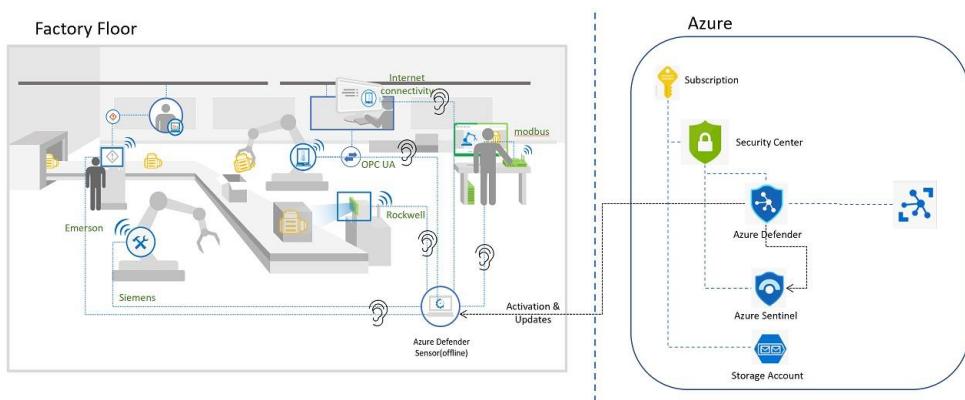


## Internet of Things - Microsoft Defender for IoT HOL

### 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

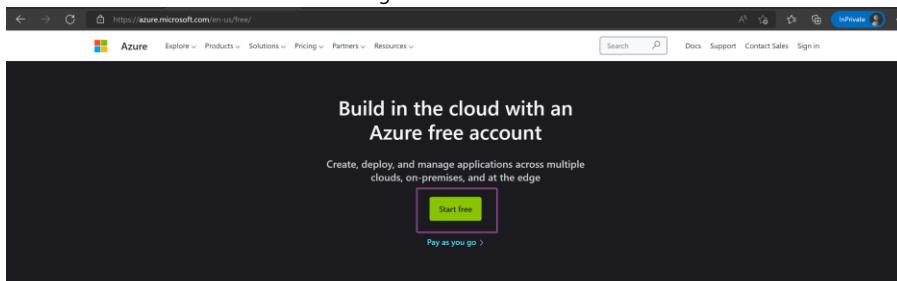
Architecture Diagram.....	1
Exercise #1: Enabling Defender.....	2
Task 1: Create an Azure Subscription .....	2
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	3
Exercise #2: Deploy the Sensor in Azure.....	5
Task 1: Create a Resource group to automatically deploy your sensor, storage 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
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 interface. In the top navigation bar, there are tabs for 'All', 'Services (12)', 'Resources (1)', 'Marketplace (20)', 'Resource Groups (0)', and 'Documentation (0)'. Below this, under 'Services', the 'Subscriptions' item is highlighted with a pink box. Other listed services include Event Hubs Clusters, Event Grid Subscriptions, Event Hubs, Web PubSub Service, and Azure Synapse Analytics (private link hubs). To the right, there's a 'More services' button. On the left, there's a sidebar with sections for 'Recent', 'Name', 'Resource', and 'Marketplace', along with a search bar and a 'Create a resource' button. At the bottom, there's a 'Navigate' section with links for 'Subscriptions', 'Resource groups', 'All resources', and 'Dashboard'.

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

This screenshot shows the 'Subscriptions' blade in the Azure portal. It lists one subscription: 'Visual Studio Enterprise Subscription'. The subscription details are as follows:

Subscription name	Subscription ID	My role	Current cost	Secure Score	Parent management group	Status
Visual Studio Enterprise Subscription	71318d18-92b8-4c80-b327-937e1b90517a	Account admin	CAS18.29	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.

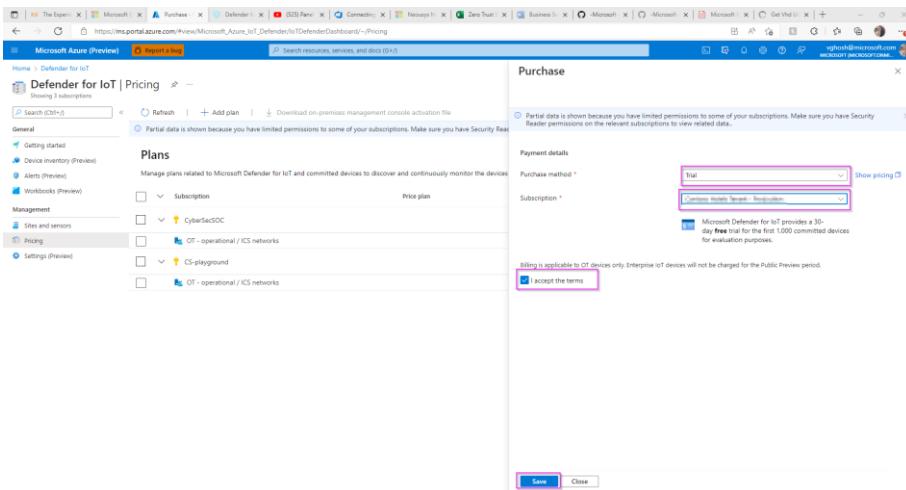
2. On the Defender for IoT page, in the **Getting Started** section, select **Pricing**.

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

4. In the popup screen, select:

- 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 3 days.*

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



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

**Custom deployment** Deploy from a custom template

Select a template   Basics   Review + create

**Template**

- Customized template (4 resources)
  - Edit template
  - Edit parameters
  - Visualize

**Project details**

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

Subscription \* (BuildEnv)   Resource group \* (Create new)

**Instance details**

Region \* (East US)   Location ([resourceGroup().location])   Deploy Public IP (true)   Put Password To Key Vault (true)   Source VHDURL \*   Sensor Count (1)

- 1) Please select your **Subscription** linked to the trial 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 trial service.
- 3) Please select the **Region** (Time zone) to which you are deploying the trial 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.

Commented [KL1]: @Vishakha Ghosh is this mandatory., or could they also set up with internal IP?

Commented [YS2R1]: agree, we should add the option for internal IP, and reminded them that if they select internal IP, customer will need to find ways to publish it to the end users

Commented [YS3]: @Vishakha Ghosh @Kineret Lowy we should add here disclaimer that if customers select this option their sensor will be open to the internet, and we will not record to upload production data

**Custom deployment** Deploy from a custom template

Validation Passed

Basics   Review + create

Summary

Customized template (3 resources)

Terms

Accept Marketplace Terms | Accept Marketplace

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.

The screenshot shows the Microsoft Azure Deployment Overview page. It displays a green checkmark indicating 'Your deployment is complete'. Below this, there's a table of resources with their types, statuses, and operation details. At the bottom left, there's a blue rectangular button with white text that says 'Go to resource group'.

- Go to the keyvault resource from the list.

The screenshot shows the Microsoft Blueprint 20220713114358 Resource Group Overview. On the left, there's a navigation menu with various options like Activity log, Metrics, Tags, and Resource Health. The main area shows a list of resources under the 'Resources' tab. One resource, 'KeyVault', is highlighted in yellow, indicating it's selected.

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

The screenshot shows the KeyVaultTest Access Policies page. On the left, there's a navigation menu with 'Access policies' highlighted. The main area has a heading 'Add Access Policy' with a red box around it. Below it, there's a table for 'Current Access Policies' with columns for Name, Email, Key Permissions, Secret Permissions, Certificate Permissions, and Action.

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

Configure from template (optional): Key & Secret Management  
Key permissions: TLS enabled  
Secret permissions: Write  
Certificate permissions: None selected  
Selected principal: None selected  
Authenticated application: None selected  
Add

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

Name	Type	Status	Expiration date
SOC-vmx24k5pt75ngp2-Play	Key	Enabled	Never

6. Click on the current version.

Version	Status	Activation date	Expiration date
cf3a7655cda64584ae6faa051ee47e9	Enabled	7/13/2022, 11:57:28 AM	Never

7. Copy the secret value to your clipboard.

Properties  
Created: 7/13/2022, 11:57:28 AM  
Updated: 7/13/2022, 11:57:28 AM  
Secret Identifier: https://soc-kv24k5pt75ngp2-play.vault.azure.net/secrets/SOC-vmx24k5pt75ng...  
Settings  
Set activation date:   
Set expiration date:   
Enabled: Yes  
Tags: 1 tag  
Secret  
Content type (optional):  
Show Secret Value  
Secret value: \*\*\*\*\* Copied

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

The screenshot shows the Microsoft Defender for IoT interface for the 'KeyVaultTest' resource group. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Deployments, Security, Policies, Properties, Links, Cost Management, Cost analysis, Cost alerts (preview), Budgets, and Advisor recommendations. The main area shows a table of resources with columns for Type, Name, Location, and Status. A filter bar at the top allows searching by name, type, location, and more. The 'Virtual machine' row for 'SOC-vm2410' is selected.

## 9. Make a note of the Public IP address.

The screenshot shows the Microsoft Azure portal's 'SOC' virtual machine details page. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, and Continuous delivery. The main area shows the 'Properties' tab with fields for Resource group, Status, Location, Subscription, Tags, and a list of properties like Computer name, Health state, Operating system, Publisher, Offer, Plan, and Networking. The 'Networking' section highlights the Public IP address (20.124.21.178) and Private IP address (10.10.10.4).

## Option #2: If you deployed without Keyvault.

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

The screenshot shows the Microsoft Azure portal's 'Deployment details' page for the completed deployment 'Microsoft.Template-20220630145822'. The left sidebar includes sections for Home, Microsoft.Template-20220630145822 | Overview, Inputs, Outputs, and Template. The main area shows a table of deployment details with columns for Resource, Type, Status, and Operation details. The 'Reset-password0' resource is highlighted.

Resource	Type	Status	Operation details
Reset-password0	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
Post-Deploy0	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
VMDeployment	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
copyhd	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>

2. 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 JSON output object contains the following data:

```
[{"VMName": "SOC-vmw7ne3eacow5cos0-Play", "Password": "KCh9dMLp3Vkar2YpB99PMZVB="}]
```

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

Your deployment is complete

Resource	Type	Status	Operation details
Reset-password0	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
Post-Deploy0	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
VMDeployment	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
copyhd	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>

Next steps

[Go to resource group](#)

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

Subscription (none) : Deployments : 13 Succeeded

Tags (edit) : Click here to add tags

Resources Recommendations

Name	Type	Location
copyhd	Deployment Script	East US
customfcwifisSekwu	Storage account	East US
SOC-NSGfcwifisSekwu-Play	Network security group	East US
<b>SOC-vmfcwifisSekwu-Play</b>	Virtual machine	East US

5. Make a note of the Public IP address.

The screenshot shows the Microsoft Azure portal interface for a virtual machine named "Play". The "Networking" section is highlighted, showing the Public IP address as 20.124.23.178. Other networking details include the Virtual network/subnet (SOC), Virtual network (Play), and DNS name (Not configured). The "Virtual machine" section shows the Computer name as "Sensor", the Operating system as Linux (Ubuntu 18.04), and the Private IP address as 10.10.10.4.

### 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.

The screenshot shows a web browser window with the URL https://xx.x.x.x/login. The page title is "Microsoft | Defender for IoT sensor" and the sub-section is "Sensor Sign in". It features fields for "User name" and "Password", a "Forgot password? (for admin users only)" link, and a "Reset" button. A "Login" button is at the bottom right. The browser status bar indicates "Not secure".

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**.

The screenshot shows the Microsoft Defender for IoT Overview page. It includes sections for General Settings (Version: 22.1.3.4162-r-7763846, Threat Intelligence: Version 2021.12.22 | Last updated Dec 22, 2021, Connectivity type: Locally Managed, Activation: Valid), Traffic Monitoring, and Interfaces (local\_listener). A user profile for 'cyberx\_host' is visible at the top right.

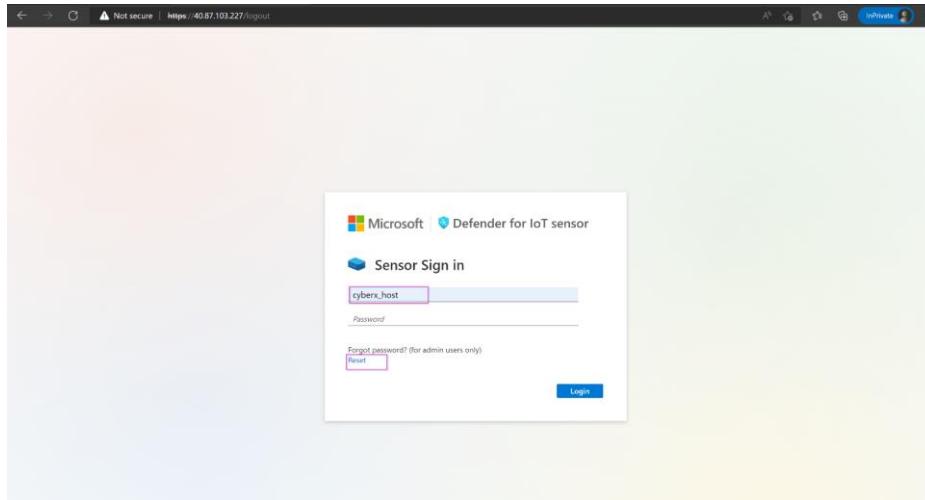
- After signing out, please return to the Azure portal and navigate to “**Defender for IoT**”. Select “**Sites and sensors**”, select your sensor from the list, and click on “**Recover my password**”.

The screenshot shows the Azure portal's Defender for IoT | Sites and sensors page. It lists two sensors: D4IOT-CxE-Site - D4IOT-CxE-Site and D4IOTsensor-TT. A context menu is open for the first sensor, with the "Recover my password" option highlighted.

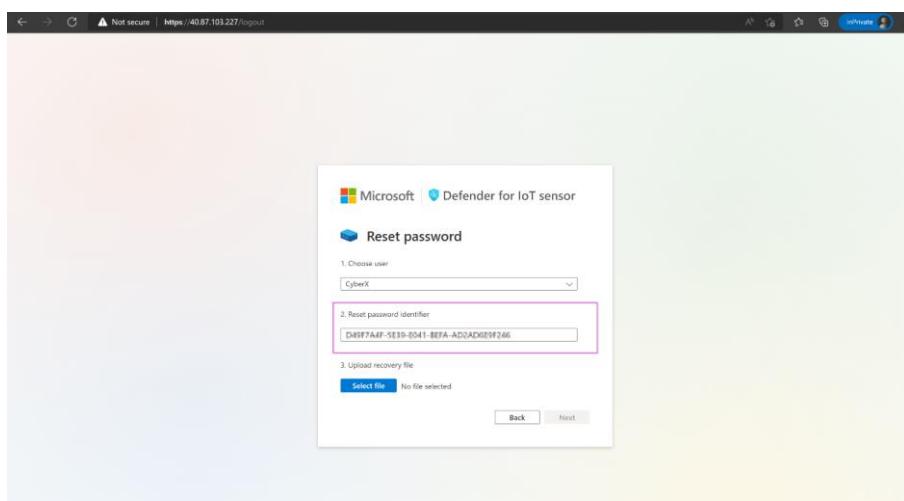
- You will see this prompt asking for the “secret identifier”.

The screenshot shows the Azure portal's "Recover" dialog box. It displays a lock icon and asks for an "Insert secret identifier". The input field contains "Sub00001-777-0057-88h12". There are "Recover" and "Cancel" buttons at the bottom.

- 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. In the center, a modal window titled 'Recover' is displayed. It features a lock icon and a key icon. Below the icons, there is a text input field containing a GUID: 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246'. At the bottom of the modal are two buttons: 'Recover' (highlighted with a pink border) and 'Cancel'.

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 Microsoft Defender for IoT sensor password reset wizard. The title bar says 'Microsoft | Defender for IoT sensor'. The main heading is 'Reset password'. Step 1, 'Choose user', has a dropdown menu set to 'CyberX'. Step 2, 'Reset password identifier', shows the same GUID as in the previous screenshot. Step 3, 'Upload recovery file', contains a 'Select file' button and a message 'No file selected'. At the bottom are 'Back' and 'Next' buttons.

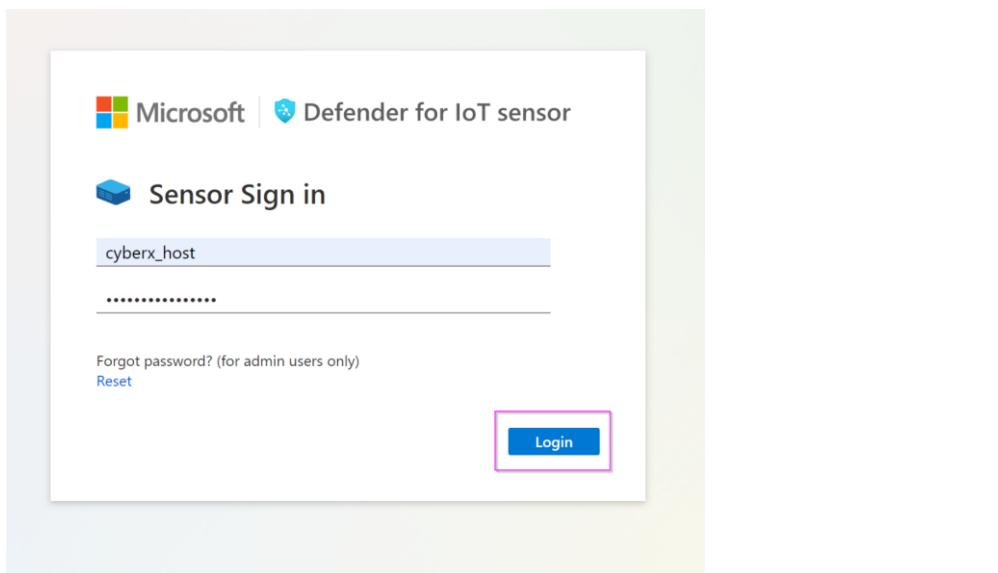
9. Click on “**Next**”.

The screenshot shows the 'Reset password' interface. Step 1, 'Choose user', has a dropdown menu set to 'CyberX\_host'. Step 2, 'Reset password identifier', contains the value 'D49F7A4F-5E19-0041-BEFA-AD2AD019F246'. Step 3, 'Upload recovery file', shows a 'Select file' button highlighted with a pink box, and a file named 'password\_recovery (1).zip' is listed. At the bottom are 'Back' and 'Next' buttons, with 'Next' also highlighted with a pink box.

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

The screenshot shows the 'Reset password' interface. Step 1, 'User name', has 'CyberX\_host' entered. Step 2, 'Password', has a field containing a temporary password 'j^hN@WTU\*7IP\_zH' highlighted with a pink box. Step 3, 'Please write your password, it will not be shown again', is present. At the bottom is a 'Next' button highlighted with a pink box.

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.

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 - 22.1.3 interface. In the left sidebar under 'Manage', 'System settings' is selected. The main area displays several 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 'Select a configuration category' dialog. On the left is a list of categories: 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 is a preview area labeled 'Advanced configurations'.

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

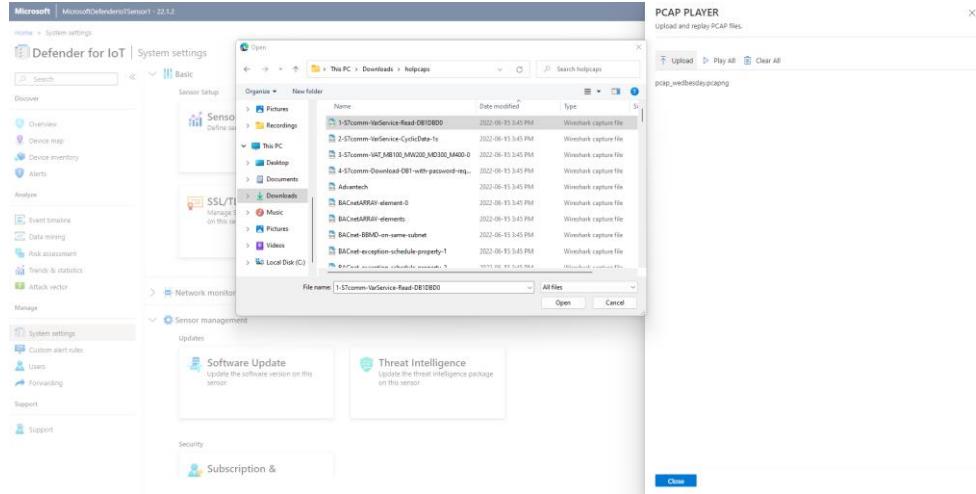
The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a sidebar with options like Analyze, Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector, Manage, System settings, Custom alert rules, Users, and Forwarding. The 'System settings' option is selected. In the main area, there's a 'Backup data and restore the latest backup' section and an 'SNMP MIB Monitoring' section. A red box highlights the 'Save' button at the bottom right of the main content area. To the right of the main content, a modal window titled 'Advanced configurations' is open, specifically the 'Pcaps' tab. It contains configuration parameters such as 'cache.should.save.pcap=1', 'archive.cache.dir...', '# 7 GB', 'filtered.archive.dir.size.megabytes.max=7168', '# 3 GB', 'filtered.archive.dir.size.megabytes.min=3072', 'filtered.archive.dir.size.megabytes.max=', 'filtered.archive.dir.size.megabytes.min=', 'player.max.size=1000', 'player.max.amount=20', 'player.params=disabled', and 'virtual.lan.hierarchy.depth.support=1'. There are 'Save' and 'Close' buttons at the bottom of the modal.

## Task 2: Play PCAP files

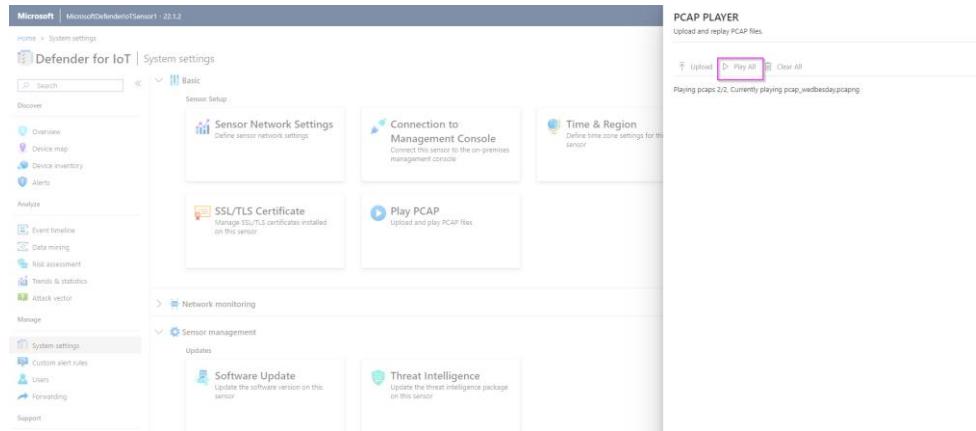
1. Use [this](#) link to download the holcaps.zip folder.
2. Unzip the folder.
3. Scroll all the way down to the bottom to locate if the PCAP Player is enabled (Shown in the image below in the red top square) or not. If the PCAP player is not shown, proceed to click on the arrow next to the **Sensor 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 'System settings' (selected), 'Custom alert rules', 'Users', and 'Forwarding'. The main content area has sections for 'SSL/TLS Certificate' and 'Play PCAP'. A red box highlights the 'Play PCAP' section. Below it, under 'Network monitoring', there's a 'Sensor management' section with a red box around its expandable arrow. Other visible sections include 'Integrations' and 'Import settings'.

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



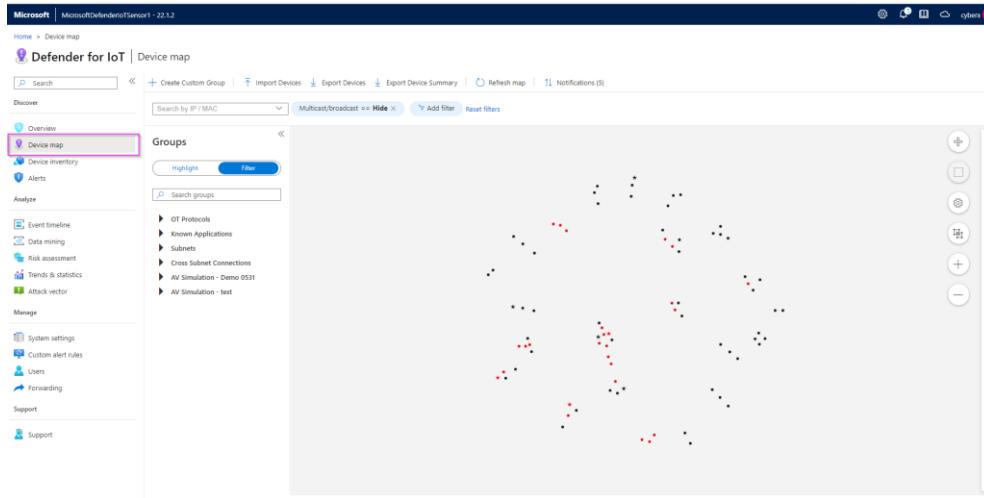
5. Click "Play All" to play the Pcaps.



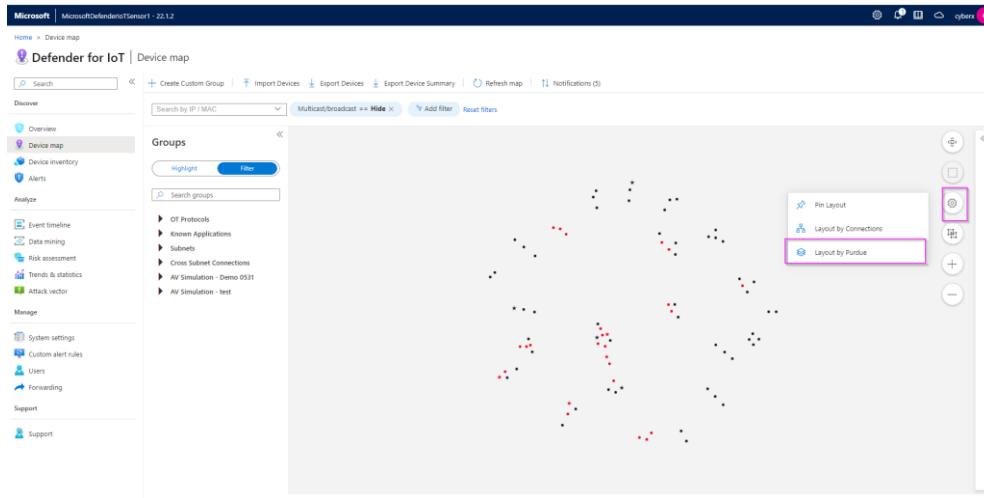
## Exercise 4: Analyzing the Data

### Task 1: Visualize on the Device Map

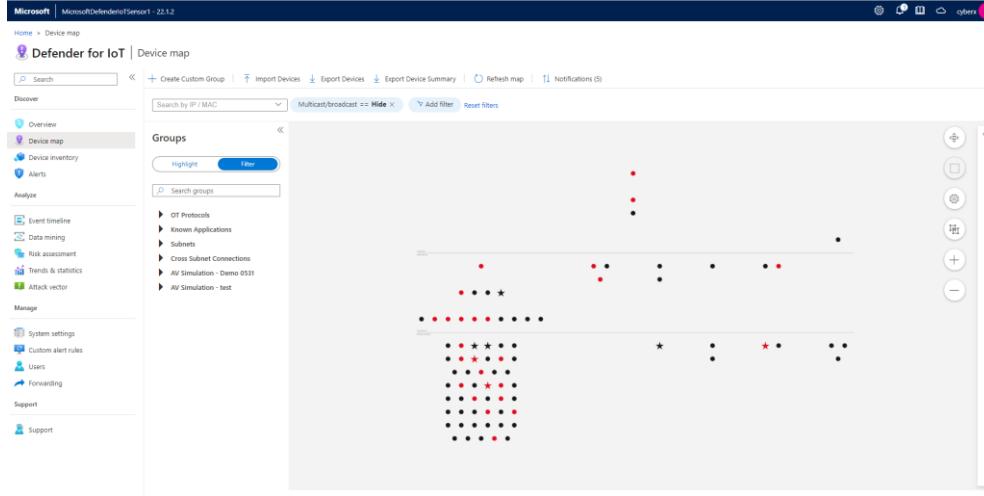
1. Click on "Device Map" from the menu on the left side.



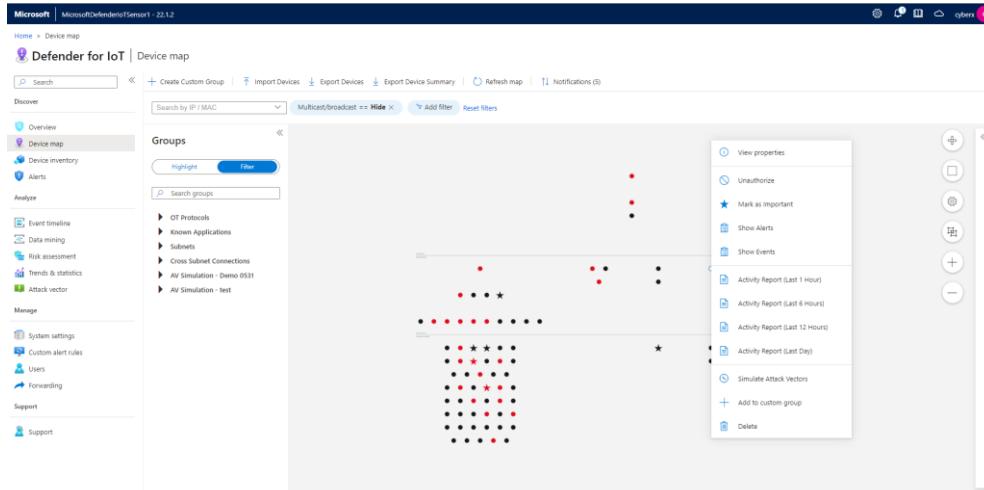
2. Click on the “Settings” option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.



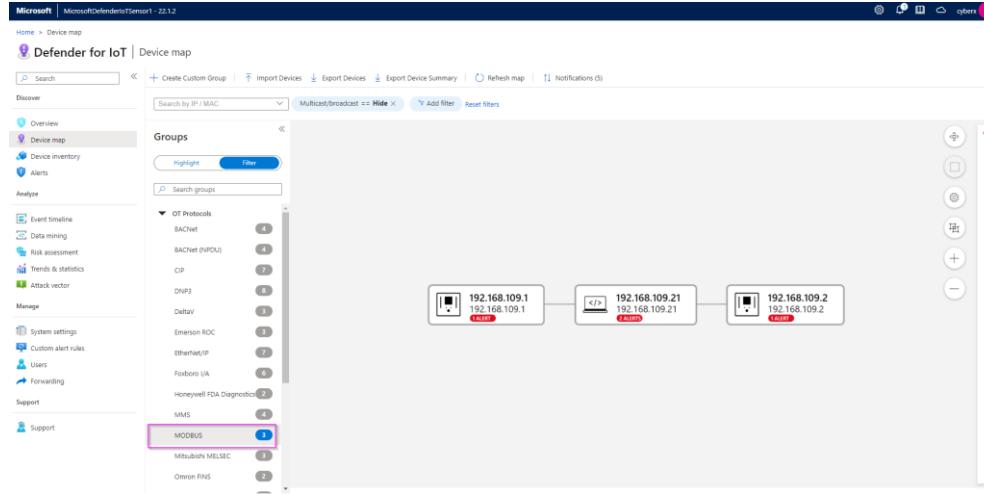
3. Once you confirm the changes, you will see the devices laid out as shown in the image below.



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

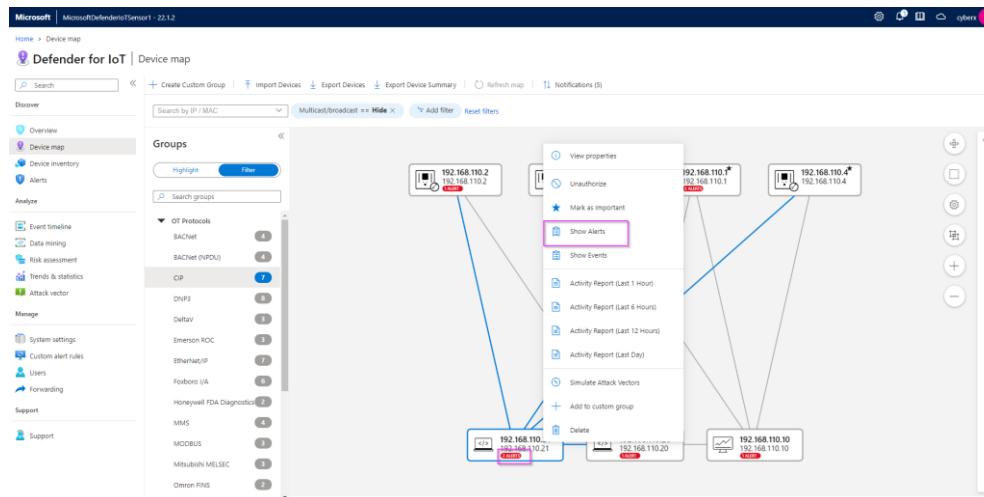


5. To filter by OT Protocols, expand the arrow, and pick the protocol you want to filter by. The console will display the devices that match the filter.



## Task 2: View the associated Alerts

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



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, Alerts, Event Timeline, Discover, Overview, Device inventory, and more. The main area displays a device card for '192.168.110.21'. The card includes sections for General Information (Type: Engineering Station, Vendor: INTEL CORPORATE, Location: Automatic, Scorer: Programming Device), Network Interfaces (IP: 192.168.110.21, MAC: acf0:ec:bb), and Protocols (SSH, Ethernet/IP, TDS, FTP, CIP). Below the device card is a table of alerts:

Severity	Name	Engine	Detection time	Status	Source Device
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 weeks ago	New	192.168.110.21
Major	Ethernet/IP Encapsulation Protocol Command Failed	Operational	2 months ago	New	192.168.110.2

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 'Discover' section with 'Alerts' selected, and other sections like Overview, Device map, Device inventory, Analyze, Manage, and Support. The main area shows a table of alerts:

Severity	Name	Engine	Detection time	Status	Source Device
Critical	Unauthorized Internet Connectivity De...	Policy Violation	2 weeks ago	New	192.168.110.21
Critical	Unauthorized Internet Connectivity De...	Policy Violation	2 weeks ago	New	192.168.112.30

One alert is highlighted with a red box. To the right of the table, a detailed view of the first alert is shown:

**Unauthorized Internet Connectivity Detected**  
 Alert ID: 33  
 See in Event timeline | See in Device map

**Critical**  
 Status: New | Detection time: 2 weeks ago

Description:  
 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.

**Related Devices**  
 Source device: 192.168.110.21 (Engineering Station) → Destination device: Internet (37.142.39.186) Internet

**Actions**  
 View full details | 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	192.168.112.30
Critical	Port Scan Detected	Anomaly	2 weeks ago	Closed	192.168.110.21
Critical	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	
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 months ago	New	192.168.100.8
Warning	Traffic Detected on Sensor Interface	Operational	2 months ago	New	
Major	EtherNet/IP Encapsulation Protocol Command Failed	Operational	3 months ago	Closed	192.168.110.1
Critical	Excessive SMB login attempts	Anomaly	3 months ago	New	192.168.101.10
Major	Event Buffer Overflow in Outstation	Operational	3 months ago	New	192.168.117.23
Warning	Controller Reset	Operational	3 months ago	New	192.168.117.239
Warning	Controller Reset	Operational	3 months ago	New	192.168.117.239
Warning	An ST Stop PLC Command was Sent	Operational	3 months ago	New	192.168.118.22
Warning	An ST Stop PLC Command was Sent	Operational	3 months ago	New	192.168.118.11
Major	GE SFTP Command Failure	Operational	3 months ago	New	192.168.122.1
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.109.1
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.109.2
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...	54:14:03:74:08:21	INTEL CORPORA...					
192.168.100.1	192.168.100.1	50 minutes ago	Server	DNS							
192.168.1.111	192.168.1.111	50 minutes ago	PLC	Siemens S7	00:0F:5A:0D:BE:F0	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:a7:08:92:06	SCHWEITZER EN...					
192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...	00:23:a4:40:5a: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...	00:00:c1:02:09:09	EATON CORPOR...					
192.168.117.7	192.168.117.7	22 hours ago	PLC	Siemens SIMAC	00:e0:a8:01:90:08	SAT GMBH & CO	15.01	CPC65 (6065)			
192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SIMAC	00:0c:28:28:00:00	VMWARE INC.					
192.168.117.8	192.168.117.8	22 hours ago	PLC	Siemens SIMAC	00:a0:a8:01:90:08	SAT GMBH & CO	15.01	CPC65 (6065)			
192.168.107.10	FC50007	22 hours ago	DCS Controller	Yokogawa VNetIP	00:00:64:94:56:10	YOKOGAWA DIG...					
192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNetIP	00:00:64:94:73:00	YOKOGAWA DIG...					
192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNetIP	00:00:64:94:84:05	YOKOGAWA DIG...					
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:a8:11:23:33	SIEMENS AG	3.2.6	6E37 315-0EH14...	0	4	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:a8:11:23:33	SIEMENS AG	3.2.6	6E37 315-0EH14...	1	2	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:a8:11:23:33	SIEMENS AG	3.2.6	6E37 315-0EH14...	1	2	

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

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	An hour ago	Unknown	DNS, MDNS, net...	54:14:03:74:08:21	INTEL CORPORAT...					
192.168.100.1	192.168.100.1	An hour ago	Server	DNS		Siemens 57	00:0f:b5:4d:be:f3	NETGEAR			
192.168.111.1	192.168.111.1	An hour ago	PLC	Siemens 57							
192.168.118.0	192.168.118.0	An hour ago	HMI	Siemens 57							
192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:92:c8	SCHWEITZER EN...					
192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	00:23:a4:94:5a:c2	CISCO SYSTEMS ...					
192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:97:09	SCHWEITZER EN...					
192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	00:c0:1c:02:09:98	EATON CORPOR...					
192.168.117.7	192.168.117.7	22 hours ago	PLC	Siemens SIMATIC 300	00:a0:b0:01:90:be	SAT GMBH & CO.	15.01	CPO5 (605)			
192.168.117.229	192.168.117.229	22 hours ago	Unknown	Siemens SIMATIC 300	00:0c:92:28:28:39	VMWARE INC.					
192.168.117.8	192.168.117.8	22 hours ago	PLC	Siemens SIMATIC 300	00:e9:a0:01:90:88	SAT GMBH & CO.	15.01	CPO5 (605)			
192.168.107.10	FC5507	22 hours ago	DCS Controller	Yokogawa VNet/IP	00:00:64:00:5d:10	YOKOGAWA DGS...					
192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:00:73:04	YOKOGAWA DGS...					
192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:00:84:05	YOKOGAWA DGS...					
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens 57	00:01:a3:11:22:33	SIEMENS AG	3.2.6	6E57 315-0E1H1...	0	4	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens 57	00:01:a3:11:22:33	SIEMENS AG	3.2.6	6E57 315-0E1H1...	1	2	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens 57	00:01:a3:11:22:33	SIEMENS AG	3.2.6	6E57 315-0E1H1...	1	2	

## 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".

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 fr...
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

## 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 like Overview, Device map, Device inventory, Alerts, Analysis, and Support. The main area displays 'Recommended' sections for Programming Commands, Internet Activity, Excluded CVEs, Remote Access, CVEs, and Non Active Devices (Last 7 Days). Below this is a 'My reports' section where a new report named 'test' is listed. A modal window titled 'Create new report' is open, prompting the user to enter a name ('Report name'), description, choose a category (Category selected), and set an order by option (Category selected). The 'Filter by' section includes dropdowns for Results within the last (3 Minutes selected), IP address, MAC address, Port, and Device group. At the bottom of the modal are 'Save' and 'Cancel' buttons.

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 previous one but with more detailed filtering. The 'Choose Category' dropdown is now set to 'Modules and Firmware Versions'. The 'Add filter type' dropdown is open, showing 'Firmware Version (GENERIC)' highlighted with a pink box. Other filter options like 'IP address', 'MAC address', 'Port', and 'Device group' are also visible. The 'Save' button at the bottom of the modal is 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 Data mining interface. On the left, there's a sidebar with various navigation options like Overview, Device map, Device inventory, Alerts, Trends & statistics, Attack vector, System settings, Custom alert rules, Users, Forwarding, and Support. The main area is titled 'Defender for IoT | Data mining'. It features a 'Recommended' section with cards for Programming Commands, Internet Activity, Excluded CVEs, Active Devices (Last 24 Hours), Remote Access, and CVEs. Below that is a 'My reports' section where a report titled 'PLC Firmware Version' is listed. This report has a description: 'Report showing the firmware version of the different PLCs.', was last modified 2 minutes ago, and was created 4 days ago. There are also 'Edit' and 'Delete' icons for this report.

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

This screenshot shows the details of the 'PLC Firmware Version' report. 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 report content area displays the text: 'Report showing the firmware version of the different PLCs.' Below this, there's a table with four rows, each representing a PLC with its name, date created, and size. The first row, 'risk-assessment-report-4.pdf', is highlighted with a pink box.

#	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

## 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 interface. The sidebar includes options for Overview, Device map, Device inventory, Alerts, Trends & statistics, Attack vector, System settings, Custom alert rules, Users, Forwarding, and Support. The main area is titled 'Defender for IoT | Risk assessment'. A 'Generate report' button is highlighted with a pink box. Below it is a 'Reports list' table showing four generated risk assessment reports. The first report, 'risk-assessment-report-4.pdf', is highlighted with a pink box.

#	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 URL [https://portal.azure.com/#blade/Microsoft\\_Azure\\_IoT\\_Solutions/DefenderForIoTBlade/Overview](https://portal.azure.com/#blade/Microsoft_Azure_IoT_Solutions/DefenderForIoTBlade/Overview). The page title is "Defender for IoT | Sites and sensors". The top navigation bar includes "Search resources, services, and docs (Ctrl+F)", "Home > Defender for IoT", and user information "vghostin@outlook.com (vghostin)". Below the title, there's a message: "Showing subscription 'BuildEnv' expired. Please contact Microsoft sales." The main content area shows a summary of sensor counts: All sensors (4), IoT (1), OT cloud connected (2), and OT (1). A table lists four sensors, including "D4IOT-CxE-Site - D4IOT-CxE-Site". The "Sites and sensors" tab is selected.

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" (with a placeholder box), "Subscription" (dropdown menu showing "Please select a subscription" and "Onboard subscription", both highlighted with a pink box), "Cloud connected" (checkbox checked and highlighted with a pink box), "Automatic Threat Intelligence updates" (checkbox unchecked), "Sensor version" (dropdown menu showing "22.X and above"), "Site" (Resource name dropdown menu showing "No subscription has been selected" and "Create site"), "Display name" (text input field), "Tags" (key-value pair input field with "+Add tag" button), and "Zone" (Subscription 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 sidebar with categories like Discover, Analyze, and Manage. Under Manage, 'System settings' is selected and highlighted with a pink box. In the main content area, under 'Updates', there are cards for 'Software Update' and 'Threat Intelligence'. Under 'Security', there is a card for 'Subscription & Activation Mode' which is also highlighted with a pink box. Below it are cards for 'Backup & Restore' and 'System Health Check'. Under 'Health and troubleshooting', there is a card for 'SNMP MIB Monitoring'.

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

This screenshot shows the 'Subscription & Activation Mode' dialog box overlaid on the Sensor management page. The dialog box has fields for Activation Mode (Cloud Connected), Activation Status (Active), Tenant ID (5f100002-dfa4-41b9-b79c-1dddf3604a4b), and Subscription ID (1cf1ccdb-7d31-45a3-a1b-848ce46d70a5). At the bottom, there is a 'Select file' button which is highlighted with a pink box, and a note saying 'No file selected'.

### Task 3: Verify Cloud connection

- On the sensor console.

The screenshot shows the Microsoft Defender for IoT Overview page. At the top, there are three summary metrics: 0 PPS, 64 Devices, and 21 Alerts. The main area is divided into four cards:

- General Settings:** Version 22.1.3.4162, Threat Intelligence Version 2022.07.12 (Last updated Jul 12, 2022), Connectivity type: Cloud connected (Valid), Activation: Valid, Certificate: Valid.
- Traffic Monitoring:** A chart placeholder stating "No chart to show".
- Top 5 OT Protocols:** A list of protocols: Modbus, DNP3, MQTT, OPC UA, and Profinet.
- Traffic By Port:** A chart placeholder with a "Trend" button.

The left sidebar includes sections for Discover, Analyze, and Manage.

## 2. On the Cloud management console.

The screenshot shows the Microsoft Defender for IoT Sites and sensors page. It displays the following information:

- Subscription: BuildEnv
- General section: Getting started, Device Inventory (Preview), Alerts (Preview), Workbooks (Preview), Management.
- Sensor count: 4 All sensors, 1 IoT, 2 OT cloud connected, 1 OT.
- Table view: Shown 4 of 4 sensors, listing:
 

Sensor name	Sensor type	Zone	Subscription	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...
D4IOT-CxE-Site - D4IOT-CxE-Site	IoT	default	BuildEnv	22.1.3.4162	Unavailable	--	--	...
sensor-Cyber	OT cloud co...	default	BuildEnv	22.1.3.4162	Disconnected	A month ago	5/25/2022	Automatic
test2	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 navigation sidebar with sections like General, Threat management, Content management, and Configuration. Under Configuration, the 'Data connectors' section is selected. In the main area, there are two tabs: 'Connected' (133) and 'Disconnected' (35). A search bar at the top says 'Search (Ctrl+F)' and filters by 'Defender for IoT'. Below the tabs, there's a table with columns for Status, Connector name, Provider, Last Log Received, and Last data received. One row is highlighted for 'Microsoft Defender for IoT' from Microsoft. To the right of the table, there's a summary card for 'Microsoft Defender for IoT' with metrics like 133 Connected, 35 Disconnected, 1 Workbooks, 2 Queries, 1 Analytics rules templates, and a chart showing data received over time.

- 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 tabs for Instructions and Next steps. Under Instructions, there's a 'Prerequisites' section with a list of requirements: Workspace (read and write permissions) and Subscription (Contributor permissions to the subscription of your IoT Hub). Below that is a 'Configuration' section with a sub-section 'Connect Microsoft Defender for IoT to Microsoft Sentinel'. It says to select 'Connect' next to each Subscription whose IoT Hub's alerts you want to stream to Microsoft Sentinel. There's a 'Select the relevant Subscriptions to connect' section with 'Connect All' and 'Disconnect All' buttons, and a search bar. A table lists subscriptions: 'Azure Pass - Sponsorship' with a 'Connect' button (which is highlighted with a red box) and a 'Disconnected' status. At the bottom, there's a footer with '32 / 39'.

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 portal interface for Microsoft Defender for IoT (Preview). The top navigation bar includes the Microsoft Azure logo, a search bar, and various navigation icons. Below the header, the breadcrumb navigation shows: Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for IoT (Preview).

The main content area is titled "Microsoft Defender for IoT (Preview)" and contains two tabs: "Instructions" (selected) and "Next steps".

**Prerequisites:** To integrate with Microsoft Defender for IoT (Preview) make sure you have:

- ✓ **Workspace:** read and write permissions.
- ℹ **Subscription:** Contributor permissions to the subscription of your IoT Hub.

**Configuration:** Connect Microsoft Defender for IoT to Microsoft Sentinel. Select Connect next to each Subscription whose IoT Hub's alerts you want to stream to Microsoft Sentinel.

[Microsoft Defender for IoT pricing model >](#)

**Select the relevant Subscriptions to connect:**

Buttons: [Connect All](#) [Disconnect All](#)

Search bar:  Search

Subscription	Status
Azure Pass - Sponsorship	<a href="#">Connect</a> <a href="#">Disconnect</a> <span style="color: green;">Connected</span>

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

The screenshot shows the Microsoft Defender for IoT (Preview) interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, a breadcrumb trail shows 'Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for IoT (Preview)'. The main area has a title 'Microsoft Defender for IoT (Preview)' and a sub-section 'Instructions'. The 'Next steps' tab is highlighted with a red box. Below it, there's a 'recommended workbooks' section with a link 'Go to workbooks gallery >'. Under 'Query samples (2)', there are two examples: 'All logs' and 'Summarize by severity', each with a 'Run' button. In the 'Relevant analytics templates (1)' section, there's a table with one row. The 'CREATE RULE' button at the end of the row is highlighted with a red box. The table columns are 'Severity ↑', 'Name ↑', 'Rule type ↑', 'Data sources', 'Tactics', and 'CREATE RULE'.

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' page. At the top, there's a breadcrumb trail: 'Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for IoT (Preview) > Analytics rule wizard - Create new rule from template'. Below it, a message says 'Create incidents based on Azure Defender for IOT alerts' with a green checkmark icon and the text 'Validation passed.' The page has tabs: 'General', 'Automated response', and 'Review and create' (which is underlined). The 'General' section contains 'Analytics rule details' with fields: Name (MyNewRule), Description (Create incidents based on all alerts generated in Azure Defender for IoT), and Status (Enabled). The 'Analytics rule logic' section includes '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)' (Not configured). At the bottom, there are 'Previous' and 'Create' buttons, with the 'Create' button 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 sidebar with various navigation options like Overview, Logs, News & guides, and Search (Preview). The main area has a search bar at the top. Below it, there are sections for Active rules, Rule templates, and Anomalies. A pink box highlights the 'Data Sources' dropdown menu where 'Microsoft Defender for IoT' is selected. To the right, there's a color-coded legend for rule severity: High (54), Medium (296), Low (54), and Informational (14). At the bottom, there are tabs for Severity, Name, Rule type, Data sources, Tactics, Techniques, and Source name, with 'Microsoft Defender for IoT' selected under Data sources. The bottom navigation includes a search bar, a 'Create' button, and links for Analytics efficiency workbook (Preview), Enable, Disable, Import, Export, Guides & Feedback, and Learn More.

## 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 Sensor console. The left sidebar includes tabs for Overview, Device map, Device inventory, Alerts, Analyze, Manage, System settings, Custom alert rules, Users, Forwarding, and Support. The main area is titled 'Defender for IoT | Alerts'. It shows a table of 22 alerts with columns for Severity, Name, Engine, Detection time, Status, and Source Device. A pink box highlights the 'Learn' button at the top right of the table. The table rows include: Critical: Unauthorized Internet Connectivity Detected, Policy Violation, 2 weeks ago, Closed, 192.168.110.21; Critical: Unauthorized Internet Connectivity Detected, Policy Violation, 2 weeks ago, New, 192.168.112.30; Critical: Port Scan Detected, Anomaly, 2 weeks ago, Closed, 192.168.110.21; Major: EtherNetIP 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, 192.168.110.1; Critical: Excessive SMB Login Attempts, Anomaly, 3 months ago, New, 192.168.101.10; Major: EtherNetIP Encapsulation Protocol Command Failed, Operational, 3 months ago, Closed, 192.168.110.1; Major: Event Buffer Overflow in Outstation, Operational, 3 months ago, New, 192.168.117.23; Warning: Controller Reset, Operational, 3 months ago, New, 192.168.117.239; Warning: Controller Reset, Operational, 3 months ago, New, 192.168.117.239; Warning: An ST Stop PLC Command was Sent, Operational, 3 months ago, New, 192.168.118.22; Warning: An ST Stop PLC Command was Sent, Operational, 3 months ago, New, 192.168.118.11; Major: GE SRTP Command Failure, Operational, 3 months ago, New, 192.168.122.1; Major: Modbus Exception, Protocol Violation, 3 months ago, New, 192.168.109.1; Major: Modbus Exception, Protocol Violation, 3 months ago, New, 192.168.109.2; Major: Honeywell Firmware Version Changed, Policy Violation, 3 months ago, New, 192.168.108.2.

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 Overview, Device map, Device inventory, Alerts, Analysis, Manage, and Support. The main area has several cards: Sensor Network Settings, Connection to Management Console, Time & Region, SSL/TLS Certificate, and Play PCAP. A modal window titled 'PCAP PLAYER' is open, showing a file list with '1-57comm-VarService-Read-0E10B00.pcap' and 'pcap\_wednesday.pcap'. It includes buttons for Upload, Play All, Clear All, and Close.

### 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 sidebar has sections like General, Threat management (with 'Incident' selected), Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, Content management, Configuration, and Settings. The main area displays a table of incidents with columns: Severity, Incident ID, Title, Alerts, Product names, Created time, Last update time, and Owner. A red box highlights the 'Product name : Microsoft Defender for IoT' filter at the top of the table. The table shows 16 Open incidents, 16 New incidents, and 0 Active incidents. The alert count is 0. The severity distribution is: High (4), Medium (10), Low (2), and Informational (0).

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

The screenshot shows the Microsoft Sentinel Incidents page. A specific alert is highlighted with a red box. The alert details are as follows:

- Description:** Unauthorized Internet Connectivity Detected
- Severity:** High
- Status:** New
- Created time:** 01/25/22, 04:41 PM
- Last update time:** 01/25/22, 04:41 PM
- Owner:** Unsigned
- Product name:** Microsoft Defender for IoT
- Alerts:** 1
- Events:** 1
- Tactics:** Initial Access
- Entities:** 144.81.0.130, 10.200.1.134, HUB-M240T-MST..., 10.200.1.124
- Tags:** None

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.

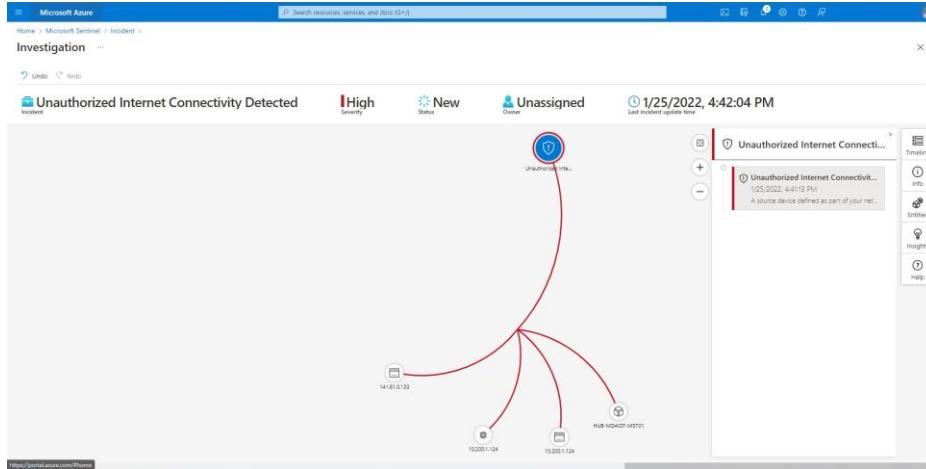
The screenshot shows the Microsoft Sentinel Incident details page for Incident ID 16. The Timeline tab is selected. A specific timeline entry is highlighted with a red box:

- Time:** Jan 25
- Type:** Unauthorized Internet Connectivity Detected
- Severity:** High
- Detected by:** Microsoft Defender for IoT
- Tactics:** Initial Access

The timeline also lists other entities involved:

- Entity 144.81.0.130
- Entity 10.200.1.134
- HUB-M240T-MST...
- Entity 10.200.1.124

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.

The screenshot shows the Microsoft Azure Microsoft Sentinel | Logs page. The search bar contains the query: "SecurityAlert | where ProviderName contains "IoTSecurity"". The results table displays 51 records from the last 24 hours, showing various log entries related to IoTSecurity alerts. The columns include TimeGenerated (UTC), DisplayName, AlertName, AlertSeverity, and Description. Some examples of log entries include:

TimeGenerated (UTC)	DisplayName	AlertName	AlertSeverity	Description
2/2/2022, 3:42:27.651 PM	Unknown Object Sent to Outstation	Unknown Object Sent to Outstation	Medium	The destination device received an invalid request.
2/2/2022, 3:42:27.511 PM	Outstation Restarts Frequently	Outstation Restarts Frequently	Low	An excessive number of cold restarts were detected on a source device.
2/2/2022, 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.
2/2/2022, 3:42:27.361 PM	Port Scan Detected	Port Scan Detected	High	A source device was detected scanning network devices. This may be authentic or malicious.
2/2/2022, 3:42:27.356 PM	Port Scan Detected	Port Scan Detected	High	A source device was detected scanning network devices. This may be authentic or malicious.
2/2/2022, 3:42:27.373 PM	Unauthorized Internet Connectivity Det...	Unauthorized Internet Connectivity Det...	High	A source device defined as part of your network is communicating with an external network.
2/2/2022, 3:42:27.499 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.
2/2/2022, 3:42:27.473 PM	Outstation Restarter	Outstation Restarter	Low	A cold restart was detected on a source device. This means it has been powered off and back on again.
2/2/2022, 3:42:27.324 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.
2/2/2022, 3:42:27.443 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.
2/2/2022, 3:42:27.407 PM	Controller Stop	Controller Stop	Low	The source device sent a stop command to a destination controller.
2/2/2022, 3:42:27.384 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 containing the query: "SecurityAlert | where CompromisedEntity == "hub-md4iot-mst01"".

Below the search bar is a toolbar with various icons: Run, Save, Share, New alert rule, Export, Pin to dashboard, and Format query. The "Run" button is highlighted in blue.

The main area displays the query results in a table format. The table has columns: TimeGenerated [UTC], DisplayName, AlertName, AlertSeverity, and Description. The results show four alerts from October 1, 2021:

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 retur
10/1/2021, 4:00:07.358 PM	Controller Stop	Controller Stop	Low	The source de
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.