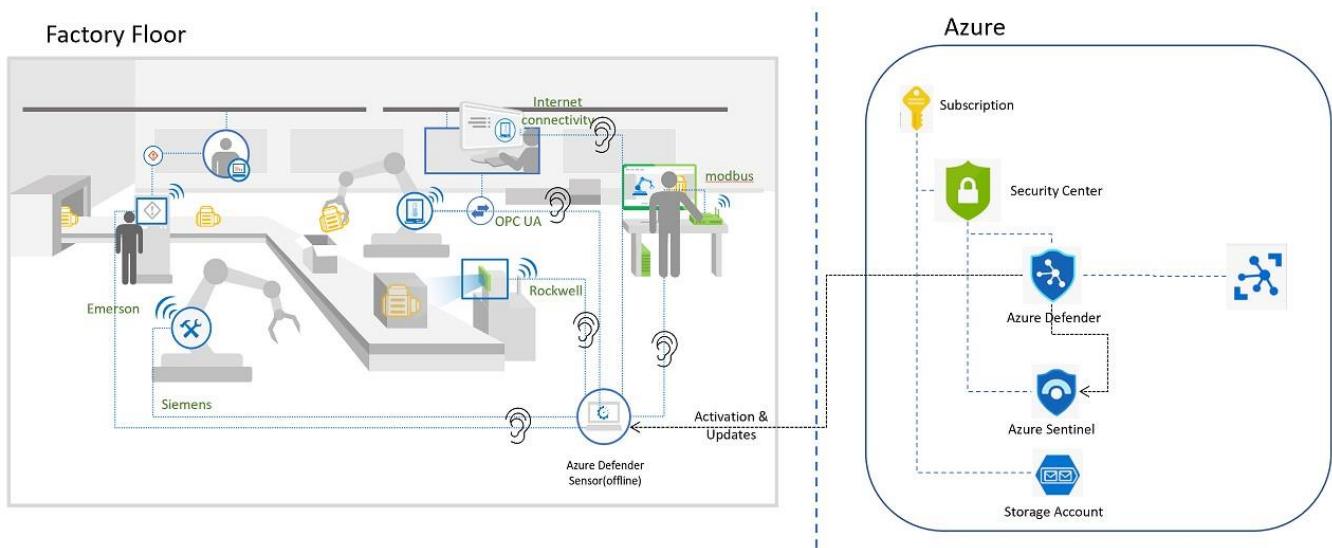


Internet of Things - Microsoft Defender for IoT HOL

!! Since the PDF contains hyperlinks, please download the file before proceeding!!

Architecture Diagram

During this workshop we will be focusing on simulating traffic by playing some Packet captures, visualizing and analyzing the data on the sensor console. We will also integrate our sensor with Microsoft Sentinel, to explore alert handling, and for writing queries to help with alert investigation. This Hands-on-Lab (HOL) will focus on securing your facilities. The scenario below is one of many you would apply these lessons to, other scenarios are Oil, Gas, Utility, and Energy companies.



Contents

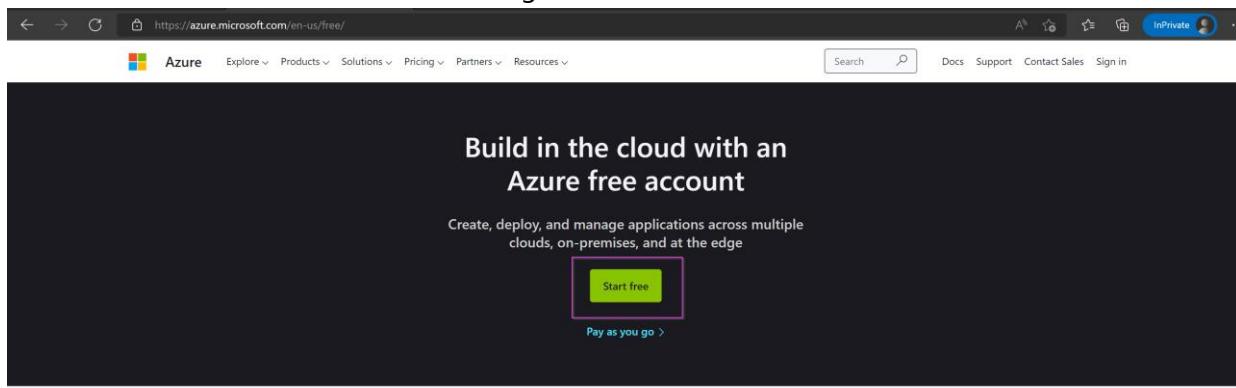
Architecture Diagram.....	1
Exercise #1: Enabling Defender	2
Task 1: Create an Azure Subscription	2
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	3
Exercise #2: Deploy the Sensor in Azure.....	5
Task 1: Create a Resource group to automatically deploy your sensor, storage account and network security group to.....	5
Task 2: Access your Virtual Machine.....	7
Task 3: Access your sensor via the console.....	11
Exercise #3: Simulate Data in your sensor.....	16
Task 1: Enabling the PCAP Player.....	16
Task 2: Play PCAP files.....	18
Exercise 4: Analyzing the Data	19

Task 1: Visualize on the Device Map.....	19
Task 2: View the associated Alerts	22
Task 3: Device Inventory	24
Task 4: View the Event Timeline.....	25
Task 5: Data Mining	25
Task 6: Generate a Risk Assessment report.....	27
Exercise 5: Cloud Connect your sensor.....	28
Task 1: Create the cloud connected sensor on the Cloud Management portal	28
Task 2: Upload the activation file to cloud connect your sensor.	28
Task 3: Verify Cloud connection	29
Exercise 6: Integrate with Microsoft Sentinel.....	30
Task 1: Connecting Data Connectors.....	30
Task 2: Acknowledge Alerts and Re-run PCAPs	35
Task 3: Sentinel interaction with IoT Incidents	36
Task 4: Kusto Query Language to Find Alert Details.....	38
Exercise 6: Clean Up.....	39
Task 1: Delete resources.....	39

Exercise #1: Enabling Defender

Task 1: Create an Azure Subscription

1. Use this link to set up your free trial: <https://azure.microsoft.com/en-free/>.
2. Click on “**Start Free**” as shown in the image



3. Follow the prompts to **Create your Account** and **Sign in**.
4. On the Azure Portal, go to type “**Subscriptions**” on the search bar on top.

The screenshot shows the Microsoft Azure portal homepage. The left sidebar has 'Azure services' and 'Resource' sections. The main area is titled 'Subscriptions' with a sub-section for 'Azure Active Directory'. Below this, there's a list of subscriptions, including 'Visual Studio Enterprise Subscription' which is highlighted with a pink box. Other listed subscriptions include 'Event Hubs Clusters', 'Notification Hubs', 'Device Update for IoT Hubs', and 'Azure Synapse Analytics (private link hubs)'. There are also sections for 'Marketplace' and 'Recent' resources.

5. Your subscription will show up on the list of “**Subscriptions**”.

The screenshot shows the 'Subscriptions' page in the Azure portal. At the top, there are buttons for '+ Add', 'Manage Policies', and 'View Requests'. Below is a search bar and filter options ('Subscriptions == global filter', 'My role == all', 'Status == all', 'Add filter'). A table lists one subscription:

Subscription name	Subscription ID	My role	Current cost	Secure Score	Parent management group	Status	More
Visual Studio Enterprise Subscription	2131d18-92b6-4c00-b377-937eb90512a	Account admin	C\$11.29	41%		Active	...

Task 2: Enabling Microsoft Defender for IoT on the Subscription

1. In the [Azure Portal](#), search for **Microsoft Defender for IoT**. Select **Microsoft Defender for IoT** in the popup window, to open the Microsoft Defender for IoT Page.

Microsoft Defender for IoT

All Services (27) Documentation (99+) Azure Active Directory (1) Resources (0) Resource Groups (0)

Marketplace (0)

Services

Microsoft Defender for IoT

IoT Hub
Microsoft Sentinel
Form recognizers
Power Platform

Recent resources

Name

mdfilesmst01
rg-md4iot-mst01
vm-md4iot-host
AIA-Personal-MST01
firmwaremst
iot-s1-mst02
rg-iothubs
rg-storage
rg-vms
rg-eflow-sample-mst01
rg-cog-services

Documentation

Microsoft Defender for IoT documentation | Microsoft Docs
Defender for IoT installation - Azure Defender for IoT ...
Integrate Microsoft Sentinel and Microsoft Defender for IoT ...
Manage your IoT devices with the ... - docs.microsoft.com

Azure Active Directory

Microsoft Defender for IoT Micro agent Public Preview
microsoft-defender-for-iot@service.microsoft.com

Group

Searching 1 of 34 subscriptions. Change

Give feedback

Resource group

3 weeks ago

Resource group

3 weeks ago

Resource group

3 weeks ago

https://ms.portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/Overview

2. On the Defender for IoT page, in the **Getting Started** section, select **Pricing**.

Home > Defender for IoT

Defender for IoT | Pricing

Showing subscription 'Visual Studio Enterprise Subscription'

Search (Ctrl+ /) Refresh Add plan Download on-premises management console activation file

General

Getting started
Device inventory (Preview)
Alerts (Preview)
Workbooks (Preview)

Management

Sites and sensors
Pricing (highlighted with a red box)
Settings (Preview)

No subscriptions onboarded

Define committed device coverage or work with the trial.

Onboard subscription

For more information on Microsoft Defender for IoT pricing, visit the [Pricing page](#).

3. On the **Pricing** page, select **+Add Plan**.

Home > Defender for IoT

Defender for IoT | Pricing

Showing subscription 'Visual Studio Enterprise Subscription'

Search (Ctrl+ /) Refresh + Add plan Download on-premises management console activation file

General

Getting started
Device inventory (Preview)
Alerts (Preview)
Workbooks (Preview)

Management

Sites and sensors
Pricing (highlighted with a purple box)
Settings (Preview)

No subscriptions onboarded

Define committed device coverage or work with the trial.

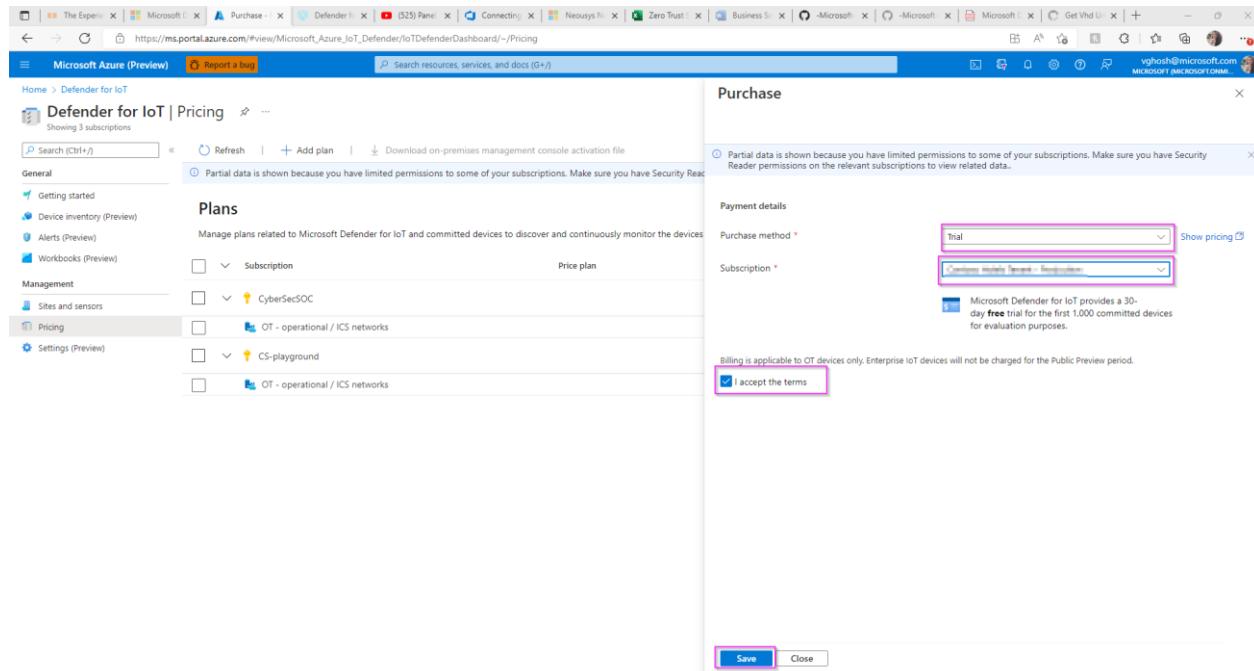
Onboard subscription

For more information on Microsoft Defender for IoT pricing, visit the [Pricing page](#).

4. In the popup screen, select:

- a. **Purchase Method: Trail**

- b. **Subscription:** pick the trial subscription you created
- c. Click “I accept the terms”, followed by “Save”.



You now have a valid Microsoft Defender for IoT Trial with **1000 committed devices**. These devices represent all those equipment/sensors connected to your network in the facility you are analyzing. This configuration allows you a **30-day trial for free**.

Exercise #2: Deploy the Sensor in Azure

Task 1: Create a Resource group to automatically deploy your sensor, storage account and network security group to

For the deployment, a **VHD file is used**. The link for the IoT sensor installation is in the email you have received.

Please note - This link is private and will expire in 5 days.

1. Click the link below to generate a template deployment installation

<https://ms.portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2F-Microsoft-Defender-for-IoT%2Fmain%2FHands%2520on%2520Lab%2520Documents%2FAzureDeploy.json>

2. You will be taken to a custom deployment page that looks like the image below:

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ① BuildEnv

Resource group * ② Create new

Instance details

Region * ③ East US

Location ④ [resourceGroup().location]

Deploy Public IP ⑤ true

Put Password To Key Vault ⑥ true

Source VHDURL * ⑦ [redacted]

Sensor Count 1

- 1) Please select your **Subscription** linked to the trail service.
- 2) Please create a new **Resource Group** (Use the hyperlink below the box). We recommend creating a new one to easily identify the relevant resources of the trail service.
- 3) Please select the **Region** (Time zone) to which you are deploying the trail service to.
- 4) Please leave the **Location** box with its default value, no need to change it.
- 5) **[OPTIONAL]** Set the **Public IP** option to "true". **However, doing this will open your sensor to the internet. If you have alternate ways to publish the sensor to end users, then just use the internal ip by setting "Deploy Public IP" to "false".**
- 6) Set this field to true if you want to store your secrets in keyvault.
- 7) Please paste the link of the **VHD** copied from the email into the **Source VHDURL** field.

3. Once complete please click on the **Review + Create** button Upon validation completion, proceed to click on the **Create** button to initiate the process. The process runs for approx. 30 to 60 minutes.

Custom deployment ...

Deploy from a custom template

Validation Passed

Basics **Review + create**

Summary

Customized template 3 resources

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Create < Previous Next

Task 2: Access your Virtual Machine.

Option #1: If you deployed with Keyvault

- Once the deployment is complete, click on "Go to resource group" as shown in the image below.

Deployment details (Download)

Resource	Type	Status	Operation details
Reset-password	Microsoft.Resources/deployments	OK	Operation details
Post-Deploy	Microsoft.Resources/deployments	OK	Operation details
VMDeployment	Microsoft.Resources/deployments	OK	Operation details
copyhd	Microsoft.Resources/deployments	OK	Operation details

Next steps

[Go to resource group](#)

- Go to the keyvault resource from the list.

Resources

Name	Type	Location
customer24k5pt7ngp2	Storage account	West US
SOC-KVx24k5pt7ngp2-Play	Key vault	West US
SOC-NSOc24k5pt7ngp2-Play	Network security group	West US
SOC-Identity24k5pt7ngp2-Play	Managed identity	West US
SOC-vms24k5pt7ngp2-Play-image	Image	West US
SOC-vms24k5pt7ngp2-Play-pip0	Regular Network Interface	West US
SOC-vms24k5pt7ngp2-Play-pip0	Public IP address	West US
SOC-vms24k5pt7ngp2-Play	Virtual machine	West US
SOC-vms24k5pt7ngp2-Play-disk1	Disk	West US
SOC-vms24k5pt7ngp2-Play	Virtual network	West US

- Click on "Access Policies" -> "Add Access Policies".

Access policies

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions	Action
SOC-identity24...		0 selected	3 selected	0 selected	Delete
Vishakha Ghosh	vghosh@buildacorp...	12 selected	7 selected	0 selected	Delete

- On "Configure from template" select "Key & Secret Management", on "Select Principle" select "None selected" and type in your email.

5. Go to "Secrets" and select the item on the list.

6. Click on the current version.

7. Copy the secret value to your clipboard.

8. Go back to your resource group and select the Virtual Machine resource.

The screenshot shows the Azure portal interface for the 'KeyVaultTest' resource group. The 'Resources' section displays a list of 10 items, with one item, '-Play', highlighted in pink. The highlighted item is a 'Virtual machine' located in 'West US'. Other resources listed include Storage account, Key vault, Network security group, Managed identity, Image, Regular Network Interface, Public IP address, Virtual machine, and Disk.

9. Make a note of the Public IP address.

The screenshot shows the Azure portal details for the virtual machine '-Play'. Under the 'Networking' tab, the 'Virtual machine' properties show the Public IP address as 20.124.23.178 and the Private IP address as 10.10.10.1. The 'Networking' tab also displays the Virtual network/subnet as SOC-Play/default and the DNS name as Not configured.

Option #2: If you deployed without Keyvault.

1. Once the deployment is complete, go to "Reset-password0" by clicking the button.

The screenshot shows the Azure portal deployment details for 'Microsoft.Template-20220630145822'. The deployment status is 'Your deployment is complete'. The deployment details table shows four successful operations: 'Reset-password0', 'Post-Deploy0', 'VMdeployment', and 'copyvhd'. The 'Operation details' column for each operation shows 'OK'. Below the table, the 'Next steps' section contains a 'Go to resource group' button.

- Copy the system generated random password from the "Password" field and make a note of the VMName.

The screenshot shows the 'Outputs' section of a deployment named 'Reset-password0'. The 'vmObject' output is highlighted, showing its value: {\"VMName\":\"SOC-vmw7ne3eaow5oxw0-Play\",\"Password\":\"KChR9dMLp3VFkar2Yp8I99PM2V8=\",\"Status\":true}.

- Click "go to resource group" from the previous screen.

The screenshot shows the 'Overview' page for the deployment 'Microsoft.Template-20220630145822'. The 'Deployment details' table shows four resources: 'Reset-password0', 'Post-Deploy0', 'VMdeployment', and 'copyvhd', all in 'OK' status. The 'Next steps' section contains a 'Go to resource group' button, which is highlighted with a pink border.

- Select the virtual machine from the list of resources in the group.

The screenshot shows the 'resource group' overview for 'XXX'. The 'Resources' table lists several resources, including 'copyvhd', 'customflicwi6uSatkwu', 'SOC NSGflicwi6uSatkwu Play', and 'SOC-vmflicwi6uSatkwu-Play'. The last item, 'SOC-vmflicwi6uSatkwu-Play', is highlighted with a red border.

- Make a note of the Public IP address.

SOC Virtual machine

Essentials

- Resource group: (move)
- Status: Running
- Location: East US
- Subscription: (move)
- Subscription ID:
- Tags: (edit) azsecpack : nonprod

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine		Networking	
Computer name	Sensor	Public IP address	20.124.23.178
Health state	-	Public IP address (IPv6)	-
Operating system	Linux (ubuntu 18.04)	Private IP address	10.10.10.4
Publisher	-	Private IP address (IPv6)	-
Offer	-	Virtual network/subnet	SOC
Plan	-	DNS name	Configure

Task 3: Access your sensor via the console

1. Proceed to access the console by using the selected networking method IP (Public or IP) using <https://> as shown in the image and sign in with the IP you copied in the previous step. Username is **cyberx_host** and the password is what you copied in step 2.

Not secure | https://xxx.xxx.xxx.xxx /login

Microsoft | Defender for IoT sensor

Sensor Sign in

User name _____

Password _____

Forgot password? (for admin users only)
[Reset](#)

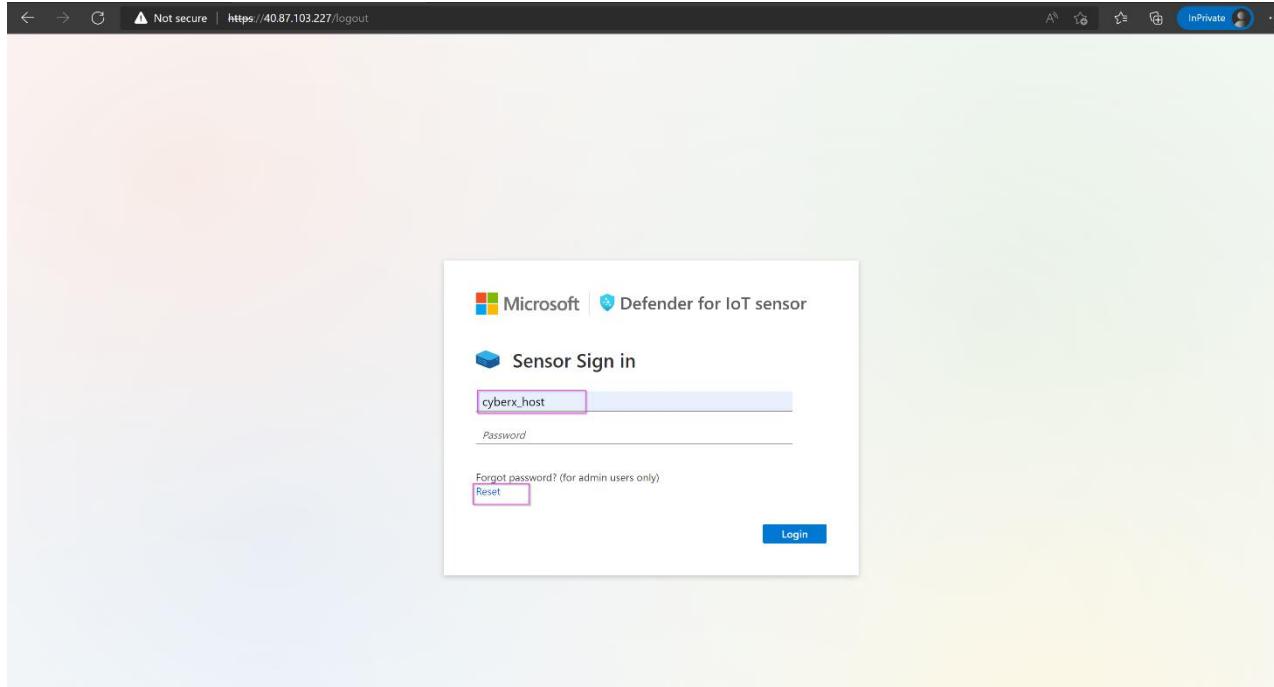
Login

2. Upon successful login please proceed immediately to change the password by clicking on the username on the top right corner and selecting **Sign out**.

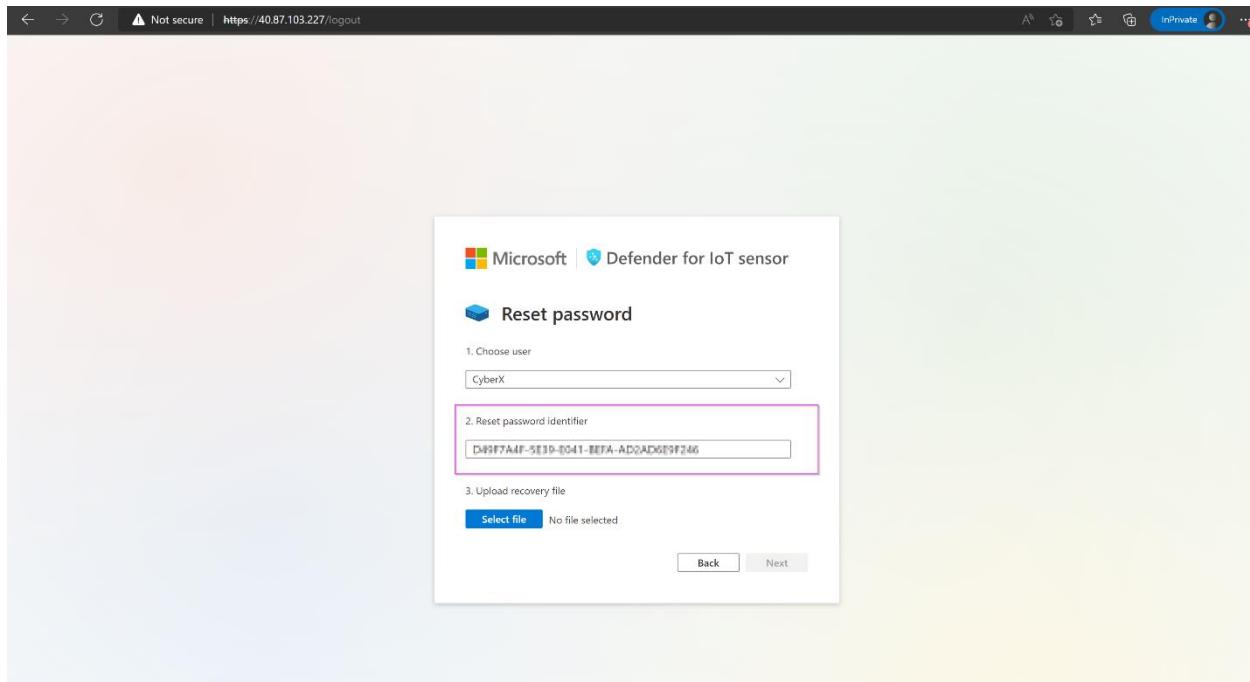
- After signing out, please return to the Azure portal and navigate to “**Defender for IoT**”. Select “**Sites and sensors**”, select your sensor from the list, and click on “**Recover my password**”.

- You will see this prompt asking for the “secret identifier”.

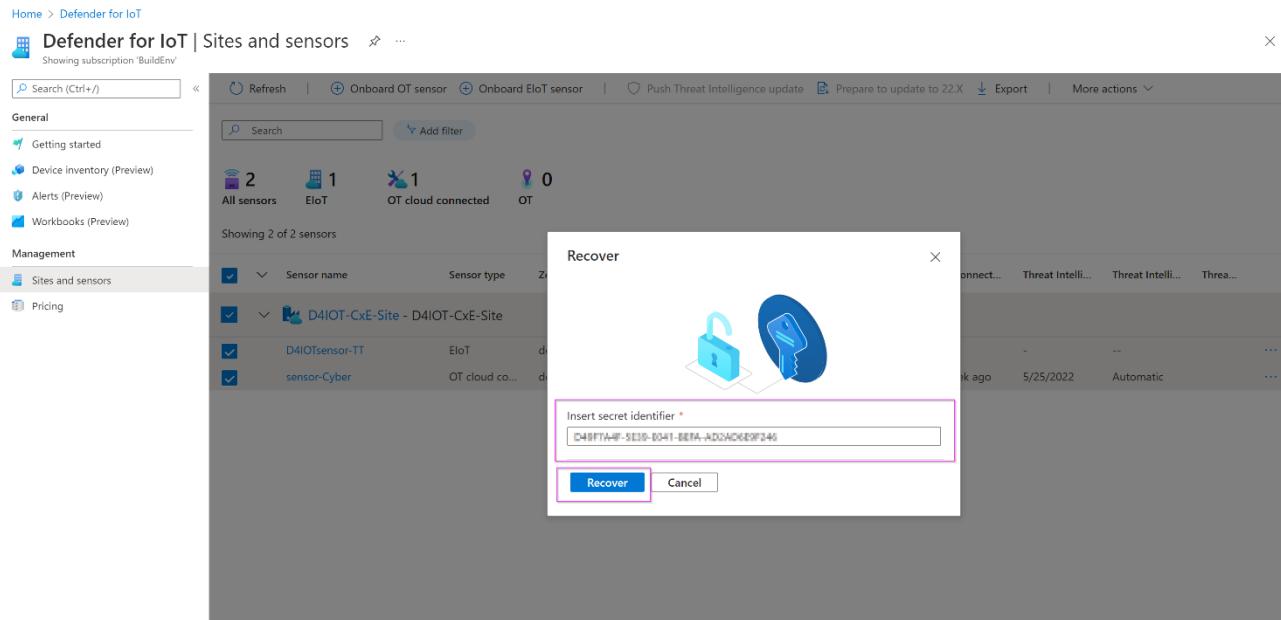
- Return to the sensor console and type in the username followed by “Reset” as shown.



6. Copy the identifier.

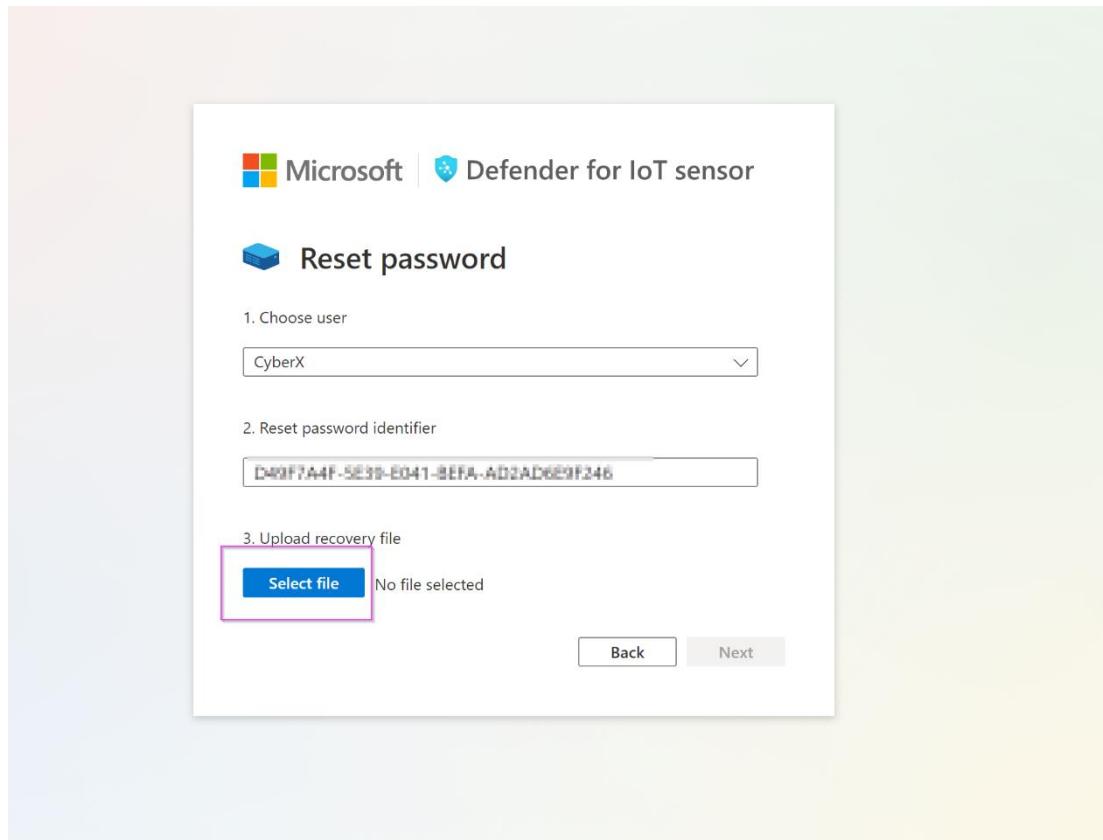


7. Paste in the box on the Defender for IoT Azure window. Click "**Recover**".



The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with 'General' and 'Management' sections. Under 'Management', 'Sites and sensors' is selected. The main area displays sensor statistics: 2 All sensors, 1 IoT, 1 OT cloud connected, and 0 OT. Below this, it says 'Showing 2 of 2 sensors'. A list of sensors is shown, including 'D4IOT-CxE-Site - D4IOT-CxE-Site', 'D4IOTSensor-TT', and 'sensor-Cyber'. A modal window titled 'Recover' is open, containing fields for 'Insert secret identifier' with the value 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246', and 'Recover' and 'Cancel' buttons.

8. The “*password_recovery*” file download starts. Once the download is complete, return to the sensor console and click on “**Upload recovery file**”. **Do not unzip the folder**.



The screenshot shows the 'Reset password' wizard. Step 1: Choose user is set to 'CyberX'. Step 2: Reset password identifier is set to 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246'. Step 3: Upload recovery file has a 'Select file' button (highlighted with a pink box) and a message 'No file selected'. Navigation buttons 'Back' and 'Next' are at the bottom.

9. Click on “**Next**”.

Microsoft | Defender for IoT sensor

Reset password

1. Choose user

CyberX_host

2. Reset password identifier

D9F7A4F-5E19-0411-BFA-AD2AD619F246

3. Upload recovery file

Select file password_recovery (1).zip

Back Next

10. After uploading the file, you will be shown a temporary password on the screen. Please note it down.

Microsoft | Defender for IoT sensor

Reset password

User name

CyberX_host

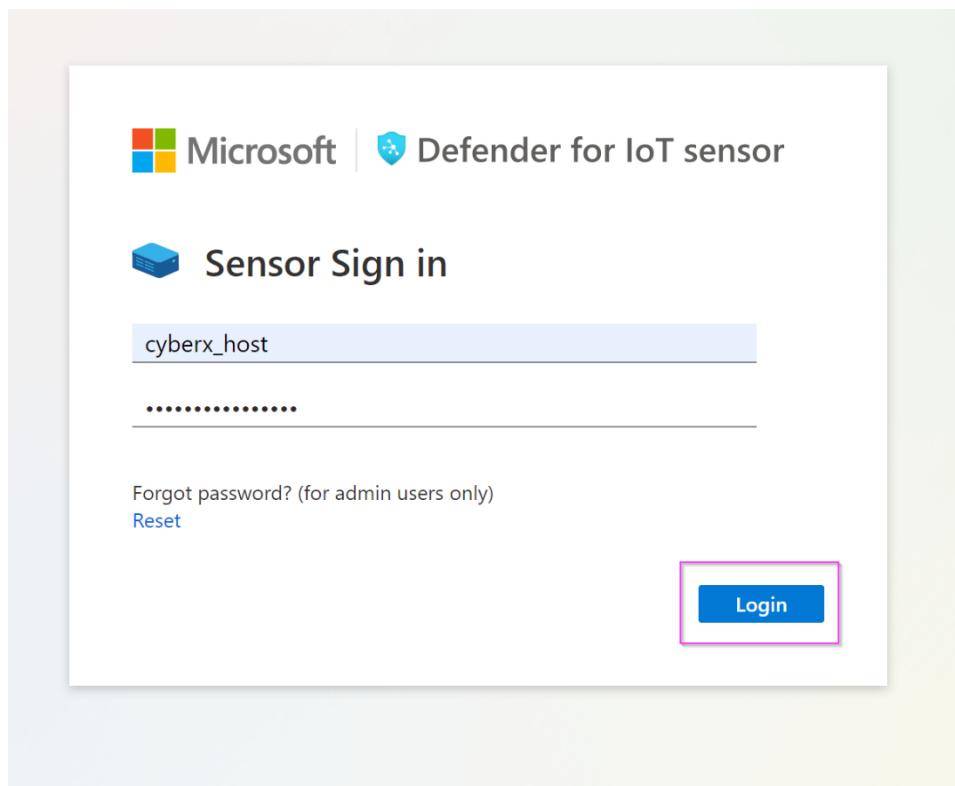
Password

j^*hn@WTU*7IP_3H

Please write your password, it will not be shown again

Next

11. Log in with the new password.



12. Repeat this step for all the usernames.

Exercise #3: Simulate Data in your sensor

Task 1: Enabling the PCAP Player

1. The PCAP player needs to be enabled to be visibly available for use in the UI. To do so, please select the "**System settings**" option from the scrolled down left side menu.

The screenshot shows the Microsoft Defender for IoT web interface. The top navigation bar includes the Microsoft logo, the title "Microsoft Defender for IoT - 22.1.3", and a user profile icon. The left sidebar has a collapsed "Alerts" section and a expanded "System settings" section, which is highlighted with a red box. Other options in the sidebar include "Analyze" (with sub-options: Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector), "Manage" (with sub-options: System settings, Custom alert rules, Users, Forwarding), and "Forwarding". The main content area features four cards under the heading "Sensor Setup": "Sensor Network Settings" (Define sensor network settings), "Connection to Management Console" (Connect this sensor to the on-premises management console), "Time & Region" (Define time zone settings for this sensor), and "Subnets" (Define which networks should be monitored by this sensor). The top right corner of the interface shows a status bar with icons for gear, battery, signal, cloud, and the host name "cyberx_host".

2. Scroll down to locate the "**Advanced Configuration**" option (Shown in the image below in the red square).

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with sections like Alerts, Analyze, and Manage. Under Manage, 'System settings' is selected. The main area is titled 'Health and troubleshooting' and contains four cards: 'Backup & Restore', 'System Health Check', 'SNMP MIB Monitoring', and 'Advanced Configurations'. The 'Advanced Configurations' card is highlighted with a red box.

3. From "Select a Configuration Category", select Pcaps.

The screenshot shows a 'Advanced configurations' dialog box. On the left, a list of categories is shown: Import, Internet Addresses, Management, Mysql, Pcaps (which is highlighted with a red box), Phrases, Ports, Profiling, Programming Diff, Purdue Layers, Query Parse Config, Redis, Remote Interfaces, Remote Upgrade, Reset System Data, and Rule Engine. On the right, there's a search bar labeled 'Select a configuration category' and a 'Close' button at the bottom.

4. Scroll down to locate the "**enabled**" variable and set it to **1**. Click **Save** and approve to commit the change.

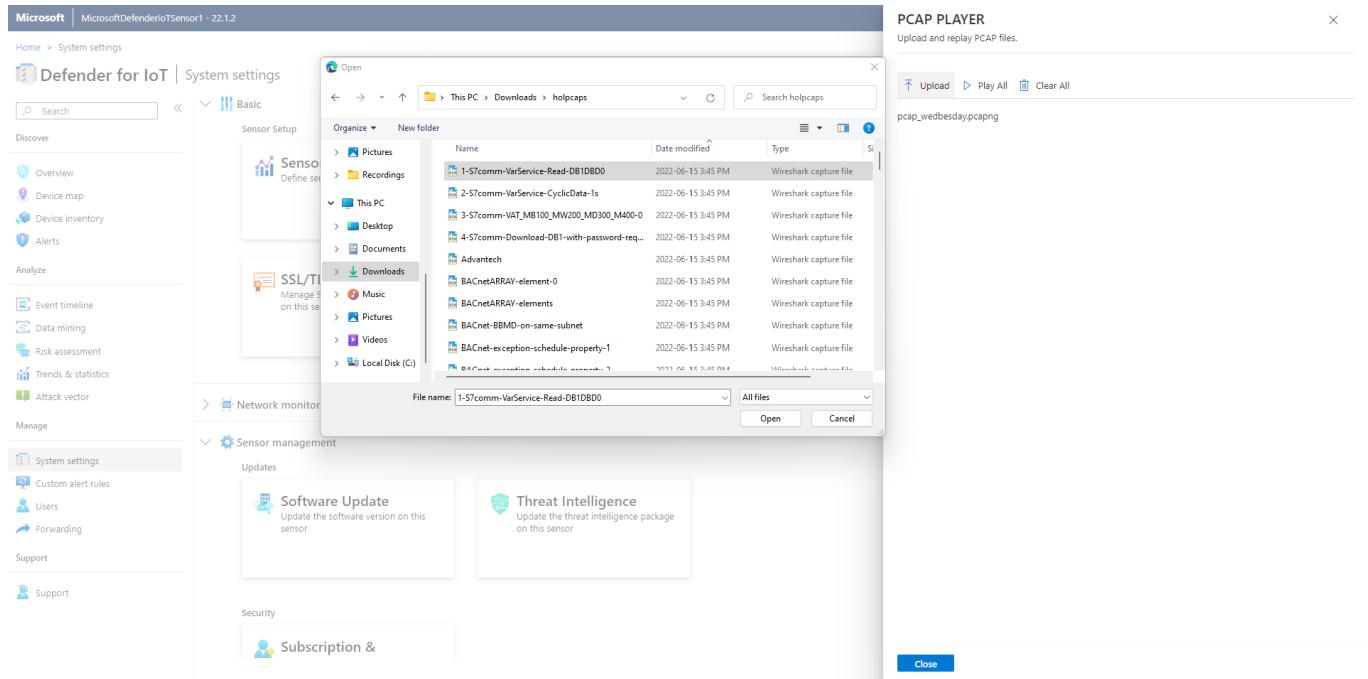
The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a sidebar with options like 'Analyze', 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', and 'Attack vector'. Under 'Manage', 'System settings' is selected. In the main area, there are sections for 'Backup data and restore the latest backup' and 'SNMP MIB Monitoring'. A modal window titled 'Advanced configurations' is open, showing configuration parameters such as 'cache.should.save.pcap=1', 'archive.cache.dir=', '# 7 GB', 'filtered.cache.dir.size.megabytes.max=7168', 'filtered.cache.dir.size.megabytes.min=3072', 'player.max_size=1000', 'player.max_amount=20', 'player.params=enabled_0', and 'virtual.lan.hierarchy.depth.support=1'. The 'Save' button at the bottom of this window is highlighted with a red box.

Task 2: Play PCAP files

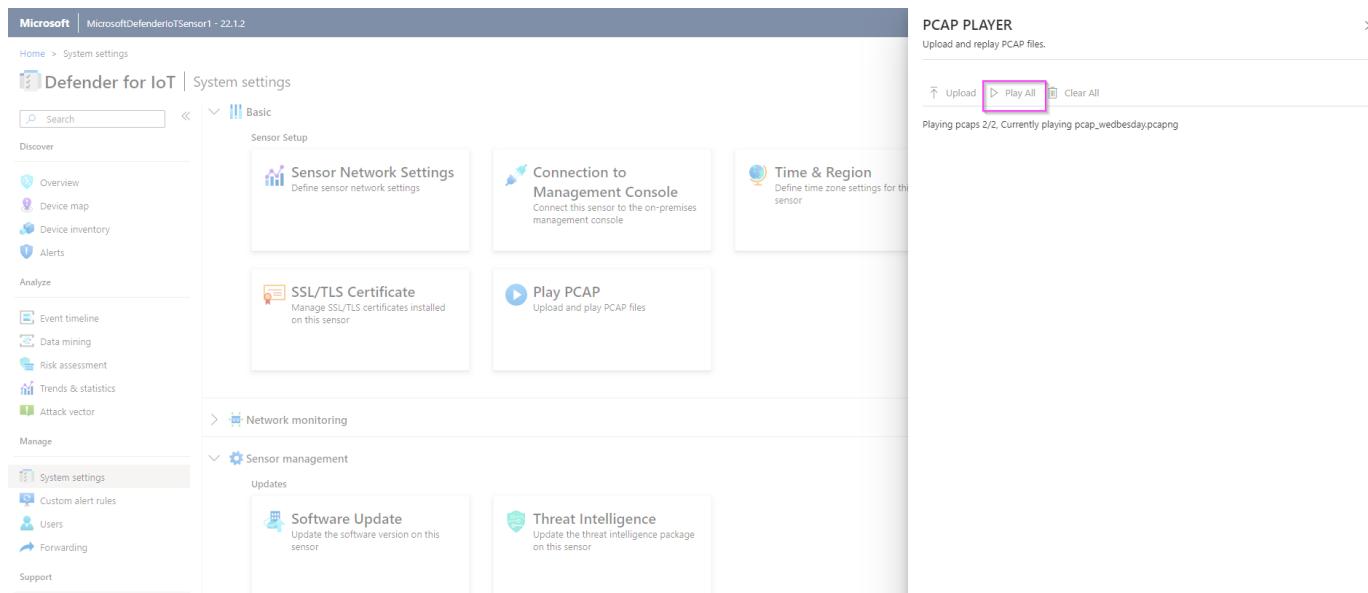
1. Use [this](#) link to download the holcaps.zip folder.
2. Unzip the folder.
3. Scroll all the way down to the bottom to locate if the PCAP Player is enabled (Shown in the image below in the red top square) or not. If the PCAP player is not shown, proceed to click on the arrow next to the **Sensor Management** button (Shown in the image below in the red lower square).

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar includes 'Analyze', 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', and 'Attack vector'. Under 'Manage', 'System settings' is selected. The main content area has sections for 'SSL/TLS Certificate' and 'Play PCAP'. A red box highlights the 'Sensor management' button in the sidebar. Another red box highlights the 'Play PCAP' button in the main content area.

4. Click on “Upload” and select your Pcap files from the unzipped folder.



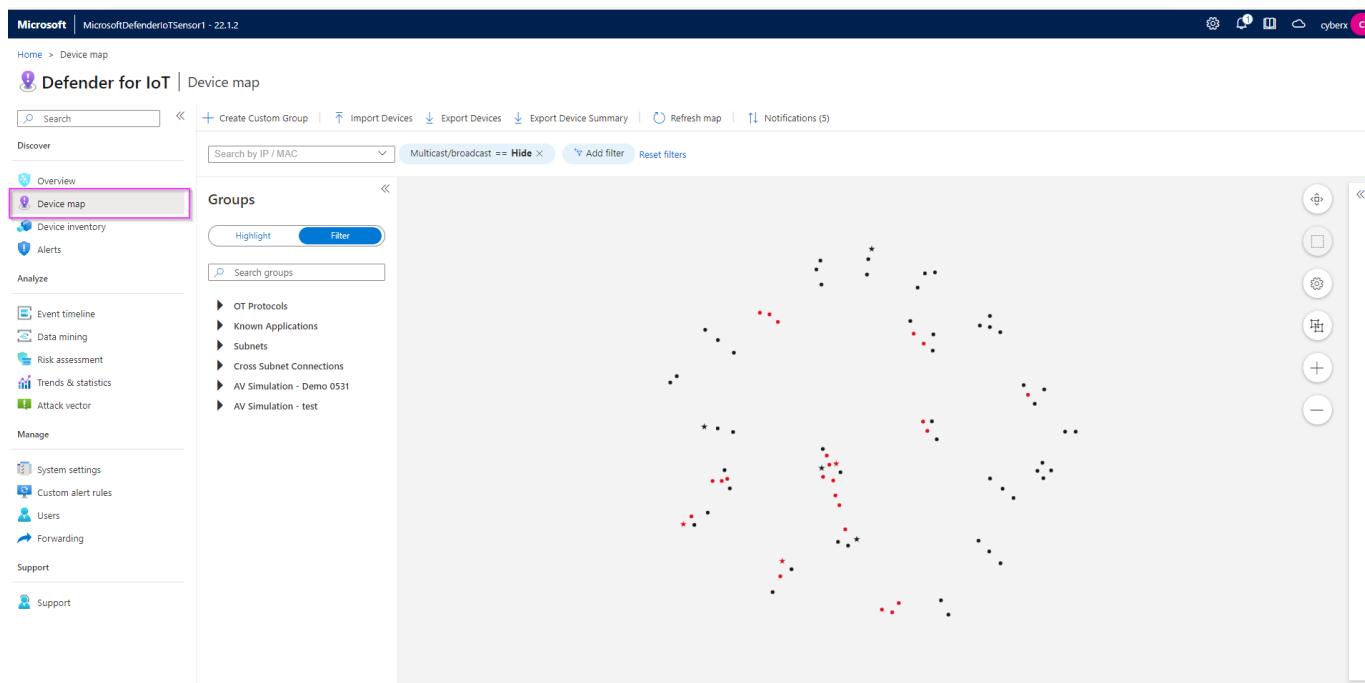
5. Click "Play All" to play the Pcaps.



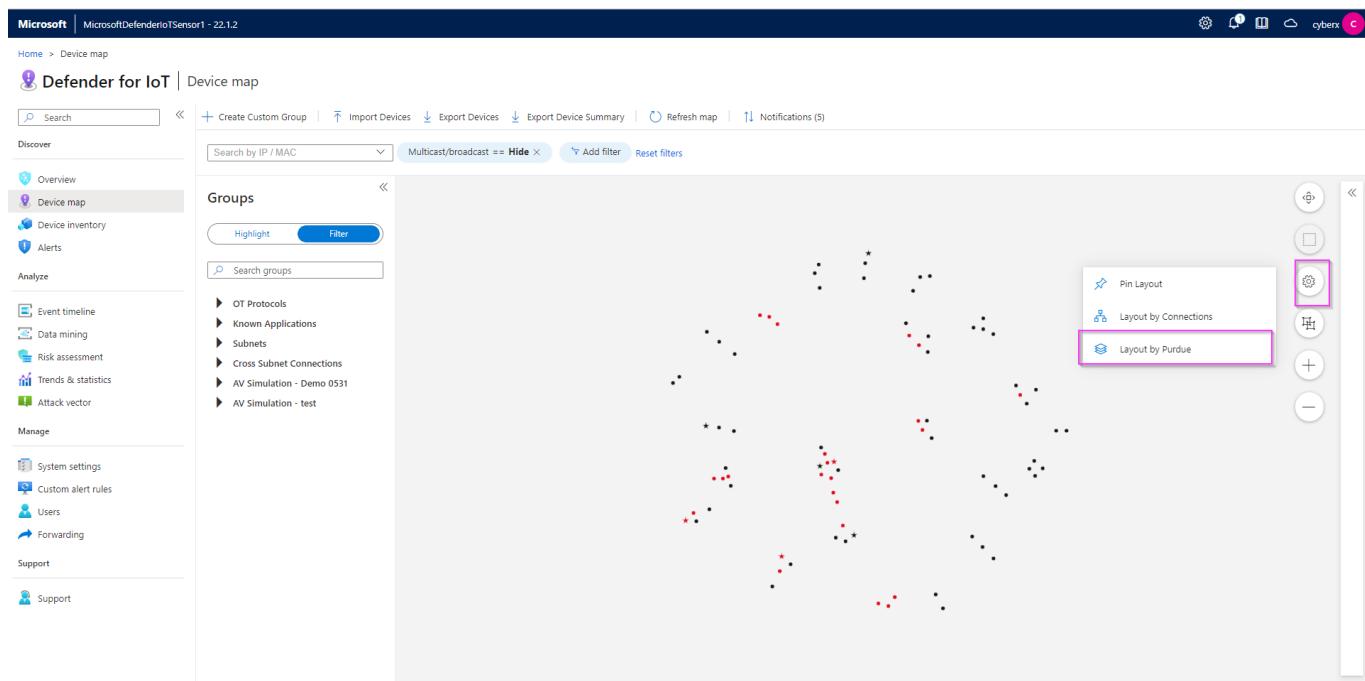
Exercise 4: Analyzing the Data

Task 1: Visualize on the Device Map

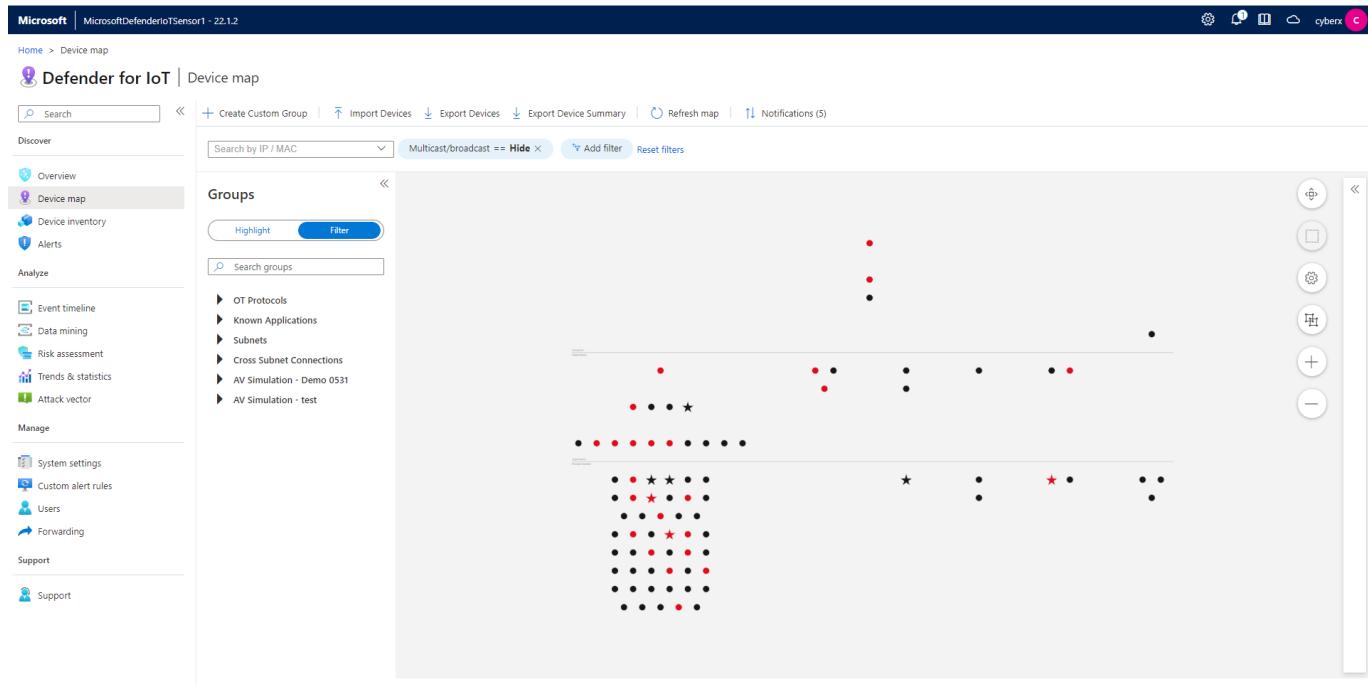
1. Click on “Device Map” from the menu on the left side.



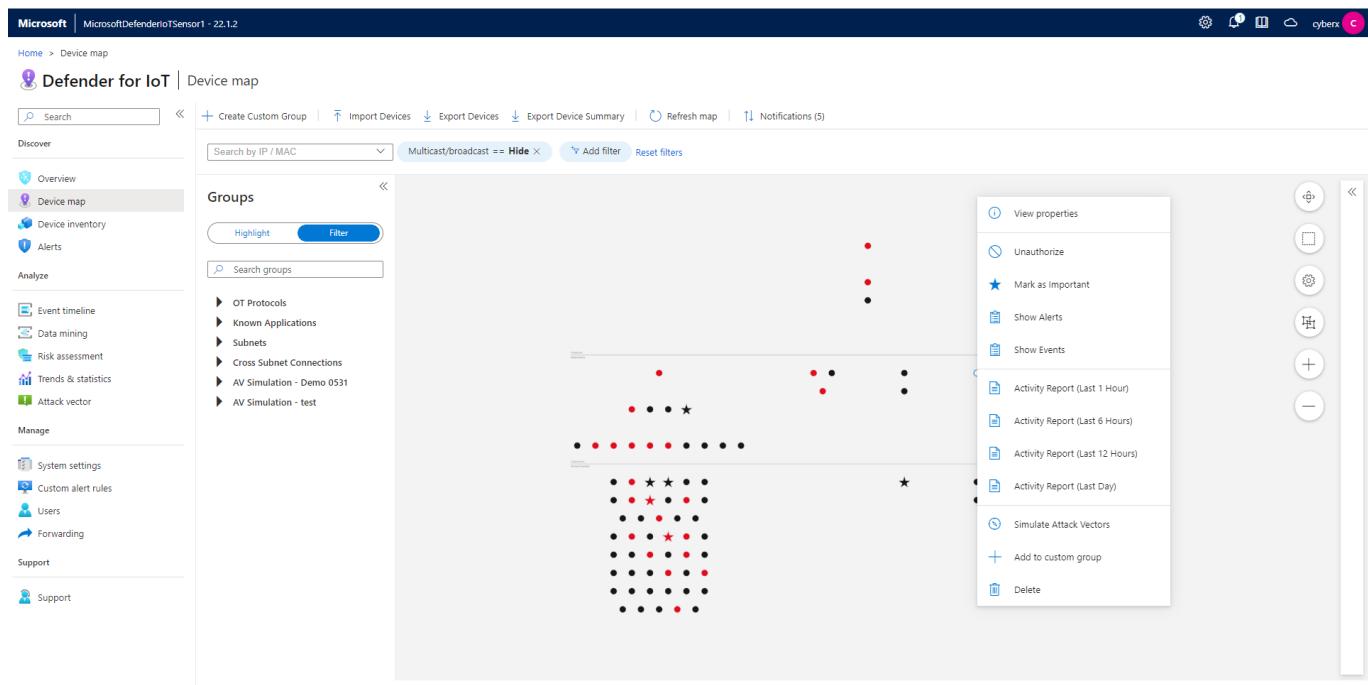
2. Click on the "Settings" option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.



3. Once you confirm the changes, you will see the devices laid out as shown in the image below.



4. Right click on any device (represented by a dot) to view properties, show related events, alerts, reports or simulate attack vectors.



5. To filter by OT Protocols, expand the arrow, and pick the protocol you want to filter by. The console will display the devices that match the filter.

The screenshot shows the Microsoft Defender for IoT Device map interface. On the left, a sidebar lists various categories like Overview, Device map, Device inventory, Alerts, Analyze, Manage, and Support. Under the 'Device map' section, there's a 'Groups' list for OT Protocols, with MODBUS highlighted. In the main pane, a network diagram shows three nodes: 192.168.109.1, 192.168.109.21, and 192.168.109.2. The node 192.168.109.1 has a red alert icon.

Task 2: View the associated Alerts

1. Right click on any device that has an Alert associated with it and click on "Show Alerts".

The screenshot shows the Microsoft Defender for IoT Device map interface with a context menu open over a device node. The menu includes options like View properties, Unauthorized, Mark as Important, Show Alerts (which is highlighted with a pink box), Show Events, Activity Report (Last 1 Hour), Activity Report (Last 6 Hours), Activity Report (Last 12 Hours), Activity Report (Last Day), Simulate Attack Vectors, Add to custom group, and Delete. The device node 192.168.110.10 also has a pink box around its alert icon.

2. The Alerts page helps you identify some important data about the alert, like Alert Severity, Engine, Detection time, as well as the Source Device IPs. It also displays general information about the type of device, network interfaces and protocols.

The screenshot shows the Microsoft Defender for IoT Device map interface. On the left, there's a sidebar with navigation links like Home, Device map, and Alerts. The main area displays a device card for 'Device | 192.168.110.21'. The card includes sections for General Information (Type: Engineering Station, Vendor: INTEL CORPORATE, Location: Automatic), Network Interfaces (IP: 192.168.110.21, MAC: ac:fd:ce:cc:bb:dd), and Protocols (SSH, EtherNet/IP, TDS, FTP, CIP). Below the card is a table of alerts with columns: Severity, Name, Engine, Detection time, Status, and Source Device. Two alerts are listed: 'Unauthorized Internet Connectivity Detected' (Critical, Policy Violation, 2 weeks ago, New, 192.168.110.21) and 'EtherNet/IP Encapsulation Protocol Command Failed' (Major, Operational, 2 months ago, New, 192.168.110.2). A search bar at the top right allows filtering by status and source/destination device.

3.To view more details about the Alert and/or to take remediation actions, select the Alert by checking the box beside it, and picking either “**View Full Details**” or “**Take Action**”.

The screenshot shows the Microsoft Defender for IoT Alerts page. The left sidebar has a menu with Discover, Alerts (selected), Analyze, Manage, and Support. The main area shows a table of alerts with the same two entries as the previous screenshot. The first alert ('Unauthorized Internet Connectivity Detected') has a checked checkbox in its row. To the right of the table is a detailed view of this alert. It shows the alert ID (53), status (New), and detection time (2 weeks ago). The description states: 'A device defined in your internal network is communicating with addresses on the internet. These addresses have not been learned as valid addresses. Device 192.168.110.21 communicated with addresses shown in External Addresses. Verify that this device is properly configured.' Below this are sections for Related Devices (Source device: 192.168.110.21, Destination device: Internet (37.142.39.186)) and a button bar with 'View full details' and 'Take action'.

4.You can view all the alerts on your sensor by clicking on the **Alerts** option on the menu on the left. Make sure all the filters are removed. You can group the alerts by picking an option from the “**Group by**” dropdown.

Showing 22 of 22 alerts

Severity	Name	Engine	Detection time	Status	Source Device
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 weeks ago	New	192.168.110.21
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 weeks ago	New	192.168.110.23
Critical	Port Scan Detected	Anomaly	2 weeks ago	Closed	192.168.110.21
Major	EtherNet/IP Encapsulation Protocol Command Failed	Operational	2 months ago	New	192.168.110.2
Critical	Unauthorized PLC Programming	Policy Violation	2 months ago	Closed	192.168.122.1
Critical	No Traffic Detected on Sensor Interface	Operational	2 months ago	New	192.168.100.8
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 months ago	New	192.168.110.8
Warning	Traffic Detected on Sensor Interface	Operational	2 months ago	New	192.168.110.1
Major	EtherNet/IP Encapsulation Protocol Command Failed	Operational	3 months ago	Closed	192.168.117.23
Critical	Excessive SMB login attempts	Anomaly	3 months ago	New	192.168.117.23
Major	Event Buffer Overflow in Outstation	Operational	3 months ago	New	192.168.117.23
Warning	Controller Reset	Operational	3 months ago	New	192.168.117.23
Warning	Controller Reset	Operational	3 months ago	New	192.168.117.23
Warning	An S7 Stop PLC Command was Sent	Operational	3 months ago	New	192.168.118.22
Warning	An S7 Stop PLC Command was Sent	Operational	3 months ago	New	192.168.118.11
Major	GE SRTP Command Failure	Operational	3 months ago	New	192.168.109.1
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.109.2
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.108.2
Major	Honeywell Firmware Version Changed	Policy Violation	3 months ago	New	192.168.108.2

Task 3: Device Inventory

1. This view allows you to see all the devices connected to your sensor as a list. To filter, click on "Add filter" on the top. For example: the "**Is Authorized**" will show you devices that are either authorized or unauthorized depending on value (True or False) you choose.

Showing 100 of 291 items

IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmware Version	Model	Operating System	Rack	Slot
192.168.100.8	192.168.100.8	50 minutes ago	Unknown	DNS, MDNS, Net...	54:14:f9:74:d8:21	INTEL CORPORA...					
192.168.100.1	192.168.100.1	50 minutes ago	Server	DNS							
192.168.1.11	192.168.1.11	50 minutes ago	PLC	Siemens S7	00:fb:54:db:ef:9	NETGEAR					
192.168.1.180	192.168.1.180	50 minutes ago	HMI	Siemens S7							
192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:92:c6	SCHWEITZER EN...					
192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	00:23:ea:49:5a:c2	CISCO SYSTEMS ...					
192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:97:0	SCHWEITZER EN...					
192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	00:cc:1c:02:09:da	EATON CORPOR...					
192.168.117.7	192.168.117.7	22 hours ago	PLC	Siemens SICAM	00:e0:a8:01:90:be	SAT GMBH & CO.	15.01	CPC65 (6065)			
192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SICAM	00:0c:29:28:28:38	VMWARE INC.					
192.168.117.8	192.168.117.8	22 hours ago	PLC	Siemens SICAM	00:e0:a8:01:90:bb	SAT GMBH & CO.	15.01	CPC65 (6065)			
192.168.107.10	FC50507	22 hours ago	DCS Controller	Yokogawa VNet/IP	00:00:64:9d:5d:10	YOKOGAWA DIG...					
192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9d:73:d4	YOKOGAWA DIG...					
192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9e:84:e5	YOKOGAWA DIG...					
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-6EH14...	0	4	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-9EH14...	1	2	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-8EH14...	1	2	

2. You can export the list to a csv file.

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Device inventory

Defender for IoT | Device inventory

Search | Save Filter | Refresh | Edit Columns | Export

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

Showing 100 of 291 Items

	IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmware Version	Model	Operating System	Rack	Slot
<input type="checkbox"/>	192.168.100.8	192.168.100.8	An hour ago	Unknown	DNS, MDNS, Net...	5:14:f3:74:d8:21	INTEL CORPORA...					
<input type="checkbox"/>	192.168.100.1	192.168.100.1	An hour ago	Server	DNS							
<input type="checkbox"/>	192.168.1.11	192.168.1.11	An hour ago	PLC	Siemens S7	0:0:fb:5:4:db:e1:f3	NETGEAR					
<input type="checkbox"/>	192.168.1.180	192.168.1.180	An hour ago	HMI	Siemens S7							
<input type="checkbox"/>	192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	0:0:3:a7:0:8:92:c6	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	0:0:23:a4:9:5:c2	CISCO SYSTEMS ...					
<input type="checkbox"/>	192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	0:0:3:a7:0:8:97:c0	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	0:0:cc1:0:2:0:9d:a	EATON CORPOR...					
<input type="checkbox"/>	192.168.117.7	192.168.117.7	22 hours ago	PLC	Siemens SICAM	0:0:e0:a8:0:19:0:be	SAT GMBH & CO.	15.01	CPC65 (6065)			
<input type="checkbox"/>	192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SICAM	0:0:c2:9:2:8:3:8	VMWWARE INC.					
<input type="checkbox"/>	192.168.117.8	192.168.117.8	22 hours ago	PLC	Siemens SICAM	0:0:e:a8:0:19:0:bb	SAT GMBH & CO.	15.01	CPC65 (6065)			
<input type="checkbox"/>	192.168.107.10	FC50507	22 hours ago	DCS Controller	Yokogawa VNet/IP	0:0:0:64:9:d:5:d:10	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	0:0:0:64:9:d:7:3:d	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	0:0:0:64:9:e:8:4:e	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1:e:3:11:2:33	SIEMENS AG	3.2.6	6E57 315-6EH14...	0	4	
<input type="checkbox"/>	192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1:e:3:11:2:33	SIEMENS AG	3.2.6	6E57 315-9EH14...	1	2	
<input type="checkbox"/>	192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1:e:3:11:2:33	SIEMENS AG	3.2.6	6E57 315-8EH14...	1	2	

Load More...

Task 4: View the Event Timeline

- This view will allow you a Forensic analysis of your alerts. You can choose to Hide or Unhide the User Operations or select more filter types from the "Add filter".

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Event timeline

Defender for IoT | Event timeline

Search | Create event | Refresh | Export

User Operations == Hide | Add filter | Reset filters

Discover

Overview
Device map
Event timeline
Data mining
Risk assessment
Trends & statistics
Attack vector
Manage

System settings
Custom alert rules
Users
Forwarding
Support

Support

Event type

Event type	Time	Description
Device Detected	6/24/2022, 2:29:04 PM	Device 192.168.1.180 was detected
Device Connection Detected	6/24/2022, 2:29:04 PM	Connected devices 192.168.1.11 and 192.168.1.180
Device Detected	6/24/2022, 2:29:04 PM	Device 192.168.1.11 was detected
Firmware Update	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 copied firmware on PLC 192.168.122.1:Client device 192.168.122.20 copied fir...
PLC Password Change	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 requested PLC 192.168.122.1 to change password
PLC Reset	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 requested PLC 192.168.122.1 to reset itself
PLC Start	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 changed the PLC 192.168.122.1 mode to start
Firmware Update	6/23/2022, 5:30:28 PM	Client device 192.168.122.21 copied firmware on PLC 192.168.122.1
PLC Programming Mode Set	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 tried to change PLC 192.168.122.1 mode to programming mode
Firmware Update	6/23/2022, 5:30:28 PM	Client device 192.168.122.21 copied firmware on PLC 192.168.122.2
PLC Password Change	6/23/2022, 5:30:28 PM	Client device 192.168.122.21 requested PLC 192.168.122.1 to change password
PLC Reset	6/23/2022, 5:30:28 PM	Client device 192.168.122.21 requested PLC 192.168.122.1 to reset itself

Load More...

Task 5: Data Mining

- In this section you can create multiple custom reports. As an example, we will create a Report based on firmware updates versions. Click on + Create report to open the wizard.

The screenshot shows the Microsoft Defender for IoT interface with the 'Data mining' section selected. On the left, there's a sidebar with various navigation options. In the center, there's a 'Recommended' section with cards for Programming Commands, Internet Activity, Excluded CVEs, Remote Access, CVEs, and Non Active Devices (Last 7 Days). Below that is a 'My reports' section showing a single entry named 'test'. On the right, a large 'Create new report' dialog box is open, prompting for report details and filters.

2. Assign a name and a description to your report. Pick “**Modules and Firmware Versions**” for Category, select “**Firmware Version (GENERIC)**” from “add filter”.

This screenshot is similar to the one above, but it highlights specific fields in the 'Create new report' dialog with pink boxes. The 'Name' field is set to 'PLC Firmware Version', and the 'Description' field contains the text 'Report showing the firmware version of the different PLCs.'. The 'Choose Category' dropdown is set to 'Modules and Firmware Versions'. Under the 'Filter by' section, the 'Firmware Version (GENERIC)' option is selected. The 'Save' button is also highlighted with a pink box.

3. Your report will show up on the list under “My reports”.

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar has 'Data mining' selected. In the main area, there's a 'Recommended' section with cards for Programming Commands, Internet Activity, Excluded CVEs, Active Devices (Last 24 Hours), Remote Access, CVEs, and Non Active Devices (Last 7 Days). Below that is a 'My reports' section with a table:

Name	Description	Last modified
PLC Firmware Version	Report showing the firmware version of the different PLCs.	2 minutes ago
ALL		4 days ago
test		3 months ago

4. You can export the report as pdf or csv.

This screenshot shows the 'PLC Firmware Version' report page. At the top, there are buttons for Refresh, Expand all, Collapse all, Export to CSV, Export to PDF, Snapshots, Manage report, and Edit mode. The 'Export to CSV' and 'Export to PDF' buttons are highlighted with a pink box.

Task 6: Generate a Risk Assessment report

1. On the Risk assessment page, run the assessment by clicking the "Generate report" button. You can download and view the report as pdf.

This screenshot shows the Microsoft Defender for IoT Risk assessment page. The 'Risk assessment' option is selected in the left sidebar. In the main area, there's a 'Generate report' button highlighted with a pink box. Below it is a 'Reports list' table:

#	Name	Date Created	Size
1	risk-assessment-report-4.pdf	just now	2 MB
2	risk-assessment-report-3.pdf	4 days ago	2 MB
3	risk-assessment-report-2.pdf	A month ago	1 MB
4	risk-assessment-report-1.pdf	3 months ago	1 MB

Exercise 5: Cloud Connect your sensor

Task 1: Create the cloud connected sensor on the Cloud Management portal

1. On the cloud management (Azure) portal, navigate to "Sites and sensors" and click on "Onboard OT sensor".

The screenshot shows the Microsoft Azure Cloud Management portal with the 'Defender for IoT | Sites and sensors' page selected. At the top, there's a search bar and several navigation icons. Below the header, there are sections for 'General' (Getting started, Device inventory (Preview), Alerts (Preview), Workbooks (Preview)) and 'Management' (Pricing, Sensor name, Sensor type, Zone, Subscription ..., Sensor version, Sensor status, Last connect..., Threat Intelli..., Threat Intelli...). A message box says 'Trial subscription "BuildEnv" expired. Please contact Microsoft sales.' In the center, there are four categories: All sensors (4), IoT (1), OT cloud connected (2), and OT (1). Below these are four sensor cards: 'Locally managed' (with a checkbox) and 'D4IOT-CxE-Site - D4IOT-CxE-Site' (with a checkbox). The 'Sites and sensors' link in the left sidebar is also highlighted with a pink box.

2. Give the sensor a meaningful name, pick the subscription from the dropdown menu, and ensure that "cloud connected" is checked. Click on "Register".

The screenshot shows the 'Step 3: Register this sensor with Microsoft Defender for IoT' form. It includes fields for 'Sensor name' (empty), 'Subscription' (dropdown menu showing 'Please select a subscription' and 'Onboard subscription'), 'Cloud connected' (checkbox checked and highlighted with a pink box), 'Automatic Threat Intelligence updates' (checkbox), 'Sensor version' (dropdown menu showing '22.X and above'), 'Site' (dropdown menu showing 'No subscription has been selected' and 'Create site'), 'Resource name' (dropdown menu showing 'No subscription has been selected' and 'Create site'), 'Display name' (dropdown menu showing 'No subscription has been selected' and 'Create zone'), 'Tags' (key-value pair input field with '+Add tag' button), and 'Zone' (dropdown menu showing 'No subscription has been selected' and 'Create zone'). At the bottom is a 'Register' button.

3. The download for the activation starts immediately. Please check your downloads.

Task 2: Upload the activation file to cloud connect your sensor.

1. Navigate back to your sensor and click on "System settings" -> "Sensor management" -> "Subscription and Activation Mode".

The screenshot shows the Microsoft Defender for IoT Sensor management interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, and Manage. Under Manage, 'System settings' is selected and highlighted with a pink box. In the main content area, there are several cards: 'Software Update', 'Threat Intelligence', 'Subscription & Activation Mode' (which is also highlighted with a pink box), 'Backup & Restore', 'System Health Check', and 'SNMP MIB Monitoring'. The 'Subscription & Activation Mode' card has a sub-instruction: 'Upload an activation file to reactivate this sensor'.

2. Upload the activation file you downloaded in the previous step. Click on "Activate".

This screenshot shows the 'Subscription & Activation Mode' dialog box open on the right side of the screen. It contains fields for Activation Mode (set to 'Cloud Connected'), Activation Status (set to 'Active'), Tenant ID (a long GUID), Subscription ID (another GUID), and a file upload input field labeled 'Upload activation file:' which is currently empty and highlighted with a pink box. The background shows the same interface as the first screenshot, with the 'System settings' section still selected in the sidebar.

Task 3: Verify Cloud connection

1. On the sensor console.

2. On the Cloud management console.

Sensor name	Sensor type	Zone	Subscription ...	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...	Threa...
D4IOTsensor-TT	EloT	default	BuildEnv		Unavailable	--	-	--	...
sensor-Cyber	OT cloud co...	default	BuildEnv	22.1.3.4162	Disconnected	A month ago	5/25/2022	Automatic	...
test1	OT cloud co...	default	BuildEnv	22.1.3.4162	OK	19 minutes a...	7/11/2022	Automatic	...

Exercise 6: Integrate with Microsoft Sentinel

Task 1: Connecting Data Connectors

1. On the Azure portal, search for **Microsoft Sentinel**.

2. Create a new workspace.

3. Go to Configuration > Data Connectors > Search **Microsoft Defender for IoT** to connect Microsoft Defender for IoT to Microsoft Sentinel.

4. Click the Open Connector Page.

The screenshot shows the Microsoft Sentinel Data connectors page. On the left, there's a sidebar with various workspace names listed. The main area shows a summary of 133 Connectors and 35 Connected ones. A search bar at the top right allows filtering by provider, data type, and status. Below the summary, a table lists connectors, with 'Microsoft Defender for IoT' by Microsoft being highlighted. To the right, a detailed card for 'Microsoft Defender for IoT' shows it's connected, last log received was 6 days ago, and data received is shown in a line chart from June 19 to June 23. A button labeled 'Open connector page' is at the bottom.

5. Review the instructions and click the “**Connect**” button to connect Microsoft Defender for IoT to Sentinel. If the connection continues to fail, this will most likely be due to the user not having the “**Contributor**” permissions and you may have missed the access step in the prerequisites.

The screenshot shows the Microsoft Defender for IoT (Preview) configuration page. It has sections for ‘Instructions’ and ‘Next steps’. Under ‘Prerequisites’, it lists ‘Workspace’ and ‘Subscription’ requirements. The ‘Configuration’ section starts with connecting to Microsoft Sentinel. It includes a note about Microsoft Defender for IoT pricing and a search bar. Below is a table for selecting subscriptions to connect. The ‘Azure Pass - Sponsorship’ row has a ‘Connect’ button highlighted with a red box. The status for this row is ‘Disconnected’.

6. If connected correctly you should expect to see the Status change to “**Connected**” and the link light up green.

The screenshot shows the Microsoft Azure Microsoft Defender for IoT (Preview) configuration page. The top navigation bar includes the Microsoft Azure logo, a search bar, and various navigation icons. The main content area has a breadcrumb trail: Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for IoT (Preview). The left sidebar has tabs for 'Instructions' (selected) and 'Next steps'. The main content starts with a 'Prerequisites' section, which lists requirements for workspace and subscription permissions. Below this is a 'Configuration' section with a 'Connect Microsoft Defender for IoT to Microsoft Sentinel' heading. It includes a search bar and a table for selecting subscriptions to connect. A single row is shown: 'Azure Pass - Sponsorship' with a 'Status' column showing 'Connected' and a red box highlighting the 'Connected' status indicator. Buttons for 'Connect All' and 'Disconnect All' are also present.

7.Click on “Next steps” tab to enable Out of the Box alerts and Workbooks

The screenshot shows the Microsoft Defender for IoT (Preview) dashboard. At the top left, there's a navigation bar with 'Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for IoT (Preview)'. Below the navigation, there's a sidebar with 'Instructions' and 'Recommended workbooks (1)'. The main area has a heading 'Azure Defender for IoT Alerts' by Microsoft. Underneath, there are sections for 'Query samples (2)', 'All logs' (with a query editor containing 'SecurityAlert | where ProductName == "Azure Security Center for IoT" | sort by TimeGenerated'), 'Summarize by severity' (with a query editor containing 'SecurityAlert | where ProductName == "Azure Security Center for IoT" | summarize count() by AlertSeverity'), and 'Relevant analytics templates (1)'. A table lists one template: 'Create incidents based on Azure Defender f...' (Severity: High, Name: Create incidents based on Azure Defender f..., Rule type: Microsoft Secur..., Data sources: Microsoft Defender ...). On the right, there's a 'CREATE RULE' button with a 'Create rule' link. A red box highlights the 'Next steps' link in the sidebar and the 'Create rule' button.

7. Fill in the “Name” and click **Review and Create**, followed by **Create**. This is enabling incidents to be created based on the Azure Defender IoT alerts that are ingested into Sentinel.

The screenshot shows the 'Analytics rule wizard - Create new rule from template' step. The URL is 'Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for IoT (Preview) > Create incidents based on Azure Defender for IOT alerts'. The tabs at the top are 'General', 'Automated response', and 'Review and create', with 'Review and create' being the active tab. A green banner at the top says 'Validation passed.' Below the tabs, there's an 'Analytics rule details' section with fields: Name (MyNewRule), Description (Create incidents based on all alerts generated in Azure Defender for IOT), and Status (Enabled). In the 'Analytics rule logic' section, there are filters: Microsoft security service (Microsoft Defender for IoT), Filter by severity (Any), Include by alert name(s) (Any), and Exclude by alert name(s) (Any). The 'Automated response' section shows 'Incident trigger (preview)' as Not configured. At the bottom, there are 'Previous' and 'Create' buttons, with 'Create' being highlighted with a red box.

8. Additionally, you can create the rule not only on the data connectors page but also on Microsoft Sentinel “**Analytics**” blade. Go to the “**Rule Templates**” tab and filter data sources by “Microsoft Defender for IoT” to see all the alerts from the IoT connector.

The screenshot shows the Microsoft Sentinel Analytics blade. On the left, there's a navigation sidebar with sections like General, Threat management, Content management, and Configuration. Under Configuration, the 'Data connectors' section is expanded, and the 'Analytics' link is highlighted with a pink box. In the main content area, the 'Rule templates' tab is selected. A search bar at the top has 'Data Sources : Microsoft Defender for IoT' typed into it and is also highlighted with a pink box. Below the search bar, there's a table with columns for Severity, Name, Rule type, Data sources, Tactics, Techniques, and Source name. The table shows several rows, with the first row being 'High (154)'.

Task 2: Acknowledge Alerts and Re-run PCAPs

1. Go back to your sensor console, select all the alerts, and click on “**Learn**”. The reason we are doing this is so we can re-run the alerts to show how they are sent and analyzed by Sentinel.

The screenshot shows the Microsoft Defender for IoT Sensor1 - 22.1.2 interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, Manage, and Support. The 'Alerts' section is selected. The main content area shows a table of alerts with columns for Severity, Name, Engine, Detection time, Status, and Source Device. There are 22 alerts listed. A pink box highlights the 'Learn' button in the top right corner of the alert list table. The table shows various types of alerts such as Policy Violation, Anomaly, and Operational.

2. From the **System Settings** tab, Click the **Play All** on the PCAP Files to replay simulating the alerts.

The screenshot shows the Microsoft Defender for IoT Sensor Settings page. On the left, there's a navigation sidebar with sections like Discover, Analyze, Manage, and Support. The main area has several cards: Sensor Network Settings, Connection to Management Console, Time & Region, SSL/TLS Certificate, and Play PCAP. On the right, a separate window titled 'PCAP PLAYER' displays a file named 'pcap_wednesday.pcapng' with a 'Play All' button highlighted.

Task 3: Sentinel interaction with IoT Incidents

1. Go back to the Sentinel console and under the **Threat Management** section, select the **Incidents** tab. Filter by Product Name **Azure Defender for IoT**.

The screenshot shows the Microsoft Sentinel Incidents page. The left navigation bar has sections like General, Threat management (with 'Incidents' selected), Content management, Configuration, and Support. The main area shows a table of incidents with the following data:

Severity	Incident ID	Title	Alerts	Product names	Created time	Last update time	Owner
High	16	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:42 PM	01/25/22, 04:42 PM	Unas...
High	15	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	14	Outstation Restarted	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	13	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	12	Firmware Change Detected	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	11	Controller Stop	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	10	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	9	EtherNet/IP CIP Service Requ...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	8	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	7	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	6	Unknown Object Sent to Out...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	5	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	4	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	3	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	2	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...

2. Select one of the alerts and click **View full details**

Microsoft Sentinel | Incidents

Selected workspace: mylogoworkspace-msiot2'

General

Threat management

Content management

Configuration

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

Content hub (Preview)

Repositories (Preview)

Community

Data connectors

Analytics

Watchlist

Automation

Settings

Open incidents: 16

New incidents: 16

Active incidents: 0

Open incidents by severity:

- High (4)
- Medium (10)
- Low (2)
- Informational (0)

Search by ID, title, tags, owner or product

Severity: All

Status: 2 selected

Product name: Microsoft Defender for IoT

Owner: All

Description: Unauthorized Internet Connectivity Detected

Incident ID: 16

Investigate in Microsoft Defender for IoT

Owner: Unassigned

Status: New

Severity: High

Alerts: 1

Events: 0

Bookmarks: 0

Last update time: 01/25/22, 04:42 PM

Creation time: 01/25/22, 04:42 PM

Entities (4): 141.81.0.139, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124

Tactics (1): Initial Access

View full details >

Incident workbook

Incident Overview

Analytics rule

MyNewRule

Tags

View full details

Actions

3. It will take you to this screen to get all the information relative to the incident. This allows analyst to get more details on the entity including what other alerts made up the incident, playbooks to enrich the context of the alert, and comments section to leave details on what the analyst discovered during review or how they came to the determination to dismiss the incident.

Microsoft Azure

Home > Microsoft Sentinel >

Incident

Incident ID: 16

Refresh

Unauthorized Internet Connectivity Detected

Incident ID: 16

Investigate in Microsoft Defender for IoT

Owner: Unassigned

Status: New

Severity: High

Description: A source device defined as part of your network is communicating with Internet addresses. The source is not authorized to communicate with Internet addresses.

Evidence

Events: N/A

Alerts: 1

Bookmarks: 0

Last update time: 01/25/22, 04:42 PM

Creation time: 01/25/22, 04:42 PM

Entities (4): 141.81.0.139, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124

Tactics (1): Initial Access

View full details >

Incident workbook

Incident Overview

Analytics rule

MyNewRule

Tags

Investigate

Actions

Timeline

Alerts

Bookmarks

Entities

Comments

Search

Timeline content: All

Severity: All

Tactics: All

Jan 25 4:41 PM Unauthorized Internet Connectivity Detected

High | Detected by Microsoft Defender for IoT | Tactics: Initial Access

View(playbooks)

Unauthorized Internet Connectivity Detected

Description: A source device defined as part of your network is communicating with Internet addresses. The source is not authorized to communicate with Internet addresses.

Severity: High

Status: New

Events: N/A

Product name: Microsoft Defender for IoT

Entities (4): 141.81.0.139, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124

Tactics (1): Initial Access

System alert ID: 741e1606-64de-5f93-8336...

Last update time: 01/25/22, 04:41 PM

Updates: 0

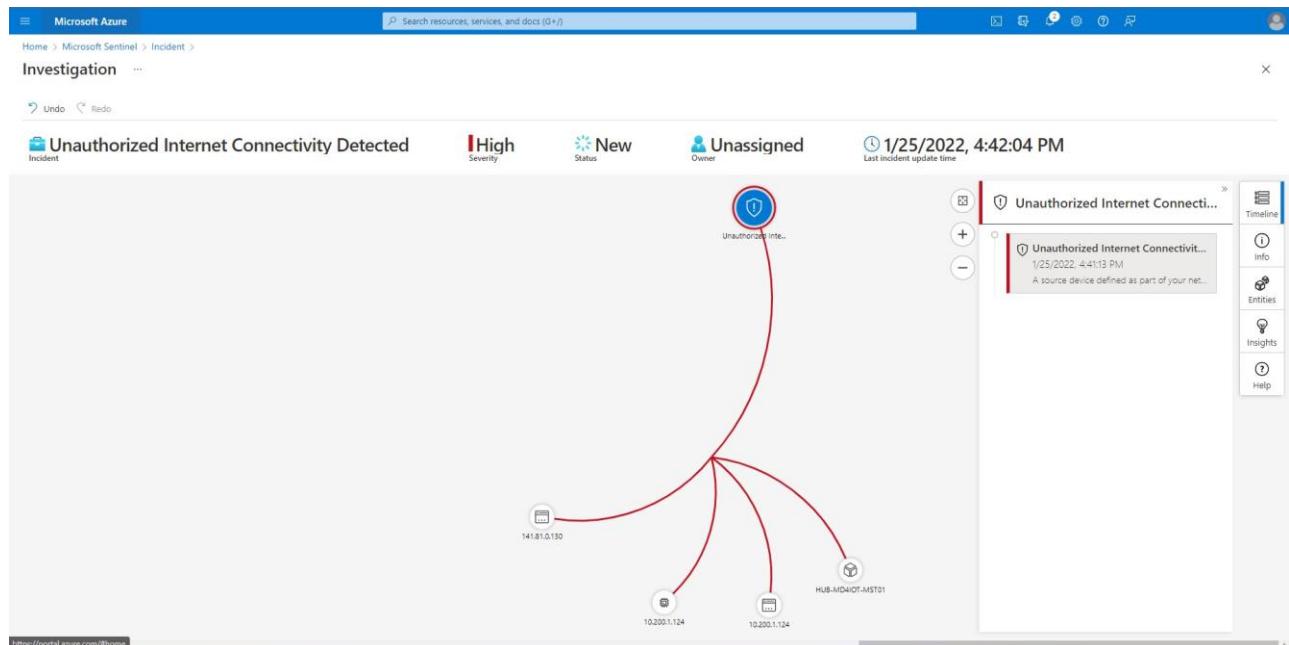
Start time: 01/25/22, 04:41 PM

End time: 01/25/22, 04:41 PM

Alert link: https://portal.azure.com/#blade/Microsoft_Azure_IoT_Defender/IAlert...

Remediation steps

4. By clicking the **Investigate** button, you can dig deeper in the cause of the incident and the relation to other incidents.



Task 4: Kusto Query Language to Find Alert Details

1. Navigate to the “Logs” tab and run the queries provided below, and view the results.

SecurityAlert | where ProviderName contains "IoTSecurity"

TimeGenerated (UTC)	DisplayName	AlertName	AlertSeverity	Description
1/25/2022, 3:41:27.651 PM	Unknown Object Sent to Outstation	Unknown Object Sent to Outstation	Medium	The destination device received an invalid request.
1/25/2022, 3:42:27.511 PM	Outstation Restarts Frequently	Outstation Restarts Frequently	Low	An excessive number of cold restarts were detected on a source device.
1/25/2022, 3:42:27.464 PM	Firmware Change Detected	Firmware Change Detected	Medium	Firmware was updated on a source device. This may be authentic or malicious.
1/25/2022, 3:43:27.361 PM	Port Scan Detected	Port Scan Detected	High	A source device was detected scanning network devices. This may be authentic or malicious.
1/25/2022, 3:44:27.356 PM	Port Scan Detected	Port Scan Detected	High	A source device was detected scanning network devices. This may be authentic or malicious.
1/25/2022, 3:43:27.373 PM	Unauthorized Internet Connectivity Detected	Unauthorized Internet Connectivity Detected	High	A source device defined as part of your network is communicating with an external network.
1/25/2022, 3:46:27.499 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.
1/25/2022, 3:42:27.473 PM	Outstation Restarted	Outstation Restarted	Low	A cold restart was detected on a source device. This means the device has been powered off and back on again.
1/25/2022, 3:41:27.324 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.
1/25/2022, 3:41:27.443 PM	EtherNet/IP CIP Service Request Failed	EtherNet/IP CIP Service Request Failed	Medium	A server returned an error code. This indicates a server error.
1/25/2022, 3:41:27.407 PM	Controller Stop	Controller Stop	Low	The source device sent a stop command to a destination component.
1/25/2022, 3:41:27.384 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.

The screenshot shows the Microsoft Defender for IoT Query Editor interface. At the top, there is a search bar with the query: `SecurityAlert | where CompromisedEntity == "hub-md4iot-mst01"`. Below the search bar is a toolbar with buttons for Run, Save, Share, New alert rule, Export, Pin to dashboard, and Format query. A time range selector shows "Last 7 days". The main area displays a table of query results:

	TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity	Description
>	10/1/2021, 4:00:04.420 PM	Unauthorized Internet Connectivity Det...	Unauthorized Internet Connectivity Det...	High	A source devi...
>	10/1/2021, 4:00:04.087 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server return...
>	10/1/2021, 4:00:07.358 PM	Controller Stop	Controller Stop	Low	The source devi...
>	10/1/2021, 4:00:07.445 PM	Port Scan Detected	Port Scan Detected	High	A source devi...

Exercise 6: Clean Up

Task 1: Delete resources

The Azure Passes will allow you to run the services for 90 days for training purposes. Although it is a best practice to delete all your resources after the training.

Search for the Resource Group created for this training.

Select Delete resource group on the top right side.

Enter your-resource-group-name for **TYPE THE RESOURCE GROUP NAME** and select Delete. This operation will take a few minutes.

After that is done go to Microsoft Defender for IoT and deactivate the subscription.