

Summary

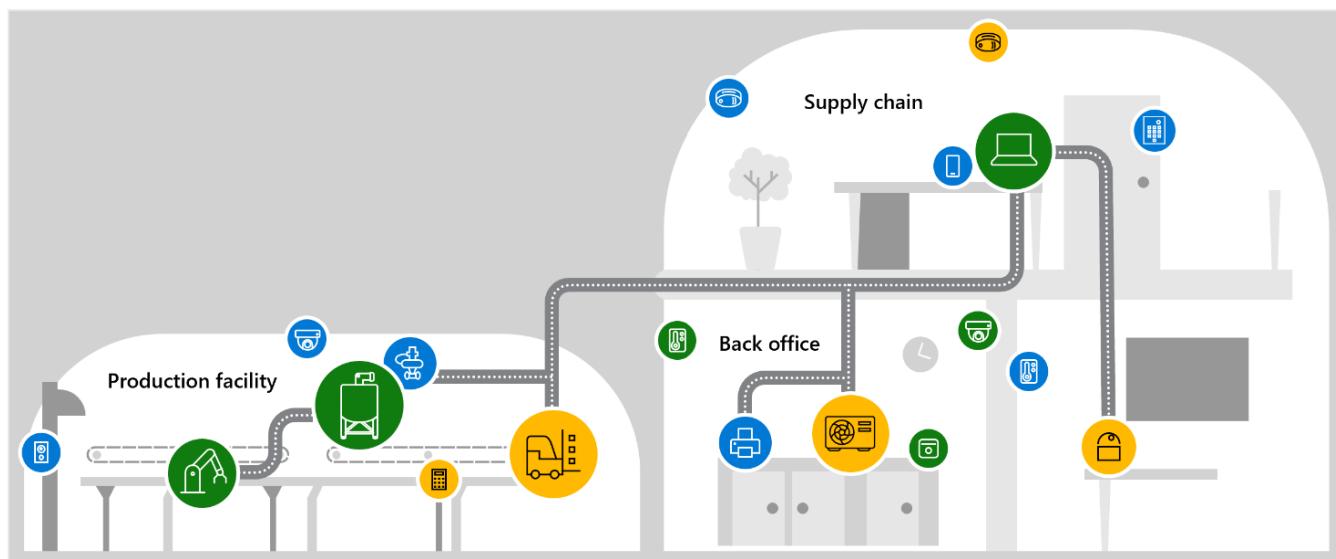
This Hands-on-Lab (HOL) will focus on securing your facilities. We will be simulating traffic by playing some Packet captures, visualizing and analyzing the data on the sensor console. Integrate our sensor with Microsoft Sentinel, to explore alert handling, and to write queries to help with alert investigation.

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 to write 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.



What is Microsoft Defender for IoT?

Microsoft Defender for IoT is a comprehensive security solution designed to detect IoT and OT devices, vulnerabilities, and threats. This powerful tool can be used to protect your entire IoT/OT environment, including devices that do not have built-in security agents.

One of the key benefits of Defender for IoT is its agentless, network layer monitoring, which ensures that all devices in your environment are secure and protected against potential threats. Additionally, the platform integrates seamlessly with both industrial equipment and security operation center (SOC) tools, allowing you to easily manage your entire security infrastructure from a single, centralized location.

By leveraging the power of Microsoft Defender for IoT, you can rest assured that your IoT and OT devices are protected against known and emerging threats, ensuring the safety and security of your entire organization.

To learn more, watch this video:

<https://youtu.be/G555j-z5Y3I>

Contents

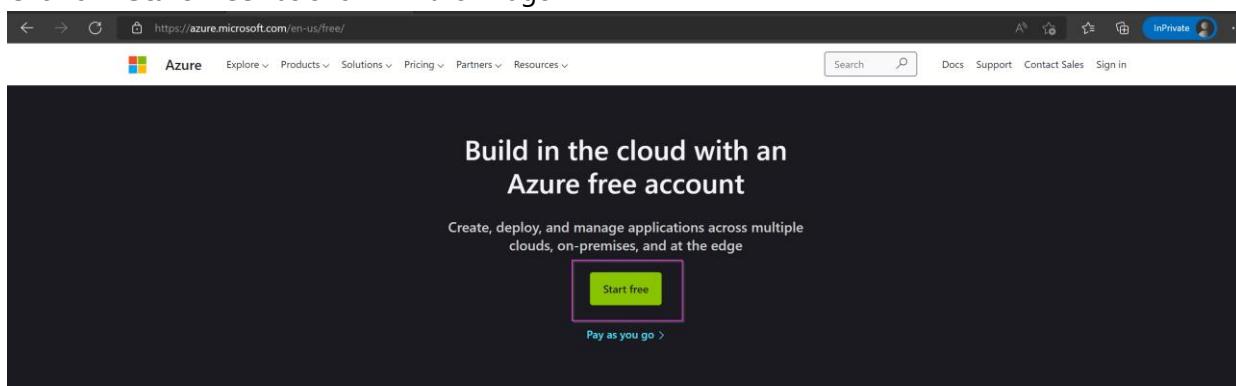
Summary.....	1
!! Since the PDF contains hyperlinks, please download the file before proceeding!!.....	1
Architecture Diagram.....	1
What is Microsoft Defender for IoT?	1
Exercise 1: Enabling Defender	3
Task 1: Create an Azure Subscription	3
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	4
Exercise 2: Deploy the Sensor in Azure.....	6
Task 1: Create a Resource group to automatically deploy your sensor, storage account and network security group to.....	6
Task 2: Access your Virtual Machine.	8
Task 3: Access your sensor via the console	14
Exercise 3: Simulate Data in your sensor.....	20
Task 1: Enabling the PCAP Player.....	20
Task 2: Play PCAP files.....	22
Exercise 4: Analyzing the Data	24
Task 1: Visualize on the Device Map	24
Task 2: View the associated Alerts	26
Task 3: Device Inventory	28
Task 4: View the Event Timeline	29
Task 5: Data Mining	30
Task 6: Generate a Risk Assessment report.....	31
Exercise 5: Cloud Connect your sensor.....	32
Task 1: Create the cloud connected sensor on the Cloud Management portal	32
Task 2: Upload the activation file to cloud connect your sensor.	33
Task 3: Verify Cloud connection.....	34
Exercise 6: Manage your sensor via the Cloud Management Portal.....	35
Task 1: Role Based Access Control on your sites and Sensors.....	35

Task 2 : Manage your devices.....	37
Task 3: View your Alerts	39
Task 4: View your recommendations	40
Task 5: Visualize Data by utilizing Workbooks	41
Exercise 7: Integrate with Microsoft Sentinel	42
Task 1: Create a Log Analytics Workspace.....	42
Task 2: Install the Defender for IoT package.....	44
Task 3: Create Incidents.....	47
Task 4: Validate Defender for IoT logs are streamed correctly to Sentinel (KQLS on the data)	48
Task 5: Investigate Defender for IoT incidents	49
Task 6: Investigate further with IoT device entities	51
Task 7: Investigate the alert in Defender for IoT	52
Task 8: Acknowledge Alerts and Re-run PCAPs.....	53
Exercise 8: Automate response to Defender for IoT alerts.....	54
Exercise 9: Clean Up	54
Task 1: Delete resources.....	54
Exercise 10: Submit Feedback	54
Appendix:.....	54

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 search bar at the top has 'Subs' typed into it. Below the search bar, there are tabs for 'All', 'Services (12)', 'Resources (1)', 'Marketplace (20)', 'Resource Groups (0)', and 'Documentation (0)'. The 'All' tab is selected. Under the 'Services' heading, 'Subscriptions' is highlighted with a pink box. Other listed services include Event Hubs Clusters, Event Grid Subscriptions, Event Hubs, Web PubSub Service, Notification Hubs, Device Update for IoT Hubs, and Azure Synapse Analytics (private link hubs). The 'Resources' section shows a Visual Studio Enterprise Subscription (Subscription), Marketplace items like Autonomous Anomaly Detection and JewelSuite Subsurface Modeling, and other subscriptions from providers like NTT DATA and SWIFT DR. At the bottom, there are links for 'Give feedback' and 'See all'. The 'Navigate' section at the bottom includes links for 'Subscriptions', 'Resource groups', 'All resources', and 'Dashboard'.

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

The screenshot shows the 'Subscriptions' blade in the Azure portal. The title is 'Subscriptions'. There are buttons for '+ Add', 'Manage Policies', and 'View Requests'. A search bar shows 'Search for any field...' and filters for 'Subscriptions == global filter', 'My role == all', 'Status == all', and 'Add filter'. Below the filters, it says 'Showing 1 to 1 of 1'. A table lists one subscription: 'Visual Studio Enterprise Subscription' with ID '21311d18-92b6-4c00-b137-937eb90512a', 'Account admin' as the 'My role', 'C\$511.29' as 'Current cost', '41%' as 'Secure Score', and 'Active' as 'Status'. The table has columns for 'Subscription name', 'Subscription ID', 'My role', 'Current cost', 'Secure Score', 'Parent management group', and 'Status'.

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

See all

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
- Integrate Palo Alto with Microsoft Defender for IoT ...
- Manage subscriptions - Azure Defender for IoT | Microsoft Docs
- Microsoft Defender for IoT trial setup - Azure Defender ...
- What is agentless solution architecture - Azure Defender ...

Azure Active Directory

Microsoft Defender for IoT Micro agent Public Preview
mst4iot-micro-agent-public@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

Partial data is shown because you have limited permissions to some of your subscriptions. Make sure you have Security Reader permissions on the relevant subscriptions to view related data.

General

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

Management

- Sites and sensors
- Pricing**
- 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

Partial data is shown because you have limited permissions to some of your subscriptions. Make sure you have Security Reader permissions on the relevant subscriptions to view related data.

General

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

Management

- Sites and sensors
- Pricing**
- Settings (Preview)

No subscriptions onboarded

Define committed device coverage or work with the trial.

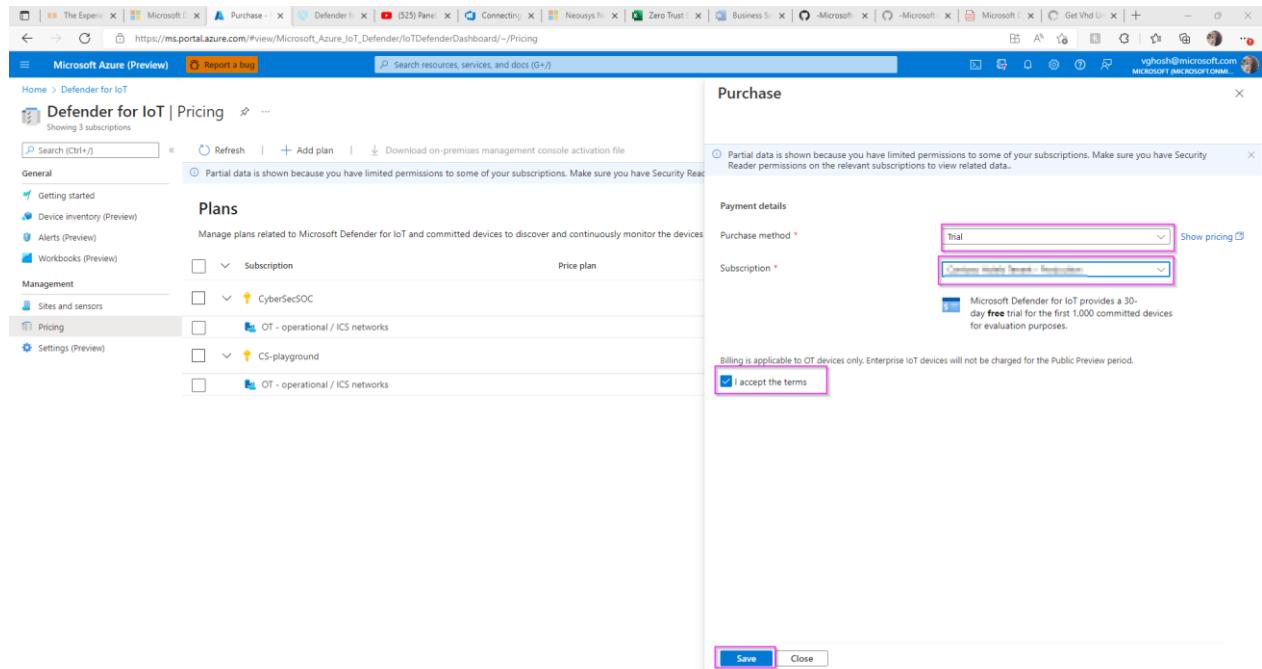
Onboard subscription

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

4. In the popup screen, select:

- Purchase Method: Trail**

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



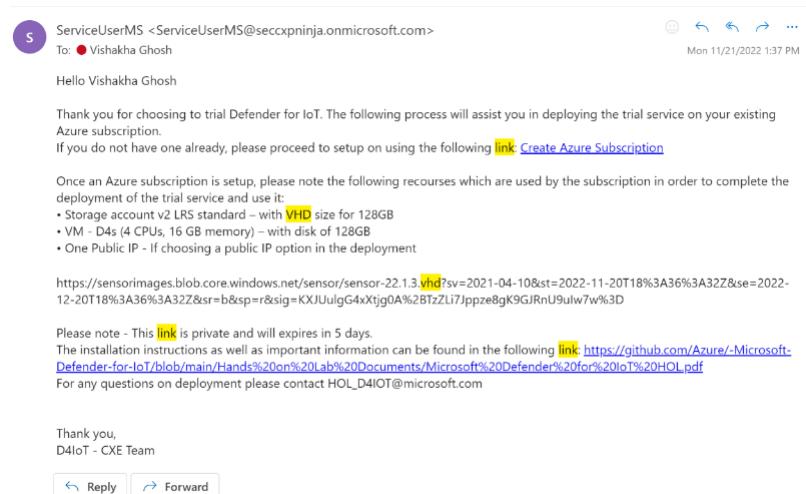
You now have a valid Microsoft Defender for IoT Trial with **1000 committed devices**. These devices represent all those equipment/sensors connected to your network in the facility you are analyzing. This configuration allows you a **30-day trial for free**.

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**. Please send a request via [this form](#) for a link for the IoT sensor installation. You will receive an email with the link once your request has been received.

It might go to your Junk/Spam by default. Please search for an email from ServiceUserMS@secxpnninja.onmicrosoft.com. It should look like this.



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:

The screenshot shows the Azure portal's 'Custom deployment' interface. At the top, there are tabs for 'Select a template', 'Basics', and 'Review + create'. The 'Basics' tab is active. Below it, there's a 'Template' section with a 'Customized template' card showing '4 resources'. To the right are three buttons: 'Edit template', 'Edit parameters', and 'Visualize'. The main area is titled 'Project details' and contains the following fields:

- Subscription *: A dropdown menu currently set to 'BuildEnv'.
- Resource group *: A dropdown menu with a 'Create new' option.
- Region *: A dropdown menu set to 'East US'.
- Location: A dropdown menu set to '[resourceGroup().location]'.
- Deploy Public IP: A dropdown menu set to 'true'.
- Put Password To Key Vault: A dropdown menu set to 'true'.
- Source VHDURL *: An empty input field.
- Sensor Count: An input field set to '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. **Please make sure there are no extra spaces after the link when you paste it.**
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

Terms

Azure Marketplace Terms | Azure 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.

Microsoft.Template-20220713114358 | Overview

Your deployment is complete

Deployment name: Microsoft.Template-20220713114358 Start time: 7/13/2022, 11:44:03 AM

Subscription: Bullshin Correlation ID: #0166659-4efc-4268-b168-5c8887ada95e

Resource group: KeyVaultTest

Deployment details (Download)

Resource	Type	Status	Operation details
Reset-password0	Microsoft.Resources/deployments	OK	Operation details
Post-Deploy0	Microsoft.Resources/deployments	OK	Operation details
VM-deployment	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.

KeyVaultTest

Subscription (move): BuildEnv Deployments: 2 Failed 10 Succeeded

Location: West US

Tags (edit): createdate: 07/13/2022 owner: vghosh

Resources Recommendations

Name	Type	Location
customxx245p7rgp0	Storage account	West US
SOC_Kv245p7rgp2_Pay	Key vault	West US
SOC_NS0d245p7rgp2_Pay	Network security group	West US
SOC_minstanzy245p7rgp2_Pay	Managed identity	West US
SOC_m245p7rgp2_Pay-image	Image	West US
SOC_vmr245p7rgp2_Pay-red10	Regular Network Interface	West US
SOC_wmz245p7rgp2_Pay-pg0	Public IP Address	West US
SOC_wmz245p7rgp2_Pay-red10	Virtual machine	West US
SOC_wmz245p7rgp2_Pay-disk1	Disk	West US
SOC_vnres245p7rgp2_Pay	Virtual network	West US

3. Select the application and click on "Access Policies" -> "+Create".

(If you have deployed multiple sensors and subsequently have multiple keys, you can use the instructions given in the appendix to export the keys instead of copying them 1 by 1).

4. Under "Permissions" select "Key & Secret Management" template.

5. Under "Principle" select a principle

Home > Resource groups > KeyVaultTest > SOC-KVuq63gjmwvo2do-Play | Access policies >

Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

Permissions Principal Application (optional) Review + create

Only 1 principal can be assigned per access policy.

Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Search by object ID, name, or email address

- [John Doe](#)
- [Administrators](#)
- [Jane Smith](#)
- [Power users](#)
- [Alice Johnson](#)
- [Developers](#)

Selected item

No item selected

6. You can skip over "Application".

Home > Resource groups > KeyVaultTest > SOC-KVuq63gjmwvo2do-Play | Access policies >

Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

Permissions Principal Application (optional) Review + create

Authorizes this application to perform the specified permissions on the User's or Group's behalf.
Use the new embedded experience to select an application. The previous popup experience can be accessed here. [Select an application](#)

Search by object ID, name, or email address

- 5d62bf487ee14fb8884e9582f29be8e1-977f-4fa3-bf83-957308750ff
- AcmeDnsValidator-ting0113im0604fb01b-9fe8-4926-b954-b922680cbf40
- aksdemoSP-20200512091755b59a0f98-632d-403b-987c-68a88ccf81c0
- amasf7056827c-0953-418c-9426-f6890b2f9e79
- aml-94dec3a3-89b7-402c-a6a6-3db32f3b2d40b179caab-f3fc-4162-a465-ea5e6f54087
- aml-9f876ca0-654b-468b-8d6b-abf6aa26fceeb0b34bd9-e88b-46f0-adf8-c7ce00a9954

Selected item

No item selected

Previous

Next

7. Click on "Create".

Home > Resource groups > KeyVaultTest > SOC-KVuq63gjmwvo2do-Play | Access policies >

Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

Permissions Principal Application (optional) **Review + create**

Key Permissions

Key Management Operations	All selected
Cryptographic Operations	None selected
Privileged Key Operations	None selected
Rotation Policy Operations	All selected

Secret Permissions

Secret Management Operations	All selected
Privileged Secret Operations	None selected

Certificate Permissions

Certificate Management Operations	None selected
Privileged Certificate Operations	None selected

Principal

Principal name	Vishakha Ghosh
Object ID	4d53f3b7-e555-4354-a330-193b4cd1ef28

Application

Authorized application ⓘ	None selected
Object ID	None selected

Create

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

Home > Microsoft.Template_20200713114358 > KeyVaultTest

KeyVaultTest Resource group

Overview + Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Open in mobile

Subscription (main) : BuildEnv Deployments : 2 Failed 10 Succeeded

Subscription ID : 1c61ccbf-70b1-45a3-a1fb-84fc446d70a6 Location : West US

Tags (edit) : createdate : 07/13/2022 , owner : vghosh

Resources Recommendations

Filter for any field... Type equals all Location equals all Add filter

Show 1 to 10 of 10 records. Show hidden types

Type	Location	...
Storage account	West US	...
Key vault	West US	...
Network security group	West US	...
Managed identity	West US	...
Image	West US	...
Regular Network Interface	West US	...
Public IP address	West US	...
Virtual machine	West US	...
Disk	West US	...

9. 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

Operating system : Linux (ubuntu 18.04)

Size : Standard D4s v3 (4 vcpus, 16 GiB memory)

Public IP address : **20.124.23.178**

Virtual network/subnet : SOC- Play/default

DNS name : Not configured

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine

Computer name	Sensor
Health state	-
Operating system	Linux (ubuntu 18.04)
Publisher	-
Offer	-
Plan	-

Networking

Public IP address	20.124.23.178
Public IP address (IPv6)	-
Private IP address	10.10.10.4
Private IP address (IPv6)	-
Virtual network/subnet	SOC-
DNS name	Configure

Option #2: If you deployed without Keyvault.

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

Microsoft.Template-20220630145822 | Overview

Your deployment is complete

Deployment name: Microsoft.Template-20220630145822 Start time: 6/30/2022, 2:58:25 PM
Subscription: BuildEnv Correlation ID: ac55ba5c-e35a-4a36-b3ee-37b01fcdb3f

Deployment details (Download)

Resource	Type	Status	Operation details
Reset-password0	Microsoft.Resources/deployments	OK	Operation details
Post-Deploy0	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](#)

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

Reset-password0 | Outputs

Deployment

vmObject

```
[{"VMName": "SOC-vmw7ne3eaow5oxw0-Play", "Password": "KChR9dMLp3VFkar2Yp8I99PM2V8="}]
```

Copied

Outputs

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

Your deployment is complete

Deployment name: Microsoft.Template-20220630145822
Subscription: BuildEnv
Resource group: Vghosh_IoTSensor

Resource	Type	Status	Operation details
Reset-password	Microsoft.Resources/deployments	OK	Operation details
Post-Deploy0	Microsoft.Resources/deployments	OK	Operation details
VMdeployment	Microsoft.Resources/deployments	OK	Operation details
copyvhd	Microsoft.Resources/deployments	OK	Operation details

Next steps

[Go to resource group](#)

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

Essentials

Subscription (move) : Deployment ID : 13_Succeeded
Subscription ID : Location : East US
Tags (edit) : Click here to add tags

Resources

Name	Type	Location
copyvhd	Deployment Script	East US
customflicwiéuSatkww	Storage account	East US
SOC NSGflicwiéuSatkww Play	Network security group	East US
SOC-vmflicwiéuSatkww-Play	Virtual machine	East US

5. Make a note of the Public IP address.

The screenshot shows the Azure portal interface for a virtual machine named 'SOC'. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Networking, Connect, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, and Continuous delivery. The main pane displays the 'Essentials' and 'Properties' tabs for the virtual machine. Under 'Essentials', the Public IP address is highlighted as 20.124.23.178. Under 'Properties', the Networking section highlights both the Public IP address (20.124.23.178) and the Private IP address (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://xxx.xxx.xxx.xxx /login>. The page title is "Microsoft | Defender for IoT sensor". The main content is a "Sensor Sign in" form with fields for "User name" and "Password". Below the fields are links for "Forgot password? (for admin users only)" and "Reset". 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**.

3. After signing out, please return to the Azure portal and navigate to "**Defender for IoT**". Select "**Sites and sensors**".
4. Click on "Onboard OT sensor".

Step 3: Register this sensor with Microsoft Defender for IoT

Sensor name *

Subscription *

Cloud connected ⓘ

Automatic Threat Intelligence updates

Sensor version *

Site *

Resource name *

No subscription has been selected

Create site

Display name *

Tags

Zone *

No subscription has been selected

Create zone

Add in a name for your sensor and pick your subscription from the dropdown. You can choose to cloud connect it. Pick your Resource name from the dropdown, give it a display name and a zone. This automatically initiates the download for the activation file.

5. Select your sensor from the list and click on "**Recover my password**".

Defender for IoT | Sites and sensors

Showing subscription 'BuildEnv'

General

Management

Sites and sensors (highlighted with a pink box)

Pricing

Sensor name	Sensor type	Zone	Subscription ...	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...	Threat...
D4IOTsensor-TT	EIoT	default	BuildEnv	22.1.3.4162	Unavailable	--	--	--	...
sensor-Cyber	OT cloud co...	default	BuildEnv		Disconnected	A week ago	5/25/2022	Automatic	...

Push Threat Intelligence update (highlighted with a pink box)

Recover my password (highlighted with a pink box)

Download activation file

Delete sensor

6. You will see this prompt asking for the "secret identifier".

Defender for IoT | Sites and sensors

Showing subscription 'BuildEnv'

General

Management

Sites and sensors (highlighted with a pink box)

Pricing

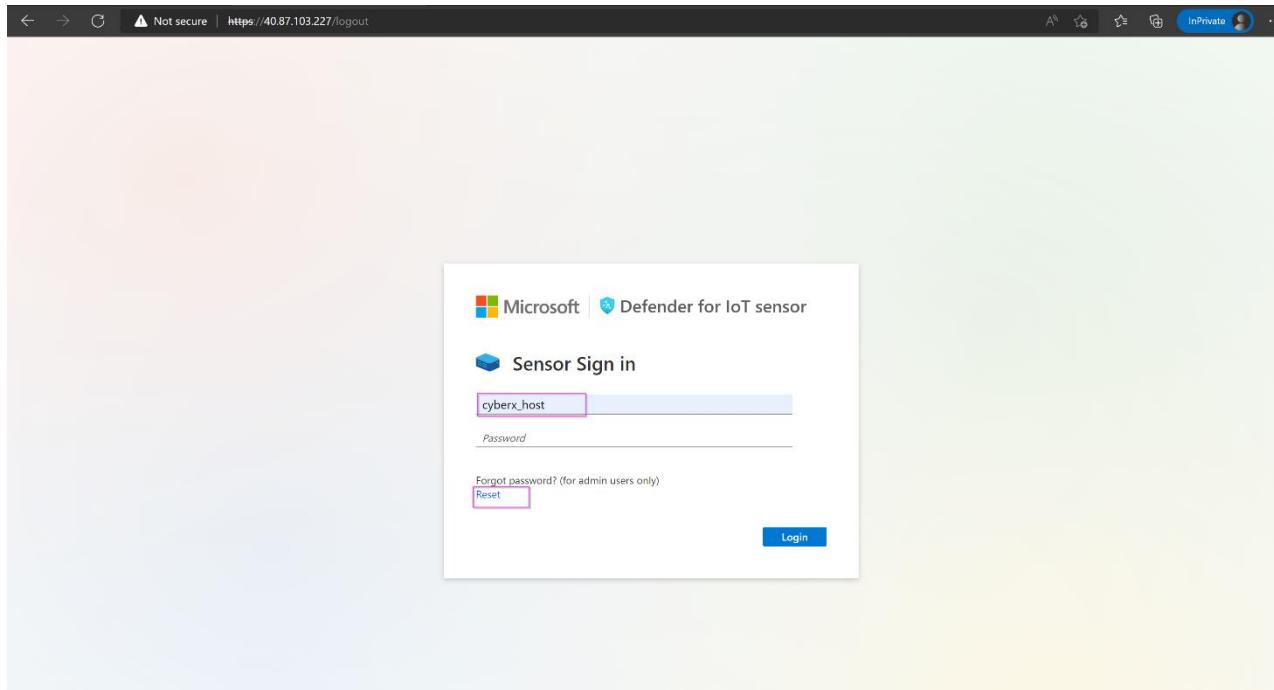
Recover

Insert secret identifier *

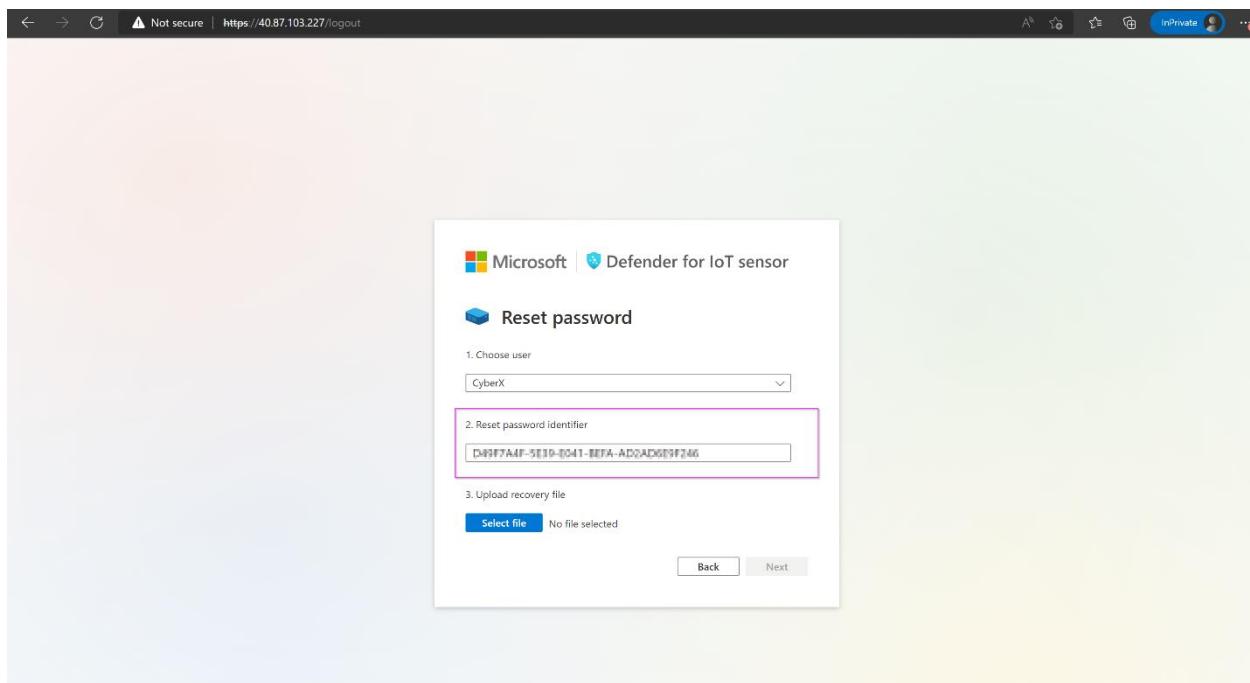
Sub0001-777-0e57-88h12

Recover Cancel

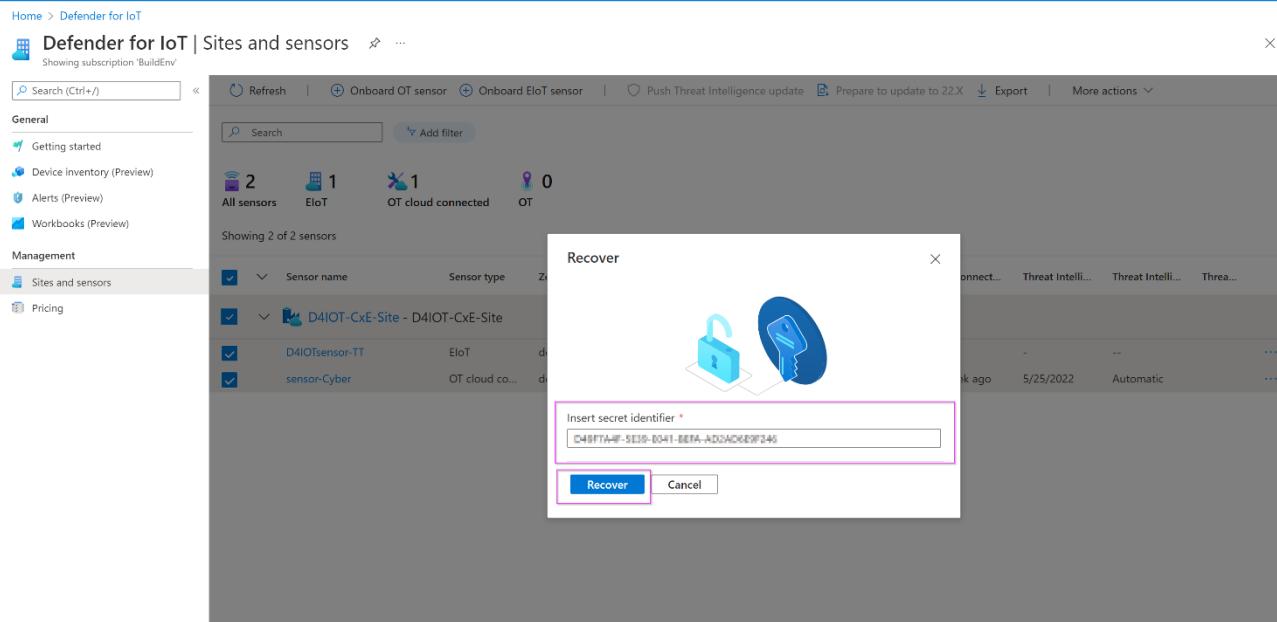
7. Return to the sensor console and type in the username followed by "Reset" as shown.



8. Copy the identifier.

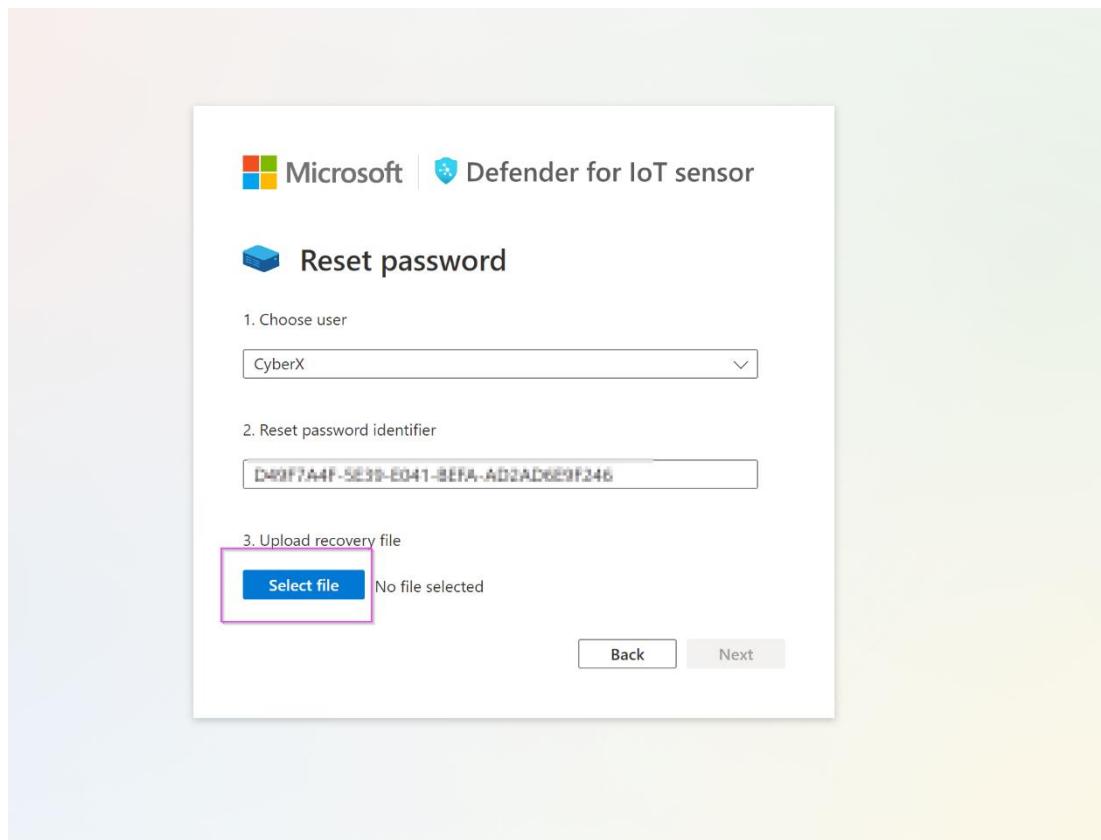


9. Paste in the box on the Defender for IoT Azure window. Click "**Recover**".



The screenshot shows the Microsoft Defender for IoT portal's 'Sites and sensors' page. At the top, there are counts for All sensors (2), EIoT (1), OT cloud connected (1), and OT (0). Below this, a table lists two sensors: 'D4IOT-CxE-Site - D4IOT-CxE-Site' and 'D4IOTsensor-TT'. A modal window titled 'Recover' is overlaid on the page, containing fields for 'Insert secret identifier' (with the value 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246') and 'Recover' and 'Cancel' buttons.

10. 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 for a Microsoft Defender for IoT sensor. Step 1: Choose user (CyberX selected). Step 2: Reset password identifier (D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246). Step 3: Upload recovery file (Select file button highlighted with a pink border). The 'No file selected' message is displayed below the file input field. At the bottom, there are 'Back' and 'Next' buttons.

11. Click on “**Next**”.

The screenshot shows the 'Reset password' process in Microsoft Defender for IoT sensor. Step 3, 'Upload recovery file', is highlighted with a pink box around the 'Select file' button and the uploaded file name 'password_recovery (1).zip'. The 'Next' button is also highlighted with a pink box.

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

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

The screenshot shows the 'Reset password' process in Microsoft Defender for IoT sensor. Step 4 displays a temporary password 'j^>h@WTU*7IP_jH' in a highlighted input field. The 'Next' button is highlighted with a pink box.

Microsoft | Defender for IoT sensor

Reset password

User name

CyberX_host

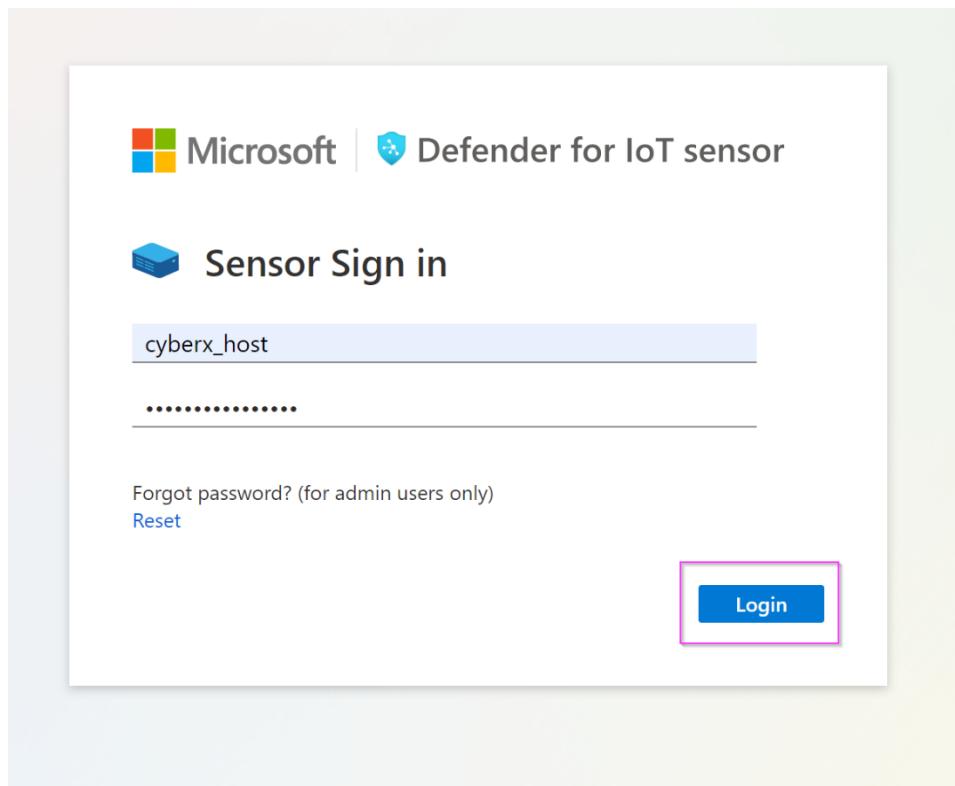
Password

j^>h@WTU*7IP_jH

Please write your password, it will not be shown again

Next

13. Log in with the new password.



14. 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 expanded "System settings" under the "Manage" heading. Other options in the sidebar include "Custom alert rules", "Users", and "Forwarding". The main content area features four cards under "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).

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 Home, System settings, Analyze, Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector, Manage, System settings, Custom alert rules, Users, and Forwarding. The main area is titled 'System settings' and contains sections for 'Backup data and restore the latest backup' and 'SNMP MIB Monitoring'. To the right, a large window is titled 'Advanced configurations' with a tab for 'Pcaps'. It displays configuration parameters such as 'cache.should.save.pcap=1', 'archive.cache.dir=' (with a note '# 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=' (with a note 'enabled_0'), and 'virtual.lan.hierarchy.depth.support=1'. At the bottom right of this window are 'Save' and 'Close' buttons, with the 'Save' button highlighted by 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 sidebar is identical to the previous screenshot. The main area shows sections for 'SSL/TLS Certificate' and 'Play PCAP'. The 'Play PCAP' section has a blue play icon and the text 'Upload and play PCAP files'. Below these sections, under the 'Manage' heading, is a button labeled 'Sensor management' with a gear icon, which is also highlighted by a red box. Other navigation items include 'Network monitoring', 'Integrations', and 'Import settings'.

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

Advanced configurations

Pcaps

```
size.megabytes.max=44032
archive.size.megabytes.max=
size.megabytes.min=17408
archive.size.megabytes.min=
cache.should.save.pcap=1
archive.cache.dir=
filtered.cache.dir.size.megabytes.max=7168
filtered.cache.dir.size.megabytes.min=3072
filtered.archive.dir.size.megabytes.max=
filtered.archive.dir.size.megabytes.min=
filtered.archive.dir=
playermax_size=10000
playermax_amount=200
playerparams=-M 20 #runs the pcaps faster in the UI
player_enabled=1
virtuallan.hierarchy.depth.support=1
filtered.timeout.seconds=10
```

Save

PCAP PLAYER

Upload and replay PCAP files.

pcap_wednesday.pcappng

Name	Date modified	Type
1-S7comm-VarService-Read-DB1DBD0	2022-06-15 3:45 PM	Wireshark capture file
2-S7comm-VarService-CyclicData-1s	2022-06-15 3:45 PM	Wireshark capture file
3-S7comm-VAT_MB100_MW200_MD300_M400-0	2022-06-15 3:45 PM	Wireshark capture file
4-S7comm-Download-DB1-with-password-req..	2022-06-15 3:45 PM	Wireshark capture file
Advantech	2022-06-15 3:45 PM	Wireshark capture file
BACnetARRAY-element-0	2022-06-15 3:45 PM	Wireshark capture file
BACnetARRAY-elements	2022-06-15 3:45 PM	Wireshark capture file
BA-Net-BBMD-on-same-subnet	2022-06-15 3:45 PM	Wireshark capture file
BACnet-exception-schedule-property-1	2022-06-15 3:45 PM	Wireshark capture file
BACnet-exception-schedule-property-2	2022-06-15 3:45 PM	Wireshark capture file

File name: 1-S7comm-VarService-Read-DB1DBD0

Upload Play All Clear All

pcap_wednesday.pcappng

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

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation menu with sections like Discover, Analyze, Manage, and Support. Under Manage, 'System settings' is selected. In the main content area, there are several cards: 'Sensor Network Settings', 'Connection to Management Console', 'Time & Region', 'SSL/TLS Certificate', 'Play PCAP' (which is highlighted with a pink box), and 'Network monitoring'. Below these, under 'Sensor management', are 'Software Update' and 'Threat Intelligence'. At the top right, there's a 'PCAP PLAYER' section with a 'Play All' button also highlighted with a pink box.

Exercise 4: Analyzing the Data

Task 1: Visualize on the Device Map

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

The screenshot shows the 'Device map' page. The left sidebar has the 'Device map' option selected (highlighted with a pink box). The main area displays a network topology map with various nodes represented by icons and colored dots (black, red, blue) indicating different device types or status. There are also some star-like symbols. On the left, there's a 'Groups' section with options like OT Protocol, Known Applications, Subnets, and Cross Subnet Connections. On the right, there are several icons for managing the map view.

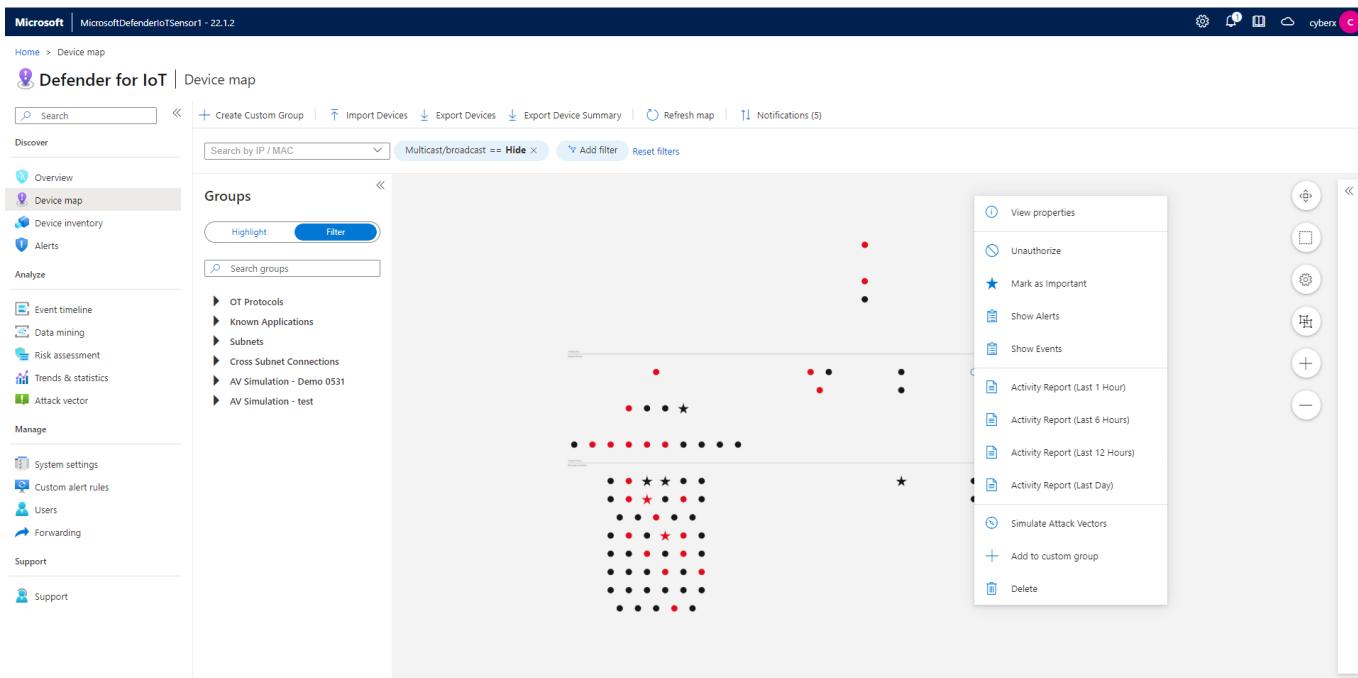
2. Click on the “Settings” option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.

The screenshot shows the Microsoft Defender for IoT Device map interface. On the left, there's a navigation sidebar with sections like Discover, Overview, Device map (which is selected), Device inventory, Alerts, Analyze, Manage, and Support. The main area displays a network graph where nodes represent devices and connections represent their relationships. A context menu is open in the top right corner, listing options: Pin Layout, Layout by Connections, and Layout by Purdue. The 'Layout by Purdue' option is highlighted with a pink box.

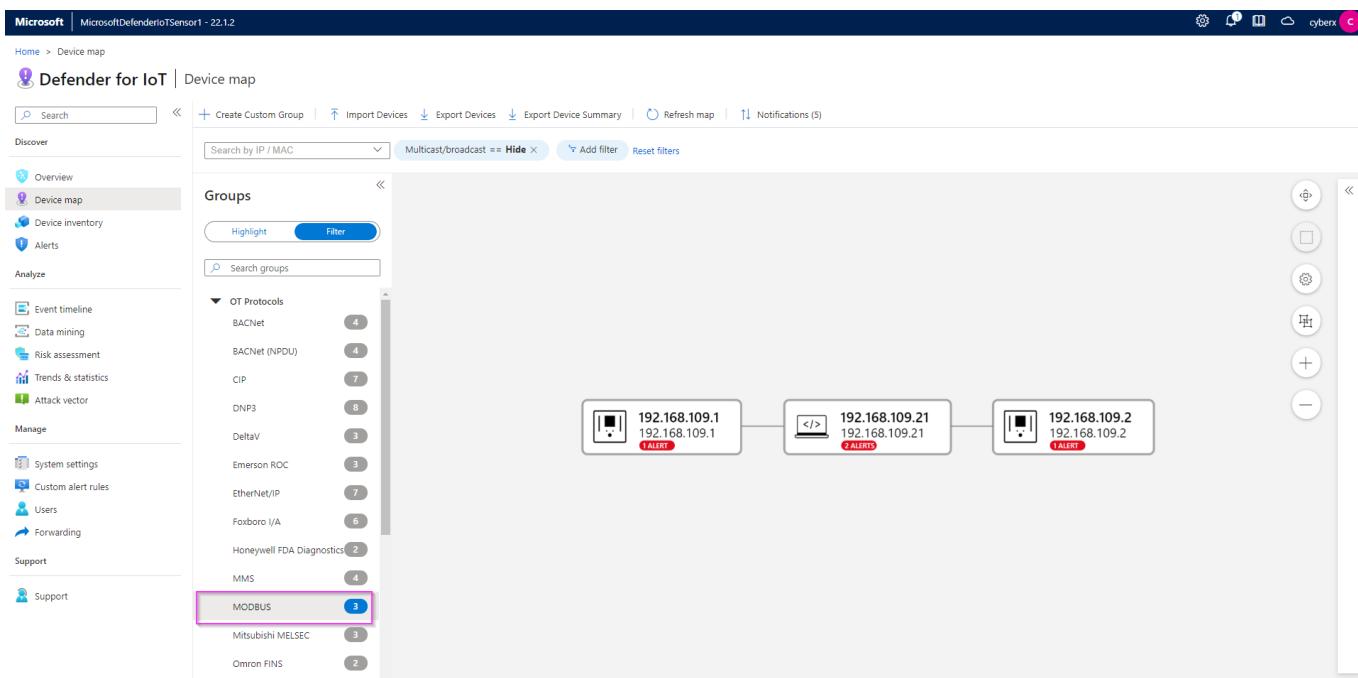
3. Once you confirm the changes, you will see the devices laid out as shown in the image below.

This screenshot shows the same Microsoft Defender for IoT Device map interface after applying the 'Layout by Purdue' changes. The network graph has been rearranged into a more organized, grid-like structure, making it easier to identify clusters of devices and their connections.

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

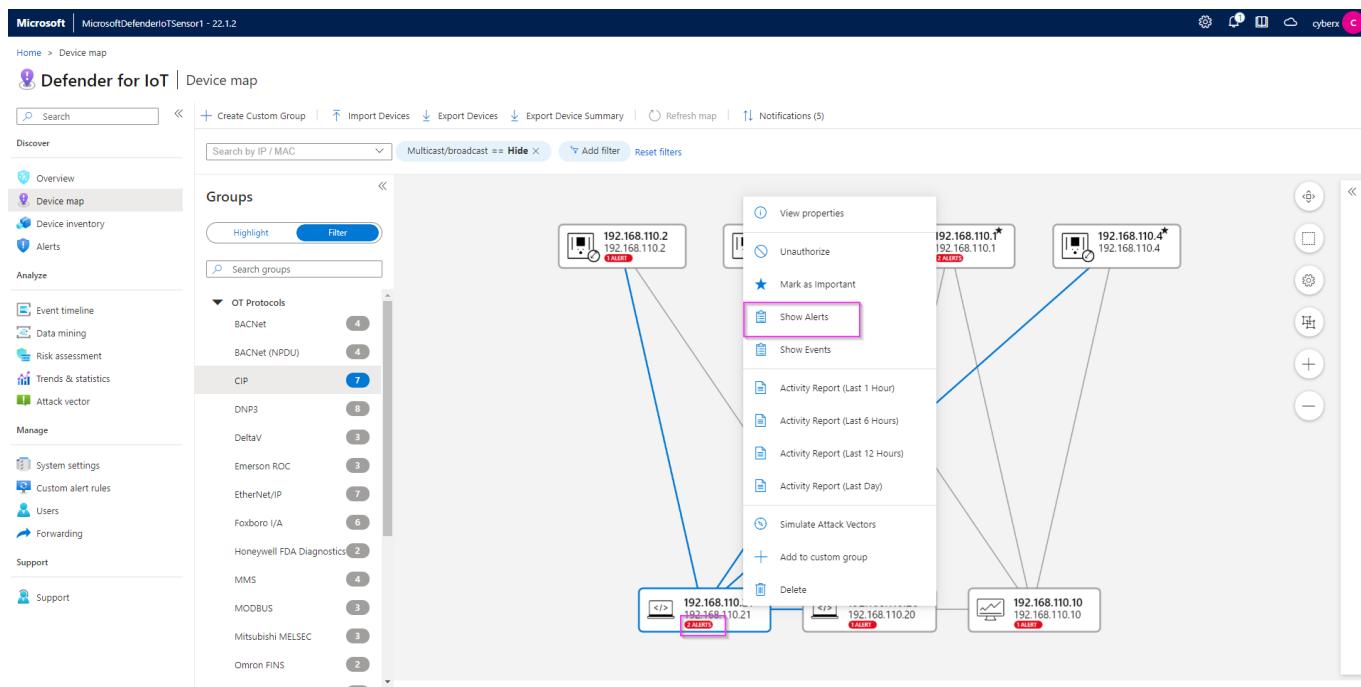


5.To filter by OT Protocols, expand the arrow, and pick the protocol you want to filter by. The console will display the devices that match the filter.



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 device details page for 192.168.110.21. The 'Alerts' tab is selected, displaying a list of 22 alerts. The table columns are: Severity, Name, Engine, Detection time, Status, and Source Device. The 'Severity' column is highlighted with a pink box. One alert entry is shown in detail:

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 interface. On the left, a sidebar menu has the 'Alerts' option highlighted with a red box. The main area displays a table of alerts. The first alert is for 'Unauthorized Internet Connectivity Detected' with a severity of 'Critical'. The second alert is also for 'Unauthorized Internet Connectivity Detected' with a severity of 'Critical'. Both alerts were detected 2 weeks ago and are marked as 'New'. A detailed view of the first alert is shown on the right, including its description, related devices, and action buttons.

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.

This screenshot shows the same Microsoft Defender for IoT interface, but with the 'Group by' dropdown set to 'Source Device'. The table now lists alerts grouped by their source device IP address. There are 22 alerts in total, mostly categorized as 'New' or 'Closed'. The 'Alerts' option in the sidebar is again highlighted with a red box.

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
<input type="checkbox"/>	192.168.100.8	192.168.100.8	50 minutes ago	Unknown	DNS, MDNS, Net...	54:14:f3:74:d8:21	INTEL CORPORA...					
<input type="checkbox"/>	192.168.100.1	192.168.100.1	50 minutes ago	Server	DNS							
<input type="checkbox"/>	192.168.1.11	192.168.1.11	50 minutes ago	PLC	Siemens S7	00:fb:54:db:ef:3	NETGEAR					
<input type="checkbox"/>	192.168.1.180	192.168.1.180	50 minutes ago	HMI	Siemens S7							
<input type="checkbox"/>	192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:92:c6	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	00:23:ea:49:8a:c2	CISCO SYSTEMS ...					
<input type="checkbox"/>	192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:97:c0	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	00:cc:1c:02:09:da	EATON CORPOR...					
<input type="checkbox"/>	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)			
<input type="checkbox"/>	192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SICAM	00:0c:29:28:28:38	VMWARE INC.					
<input type="checkbox"/>	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)			
<input type="checkbox"/>	192.168.107.10	FCS0507	22 hours ago	DCS Controller	Yokogawa VNet/IP	00:00:64:9d:5d:10	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9d:73:d4	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9e:84:e5	YOKOGAWA DIG...					
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	

Load More...

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

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...	54:14: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	00:fb:54:db:ef:3	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...)	00:30:a7:08:92:c6	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	00:23:ea:49:8a:c2	CISCO SYSTEMS ...					
<input type="checkbox"/>	192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:97:c0	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	00:cc:1c:02:09:da	EATON CORPOR...					
<input type="checkbox"/>	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)			
<input type="checkbox"/>	192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SICAM	00:0c:29:28:28:38	VMWARE INC.					
<input type="checkbox"/>	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)			
<input type="checkbox"/>	192.168.107.10	FCS0507	22 hours ago	DCS Controller	Yokogawa VNet/IP	00:00:64:9d:5d:10	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9d:73:d4	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9e:84:e5	YOKOGAWA DIG...					
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	

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".

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with various sections like Overview, Device map, Device inventory, Alerts, Analyze, Manage, Support, and Help. The 'Event timeline' section is currently selected. The main area displays a table of events. The columns are 'Event type', 'Time', and 'Description'. Some examples of events listed include 'Device Detected' (Device 192.168.1.180 was detected), 'Device Connection Detected' (Connected devices 192.168.1.11 and 192.168.1.180), and multiple entries for 'Firmware Update' and 'PLC Reset' from different IP addresses.

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 navigation sidebar. In the center, there's a 'Create new report' wizard. It has fields for 'Name' (Report name), 'Description', 'Send to CM' (checkbox), 'Choose Category' (dropdown with 'Category' and 'Activity' options), 'Order by' (dropdown), 'Filter by' (with sub-options for 'Results within the last', 'IP address', 'MAC address', 'Port', and 'Device group'), and a search bar. At the bottom, there are 'Save' and 'Cancel' buttons.

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

Create new report

Name *

Description

PLC Firmware Version Report showing the firmware version of the different PLCs.

Choose Category

Order by

Filter by

Results within the last Minutes +

IP address

MAC address

Port

Device group

Firmware Version (GENERIC)

+ Add filter type

Save Cancel

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

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.

Defender for IoT | Data mining

Refresh Expand all Collapse all Export to CSV Export to PDF Snapshots Manage report Edit mode

PLC Firmware Version

Report showing the firmware version of the different PLCs.

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.

The screenshot shows the Microsoft Defender for IoT Risk assessment interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, and Manage. Under Analyze, the 'Risk assessment' option is selected and highlighted with a pink box. In the main content area, there's a 'Reports list' table with four entries. The first entry, 'risk-assessment-report-4.pdf', is also highlighted with a pink box. A 'Generate report' button is located above the 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 Defender for IoT Sites and sensors page. The left sidebar has sections like General, Management, and Pricing, with 'Sites and sensors' selected and highlighted with a pink box. The main area displays sensor counts: All sensors (4), EIoT (1), OT cloud connected (2), and OT (1). Below this, a table lists four sensors, both locally managed and cloud connected.

Sensor name	Sensor type	Zone	Subscription ...	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...
D4IOT-CxE-Site - D4IOT-CxE-Site	Locally managed							

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

Step 3: Register this sensor with Microsoft Defender for IoT

Sensor name *

Subscription * Please select a subscription
Onboard subscription

Cloud connected ⓘ

Automatic Threat Intelligence updates

Sensor version * 22.X and above

Site *

- Resource name *** No subscription has been selected
Create site
- Display name ***
- Tags** Key : Value

Zone * No subscription has been selected
Create zone

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

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

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

Home > System settings

Defender for IoT | System settings

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

Sensor management

Updates

- Software Update
- Threat Intelligence

Subscription & Activation Mode

Upload an activation file to reactivate this sensor

Security

Health and troubleshooting

- Backup & Restore
- System Health Check
- SNMP MIB Monitoring

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

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. The main area has sections for Updates (Software Update, Threat Intelligence), Security (Subscription & Activation Mode), Health and troubleshooting (Backup & Restore, System Health Check). A right-hand panel titled 'Subscription & Activation Mode' displays activation status: Activation Mode is 'Cloud Connected', Activation Status is 'Active', Tenant ID is '5f1d60f2-d8a4-4f50-bf0c-1dd1813604a4b', and Subscription ID is '1cb61ccdf1-70d3-4fa3-a7fb-848ca65c10a6'. It also includes a 'Select file' button for uploading an activation file.

Task 3: Verify Cloud connection

1. On the sensor console.

The screenshot shows the Microsoft Defender for IoT Overview page. It features a summary section with metrics: 0 PPS, 64 Devices, and 21 Alerts. Below this are four cards: General Settings (Version 22.1.3.4162, Threat Intelligence Version 2022.07.12, Connectivity type Cloud connected, Activation Valid, Certificate Valid), Traffic Monitoring (No chart to show), Top 5 OT Protocols, and Traffic By Port. The left sidebar mirrors the one from the previous screenshot, listing Overview, Device map, Device inventory, Alerts, Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector, System settings, Custom alert rules, and Users.

2. On the Cloud management console.

The screenshot shows the Microsoft Defender for IoT Cloud Management Portal. The top navigation bar includes 'Home', 'Defender for IoT | Sites and sensors', and 'More actions'. A banner at the top right indicates a 'Trial subscription "BuildEnv" expired. Please contact Microsoft sales.' Below this, the 'General' section has links for 'Getting started', 'Device inventory (Preview)', 'Alerts (Preview)', and 'Workbooks (Preview)'. The 'Management' section shows 'Sites and sensors' selected, with a sub-section for 'Pricing'. The main content area displays a table of sensors:

Sensor name	Sensor type	Zone	Subscription ...	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...	Threat...
D4IOTsensor-TT	EIoT	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	...
test123	OT cloud co...	default	BuildEnv	22.1.3.4162	OK	19 minutes a...	7/11/2022	Automatic	...

Exercise 6: Manage your sensor via the Cloud Management Portal

The cloud management portal serves as a central management tool when you deploy multiple sensors, and gives you a consolidated view of all the devices, alerts and incidents across different sites and zones.

Task 1: Role Based Access Control on your sites and Sensors

1.Click on the site you just created. When the "Edit Site" panel on the side opens up, click on "Manage Site Access Control".

The screenshot shows the Microsoft Defender for IoT Cloud Management Portal. The top navigation bar includes 'Home', 'Defender for IoT | Sites and sensors', and 'More actions'. A banner at the top right indicates 'You have exceeded the maximum number of devices for your subscription. Get more device coverage'. Below this, the 'General' section has links for 'Getting started', 'Device inventory', 'Alerts', 'Incidents (Preview)', 'Recommendations (Preview)', 'Workbooks', and 'Firmware analysis (Preview)'. The 'Management' section shows 'Sites and sensors' selected, with a sub-section for 'Plans and pricing' and 'Settings (Preview)'. The main content area displays a table of sites:

Sensor name	Sensor type	Zone	Subscription ...	Sensor health	Sensor version
Ah2225	OT - Cloud conn.	default	CS-playground	No traffic...	23.1.2
BetterTogetherSite	BettertogetherSite				
cs-playground	VishakhaSensor				
cybersecurityiohub	Hub				
Enterprise-network	Enterprise network				
Muli	Muli				
testsitename	TestSiteName				
tresttesttest	TestTestTest				
Locally managed					

An 'Edit site' panel is open on the right, showing fields for 'Site resource name' (cs-playground), 'Display name' (VishakhaSensor), 'Owners' (example@mail.com), and 'Tags' (Key: Value). A button labeled 'Manage site access control (Preview)' is highlighted with a pink box.

2.Click on "Add role assignment".

[Home](#) > [Defender for IoT | Sites and sensors](#) >

Access Control

My access
View my level of access to this resource.

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Grant access to this resource
Grant access to resources by assigning a role. [Learn more](#)

View access to this resource
View the role assignments that grant access to this and other resources. [Learn more](#)

View deny assignments
View the role assignments that have been denied access to specific actions at this scope. [Learn more](#)

3.Type the security role you would like to grant and select it from the list. For example: "Security Reader".

Add role assignment

Role Members * Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Assignment type

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Name	Description	Type	Category	Details
D4IoT Security Analyst2	Defender for IoT security analyst role can conduct the following operations: - Edit alerts (change status, learn, download PCAP) - View Alert suppression rules	CustomRole	None	View
Security Admin	Security Admin Role	BuiltinRole	Security	View
Security Reader	Security Reader Role	BuiltinRole	Security	View

Showing 1 - 3 of 3 results.

4.Click on "Members" -> "+Select Members". Type the name of the user you want to assign the role to.

Add role assignment

Role Members * Review + assign

Selected role Security Reader

Assign access to User, group, or service principal

Members + Select members

Description Optional

Select Search by name or email address

- Alvin1_Wu (Guest) Alvin1_Wu@pegatroncorp.com
- Cara_Pham (Guest) Cara_Pham@pegatroncorp.com
- James55_Liu (Guest) James55_Liu@pegatroncorp.com
- Owen_Chen (Guest) Owen_Chen@pegatroncorp.com
- QuanLind_Zhao (Guest) QuanLind_Zhao@pegatroncorp.com

Vishakha Ghosh vghosh@microsoft.com Remove

5.Click on review and assign after reviewing the permission level and the user.

Add role assignment ...

Selected role Security Reader

Assign access to User, group, or service principal Managed identity

Members [+Select members](#)

Name	Object ID	Type
Vishakha Ghosh	4d53f3b7-e555-4354-a330-193b4cd1ef28	User

Description Optional

[Review + assign](#) [Previous](#) [Next](#)

6. To review permissions, go to “Role Assignments”, and change “Scope = This Resource”. This allows you to audit who has what level of permissions.

Access Control ...

Number of role assignments for this subscription 116 / 4000

Check access [Role assignments](#) Roles Deny assignments Classic administrators

Name	Type	Role	Scope	Condition
D4IoT Security Analyst2	User	Contributor	This resource	None
Vishakha Ghosh	User	Security Admin	This resource	None
Vishakha Ghosh	User	Security Reader	This resource	None

Task 2 : Manage your devices

1. Click on “Device Inventory”, and see your total number of devices, new devices, and classification of devices.

Device inventory

Total devices 447 **New devices** 78

Devices by class

- OT (105)
- Endpoint (86)
- Network (20)
- IoT (6)

Site	IPv4 address	Name	Type	Subtype	Vendor	Model	MAC address	VLAN
cs-playground	192.168.111.1	192.168.111.1	Industrial	DCS controller	FISHER CONTROLS	DeltaV MD/MD Plus	00:80:74:02:0F:42	--
cs-playground	192.168.111.20	192.168.111.20	Industrial	Engineering station	DELL INC.	--	18:66:DA:FA:4B:0C	--
cs-playground	192.168.111.2	192.168.111.2	Industrial	DCS controller	FISHER CONTROLS	DeltaV MD/MD Plus	00:80:74:02:0F:44	--
cs-playground	192.168.109.1	PLC_B	Industrial	PLC	INTEL CORPORATE	BME P58 1020	00:1C:C0:5F:49:0C	--
cs-playground	192.168.118.4	PLC_A	Industrial	PLC	SIEMENS AG	6ES7 315-2EH14-0A	00:01:E3:11:22:34	--
cs-playground	192.168.114.2	192.168.114.2	Industrial	Engineering station	MITSUBISHI ELECTR	QJ71GF11-T2	58:52:8A:B4:B1:4D	--
cs-playground	192.168.122.21	192.168.122.21	Industrial	Engineering station	--	--	--	--
b25eiottlab	192.168.0.17	192.168.0.17	Industrial	PLC	Acuity Brands Lighti	255F T2550 PAC	00:11:00:4E:51:62	--
b25eiottlab	192.168.0.3	192.168.0.3	Industrial	PLC	KNX LTD.	BACnet Server	00:C0:72:3F:FF:A3	--

2. Click on any device to open details about that device.

The screenshot shows a list of devices under the 'Site' column, with 10.140.32.30 selected. The details pane on the right shows the following information for 10.140.32.30:

- Address:** 10.140.32.30
- Type:** Unclassified
- Vendor:** PROCURVE NETWORKING BY HP
- Status:** Authorized (7 days ago, Last Seen 7 days ago)
- Network interfaces:** IP 10.140.32.30, MAC 00:16:B9:8C:AB:00
- Protocols:** SNMP
- Tags:** 10.140.32.0/24, 10.9.14.0/24-10.140.32.0/24

3.Click on "View Full Details" to open the full device page.

The full device details page for 10.140.32.30 includes the following sections:

- General information:** Type: Unclassified, Subtype: Unclassified; Vendor: PROCURVE NETWORKING BY HP, Location: cs-playground | EMEA | Supervisory.
- Network interfaces:** IP: 10.140.32.30, MAC: 00:16:B9:8C:AB:00.
- Protocols:** SNMP.
- Tags:** 10.140.32.0/24, 10.9.14.0/24-10.140.32.0/24.
- Attributes:** A table showing device attributes like Authorization (Authorized), Class (Unclassified), Data source (OT sensor), First seen (3/8/2023, 11:54:19 a.m.), Importance (Normal), Last activity (3/9/2023, 4:56:05 a.m.), Network location (Local), Parent slot (0), Programming device (No), Protocols (SNMP), Purdue level (Supervisory), Rack (0), Scanner device (No), Sensor (css-eee-1722024942), Site (cs-playground), and Subtype (Unclassified).

4.Click on the "Group by" dropdown, and pick any of the other options, for example: Zone or Vendor, to see the different views.

The Device inventory page shows the following interface:

- Device inventory:** Device count: 447 Total devices, 76 New devices.
- Devices by class:** OT (105), Endpoint (86), Network (20), IoT (6).
- Search and filters:** Search bar, Last active time: 03/02/2023 - 03/16/2023, Network location: All, Add filter.
- Group by:** A dropdown menu set to 'Vendor'.
- Table:** A list of 52 groups by vendor, including:
 - AAEON TECHNOLOGY INC. (24)
 - ACT'L (1)
 - Acuity Brands Lighting, Inc. (1)
 - AMERICAN POWER CONVERSION CORP (1)
 - AUTOMATEDLOGIC CORPORATION (1)
 - B&R INDUSTRIAL AUTOMATION GMBH (1)
 - BROCADE COMMUNICATIONS SYSTEMS LLC (1)

Task 3: View your Alerts

1. Click on the "Alerts" tab and view your Open Alerts, New Alerts and Alert count by severity.

The screenshot shows the Microsoft Defender for IoT Alerts page. At the top, there are three summary boxes: 'Open alerts' (584), 'New alerts' (584), and 'Active alerts' (0). Below these is a 'Severity' bar with three segments: High (228), Medium (196), and Low (160). The main area displays a table of 278 alerts, filtered by 'Last detection == Last month' and 'Status == 2 selected'. The table columns include Severity, Name, Site, Engine, First detection, Status, Source device, and Tactics. The alerts listed are mostly POLICY_VIOLATION type, primarily from b25eioltlab, involving unauthorized PLC programming and internet connectivity.

2. Click on any alert to see the details.

The screenshot shows the details of a specific alert titled 'Unauthorized Internet Connectiv...'. The alert ID is 95a746d9-021a-4223-819c-a8a73e9346de. The alert is categorized as High severity, New status, and occurred 21 hours ago. The description states: 'A device defined as part of your network is communicating with Internet addresses. The device is not authorized to communicate with Internet addresses.' The source device is 'Internet (137.220.100.146)' and the destination device is '192.168.0.110'. The alert is associated with the MITRE ATT&CK® framework.

3. Click on "View full details" to view the alert page.

Alerts | Unauthorized Internet Connectivity Detected

Refresh | Download PCAP

Unauthorized Internet Connectivity Detected

Alert ID: 95a746d9-021a-4223-819c-a8a73e9346de

Severity: High | **Status**: New | **Last detection**: 21 hours ago

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

Source device: Internet (137.220.100.146) Unknown → **Destination device**: 192.168.0.110 Unclassified

MITRE ATT&CK®

Tactics: Initial access

Initial access: The adversary is trying to get into your network. [read more on attack.mitre.org](#)

Techniques: Internet accessible device T0883

Alert details

Site	b25eiotlab
Internet	
Source device address	137.220.100.146
Zone	default
Destination device	192.168.0.110
Sensor	ahi2225
Destination device address	192.168.0.110
Category	Internet Access
Protocol	GENERIC

Take action

Device IP type	Internal
First detection (in the network)	3/15/2023, 6:08:42 p.m.
Last detection (in the network)	3/15/2023, 6:08:42 p.m.
Last activity (manual or automated changes)	3/15/2023, 10:18:00 p.m.

Entities

- Devices (1)**

ID	Name	Subtype	Protocols	Vendor
4d09a3fc-8818-42c7-a339-a5	192.168.0.110	Unclassified	FTP, MDNS, Netbios Name Se	INTEL CORPORATE
- IP (1)**

Address
137.220.100.146

4.Click on the "Group by" dropdown to view the alerts by severity, site, engine, etc.

Device inventory

Alerts

Incidents (Preview)

Recommendations (Preview)

Workbooks

Firmware inventory (Preview)

Management

Sites and sensors

Plans and pricing

Settings (Preview)

Troubleshooting + Support

Diagnose and solve problems

New support request (Preview)

Open alerts: 584

New alerts: 584

Active alerts: 0

Open alerts by severity

High (228) | Medium (196) | Low (160)

Search: Last detection == Last month | Status == 2 selected | Add filter

Showing 278 of 278 alerts

Group by: Severity

Severity	Name	Site	Engine	First detection	Status	Source device	Tactics
High (88)							
Low (96)							
Medium (94)							

Task 4: View your recommendations

1.Click on the "Recommendations" tab, to view the list of recommended fixes/remediation steps for alerts or misconfigurations on the sensors.

General

Getting started

Device inventory

Alerts

Recommendations (Preview)

Workbooks

Management

Sites and sensors

Plans and pricing

Settings (Preview)

Troubleshooting + Support

Diagnose and solve problems

Active recommendations: 2

Search: Unhealthy devices > 0 | Add filter

Showing 2 of 2 recommendations

Severity	Name	Unhealthy devices	Healthy devices	Last update time
Medium	Review PLC operating mode	16 devices	0 devices	3/20/2023
Low	Review unauthorized devices	31 devices	616 devices	3/20/2023

2.Click on any recommendation to view full details.

Review PLC operating mode

Description
To reduce the threat of malicious PLC programming, we recommend setting the PLC operating mode to the secure Run state if access is no longer required to this PLC.

Remediation steps

1. Check whether each PLC must be in unsecure state, such as Program or Remote.
2. If the PLC can be configured to the secure Run mode, check that the PLC has a physical key switch.
3. Do one of the following: If the PLC has a physical key switch, change the switch position to Run. If the PLC does not have a physical key switch, change the PLC operating mode to Run using the Engineering Station software.

Name	IP	Site	Last update time
EIP-Line1	192.168.110.1	bettertogethersite	3/20/2023
10.0.100.105	10.0.100.105	b25eiotlab	3/16/2023
192.168.0.17	192.168.0.17	b25eiotlab	3/15/2023
10.0.101.105	10.0.101.105	b25eiotlab	3/15/2023
10.0.101.110	10.0.101.110	b25eiotlab	3/15/2023
10.0.100.104	10.0.100.104	b25eiotlab	3/15/2023
10.0.100.110	10.0.100.110	b25eiotlab	3/15/2023
EIP-Line4	192.168.110.4	bettertogethersite	3/14/2023
192.168.90.122	192.168.90.122	cs-playground	3/12/2023
EIP-Line1	192.168.110.1	muli	3/1/2023
EIP-Line3	192.168.110.3	muli	3/1/2023
EIP-Line2	192.168.110.2	muli	3/1/2023
FIP-Line4	192.168.110.4	muli	3/1/2023

Task 5: Visualize Data by utilizing Workbooks

1. Click on the "Workbooks" tab, to view the list of Defender for IoT workbooks.

General

- Getting started
- Device inventory
- Alerts
- Recommendations (Preview)
- Workbooks**

Management

- Sites and sensors
- Plans and pricing
- Settings (Preview)

Troubleshooting + Support

- Diagnose and solve problems

Workbooks

All Workbooks Public Templates My Templates

Filter by name or category Subscription : CS-playground Resource Group : All Reset filters

Quick start

- Empty A completely empty workbook.

Recently modified workbooks (8)

- Alerts Specific
- Sensors Data
- Detected MAC
- Devices by Protocols
- ByOS type
- Workbook 3
- DeviceInvestigation
- Workbook 2

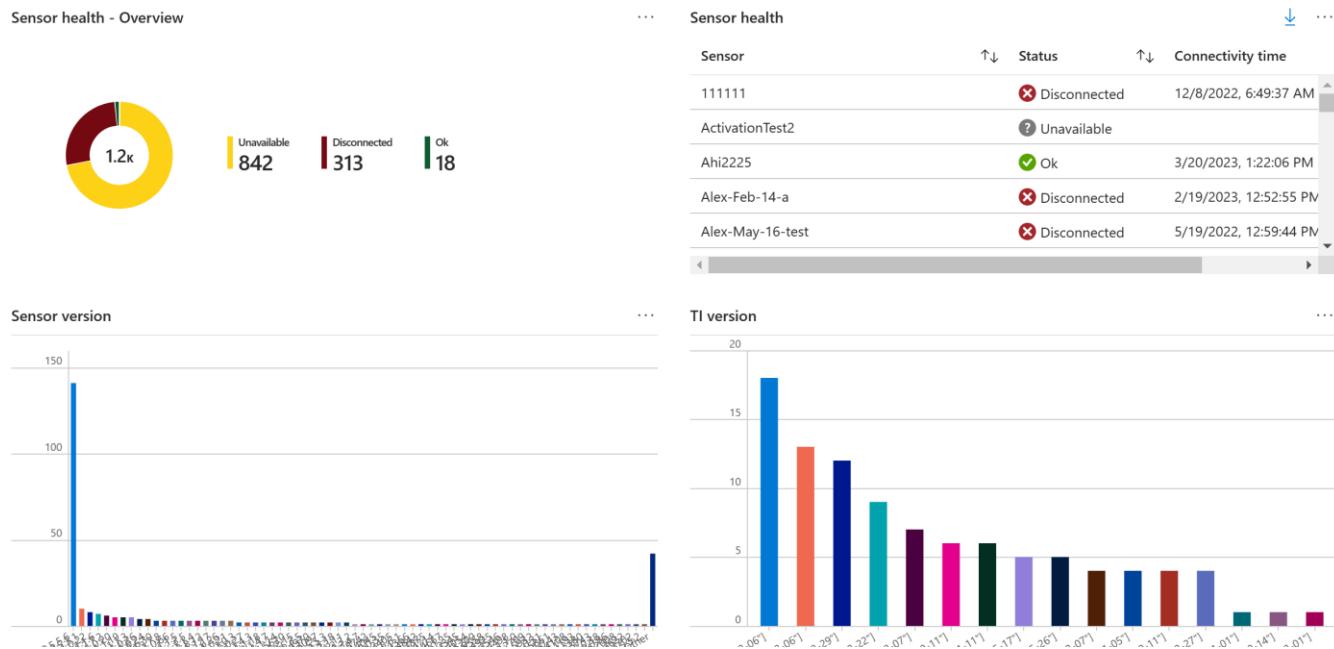
Defender for IoT (4)

- Sensor health See an overview of your sensor health...
- Alerts See an overview of your alerts inform...
- Devices See an overview of your devices infor...
- Vulnerabilities See an overview of your vulnerabilitie...

2. Click on any workbook, for example: "Sensor Health" , to view the preconfigured widgets on the workbook

Sensors

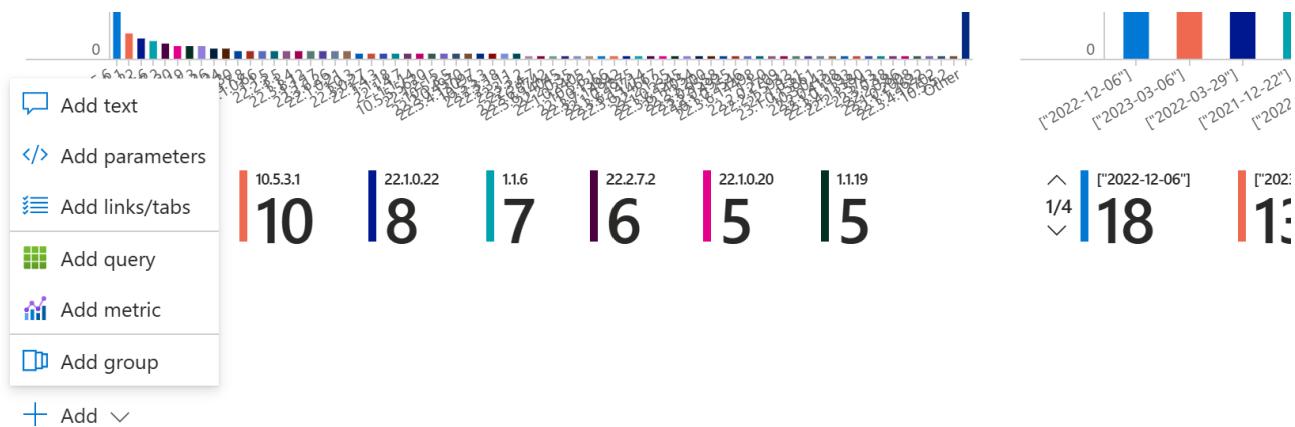
This report consolidates data regarding your sensors' health.



3. Click on the "Edit" option on the top ribbon to edit the existing widgets.



4. Click on "+Add" at the bottom of the workbook to add a widget to the workbook.

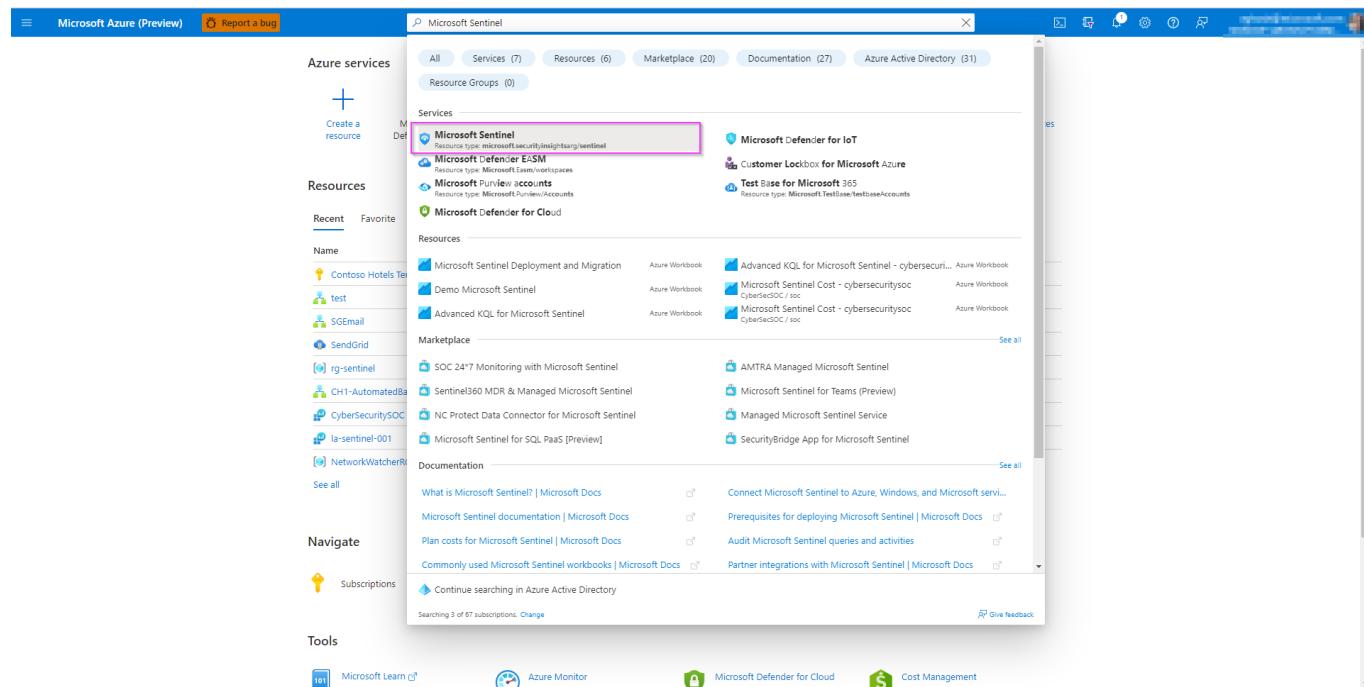


5. Click on "Save" to view your added widget.

Exercise 7: Integrate with Microsoft Sentinel

Task 1: Create a Log Analytics Workspace

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



2. Click on "+Create" -> "+Create a new workspace".

3. Pick your subscription, Resource Group, Name and Region

Create Log Analytics workspace

[Basics](#) [Tags](#) [Review + Create](#)

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) X

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription *	<input type="text" value="CS-playground"/>
Resource group *	<input type="text" value="CS-playground"/> Create new

Instance details

Name *	<input type="text" value="VishakhaSentinel"/> ✓
Region *	<input type="text" value="Canada East"/> ✓

4. Click on "Review +Create" -> "Create".
5. Go to Sentinel -> find the workspace you just created -> Click "Add" to add the workspace to Sentinel.

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
DemoTogether	centralus	demotogther	CS-playground	Microsoft
HandsOnLab	canadacentral	cs-playground	CS-playground	Microsoft
Hank-HOL	eastus	hank_hol	CS-playground	Microsoft
test	westeurope	cs-playground	CS-playground	Microsoft

Add **Cancel**

Task 2: Install the Defender for IoT package

1. Go to Sentinel, make sure your workspace is selected.

Selected workspace: 'handsontlab'

General What's new Get started Free trial

Overview Logs News & guides

2. Go to "Content Hub" -> Type "Defender for IoT" and click on "Install". The package includes Analytic Rukles, Data Connector, Playbooks and Workbooks.

Search: Defender for IoT

Solutions: 282 | Standalone contents: 269 | Installed: 0 | Updates: 0

Status: All | Content type: All | Support: All | Provider: All

Solutions (1)

Category: All | Content sources: All

Microsoft Defender for IoT
Microsoft Sentinel, Microsoft Corporation
Internet of Things (IoT), Security - Threat Protection
Analytics rule (15) | Data connector +2

Standalone (2)

Workbook (2)

See more

Content type

- 15 Analytics rule
- 1 Data connector
- 7 Playbook
- 1 Workbook

Category

Internet of Things (IoT), Security - Threat Protection

Pricing

Free

Install

3.Click on "Create".

Microsoft Defender for IoT solution for Microsoft Sentinel

Microsoft Sentinel, Microsoft Corporation | Azure Application

Plan

Microsoft Defender for IoT

Create

(OT) / Operational Technology (OT) infrastructure.

Underlying Microsoft Technologies used:

This solution takes a dependency on the following technologies, and some of these dependencies either may be in Preview state or might result in additional ingestion or operational costs:

Codeless Connector Platform/Native Sentinel Polling

4.Select the workspace and click on "Review and Create".

Data Connectors: 1, Workbooks: 1, Analytic Rules: 15, Playbooks: 7

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Project details

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

Subscription * ⓘ

C3-playground

Resource group * ⓘ

C3-playground

Create new

Instance details

Workspace * ⓘ

HandsOnLab

Review + create

< Previous

Next : Data Connectors >

5. Go to "Data Connectors" and verify that the Defender for IoT Connector is connected.

The screenshot shows the Microsoft Sentinel interface. On the left, there's a navigation sidebar with sections like Threat management, Content management, and Configuration. The Configuration section has a pink box around the 'Data connectors' link. In the main area, there's a summary bar with 'Logs' (126), 'Connectors' (1 Connected), and a 'Content hub' link. Below this is a table titled 'Data connectors' with columns 'Status' and 'Connector name'. It shows one entry: 'Microsoft Defender for IoT' by Microsoft, which is 'Connected'. There are also filters for 'Providers : All', 'Data Types : All', and 'Status : Connected'.

6. Go to the package and click on "Manage" to see a list of resources installed as a part of the package.

Solutions (1) Content sources . All

Microsoft Defender for IoT
Microsoft Sentinel, Microsoft Corporation
Internet of Things (IoT), Security - Threat Protection
Analytics rule (15) Data connector +2
Installed

Standalone (2)

Workbook (2)

Content name	Created content	Content type	Version
Microsoft Defender for IoT	1 item	Data connector	1.0.0
PLC unsecure key state (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Unauthorized PLC changes (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Unauthorized remote access to the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Unauthorized DHCP configuration in the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Multiple scans in the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Internet Access (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Excessive Login Attempts (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Firmware Updates (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
No traffic on Sensor Detected (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Illegal Function Codes for ICS traffic (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Suspicious malware found in the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
PLC Stop Command (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Denial of Service (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
High bandwidth in the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1

Content type i 15 Data connector 7 Playbook 1 Workbook

Category i Internet of Things (IoT), Security - Threat Protection

Manage Actions View details

24 Installed content items

Microsoft Defender for IoT

Provider Microsoft Provider **Support** Microsoft Support **Version** 2.0.2

Description
The Microsoft Defender for IoT solution for Microsoft Sentinel allows you to ingest Security alerts reported in Microsoft Defender for IoT on assessing your Internet of Things (IoT)/Operational Technology (OT) infrastructure.

Underlying Microsoft Technologies used:
This solution takes a dependency on the following technologies, and some of these dependencies either may be in [Preview](#) state or might result in additional ingestion or operational costs:

- a. [Codeless Connector Platform/Native Sentinel Polling](#)

Data Connectors: 1, **Workbooks:** 1, **Analytic Rules:** 15, **Playbooks:** 8

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Content type i 15 Data connector 7 Playbook 1 Workbook

Category i Internet of Things (IoT), Security - Threat Protection

Pricing i

Manage Actions View details

Task 3: Create Incidents

1.Go to the Defender for IoT connector and click on "Open Connector Page".

Status	Connector name ↑	Disconnect... Status	Microsoft Provider	Last Log Rec...
	Microsoft Defender for Cloud Microsoft			
	Microsoft Defender for Cloud Apps Microsoft			
	Microsoft Defender for Endpoint Microsoft			
	Microsoft Defender for Identity Microsoft			
	Microsoft Defender for IoT Microsoft	Last data received		
	Microsoft Defender for Office 365 (Preview) Microsoft	--		

Description
Gain insights into your IoT security by connecting Microsoft Defender for IoT alerts to Microsoft Sentinel. You can get out-of-the-box alert metrics and data, including alert trends, top alerts, and alert breakdown by severity. You can also get information about the recommendations provided for your IoT hubs including top recommendations and recommendations by severity.

Last data received

--

Content source ⓘ IoT Threat Monitoring with Defender for IoT

Version 1.0.0 Author Microsoft

Supported by Microsoft Corporation | Email

[Open connector page](#)

2.Click on “Create Incidents” to automatically create alerts from the connector.



Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service.

[Enable](#)

Task 4: Validate Defender for IoT logs are streamed correctly to Sentinel (KQLS on the data)

1.In Microsoft Sentinel, select Logs > AzureSecurityOfThings > SecurityAlert, or search for SecurityAlert.

2.Use the following sample queries to filter the logs and view alerts generated by Defender for IoT:

To see all alerts generated by Defender for IoT:

```
SecurityAlert | where ProductName == "Azure Security Center for IoT"
```

To see specific sensor alerts generated by Defender for IoT:

```
SecurityAlert
```

```
| where ProductName == "Azure Security Center for IoT"
| where tostring(parse_json(ExtendedProperties).SensorId) == "<sensor_name>"
```

To see specific OT engine alerts generated by Defender for IoT:

SecurityAlert

```
| where ProductName == "Azure Security Center for IoT"  
| where ProductComponentName == "MALWARE"
```

SecurityAlert

```
| where ProductName == "Azure Security Center for IoT"  
| where ProductComponentName == "ANOMALY"
```

SecurityAlert

```
| where ProductName == "Azure Security Center for IoT"  
| where ProductComponentName == "PROTOCOL_VIOLATION"
```

SecurityAlert

```
| where ProductName == "Azure Security Center for IoT"  
| where ProductComponentName == "POLICY_VIOLATION"
```

SecurityAlert

```
| where ProductName == "Azure Security Center for IoT"  
| where ProductComponentName == "OPERATIONAL"
```

To see high severity alerts generated by Defender for IoT:

SecurityAlert

```
| where ProductName == "Azure Security Center for IoT"  
| where AlertSeverity == "High"
```

To see specific protocol alerts generated by Defender for IoT:

SecurityAlert

```
| where ProductName == "Azure Security Center for IoT"  
| where tostring(parse_json(ExtendedProperties).Protocol) == "<protocol_name>"
```

Task 5: Investigate Defender for IoT incidents

1. In Microsoft Sentinel, go to the **Incidents** page.
2. Above the incident grid, select the **Product name** filter and clear the **Select all** option. Then, select **Microsoft Defender for IoT** to view only incidents triggered by Defender for IoT alerts. For example:

The screenshot shows the Microsoft Sentinel Incidents page. On the left, there's a navigation sidebar with sections like General, Threat management, Content management, and Configuration. The Threat management section has 'Incidents' selected. The main area shows three counts: 917 Open incidents, 917 New incidents, and 0 Active incidents. Below these are filters for Severity (All), Status (2 selected), and a dropdown for Product name. A red box highlights the 'Product name' dropdown, which lists several Microsoft products. The 'Microsoft Defender for IoT' checkbox is checked. To the right, there's a large grid of incidents with columns for Severity, Incident ID, Title, Alerts, Product names, Created time, and Last update time. A modal window titled 'No incidents selected' with the sub-instruction 'Select an incident to view more details' is overlaid on the grid.

3. Select a specific incident to begin your investigation.

In the incident details pane on the right, view details such as incident severity, a summary of the entities involved, any mapped MITRE ATT&CK tactics or techniques, and more.

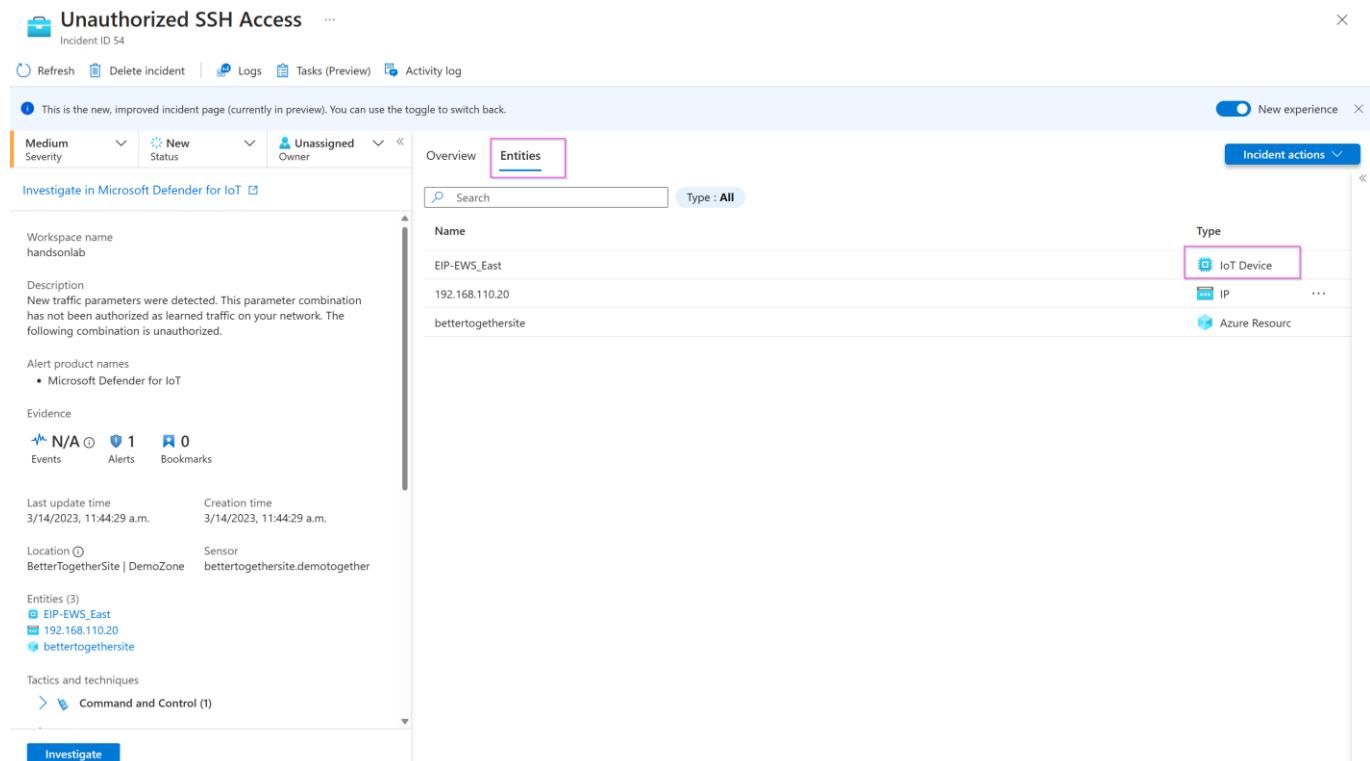
This screenshot shows the Microsoft Sentinel Incidents page with the 'Incidents' section selected in the sidebar. The main grid shows 676 Open incidents, 676 New incidents, and 0 Active incidents. The Product name filter is set to 'Microsoft Defender for IoT'. The incident details pane on the right is open for an incident with ID 107793, titled 'Malicious Domain Name Request'. It includes sections for Description (mentioning suspicious network activity), Alert product names (listing Microsoft Defender for IoT), Evidence (Events, Alerts, Bookmarks), Last update time (09/22/22, 10:36 AM), Creation time (09/22/22, 03:05 AM), Entities (IP address 192.168.42.29), Tactics and techniques (Command and Control, Initial Access), and Incident workbook/Overview links. At the bottom of the pane are 'View full details' and 'Actions' buttons.

Task 6: Investigate further with IoT device entities

The IoT device entity page provides contextual device information, with basic device details and device owner contact information. The device entity page can help prioritize remediation based on device importance and business impact, as per each alert's site, zone, and sensor.

1. When you are at the incident details page, click on "Entities".

2. Find the IoT identity categorized by this device icon: 



The screenshot shows the Microsoft Defender for IoT incident details page for an 'Unauthorized SSH Access' incident (Incident ID 54). The 'Entities' tab is selected. A table lists three entities:

Name	Type
EIP-EWS_East	IoT Device
192.168.110.20	IP
bettertogethersite	Azure Resource

The 'IoT Device' row is highlighted with a pink box. Other tabs include Overview, Logs, Tasks (Preview), Activity log, and Incident actions. The page also displays incident details like workspace name, description, alert product names, evidence count (N/A, 1 alert, 0 bookmarks), last update time, creation time, location, and entities.

3. To drill down even further, select the IoT device entity link and open the device entity details page.

4. Alternatively, you can hunt for vulnerable devices on the Microsoft Sentinel Entity behavior page. For example, view the top five IoT devices with the highest number of alerts, or search for a device by IP address or device name:

The screenshot shows the Microsoft Sentinel Entity behavior page. On the left, a sidebar navigation includes General, Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior - highlighted with a red box), Content management (Content hub, Repositories, Community), and Configuration (Data connectors, Analytics). The main area displays several cards: 'Accounts by # of alerts' (No data to display), 'Hosts by # of alerts' (1 host, 1 alert), 'IPs by # of alerts (Preview)' (list of IP addresses and alert counts), 'IoT devices by # of alerts (Preview)' (list of IoT devices and alert counts, highlighted with a red box), and 'Azure resources by # of alerts (Preview)' (list of Azure resources and alert counts).

Task 7: Investigate the alert in Defender for IoT

1. Go to your incident details page and view the alerts listed under "Timeline".

The screenshot shows the Microsoft Sentinel Incident details page for Incident ID 319410. The left sidebar shows basic incident information: Unassigned owner, New status, High severity, and the alert product name Microsoft Defender for IoT. The main area has tabs for Timeline, Similar incidents (Preview), Alerts, Bookmarks, Entities, and Comments. The Timeline tab is selected, showing a single entry: 'Unauthorized PLC Programming' at Nov 29 1:03 PM. The right side of the screen shows detailed information for this alert, including its description, severity (High), status (New), and entities involved (4 entities: 192.178.1.1, 192.178.2.2, contoso-site1, 192.178.1.1).

Task 8: 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 that we can re-run the alerts to show how they are sent and analyzed by Sentinel.

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Alerts

Defender for IoT | Alerts

Search Refresh Edit Columns Export to CSV Change Status Learn

Discover Overview Device map Device inventory Alerts Analyze Event timeline Data mining Risk assessment Trends & statistics Attack vector Manage System settings Custom alert rules Users Forwarding Support Support

Showing 22 of 22 alerts Group by No grouping

Severity	Name	Engine	Detection time	Status	Source Device
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	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	192.168.100.1
Warning	Traffic Detected on Sensor interface	Operational	2 months ago	New	192.168.101.10
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	192.168.117.239
Major	Event Buffer Overflow in Outstation	Operational	3 months ago	New	192.168.117.239
Warning	Controller Reset	Operational	3 months ago	New	192.168.118.22
Warning	Controller Reset	Operational	3 months ago	New	192.168.118.11
Warning	An S7 Stop PLC Command was Sent	Operational	3 months ago	New	192.168.122.1
Warning	An S7 Stop PLC Command was Sent	Operational	3 months ago	New	192.168.109.1
Major	GE SRTP Command Failure	Operational	3 months ago	New	192.168.109.2
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.108.2
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.108.2
Major	Honeywell Firmware Version Chanoed	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.

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > System settings

Defender for IoT | System settings

Search Basic Sensor Setup

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

PCAP PLAYER Upload and replay PCAP files.

Upload Play All Clear All

1-S7comm-VaService-Read-D61DBD0.pcap
pcap_wednesdaypcapng

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

SSL/TLS Certificate Manage SSL/TLS certificates installed on this sensor

Play PCAP Upload and play PCAP files

Network monitoring Sensor management Integrations Import settings

Close

Exercise 8: Automate response to Defender for IoT alerts.

[Playbooks](#) are collections of automated remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually or set to run automatically in response to specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.

Before using the out-of-the-box playbooks, make sure you perform the following prerequisites, as needed for each playbook:

- [Ensure valid playbook connections](#)
- [Add a required role to your subscription](#)
- [Connect your incidents, relevant analytics rules, and the playbook](#)

For a full list of DIoT Playbooks, refer to [this](#) document.

Exercise 9: Clean Up

Task 1: Delete resources

It is 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.

Exercise 10: Submit Feedback

It is through your feedback and suggestions that we can continue to improve the experience. Please share how your experience was via [this form](#).

Appendix:

Export Keys and VMs from Keyvault

Download and run this script hosted on Github [-Microsoft-Defender-for-IoT/Hands on Lab Documents/vmsexporter at main · Azure/-Microsoft-Defender-for-IoT \(github.com\)](#), to export a list of your passwords and VM names.

Ensure that you have:

1. Fill in your subscription id on line 8, resource group name on line 9, and key vault name on line 19.

2. Install all the modules mentioned in line 1 to line 5 mentioned in the code.

3. Install Azure CLI using this document - [Install the Azure CLI for Windows | Microsoft Learn](#)