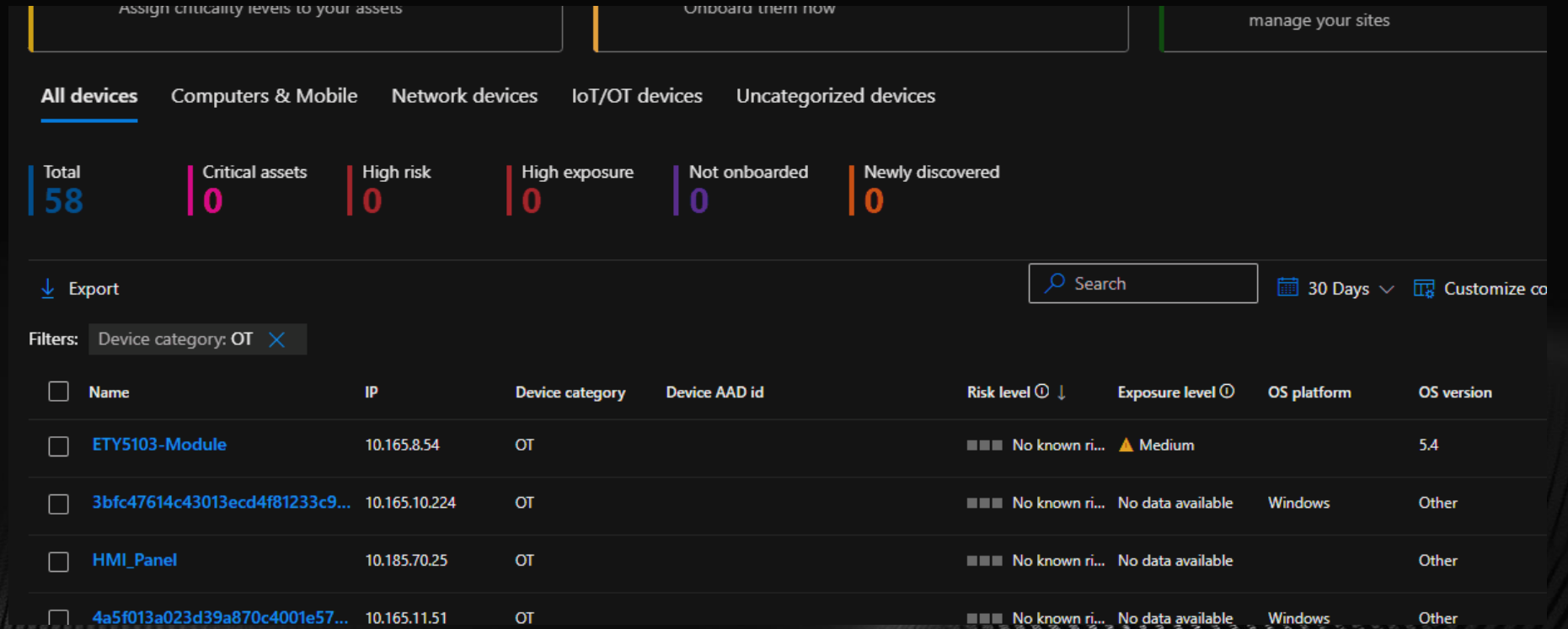
Microsoft Defender for IoT

Vulnerability [**MDVM**] and Posture [**MSEM**] Management

nedscaper

Defender XDR | Assets | Exposure Level

Microsoft Defender Vulnerability Management for EIoT & OT



nedscaper

Exposure Management | Initiative | EIoT Security

Name ↑	State	Impact	Workload	Domain
Disable insecure administration protocol - Telnet	NOT AVAILABLE	Medium	Microsoft Defender for IoT - OT site license	network
Mitigate critical vulnerabilities on devices	NOT AVAILABLE	High	Defender for Endpoint	deviceMisconfiguration
Remove insecure administration protocols SNMP V1 and SNMP V2	NOT AVAILABLE	Medium	Microsoft Defender for IoT - OT site license	network
Require authentication for Telnet management interface	NOT AVAILABLE	High	Microsoft Defender for IoT - OT site license	network
Require authentication for VNC management interface	NOT AVAILABLE	Medium	Microsoft Defender for IoT - OT site license	network
Secure your IoT devices with critical vulnerabilities	NOT AVAILABLE	High	E5 - IoT security opt-in	deviceMisconfiguration
Secure your IoT devices with high exposure level	NOT AVAILABLE	Medium	E5 - IoT security opt-in	deviceMisconfiguration
Turn on Microsoft Defender for Endpoint for IoT device discovery	NOT AVAILABLE	High	E5 - IoT security opt-in	deviceMisconfiguration

nedscaper

Exposure Management | Initiative | OT Security

Name ↑	State	Impact	Workload	Domain
Disable insecure administration protocol - Telnet	NOT AVAILABLE	Medium	Microsoft Defender for IoT - OT site license	network
Onboard Microsoft Defender for IoT to protect OT devices	NOT AVAILABLE	High	Microsoft Defender for IoT - OT site license	deviceMisconfiguration
Remove insecure administration protocols SNMP V1 and SNMP V2	NOT AVAILABLE	Medium	Microsoft Defender for IoT - OT site license	network
Require authentication for Telnet management interface	NOT AVAILABLE	High	Microsoft Defender for IoT - OT site license	network
Require authentication for VNC management interface	NOT AVAILABLE	Medium	Microsoft Defender for IoT - OT site license	network
Secure your devices with critical vulnerabilities linked to a site	NOT AVAILABLE	High	Microsoft Defender for IoT - OT site license	deviceMisconfiguration

nedscaper

Initiative | OT Security | Anonymous Telnet

nedscaper

Azure | D4IOT | Recommendations

Defender for IoT | Getting started

Showing 5 subscriptions

Search

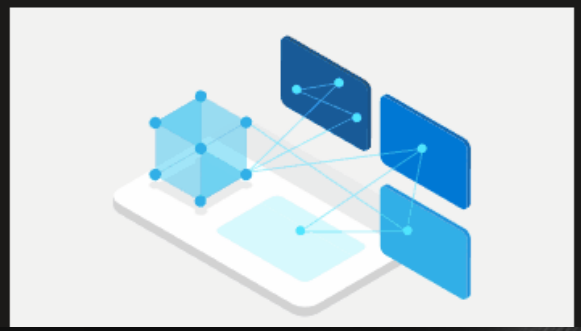
Get started | Sensor | On-premises management console

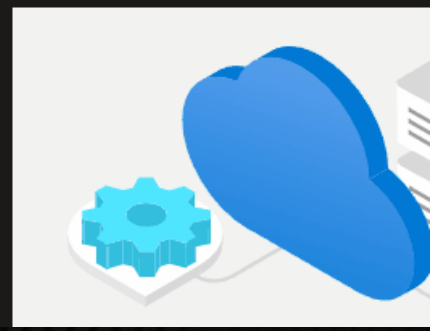
- General
  - Getting started
  - Device inventory
  - Alerts
  - Recommendations (Preview)
  - Workbooks
- Management
- Troubleshooting + Support

Welcome to Microsoft Defender for IoT

Defender for IoT delivers agentless, network-layer security for continuous IoT/OT asset discovery, vulnerability management, and threat detection in operational and enterprise
No changes to existing environments are required. In addition, the solution integrates with Microsoft Sentinel and 3rd-party SOC tools such as Splunk, IBM QRadar, ServiceNow,
Defender for IoT has zero impact on network performance and can be deployed fully on-premises or in Azure-connected environments.

Read more about the solution

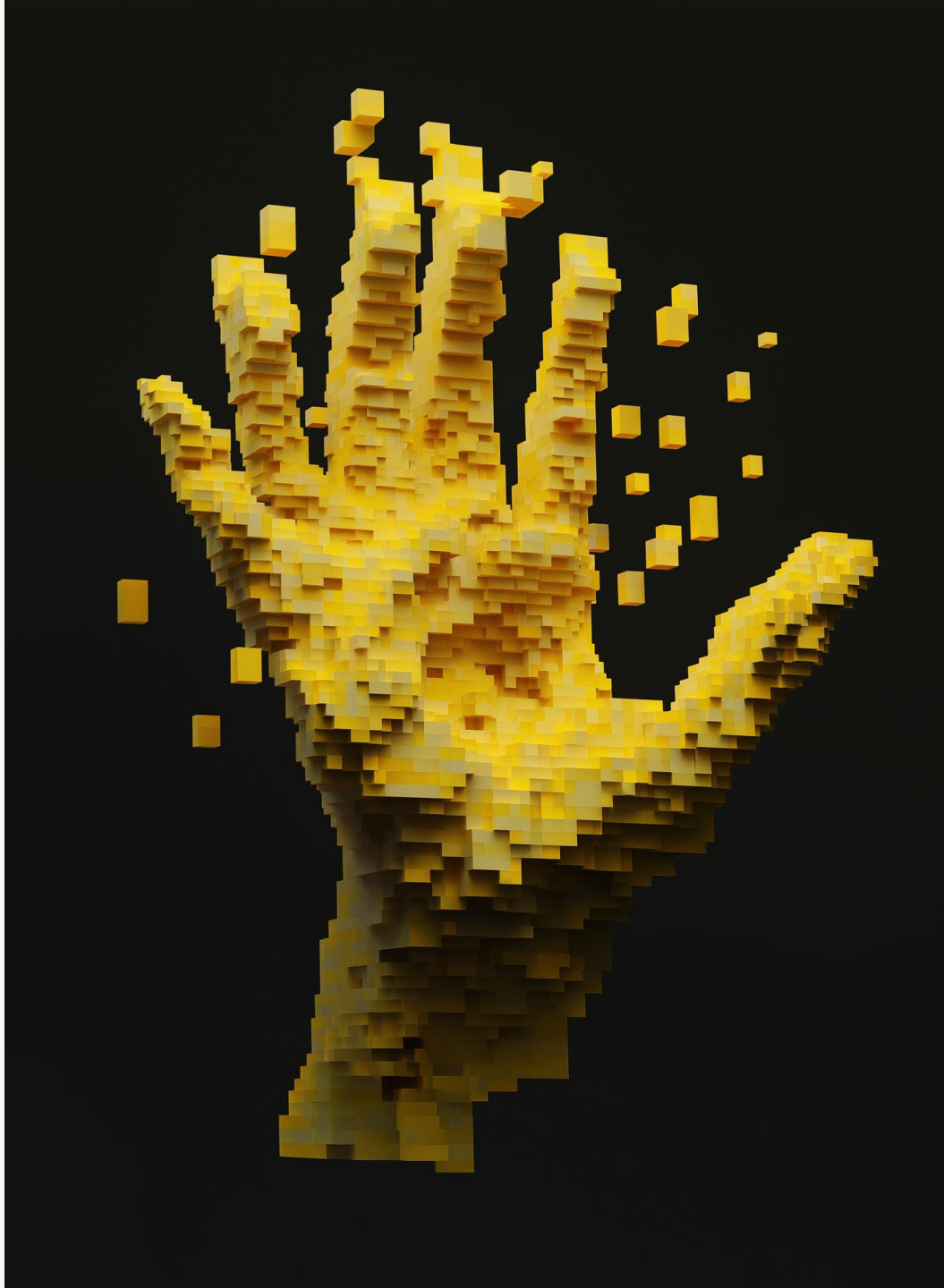




Microsoft Defender for IoT

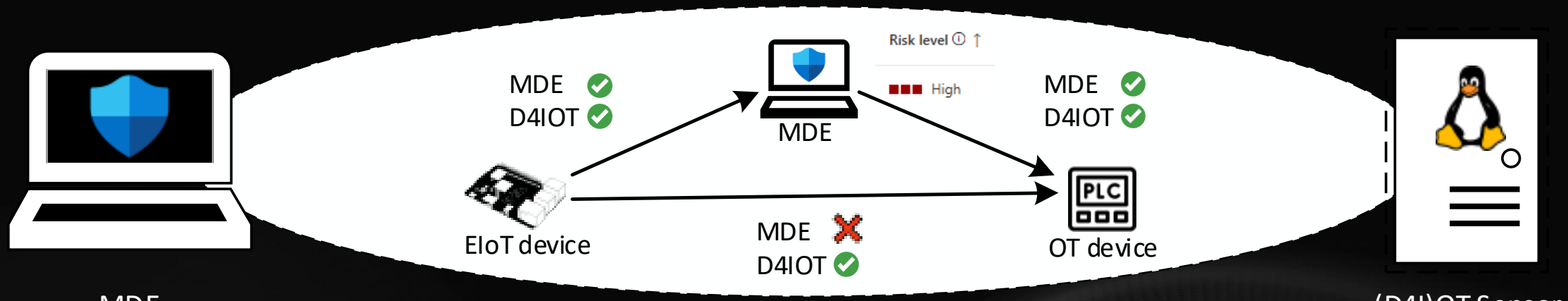
Threat Protection

100% prevention does not exist, e.g. 0-days



nedscaper

Defender XDR | OT Incident

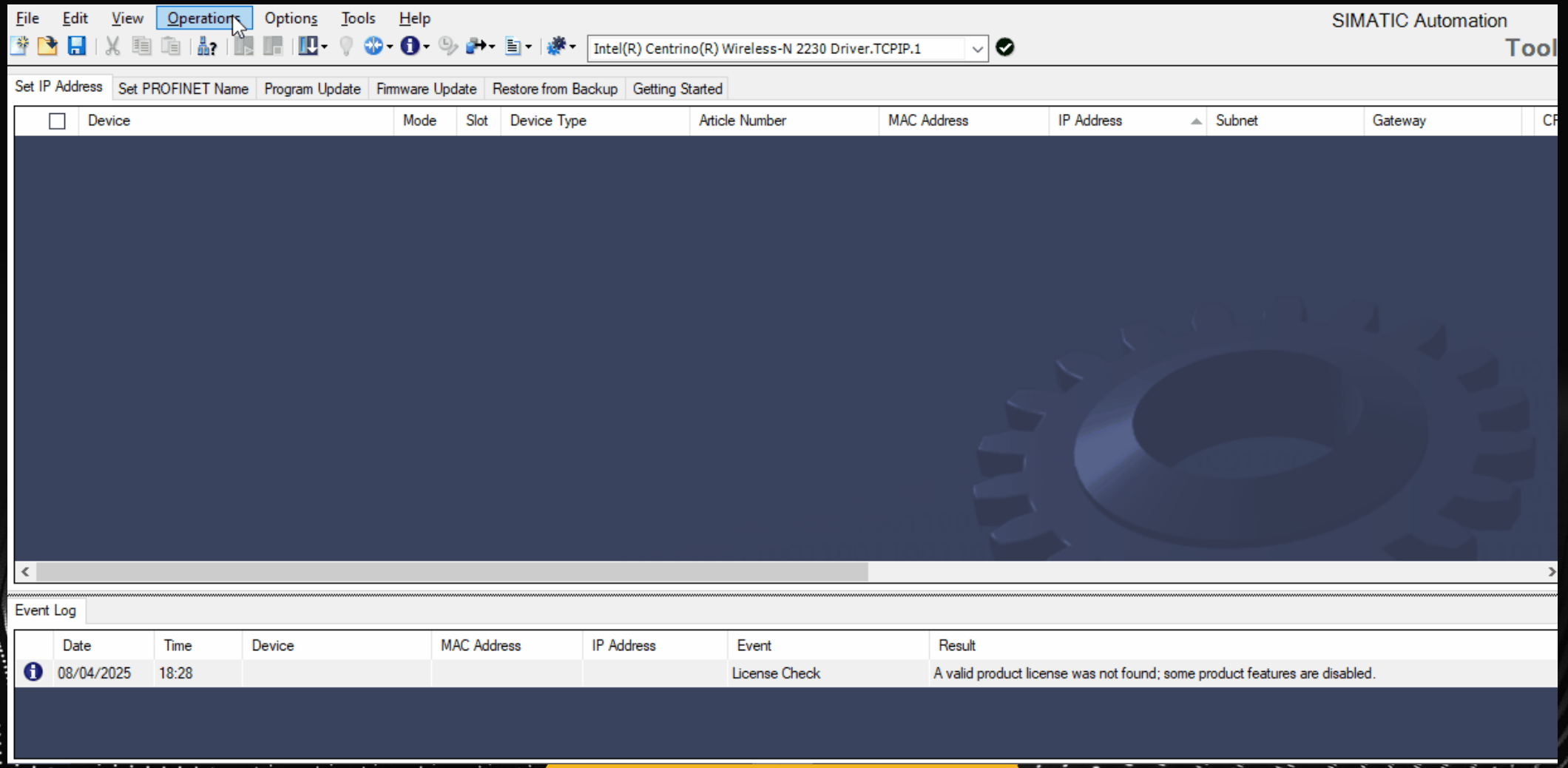


multi-stage incident from compromised MDE device

XDR | Attack Disruption

nedscaper

Defender XDR | Incident



nedscaper

Azure | D4IOT | Alerts 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

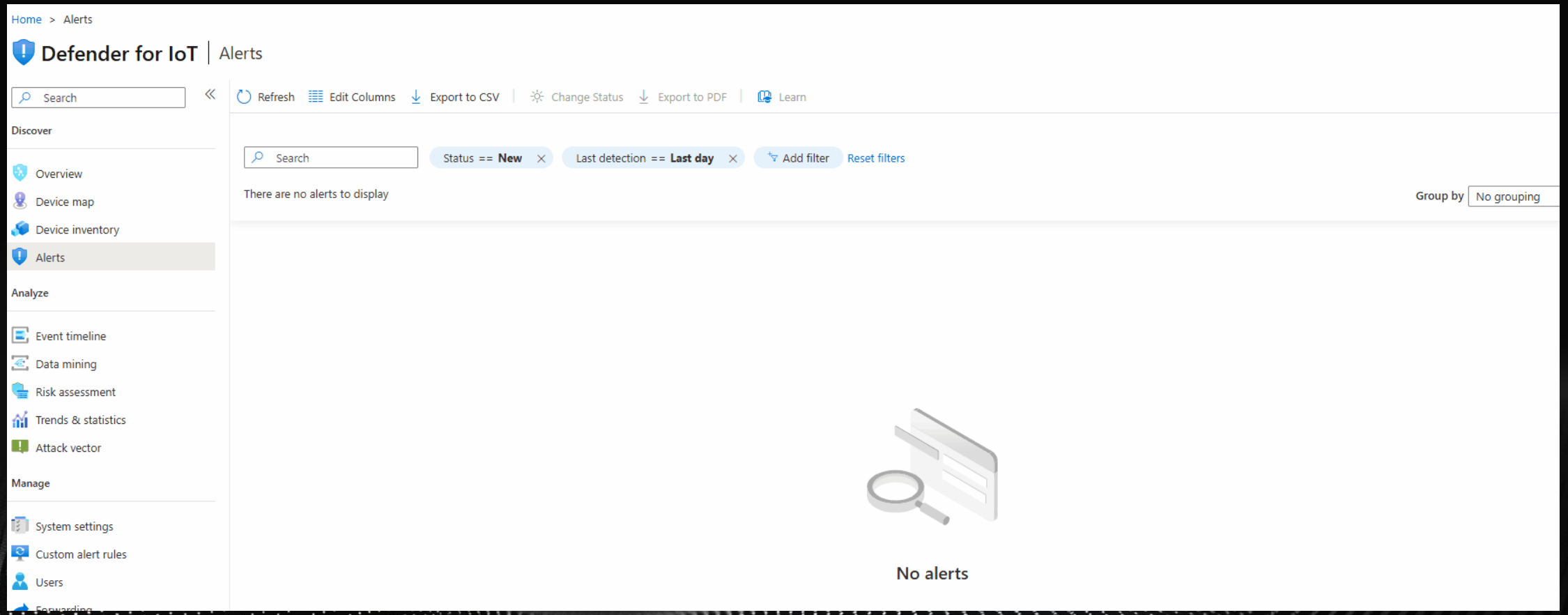
100+ OT Alert use-case(s)

nedscaper

Azure | D4IOT | Alerts

nedscaper

Sensor | D4IOT | PCAP



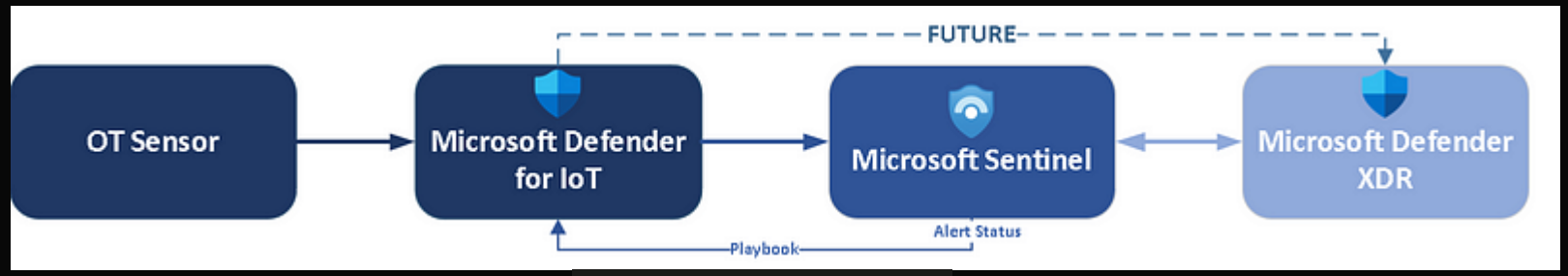
nedscaper

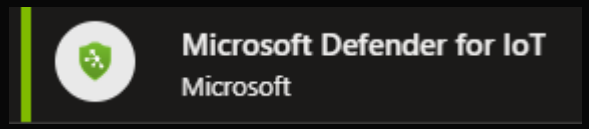
Sentinel | D4IOT Content Hub solution

Microsoft Defender for IoT	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Microsoft Defender for IoT	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Internet Access (Microsoft Defender for IoT)	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Microsoft Defender for IoT	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Unauthorized device in the network (Micro...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Multiple scans in the network (Microsoft D...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Suspicious malware found in the network (...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
No traffic on Sensor Detected (Microsoft D...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Unauthorized remote access to the networ...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
High bandwidth in the network (Microsoft ...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
PLC unsecure key state (Microsoft Defende...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Firmware Updates (Microsoft Defender for ...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Denial of Service (Microsoft Defender for I...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Excessive Login Attempts (Microsoft Defen...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
PLC Stop Command (Microsoft Defender fo...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Illegal Function Codes for ICS traffic (Micro...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Unauthorized PLC changes (Microsoft Defe...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
Unauthorized DHCP configuration in the n...	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
AD4IoT-AutoAlertStatusSync	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
AD4IoT-AutoCloseIncidents	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
AD4IoT-AutoTriageIncident	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
AD4IoT-CVEAutoWorkflow	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
AD4IoT-MailByProductionLine	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
AD4IoT-NewAssetServiceNowTicket	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
AD4IoT-SendEmailtoIoTOwner	Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu

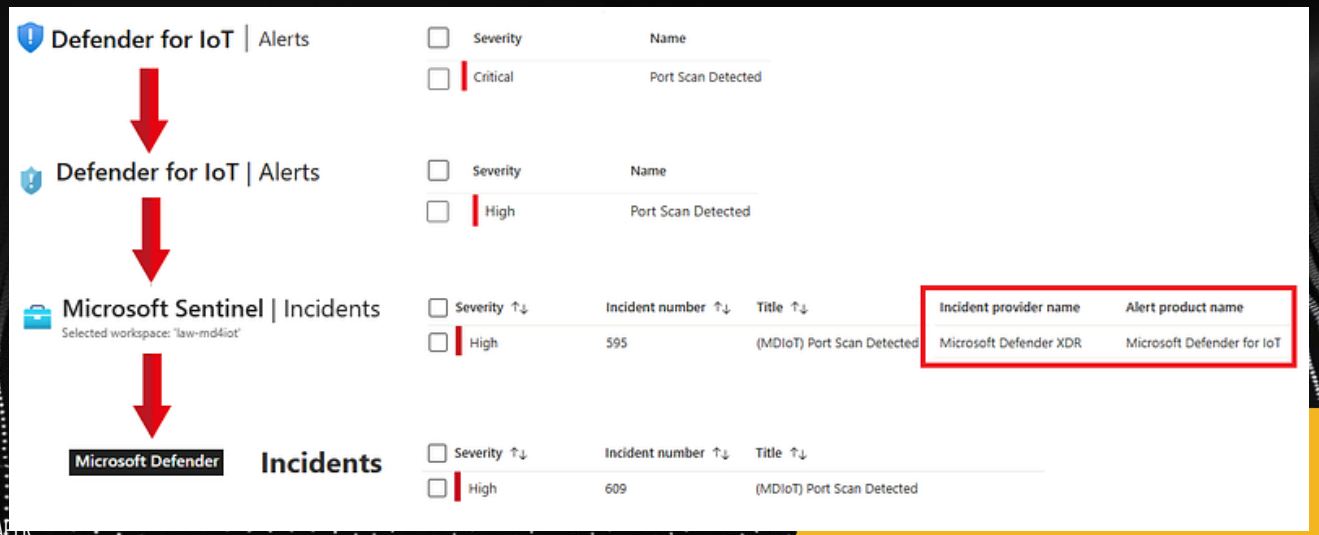
nedscaper

Sentinel | D4IOT Content Hub solution



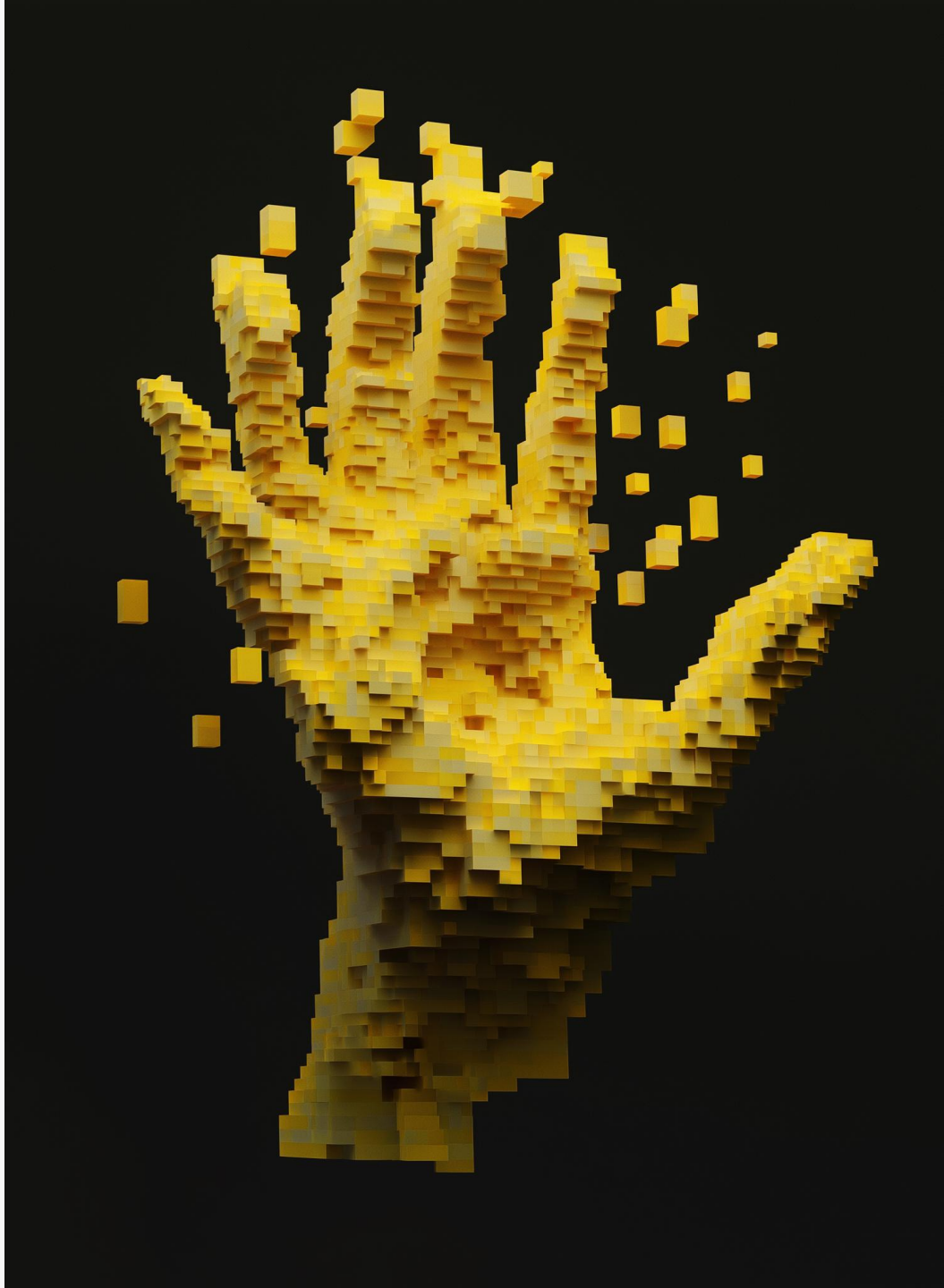


Alerts from Defender for IoT are streamed in Microsoft Sentinel and synced to Microsoft Defender XDR



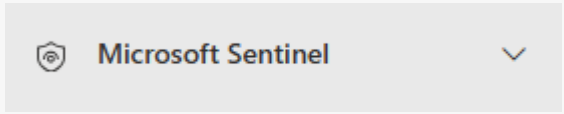
Microsoft Defender for IoT

The Future
#OneSOC

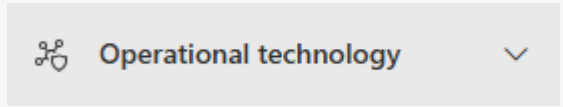


Azure Security -> Defender XDR

Microsoft Sentinel



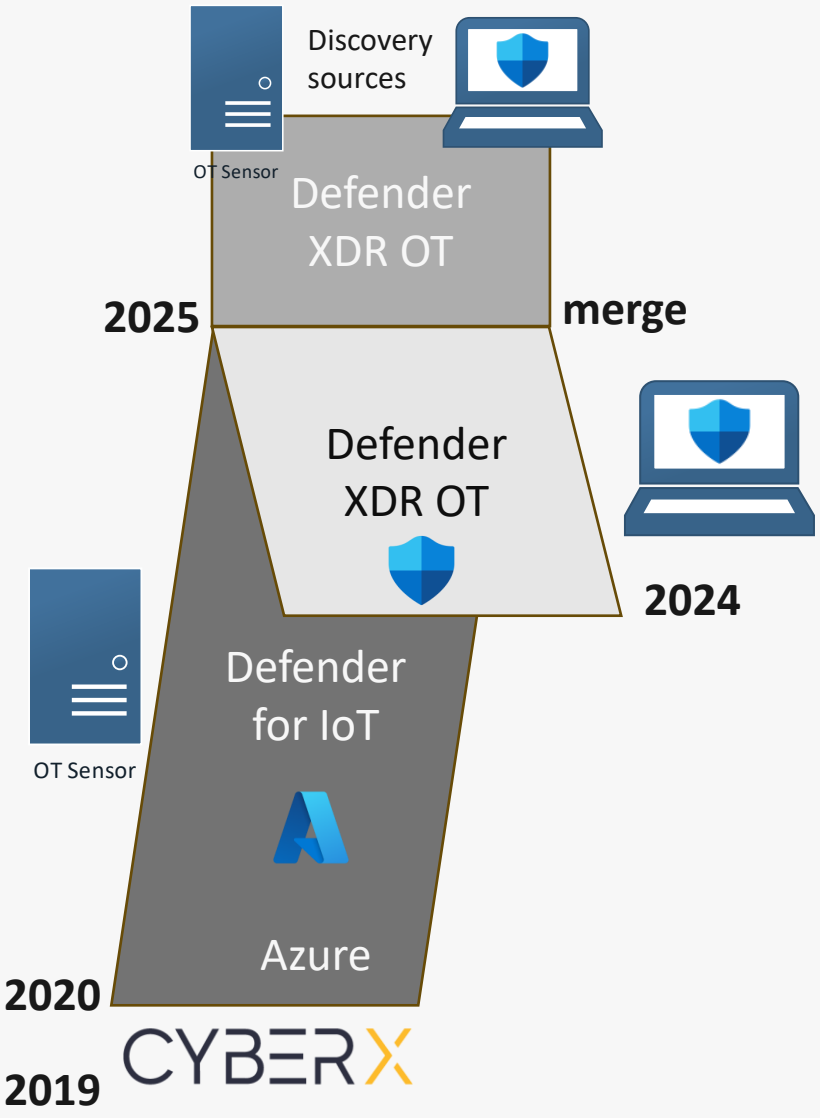
Microsoft Defender for IoT



Microsoft Defender EASM

?

Azure Security -> Defender XDR



PRESENTATION NEDSCAPER

Why Microsoft Defender XDR

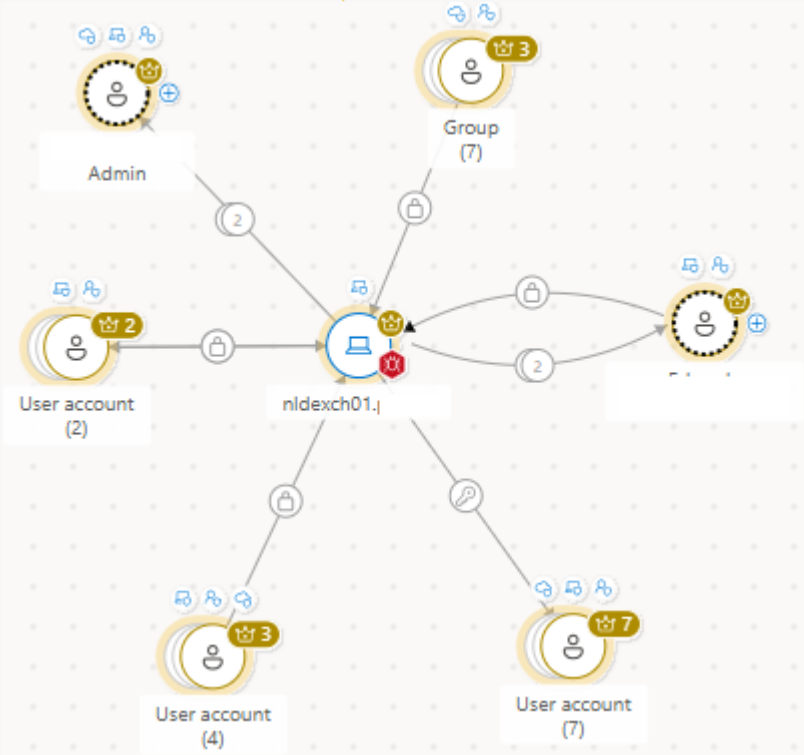
Azure (internal hosting) cost $$$

Microsoft Security Copilot

Microsoft Graph

XDR | Automatic Attack Disruption

XSPM | Autonomous Remediation



What to choose?

It depends … ☺

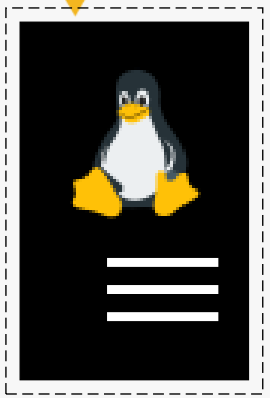
Defender for Endpoint

OT in IT Network

?

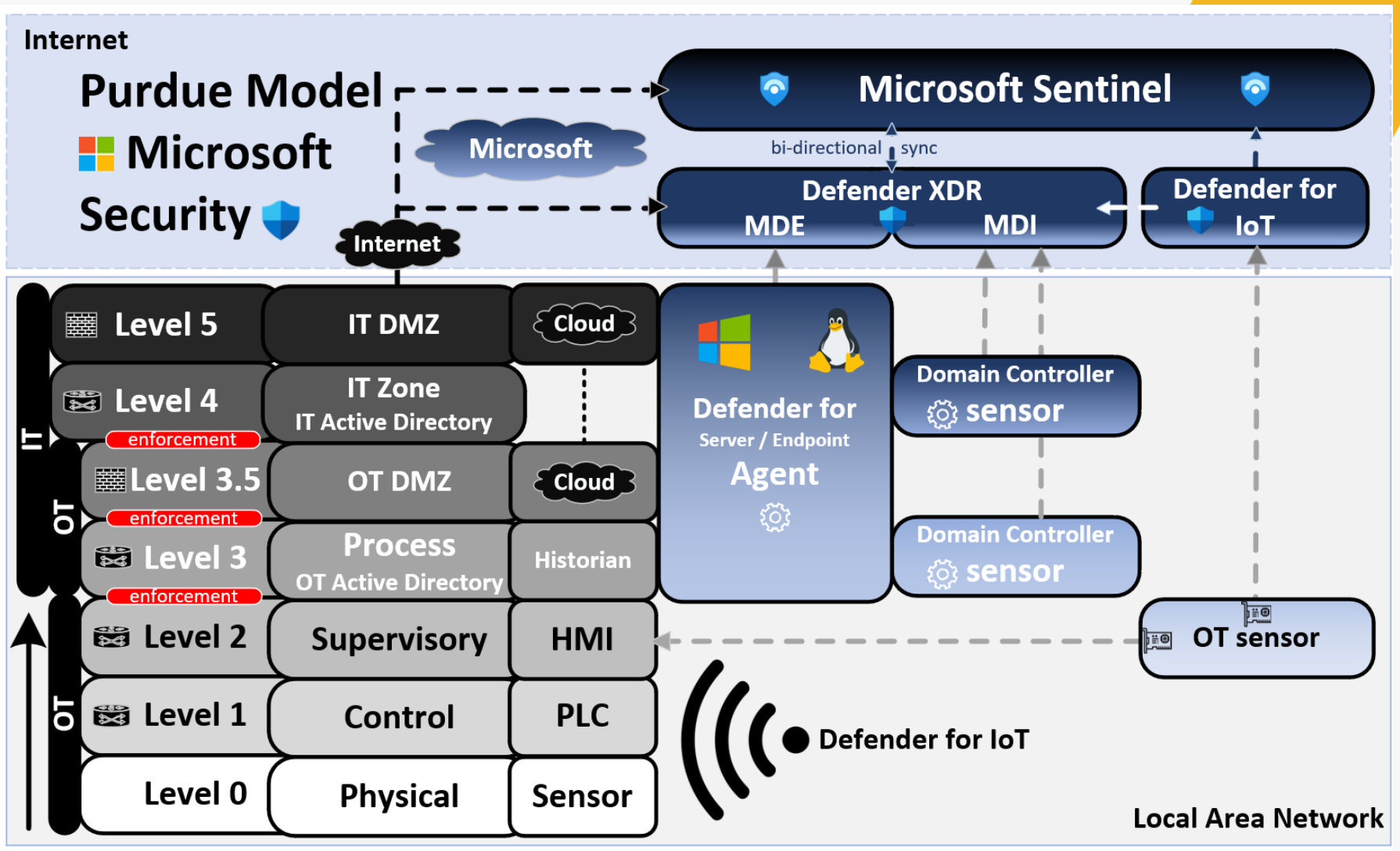
OT Network

OT Sensor



Better Together

Better Together



Homelab Physical

Microsoft

Siemens S7 PLC

MDE

OT Sensor

SPAN

Siemens S7 PLC

Moxa Nport

Homelab Virtual

Microsoft Hyper-V

vmware