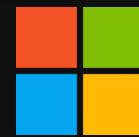


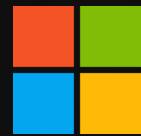
# Demystifying



# Microsoft Defender for IoT



# Demystifying



# Microsoft Defender for OT





# Welcome



MICROSOFT SECURITY

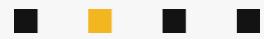
**Derk van der Woude**

CTO Nedscaper

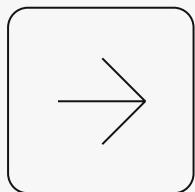
Microsoft Security **MVP**

Microsoft **CCP** Discussion Leader | **Defender for IoT**



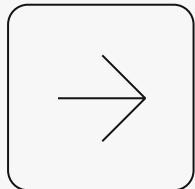


# What keeps me Awake at Night?

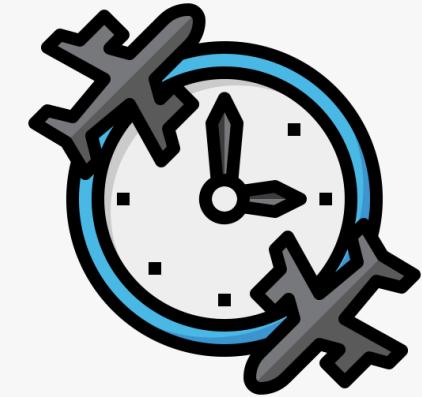
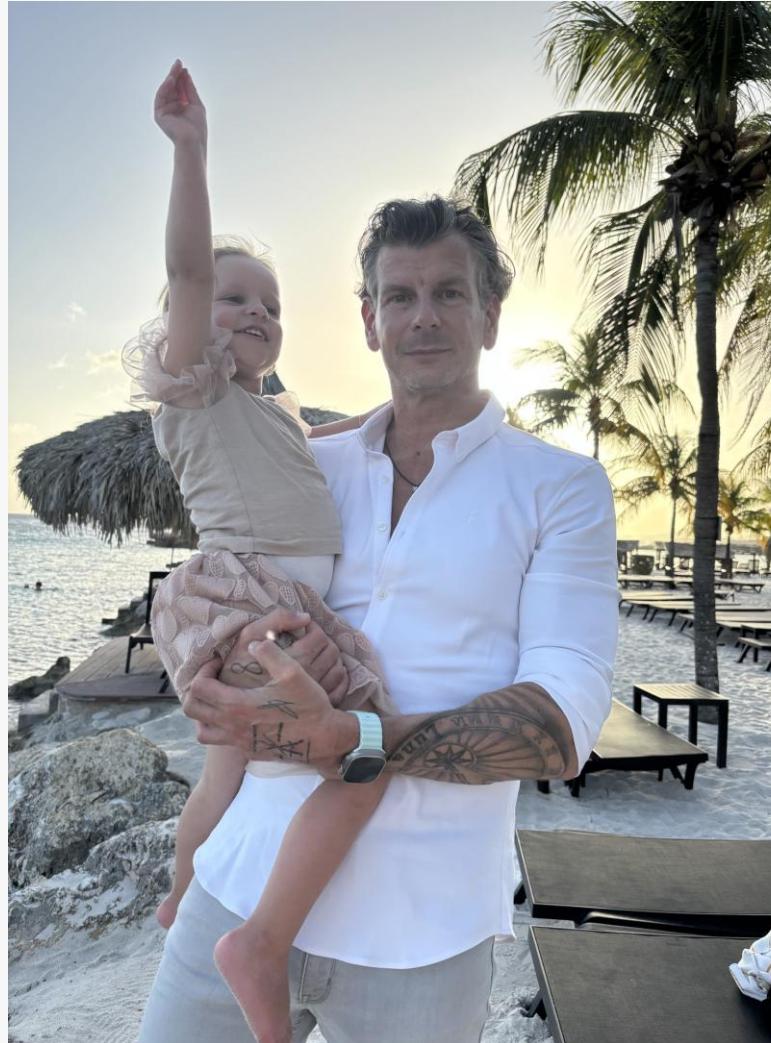




# What keeps me Awake at Night?



PRESENTATION NEDSCAPER



# What keeps me Awake at Night?

The collage consists of nine images arranged in a grid-like pattern:

- Top Left:** A banner for "STUXNET" featuring the flags of the United States, Israel, and the Netherlands. Below it is a screenshot of a Stuxnet exploit code.
- Top Middle:** An image of a hand being scanned by a glowing blue light, with the text "Oil India HQ Cyber Attack" overlaid.
- Top Right:** A banner for "BLACK ENERGY ICS Threat Intelligence Timeline".
- Middle Left:** A banner for "SNAKE / EKANS Ransomware" with the text "Hostile Nation-State Attackers Start Deploying OT-Oriented Malware".
- Middle Center:** An image of a power grid with red energy arcs, labeled "INDUSTROYER2 BY SANDWORM APT" and "Second Power Outage Attack in Human History".
- Middle Right:** An image of an industrial facility with a large red "HACKED" stamp across it.
- Bottom Left:** A banner for "Cyber Attack on Kudankulam Nuclear Power Plant" with the subtitle "A Wake Up Call".
- Bottom Right:** A map of Russia and Ukraine showing a timeline of cyber attacks from 2014 to 2022, including the "Russia-Ukraine Cyber War".



# Stuxnet

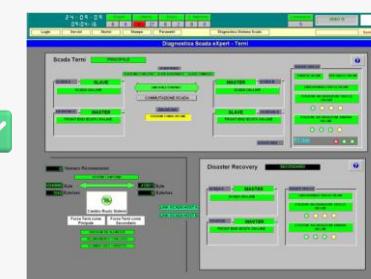
## 1981 Operation Opera

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

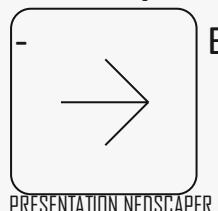


## 2005 Operation Olympic games

- Stuxnet development for **Iran** (Natanz) nuclear plant **30m underground**
- **150.000** lines of code ( $\sim 10x$  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



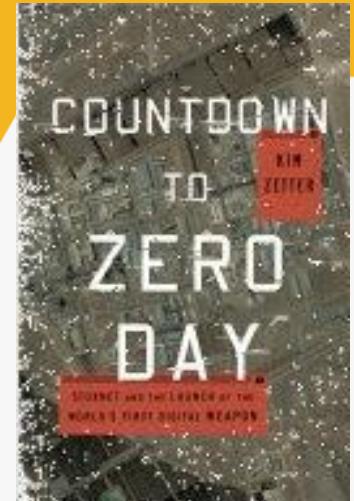
## 2025 Operation Rising Lion ...



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



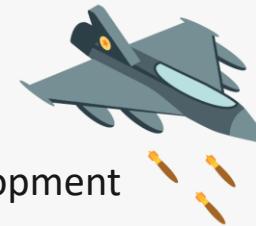
## Booktip



# Stuxnet

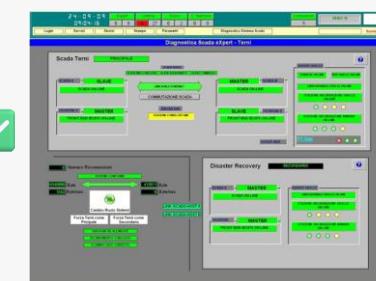
### 1981 Operation Opera

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



### 2005 Operation Olympic games

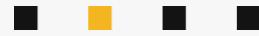
- Stuxnet development for **Iran** (Natanz) nuclear plant **30m underground**
- **150.000** lines of code ( $\sim 10x$  average malware lines of code)
- **2007** initial access via USB / equipment (**AIVD**)
- **2010** Stuxnet Detected (*VirusBlokAda*)
- Malware for Windows & Siemens PLCs (Mossad & CIA)
- **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 ...





# Abbreviations



OT      Operational technology



EIoT Enterprise IoT

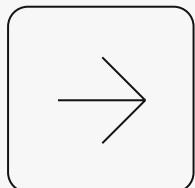


IIoT Industrial IoT

MIoT Medical IoT



BMS      Building Management System





# Abbreviations



OT      Operational technology



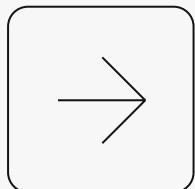
**EIoT** Enterprise IoT

*IIoT* Industrial IoT

*MIoT* Medical IoT



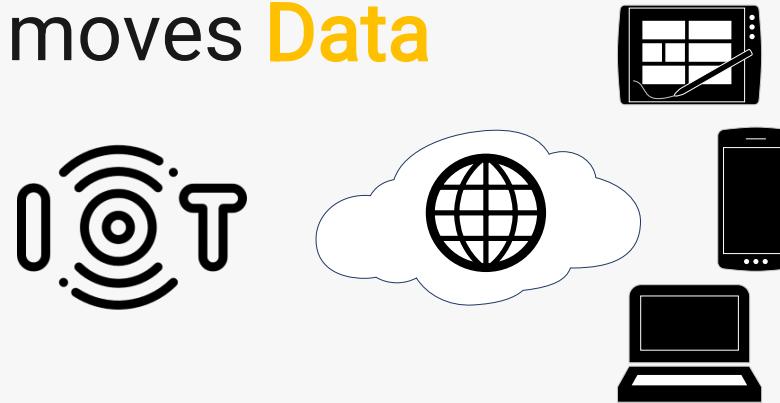
BMS      Building Management System



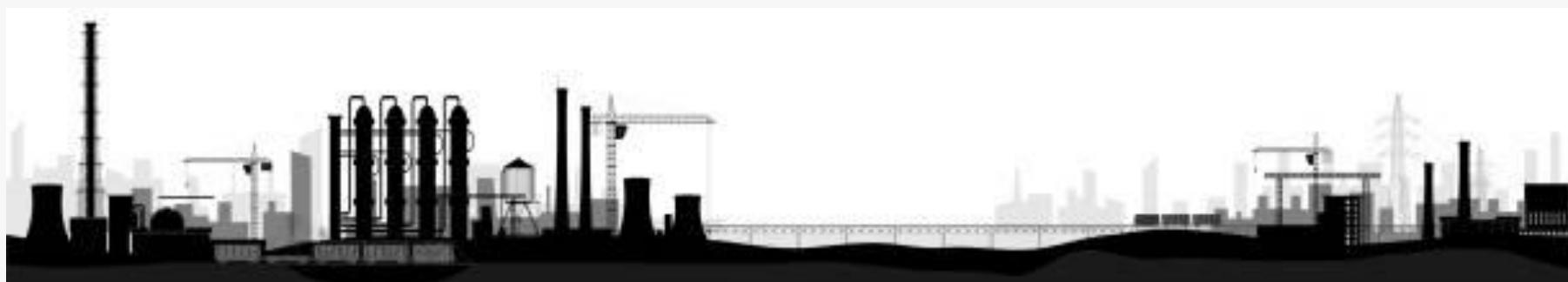


# Difference in use-case(s)

- EIoT moves Data



- OT (BMS) moves Physical Systems



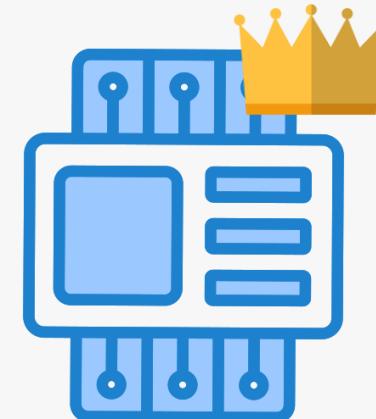
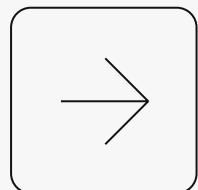


# An Attacker perspective

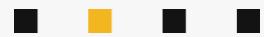
Rule of thumb 



EIoT devices are LMPs [Lateral Movement Paths]



OT devices are Crown Jewels / Critical Assets



# Example of IoT as entry-point



## BUSINESS INSIDER

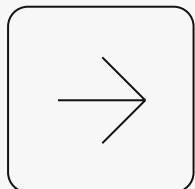
[Subscribe](#)

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

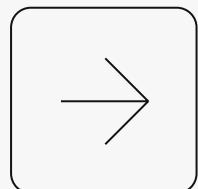
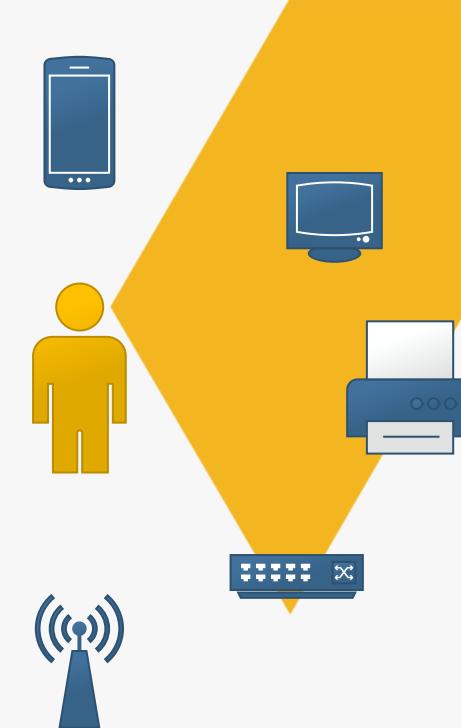
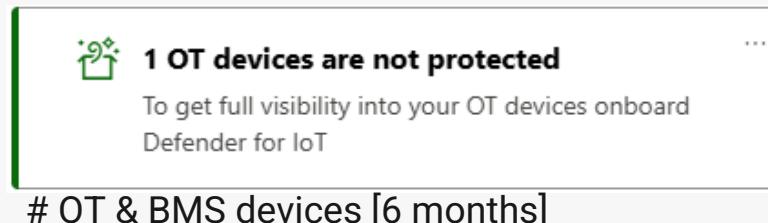


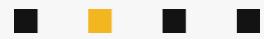
Pierluigi Paganini April 16, 2018



# Microsoft License(s) – part I

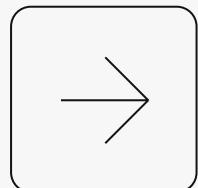
- Microsoft 365 E5 | E5 Security [1:5] →
  - Risk Level & Exposure Level for EloT devices
  - MDE P2 requires EloT add-on per device
  - OT Device Discovery

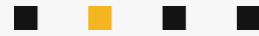




# Microsoft License(s) – part II

- 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

Device Discovery



Identity

Vulnerability Management



Protect

Threat Detection



Detect & Respond

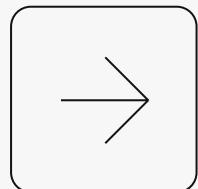
- The Future of Microsoft OT

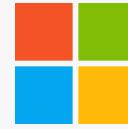
## NIST Cybersecurity Framework



## Solution Type(s)

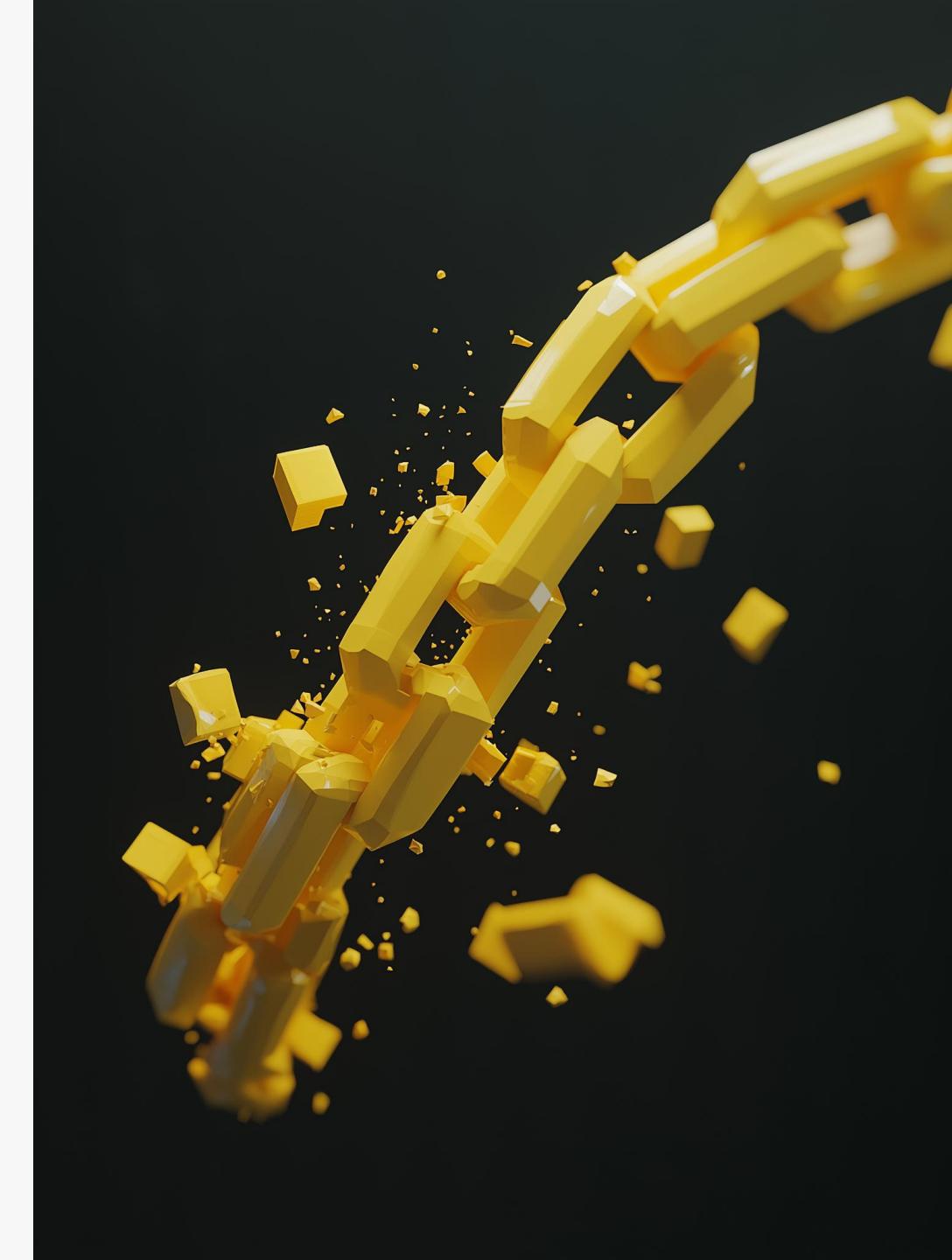
- Defender XDR | MDE | Enterprise IoT
- Defender XDR | MDE | D4IOT
- Azure | Sensor | D4IOT





Microsoft Defender for IoT

# Device Discovery

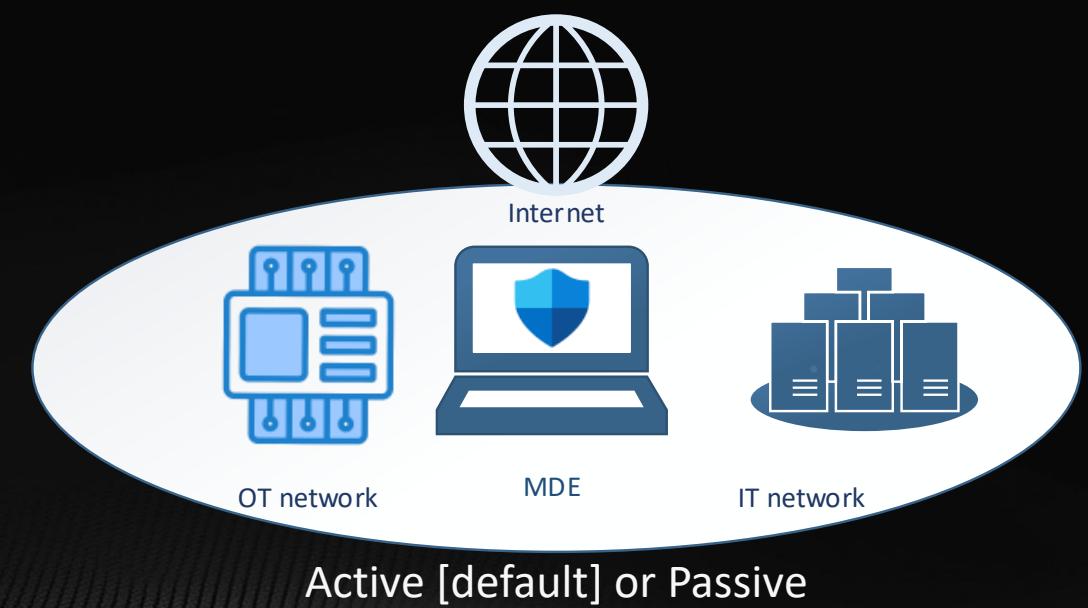


# You cannot Protect what you don't know



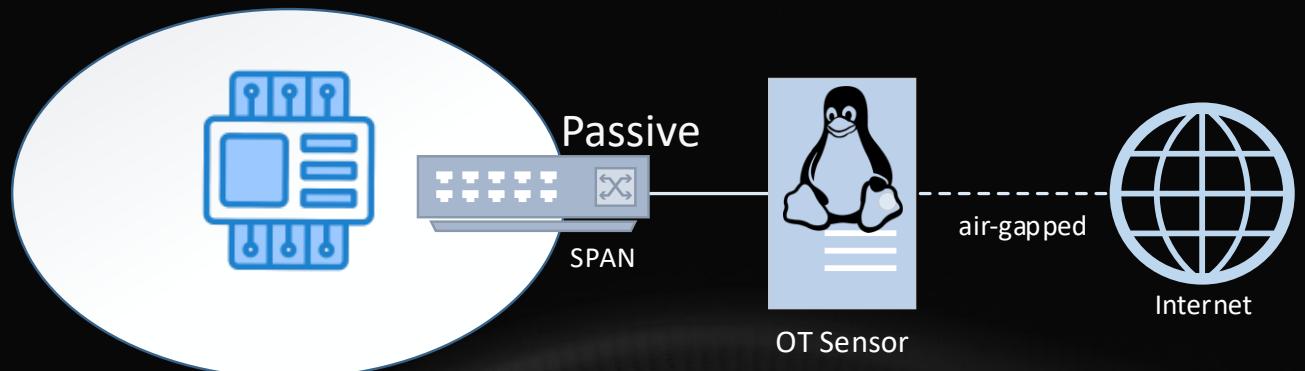
# Device Discovery Overview

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



Active [default] or Passive

- Basic  
Discover and identify unmanaged devices by passively listening to network events captured by onboarded devices.
- Standard discovery (recommended)  
Enrich device information and discover even more devices by using smart, active device probing.



OT Device Discovery via  
OT Sensor [SPAN/TAP]

# Enterprise IoT Device discovery settings



**Settings**

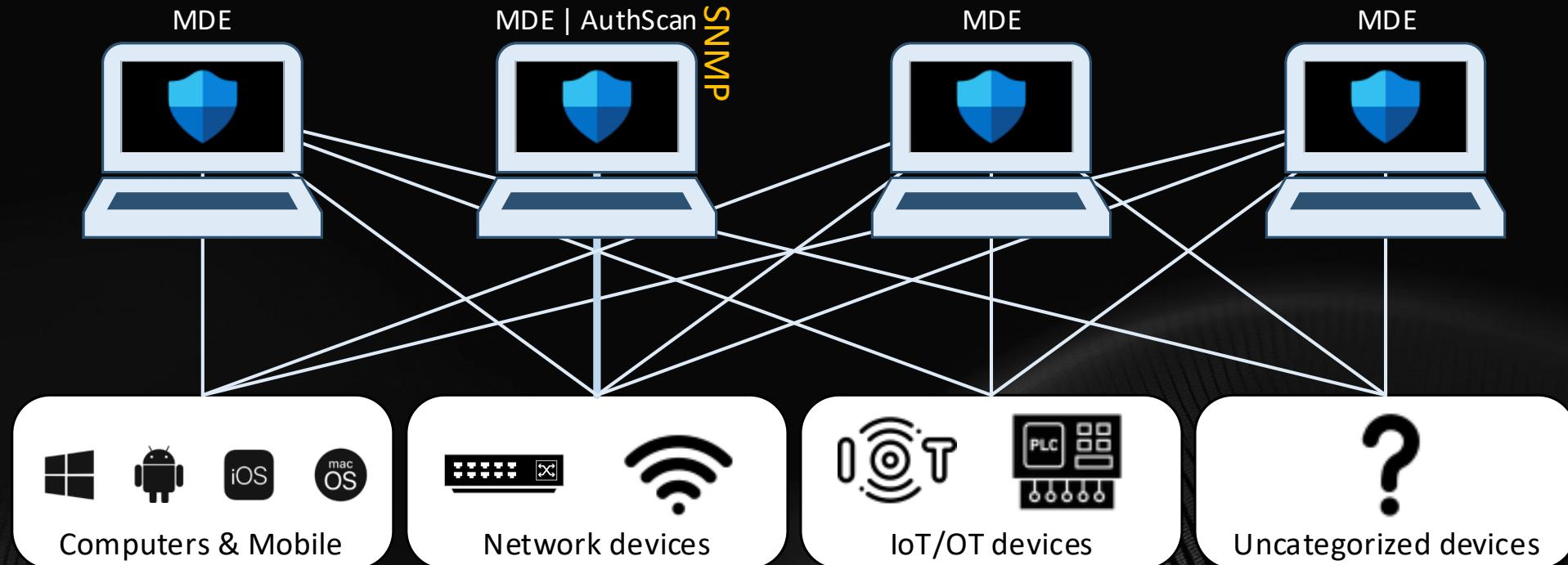
---

8 items

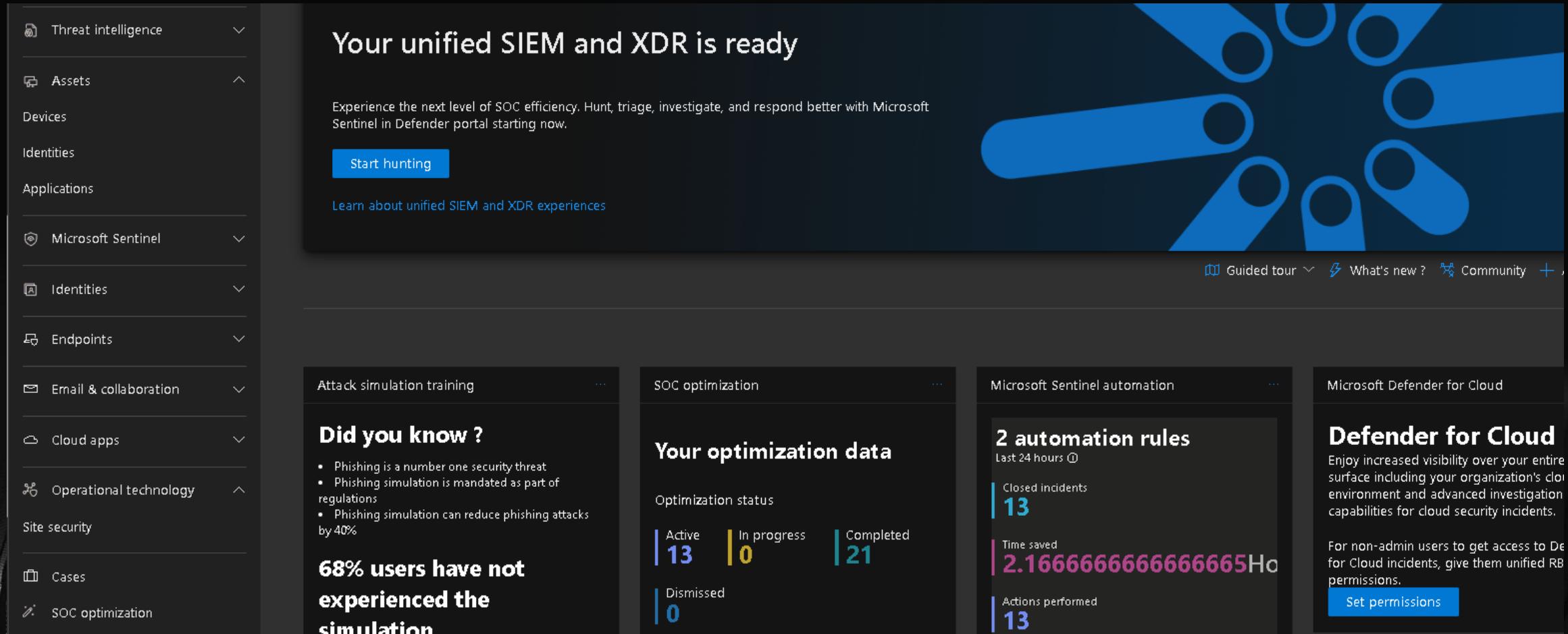
Name	Description
 Microsoft Defender portal	General settings for the Microsoft Defender portal
 Microsoft Defender XDR	General settings for Microsoft Defender XDR
 Endpoints	General settings for endpoints
 Email & collaboration	General settings for email & collaboration
 Identities	General settings for 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

# Device Discovery via MDE

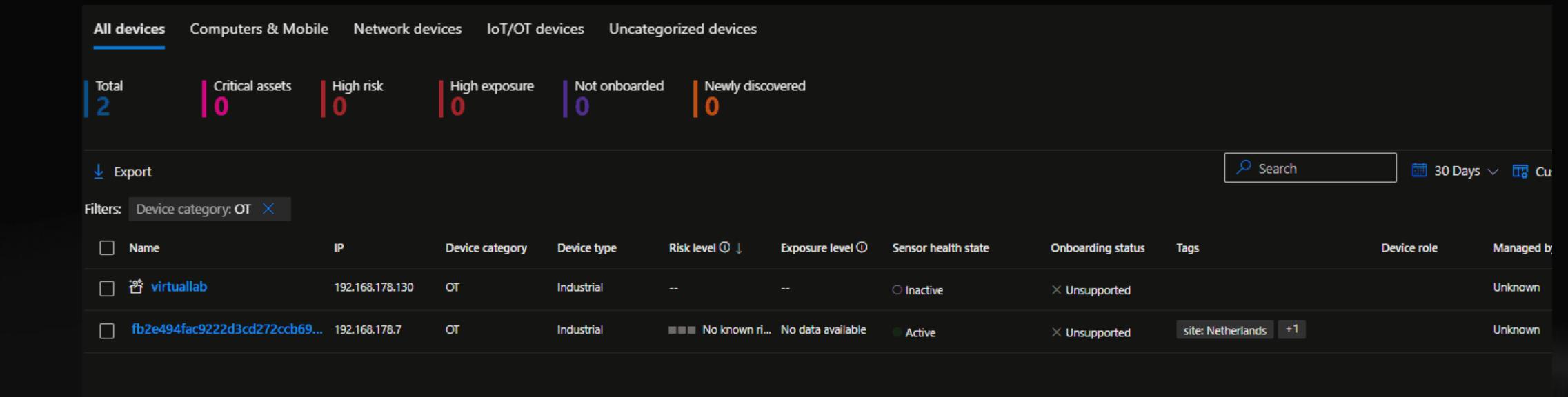


# Defender XDR | Assets | Devices [OT]



The screenshot shows the Microsoft Defender XDR portal interface. On the left, a navigation sidebar lists categories: Threat intelligence, Assets, Devices, Identities, Applications, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, Operational technology (selected), Site security, Cases, and SOC optimization. The main content area features a large banner with the text "Your unified SIEM and XDR is ready" and a "Start hunting" button. Below the banner, sections include "Attack simulation training" (Did you know? Phishing is a number one security threat. Phishing simulation is mandated as part of regulations. Phishing simulation can reduce phishing attacks by 40%. 68% users have not experienced the simulation.), "SOC optimization" (Your optimization data: Active 13, In progress 0, Completed 21, Dismissed 0), "Microsoft Sentinel automation" (2 automation rules: Last 24 hours 13 Closed incidents, Time saved 2.1666666666666665 hours, Actions performed 13), and "Microsoft Defender for Cloud" (Defender for Cloud: Enjoy increased visibility over your entire surface including your organization's cloud environment and advanced investigation capabilities for cloud security incidents. For non-admin users to get access to Defender for Cloud incidents, give them unified RB permissions). The bottom right corner has a "Set permissions" button.

# Assets | Devices | Set criticality

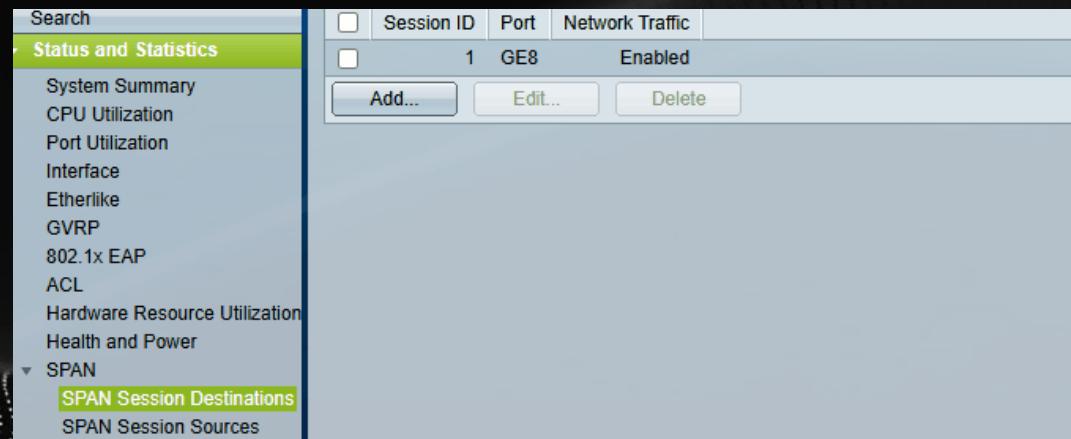
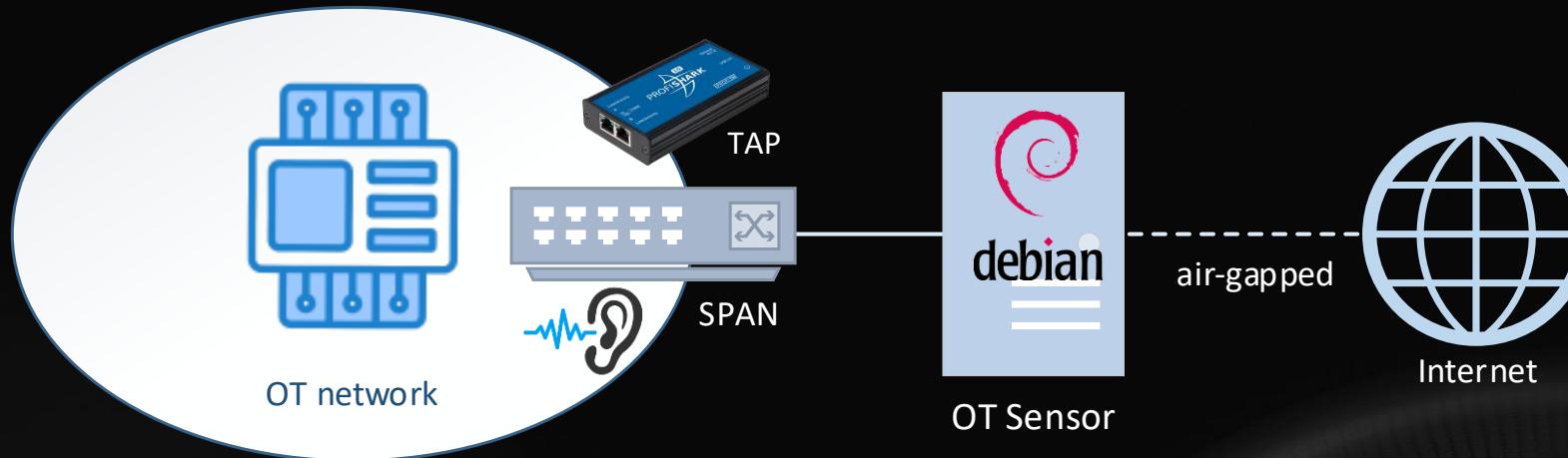


The screenshot shows the nedscaper web interface for managing assets and devices. At the top, there are navigation tabs: All devices (selected), Computers & Mobile, Network devices, IoT/OT devices, and Uncategorized devices. Below the tabs, a summary bar displays the following counts: Total (2), Critical assets (0), High risk (0), High exposure (0), Not onboarded (0), and Newly discovered (0). To the right of the summary bar are buttons for Export, Search (with a placeholder "Search"), and filters (30 Days, Current). A "Filters" dropdown is open, showing a selected filter: Device category: OT. The main content area is a table listing two devices:

Name	IP	Device category	Device type	Risk level ⓘ ↓	Exposure level ⓘ ↓	Sensor health state	Onboarding status	Tags	Device role	Managed by
virtualab	192.168.178.130	OT	Industrial	--	--	Inactive	Unsupported			Unknown
fb2e494fac9222d3cd272ccb69...	192.168.178.7	OT	Industrial	■■■■ No known ri...	No data available	Active	Unsupported	site: Netherlands +1		Unknown

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

# Azure | D4IOT | Device inventory [SPAN]



# Azure | D4IOT | Device inventory

Microsoft Azure    Search resources, services, and docs (G+)    Copilot    8

Home > Defender for IoT

## Defender for IoT | Device inventory

Showing 5 subscriptions

Search    Refresh    Edit columns    Export    Delete    Edit

General

Getting started    Total devices: 8    New devices: 0

Devices by class

Network (5)    OT (2)    Unclassified (1)

Alerts    Recommendations (Preview)    Workbooks

Search    Last active time = 03/24/2025 - 04/07/2025    Network location = Local    Add filter

Showing 8 of 8 devices

	Name	IPv4 address	Type	Sub-type	Last activity	Vendor	Model	Importance
<input type="checkbox"/>	10.0.0.6	10.0.0.6, 192.168.178.7	Industrial	PLC	24 minutes ago	SIEMENS NUMERICAL CC	6EST 212-1BD30-0XB0	Normal
<input type="checkbox"/>	10.0.0.7	10.0.0.7	Industrial	PLC	4 hours ago	SIEMENS AG	CPU-1200, 6EST 211-1BI	Normal
<input type="checkbox"/>	cc:5d:4e:ed:d9:a7	--	Network device	Switch	5 minutes ago	ZYXEL COMMUNICATION	--	Normal
<input type="checkbox"/>	f0:1d:2d:a9:db:13	--	Network device	Router	5 minutes ago	CISCO SYSTEMS INC	--	Normal
<input type="checkbox"/>	f0:1d:2d:a9:db:1b	--	Network device	Router	5 minutes ago	CISCO SYSTEMS INC	2.5.0.83	Normal
<input type="checkbox"/>	84:f1:47:22:74:f7	--	Network device	Switch	6 hours ago	CISCO SYSTEMS INC	--	Normal
<input type="checkbox"/>	84:f1:47:22:74:fc	--	Network device	Router	6 hours ago	CISCO SYSTEMS INC	Cisco SG250-08HP (PID: S)	Normal
<input type="checkbox"/>	54:b2:03:9b:cc:a3	--	Unclassified	Unclassified	11 minutes ago	PEGATRON CORPORATIC	Intel(R) Client Systems NL	Normal

# User Asset security. #ZeroTrust



Microsoft 365



**ZERO TRUST**

# XDR | OT Physical Site security

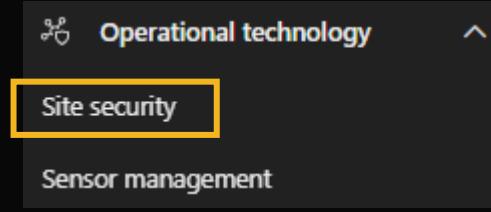


# XDR | Operational technology | Site security



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



## OT | Site security | Create new site

Site security > Create new site

Site details

Associate devices

Preview devices

Review and finish

Site details

Each Defender for IoT site represents a physical location where your organization has an office, factory, or other building connected to your network. Start by defining site details.

Site name\*

Set site name

Location

Set location name

Description

Add description

Owners

example@mail.com

Next

Cancel

Requires active OT device(s)

# OT | Site security | Overview



## Site security

**How protected are your sites?**

Defender for IoT monitors and protects your OT environments, [learn more](#)

Monitored OT sites	Total devices (last 30 days)	Unmonitored OT devices
<b>25</b> <a href="#">Get more sites</a>	<b>2796</b> <a href="#">View inventory</a>	<b>119</b> <a href="#">View inventory</a>

**Top vendors** [View all](#)



Vendor	Count
Cisco	1
Cisco Meraki	1
1 more	1

**Top sites with high risk devices**

Site	Devices
OT Site VLAN 1...	2 devices

**Top sites with highly exposed devices**

Site	Devices
OT Site VLAN ...	64 devices
OT Site VLAN ...	49 devices
OT Site VLAN ...	46 devices

25 items  [Create new site](#)

Site name	Total devices <small>①</small>	Location	Owners	Critical devices	Highly-exposed devices <small>①</small>	Devices with high risk <small>①</small>
OT Site VLAN 10.	275	Italy		3	64	1
OT Site VLAN 10.	260	Italy		0	46	0
OT Site VLAN 10..	132	Italy		1	31	0
OT Site VLAN 10.	34	Netherlands		0	1	2
OT Site VLAN 10.	335	Netherlands		0	6	0
OT Site VLAN 10.1	24	India		0	3	0



# XDR | Devices | Discovery sources



## Device Inventory

Create rules for devices



**1 OT devices are not protected**

To gain full visibility into your OT/IoT devices  
manage your sites

...

All devices Computers & Mobile Network devices IoT/OT devices Uncategorized devices Partially identified devices

Total **153** | Critical assets **4** | High risk **4** | High exposure **6** | Not onboarded **21** | Newly discovered **21** | Partially identified devices **24**

Export

Search



30 Days



Customize columns



Filter

<input type="checkbox"/> Name	IP	Device category	Risk level	Exposure level	Sensor health state	Onboarding status	Discovery sources	Tags
<a href="#">fb2e494fac9222d3cd272ccb69...</a>	192.168.178.7	OT	No known ri...	No data available	Active	Unsupported		site: Nethe...
<a href="#">f8bb0d79dbb969ec994a059d5...</a>	10.0.0.7	OT	No known ri...	No data available	Active	Unsupported		site: ot-site...
<a href="#">virtuallab</a>	192.168.178.117	OT	--	--	Active	Unsupported		
<a href="#">nedscaperlab-sr.nedscaperlab.l...</a>	10.2.0.5	Computers and Mo...	High	Medium	Active	Onboarded		
<a href="#">wsrv1601</a>	192.168.178.15	Computers and Mo...	High	High	Active	Onboarded		Device val...



Microsoft **Defender for IoT**

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



# Defender XDR | Assets | Exposure Level

Microsoft Defender Vulnerability Management for EIoT & OT

Assign criticality levels to your assets      Onboard them now      manage your sites

All devices    Computers & Mobile    Network devices    IoT/OT devices    Uncategorized devices

Total **58**    Critical assets **0**    High risk **0**    High exposure **0**    Not onboarded **0**    Newly discovered **0**

Export    Search    30 Days    Customize

Filters: Device category: OT X

Name	IP	Device category	Device AAD id	Risk level	Exposure level	OS platform	OS version
ETY5103-Module	10.165.8.54	OT		■■■■ No known ri...	▲ Medium		5.4
3bfc47614c43013ecd4f81233c9...	10.165.10.224	OT		■■■■ No known ri...	No data available	Windows	Other
HMI_Panel	10.185.70.25	OT		■■■■ No known ri...	No data available		Other
4a5f013a023d39a870c4001e57...	10.165.11.51	OT		■■■■ No known ri...	No data available	Windows	Other

# Exposure Management | Initiative | EloT 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

# 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

# Initiative | OT Security | Anonymous Telnet

```
(kali㉿kali)-[~]
└─$ nmap 10.0.0.0/24 -p23 --open
```

# 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

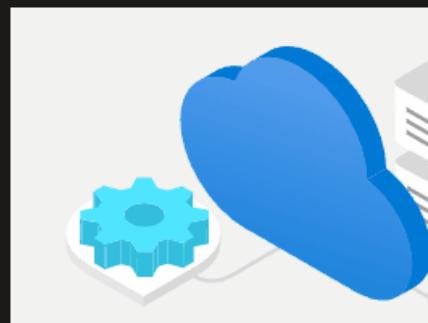
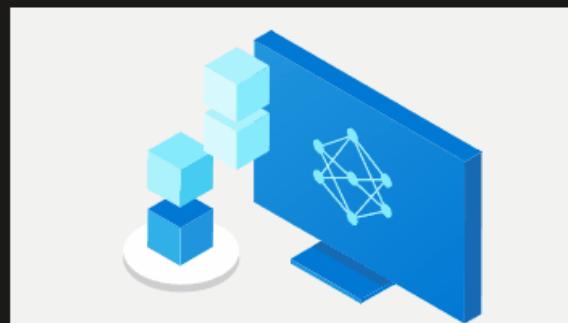
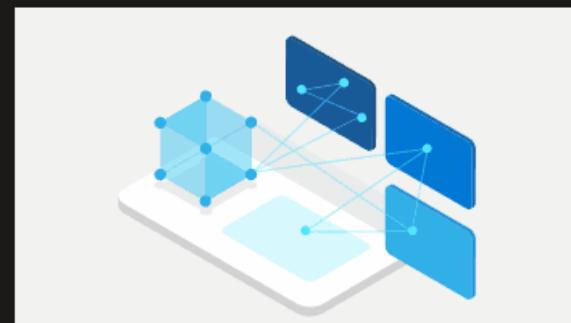
> Troubleshooting + Support

## 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 environments. 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, and more.

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](#)

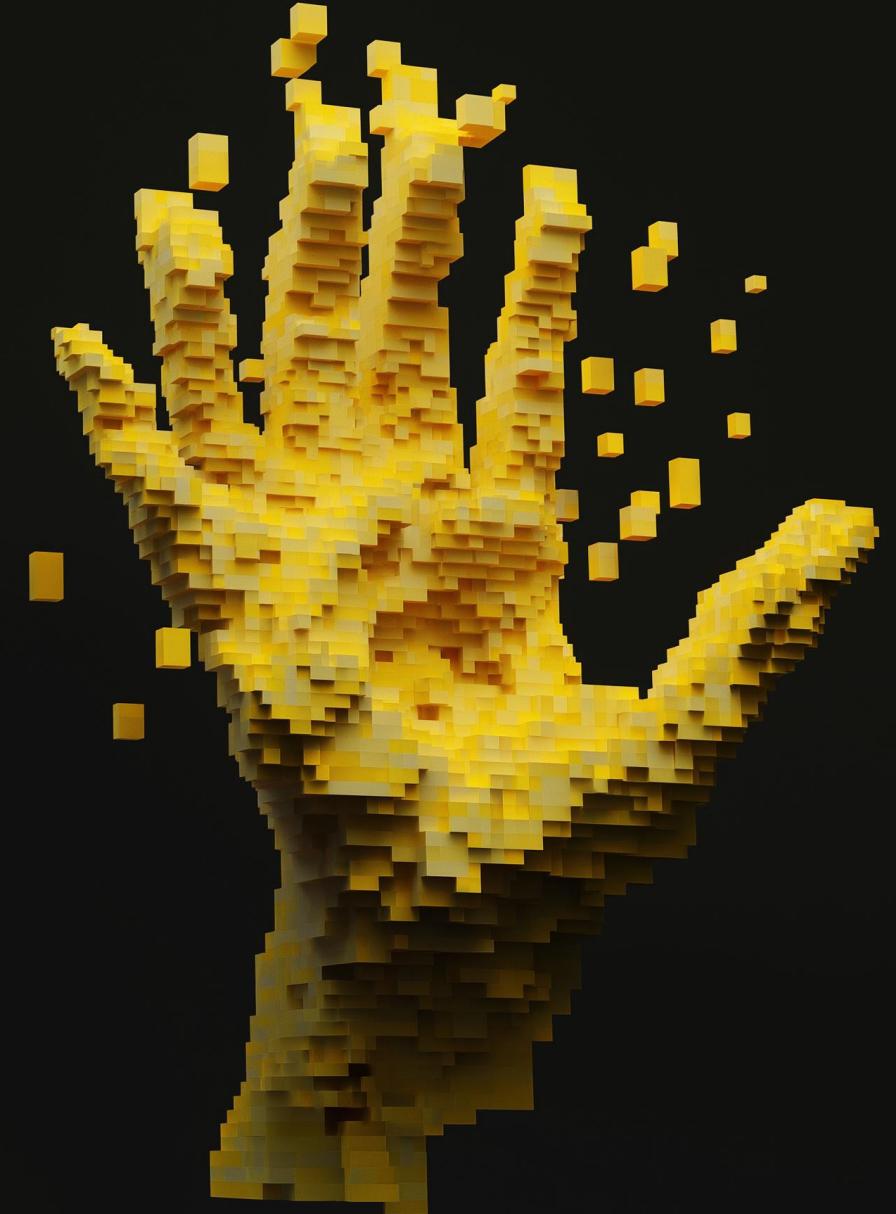




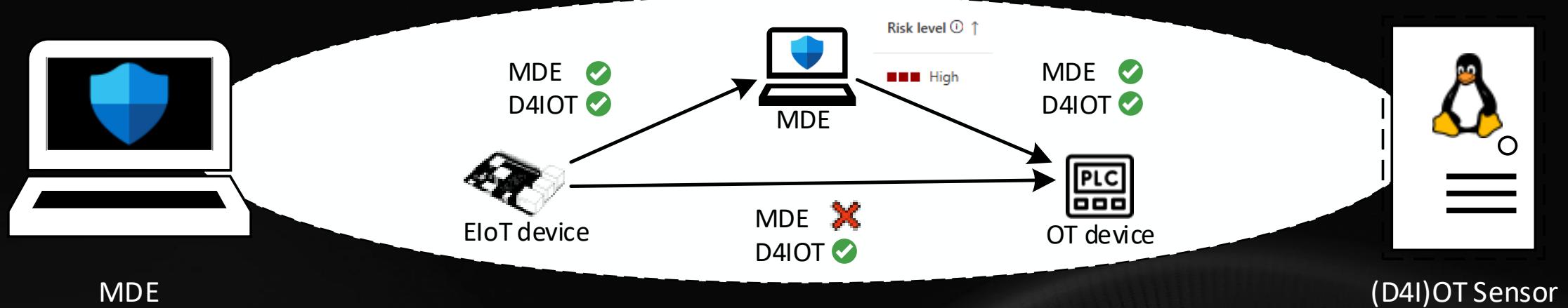
Microsoft **Defender for IoT**

# Threat Protection

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



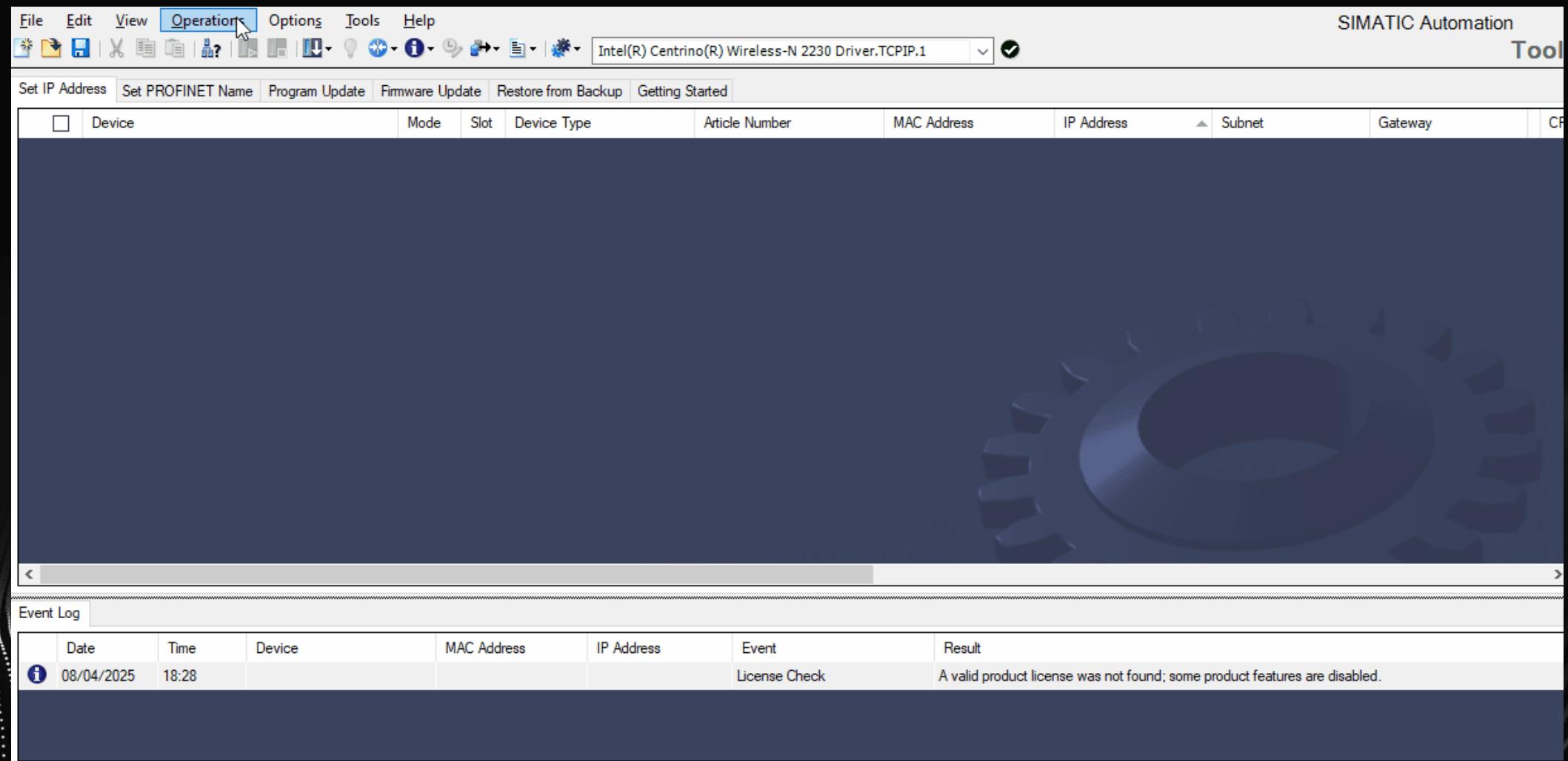
# Defender XDR | OT Incident



multi-stage incident from compromised MDE device

## XDR | Attack Disruption

# Defender XDR | Incident



The screenshot shows a software interface for SIMATIC Manager. The menu bar includes File, Edit, View, Operation (which is highlighted), Options, Tools, and Help. The toolbar contains various icons for file operations and device management. A dropdown menu shows "Intel(R) Centrino(R) Wireless-N 2230 Driver.TCPIP.1" with a checked checkbox. The main window has tabs for Set IP Address, Set PROFINET Name, Program Update, Firmware Update, Restore from Backup, and Getting Started. Below these tabs is a table header with columns: Device, Mode, Slot, Device Type, Article Number, MAC Address, IP Address, Subnet, Gateway, and a column for checkboxes. The "Event Log" section at the bottom shows a single entry:

Date	Time	Device	MAC Address	IP Address	Event	Result
08/04/2025	18:28				License Check	A valid product license was not found; some product features are disabled.

# Azure | D4IOT | Alerts categories



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

100+ OT Alert use-case(s)

# Azure | D4IOT | Alerts

```
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ ifconfig
1: eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    netmask 255.255.254.0 broadcast 192.168.1.254
    ether 00:0c:29:5a:51:77 txqueuelen 1000 (Ethernet)
    RX packets 6180 bytes 915895 (894.4 KiB)
    RX errors 0 dropped 1902 overruns 0 frame 0
    TX packets 8749 bytes 601616 (587.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

2: lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    netmask 255.0.0.0
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 2636 bytes 231060 (225.6 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
```

# Sensor | D4IOT | PCAP

■ ■ ■ ■ ■

Home > Alerts

## Defender for IoT | Alerts

Search Refresh Edit Columns Export to CSV Change Status Export to PDF Learn

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

Search Status == New Last detection == Last day Add filter Reset filters Group by No grouping

There are no alerts to display



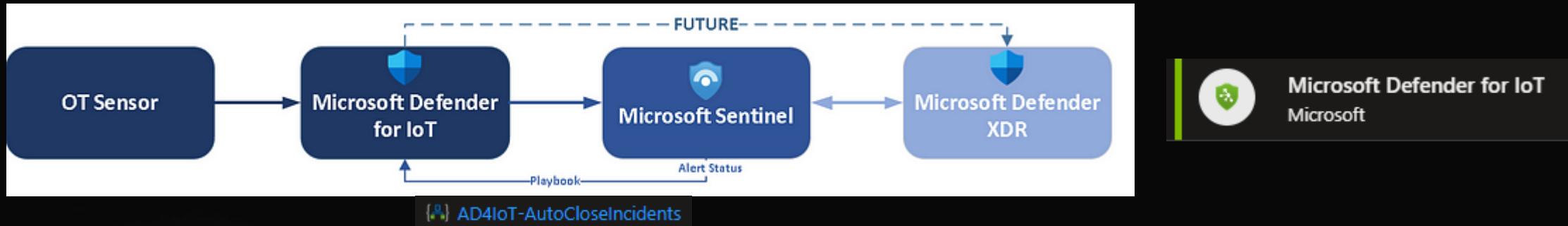
No alerts

# Sentinel | D4IOT Content Hub solution

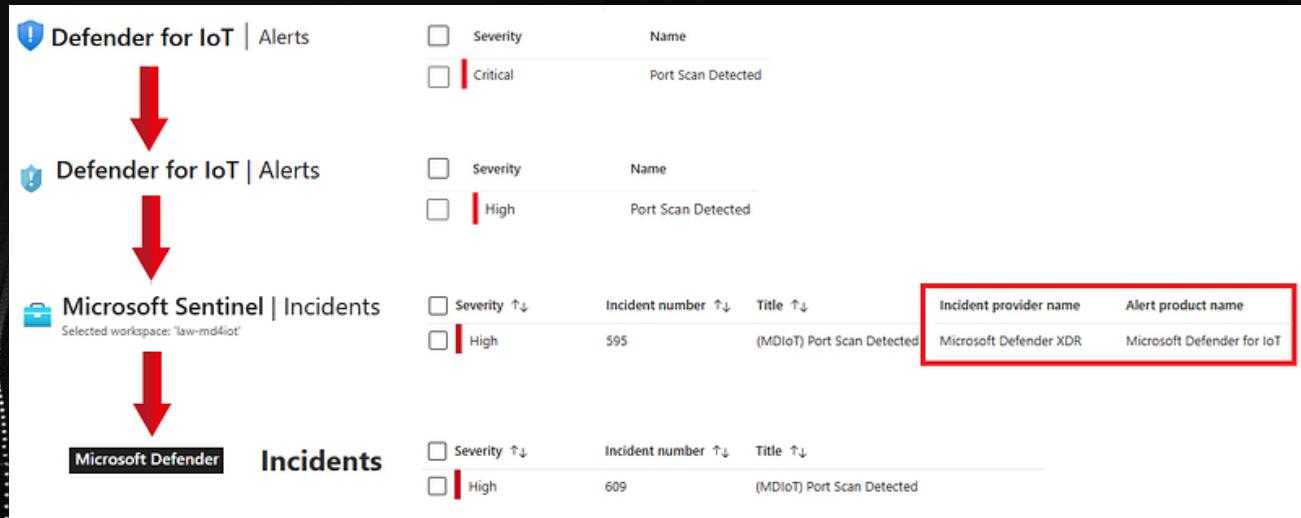


<input type="checkbox"/>	▼  Microsoft Defender for IoT	 Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
	Microsoft Defender for IoT	 Installed	Solution	Microsoft	Microsoft	Internet of Things (IoT), Secu
	Internet Access (Microsoft Defender for IoT)	 Installed	Solution	Microsoft	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 Defend...	 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

# Sentinel | D4IOT Content Hub solution

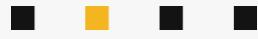


Alerts from Defender for IoT are streamed in Microsoft Sentinel and synced to Microsoft Defender XDR



The screenshot shows the workflow of alert processing:

- Defender for IoT | Alerts**: Shows a critical alert for "Port Scan Detected".
- Defender for IoT | Alerts**: Shows a high-severity alert for "Port Scan Detected".
- Microsoft Sentinel | Incidents**: Shows the same alerts as they appear in the Microsoft Sentinel workspace. The incident details show "Incident provider name: Microsoft Defender XDR" and "Alert product name: Microsoft Defender for IoT".
- Microsoft Defender | Incidents**: Shows a high-severity alert for "(MDIoT) Port Scan Detected".

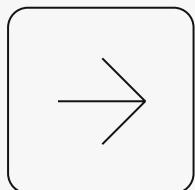


Microsoft Defender for IoT

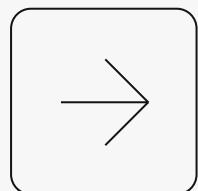
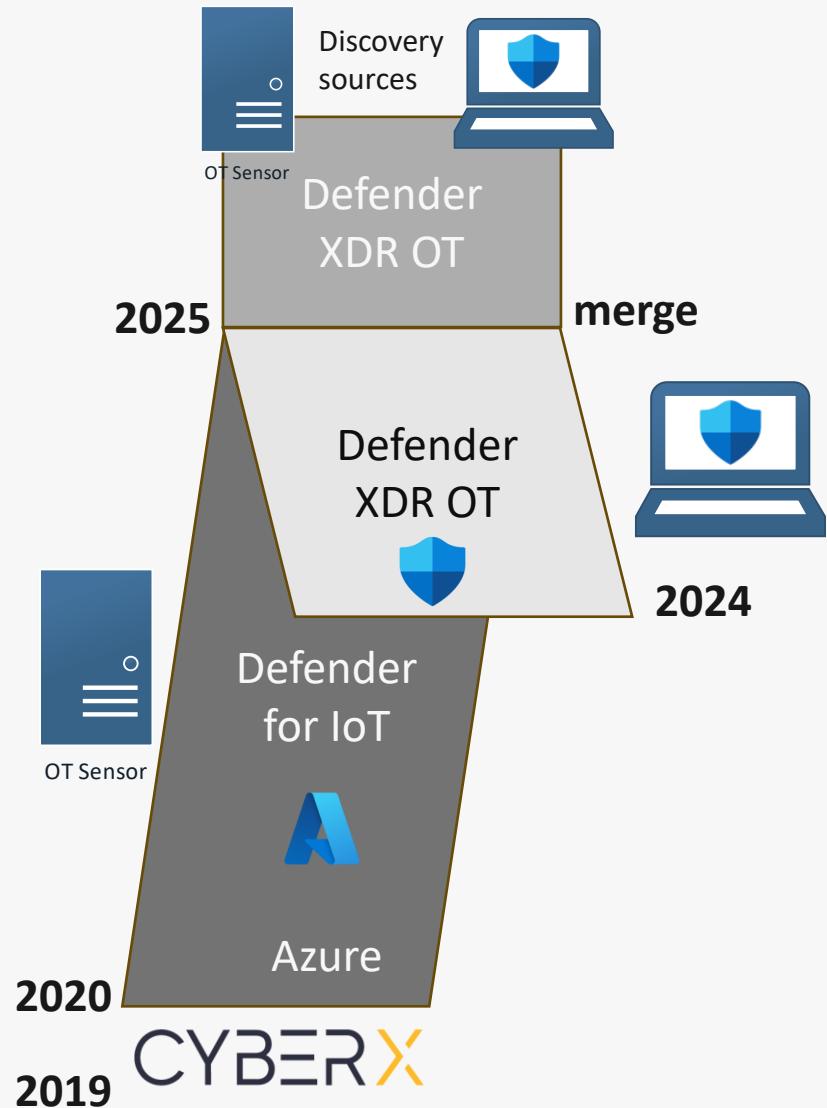
The Future  
#OneSOC



# Azure Security -> Defender XDR



# Azure Security -> Defender XDR



- ▪ ▪
- Why Microsoft Defender XDR

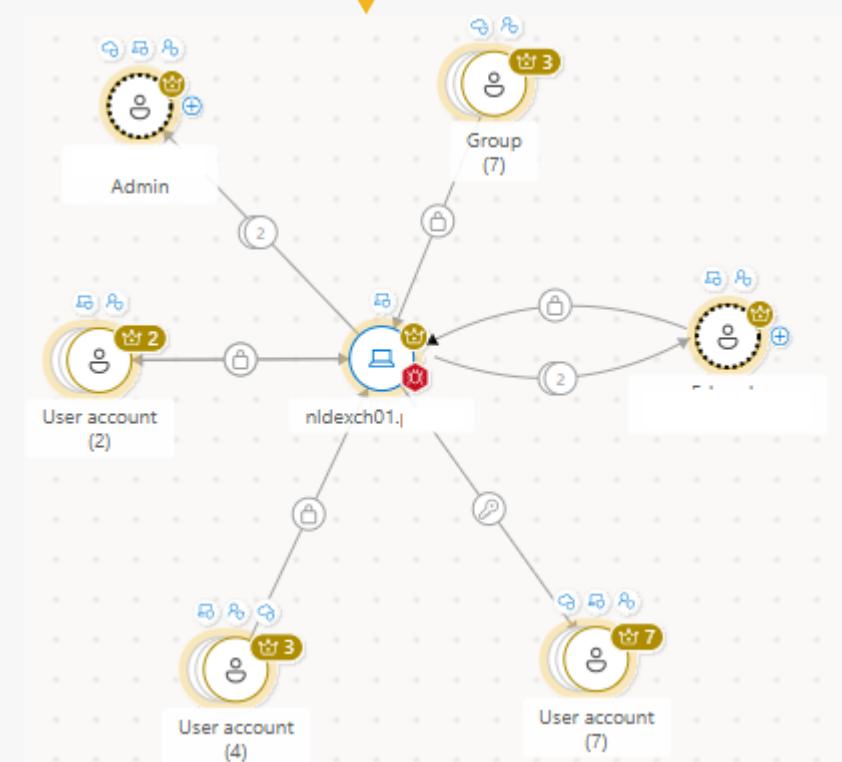
A Azure (internal hosting) cost \$\$\$

S Microsoft Security Copilot

M Microsoft Graph

XDR | Automatic Attack Disruption

XSPM | Autonomous Remediation





# What to choose?

It depends ... 😊

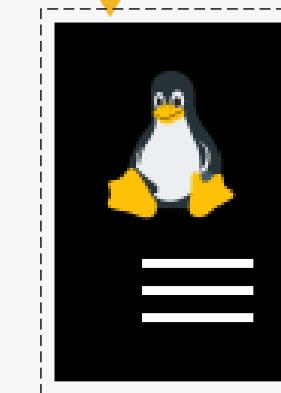


Defender for Endpoint

OT in IT Network

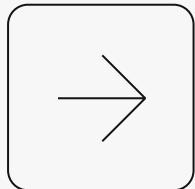
?

OT Network

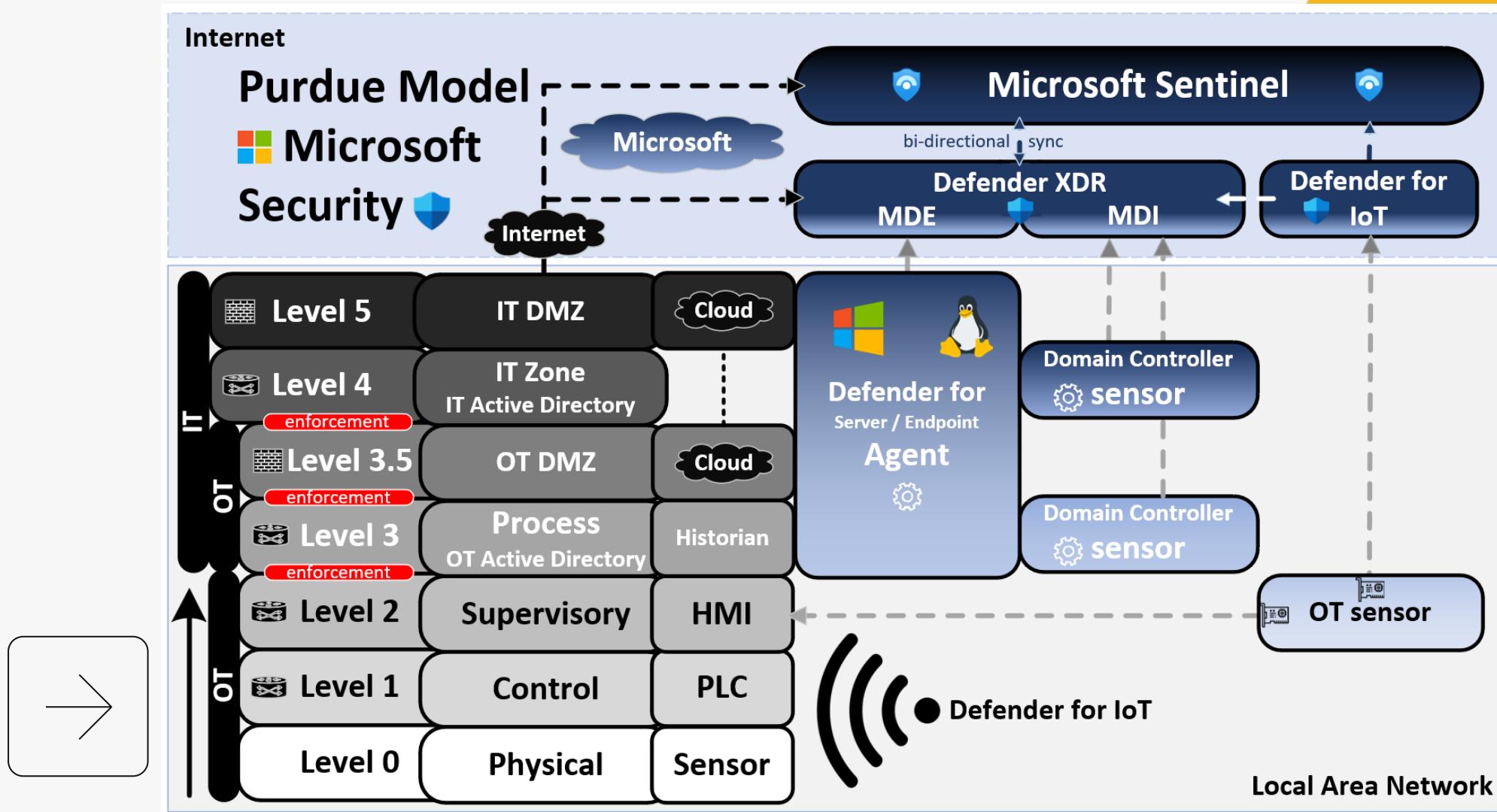


OT Sensor

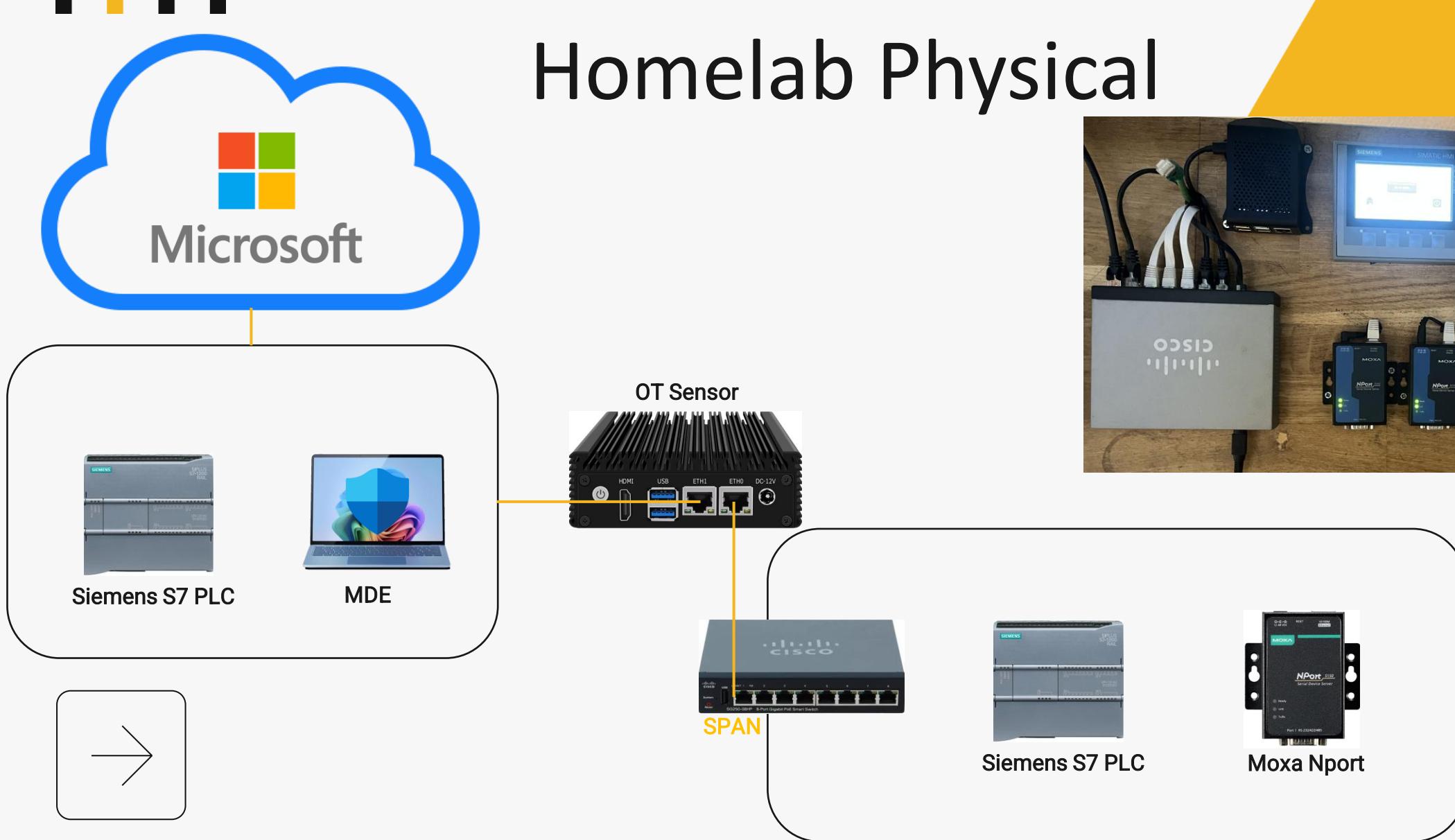
Better Together



# Better Together



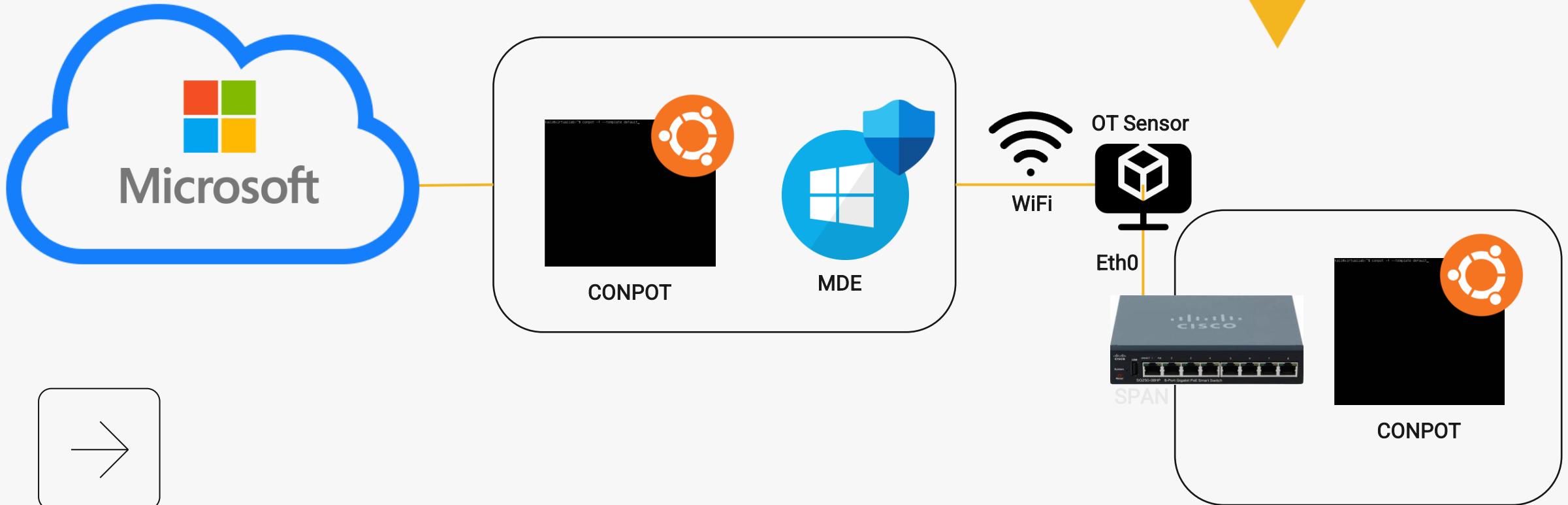
# Homelab Physical





# Homelab Virtual

Microsoft **Hyper-V**     **vmware®**



A dark background featuring a complex, multi-layered wireframe model of a mountain range, rendered in white against a black background.

THANK YOU FOR YOUR ATTENTION  
Questions?