

Summary

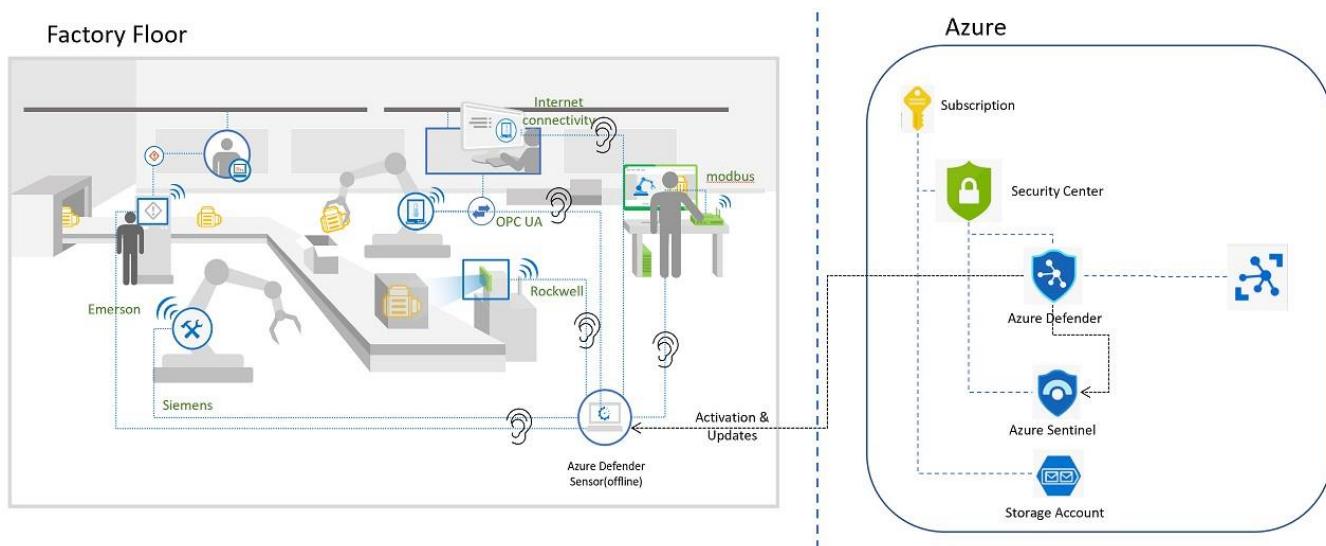
This Hands-on-Lab (HOL) will focus on securing your facilities. We will be simulating traffic by playing some Packet captures, visualizing and analyzing the data on the sensor console. Integrate our sensor with Microsoft Sentinel, to explore alert handling, and for writing queries to help with alert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

Internet of Things - Microsoft Defender for IoT HOL

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

Architecture Diagram

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



Contents

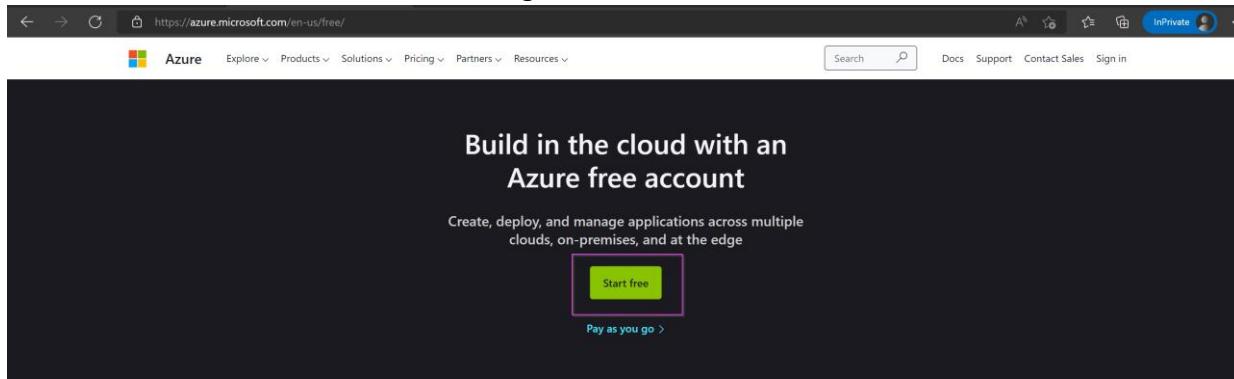
Summary.....	1
!! Since the PDF contains hyperlinks, please download the file before proceeding!!.....	1
Architecture Diagram.....	1
Exercise 1: Enabling Defender	3
Task 1: Create an Azure Subscription	3
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	4
Exercise 2: Deploy the Sensor in Azure.....	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.....	13
Exercise 3: Perform an Upgrade	19
Task 1: Download the Upgrade ISO file.....	19
Task 2: Upgrade your sensor.....	19
Exercise 4: Simulate Data in your sensor.....	21
Task 1: Enabling the PCAP Player.....	21
Task 2: Play PCAP files.....	22
Exercise 5: Analyzing the Data	24
Task 1: Visualize on the Device Map.....	24
Task 2: View the associated Alerts	27
Task 3: Device Inventory	29
Task 4: View the Event Timeline	30
Task 5: Data Mining	30
Task 6: Generate a Risk Assessment report.....	32
Exercise 6: Cloud Connect your sensor.....	33
Task 1: Create the cloud connected sensor on the Cloud Management portal	33
Task 2: Upload the activation file to cloud connect your sensor.....	33
Task 3: Verify Cloud connection.....	34
Exercise 7: Manage your sensor via the Cloud Management Portal.....	35
Task 1: Manage your devices	35
Task 2: View your Alerts	37
Task 3: View your recommendations	39
Task 4: Visualize Data by utilizing Workbooks	39
Exercise 8: Integrate with Microsoft Sentinel	41
Task 1: Create a Log Analytics Workspace.....	41
Task 2: Install the Defender for IoT package.....	43
Task 3: Create Incidents.....	45
Task 4: Validate Defender for IoT logs are streamed correctly to Sentinel (KQLS on the data)	46
Task 5: Investigate Defender for IoT incidents	47
Task 6: Investigate further with IoT device entities	49
Task 7: Investigate the alert in Defender for IoT	50
Task 8: Acknowledge Alerts and Re-run PCAPs.....	51
Exercise 9: Automate response to Defender for IoT alerts.....	52
Exercise 10: Clean Up	52
Task 1: Delete resources.....	52

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.

A screenshot of the Microsoft Azure portal at https://portal.azure.com/#home. The search bar at the top contains the text "Subs". On the left, there's a sidebar with sections for "Azure services", "Recent", "Name", and "Marketplace". The main area shows a list of subscriptions. One subscription, "Visual Studio Enterprise Subscription", is highlighted with a pink rectangle. Other visible subscriptions include "Event Hubs Clusters", "Notification Hubs", "Device Update for IoT Hubs", and "Azure Synapse Analytics (private link hubs)". There are also sections for "Services" (with "Subscriptions" highlighted) and "Marketplace". At the bottom, there are navigation links for "Subscriptions", "Resource groups", "All resources", and "Dashboard".

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

The screenshot shows the Microsoft Azure Subscriptions page. At the top, there are filter options: 'Subscriptions == global filter', 'My role == all', 'Status == all', and '+ Add filter'. Below the filters, a table lists one subscription: 'Visual Studio Enterprise Subscription'. The table columns include: Subscription name, Subscription ID, My role, Current cost, Secure Score, Parent management group, Status, and an ellipsis column. The 'Visual Studio Enterprise Subscription' row is highlighted with a red border.

Task 2: Enabling Microsoft Defender for IoT on the Subscription

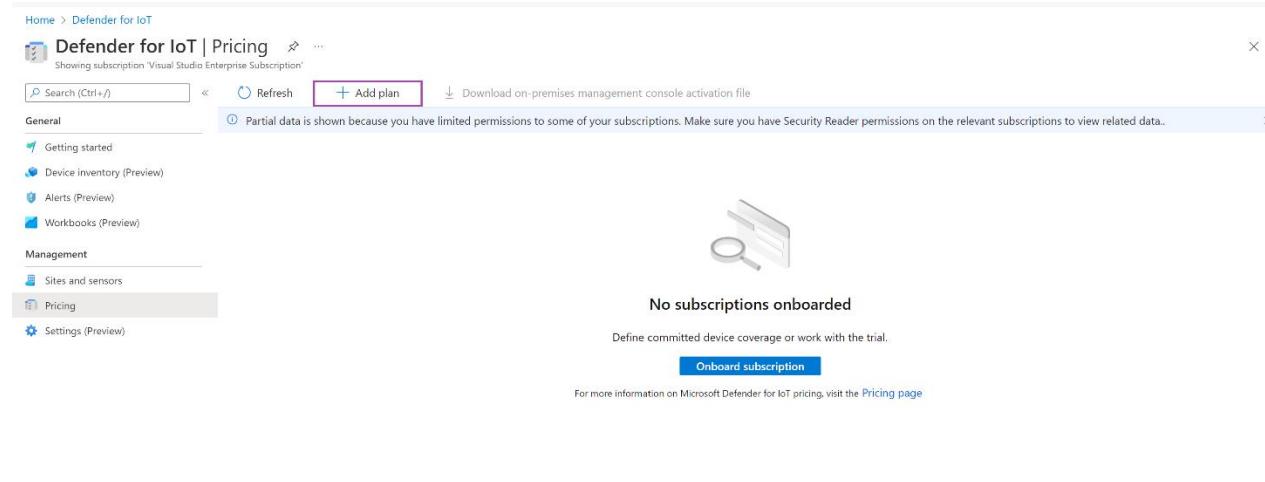
1. In the [Azure Portal](#), search for **Microsoft Defender for IoT**. Select **Microsoft Defender for IoT** in the popup window, to open the Microsoft Defender for IoT Page.

The screenshot shows the Microsoft Azure search results for 'Microsoft Defender for IoT'. The search bar at the top contains the query. Below the search bar, there are tabs for 'All', 'Services (27)', 'Documentation (99+)', 'Azure Active Directory (1)', 'Resources (0)', and 'Resource Groups (0)'. The 'Services' section contains several items, with 'Microsoft Defender for IoT' highlighted with a red box. Other items listed include 'IoT Hub', 'Microsoft Sentinel', 'Form recognizers', and 'Power Platform'. Below the services, there are sections for 'Documentation' and 'Azure Active Directory', each with a few links. On the left side, there's a sidebar for 'Recent resources' and a 'Create a resource' button.

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

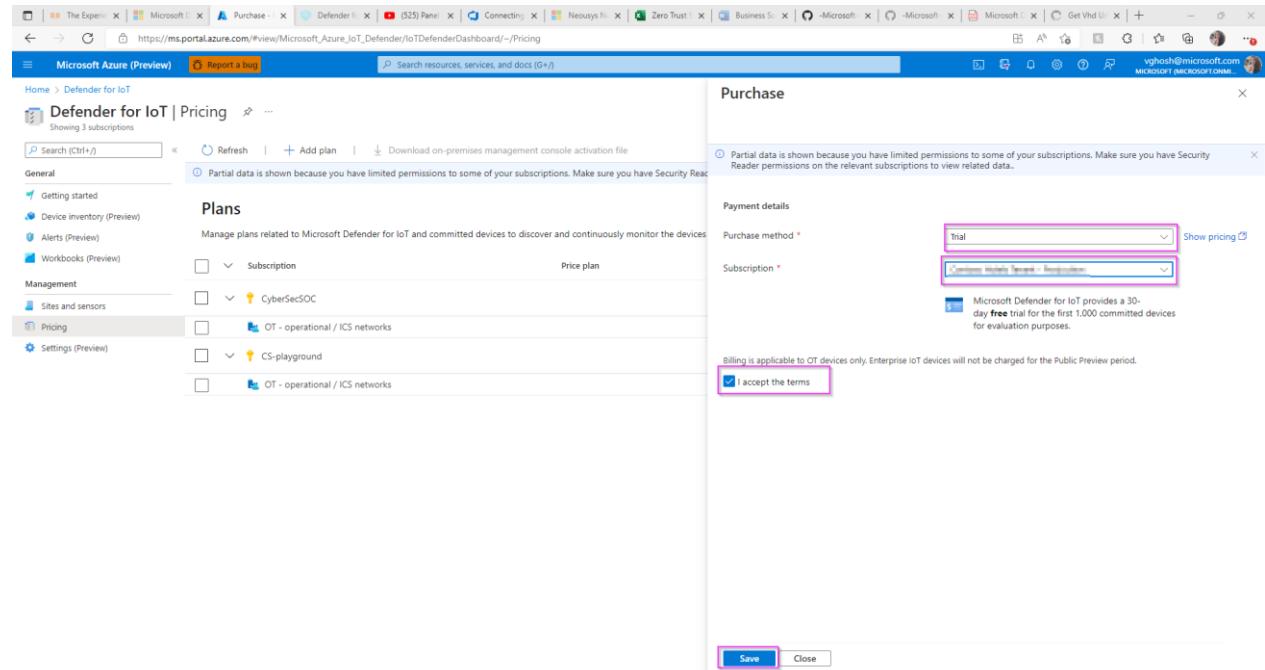
The screenshot shows the Microsoft Defender for IoT Pricing page. The top navigation bar includes 'Home > Defender for IoT | Pricing'. The main content area has a heading 'Defender for IoT | Pricing' with a note 'Showing subscription "Visual Studio Enterprise Subscription"'. Below this are sections for 'General' (with 'Getting started', 'Device inventory (Preview)', 'Alerts (Preview)', and 'Workbooks (Preview)'), 'Management' (with 'Sites and sensors', 'Pricing' highlighted with a purple box, and 'Settings (Preview)'), and 'No subscriptions onboarded' (with a magnifying glass icon). A large blue button at the bottom right says 'Onboard subscription'. A note at the bottom states 'For more information on Microsoft Defender for IoT pricing, visit the [Pricing page](#)'.

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



4. In the popup screen, select:

- Purchase Method:** Trail
- Subscription:** pick the trial subscription you created
- 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 to HOL_D4IOT@microsoft.com for a link for the IoT sensor installation. You will receive an email with the link once your request has been received.

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

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

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

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

The screenshot shows the 'Custom deployment' page in the Azure portal. The 'Basics' tab is selected. The 'Template' section shows a 'Customized template' with 4 resources. Below it, the 'Project details' section includes fields for 'Subscription' (BuildEnv), 'Resource group' (Create new), 'Region' (East US), 'Location' ([resourceGroup().location]), 'Deploy Public IP' (true), 'Put Password To Key Vault' (true), 'Source VHDURL' (empty), and 'Sensor Count' (1). Step numbers 1 through 7 are overlaid on the fields: 1 on the Subscription dropdown, 2 on the Resource group dropdown, 3 on the Region dropdown, 4 on the Location field, 5 on the Deploy Public IP dropdown, 6 on the Put Password To Key Vault dropdown, and 7 on the Source VHDURL field.

- 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
VMDeployment	Microsoft.Resources/deployments	OK	Operation details
copyhd	Microsoft.Resources/deployments	OK	Operation details

Next steps

Go to resource group

- Go to the keyvault resource from the list.

KeyVaultTest | Overview

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

Subscription ID : 1a61ccb1-70b3-45a3-a1b0-548c44d70a6 Location : West US

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

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_minstanxx245p7rgp2_Pay	Managed identity	West US
SOC_mra245p7rgp2_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-pg0	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".

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

Key vault | Directory: Microsoft

+ Create Refresh Delete Edit

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Access policies Events Objects Keys Secrets Certificates Settings Access configuration Networking Microsoft Defender for Cloud

Access policies

Showing 1 to 1 of 1 records.

Name Email Key Permissions

APPLICATION

SOC-vmsidentityuq63gjmwvo2do-Play

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

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

Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

① Permissions ② Principal ③ Application (optional) ④ Review + create

Configure from a template Key & Secret Management

Key permissions	Secret permissions	Certificate permissions
<input checked="" type="checkbox"/> Select all <input checked="" type="checkbox"/> Get <input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Update <input checked="" type="checkbox"/> Create <input checked="" type="checkbox"/> Import <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Recover <input checked="" type="checkbox"/> Backup <input checked="" type="checkbox"/> Restore	<input checked="" type="checkbox"/> Select all <input checked="" type="checkbox"/> Get <input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Set <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Recover <input checked="" type="checkbox"/> Backup <input checked="" type="checkbox"/> Restore	<input checked="" type="checkbox"/> Select all <input type="checkbox"/> Get <input type="checkbox"/> List <input type="checkbox"/> Update <input type="checkbox"/> Create <input type="checkbox"/> Import <input type="checkbox"/> Delete <input type="checkbox"/> Recover <input type="checkbox"/> Backup <input type="checkbox"/> Restore <input type="checkbox"/> Manage Contacts <input type="checkbox"/> Manage Certificate Authorities <input type="checkbox"/> Get Certificate Authorities <input type="checkbox"/> List Certificate Authorities <input type="checkbox"/> Set Certificate Authorities <input type="checkbox"/> Delete Certificate Authorities
<input type="checkbox"/> Select all <input type="checkbox"/> Decrypt <input type="checkbox"/> Encrypt <input type="checkbox"/> Unwrap Key <input type="checkbox"/> Wrap Key <input type="checkbox"/> Verify <input type="checkbox"/> Sign		
<input type="checkbox"/> Select all <input type="checkbox"/> Purge		
<input type="checkbox"/> Select all		

Previous Next

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

- 5d62bf487e14fb8884e9582f29be8e1-977f-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-KVuq63gjmwv02do-Play | Access policies >

Create an access policy ...

SOC-KVuq63gjmwv02do-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 Resource group

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

Essentials

Subscription (more) : **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**

Showing 1 to 10 of 10 records. Show hidden types Add filter

	Type	Location	...
<input type="checkbox"/>	Storage account	West US	...
<input type="checkbox"/>	Key vault	West US	...
<input type="checkbox"/>	Network security group	West US	...
<input type="checkbox"/>	Managed identity	West US	...
<input type="checkbox"/>	Image	West US	...
<input type="checkbox"/>	Regular Network Interface	West US	...
<input type="checkbox"/>	Public IP address	West US	...
<input checked="" type="checkbox"/>	Virtual machine	West US	...
<input type="checkbox"/>	Disk	West US	...

9. Make a note of the Public IP address.

SOC Virtual machine

-Play

Essentials

Resource group (move) : **SOC**
 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 default
DNS name	Configure

Option #2: If you deployed without Keyvault.

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

Home > Microsoft.Template-20220630145822 | Overview

Deployment

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.

Home > Microsoft.Template-20220630145822 > Reset-password0

Deployment

Reset-password0 | Outputs

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
copyvhdl	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
copyvhdl	Deployment Script	East US
customflicwiéuSatkwwu	Storage account	East US
SOC NSGflicwiéuSatkwwu Play	Network security group	East US
SOC-vmflicwiéuSatkwwu-Play	Virtual machine	East US

5. Make a note of the Public IP address.

SOC Virtual machine

Essentials

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

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine

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- default
DNS name	Not configured

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.

Microsoft | Defender for IoT sensor

Sensor Sign in

User name

Password

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

Login

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

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)

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	...

Context menu options (highlighted):

- Edit
- Push Threat Intelligence update
- Recover my password (highlighted)
- 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)

Pricing

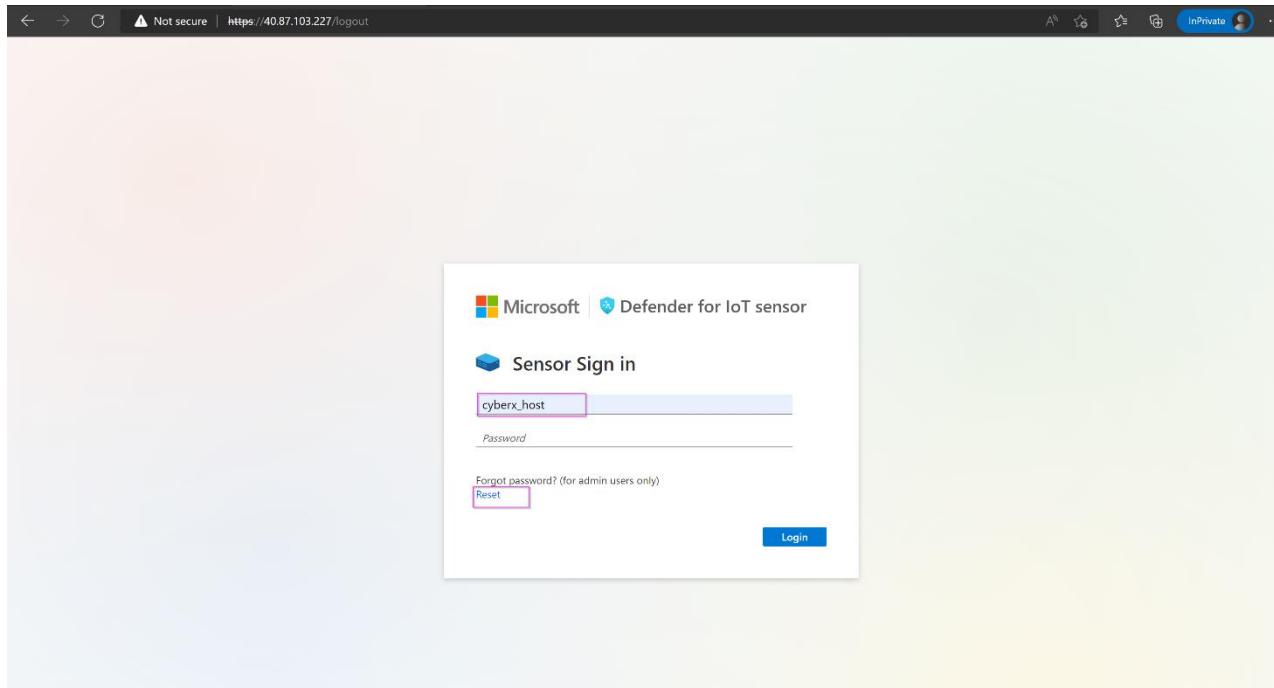
Recover

Insert secret identifier *

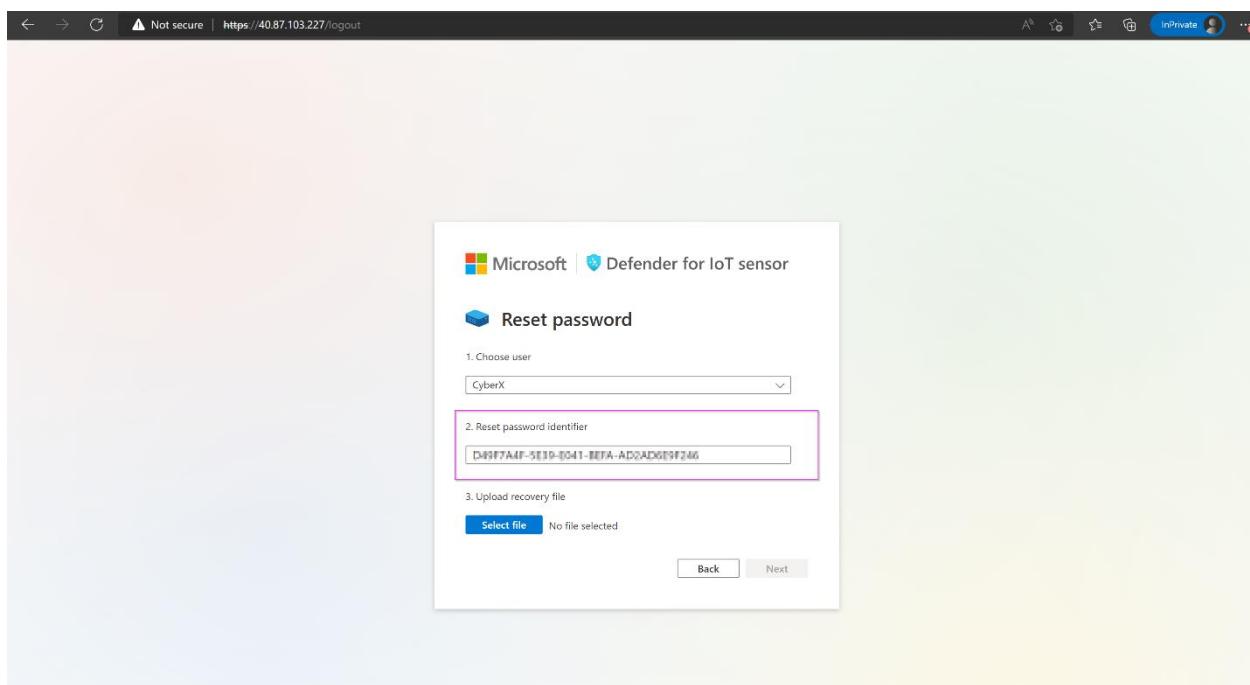
Sub0001-777-0e57-88h12

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 interface. On the left, there's a navigation sidebar with 'General' and 'Management' sections. Under 'Management', 'Sites and sensors' is selected. The main area displays sensor statistics: 2 All sensors, 1 IoT, 1 OT cloud connected, and 0 OT. Below this, it says 'Showing 2 of 2 sensors'. A modal window titled 'Recover' is open, featuring a lock icon and a key icon. It has a text input field containing a GUID ('D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246') and two buttons: 'Recover' and 'Cancel'.

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. Step 1: Choose user dropdown set to 'CyberX'. Step 2: Reset password identifier input field containing 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246'. Step 3: Upload recovery file section with a 'Select file' button (highlighted with a pink box) and 'No file selected' message. At the bottom are 'Back' and 'Next' buttons.

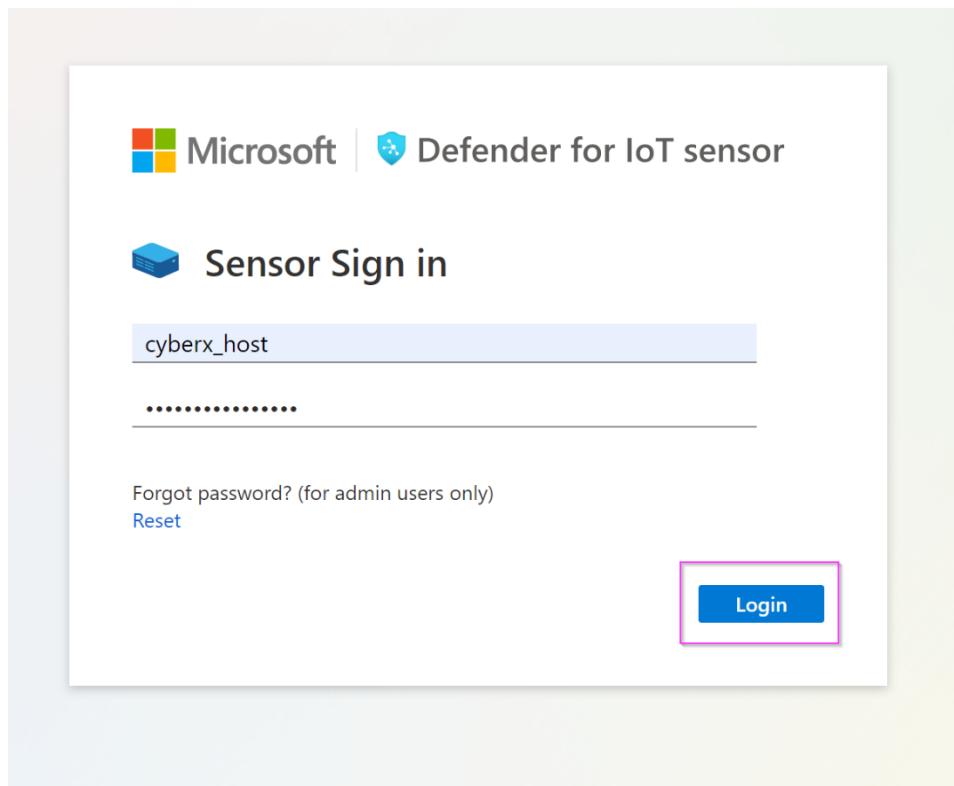
11. Click on “**Next**”.

The screenshot shows the 'Reset password' process in Microsoft Defender for IoT sensor. Step 3 involves uploading a recovery file. A blue 'Select file' button is highlighted with a pink box, and the file 'password_recovery (1).zip' is listed next to it. Below the file list are 'Back' and 'Next' buttons, with 'Next' also highlighted with a pink box.

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 in a redacted text field, which is highlighted with a pink box. Below the field, a note says 'Please write your password, it will not be shown again'. At the bottom right is a blue 'Next' button, which is also highlighted with a pink box.

13. Log in with the new password.



14. Repeat this step for all the usernames.

Exercise 3: Perform an Upgrade

Task 1: Download the Upgrade ISO file

1. Go to the Azure portal and navigate to the Defender for IoT page.
2. Go to "Getting Started" -> "Sensor" -> Download the latest recommended upgrade version.

Home >

Defender for IoT | Getting started Showing 3 subscriptions

Get started Windows IoT Enterprise (Preview) **Sensor** On-premises management console Updates

General

Getting started

Device inventory (Preview)

Alerts (Preview)

Recommendations (Preview)

Workbooks

Management

Sites and sensors

Plans and pricing

Settings (Preview)

Troubleshooting + Support

Diagnose and solve problems

Version 22.2.9 supports a new cloud connectivity model that requires sensor reactivation when updating from 10.5.X. [Learn more](#)

Use the information here to help you purchase hardware and install software.

Buy preconfigured appliance

Buy a preconfigured appliance from Arrow. The appliance will be delivered to your facility. Contact Arrow directly by mail to purchase the appliance.

[Identify required appliances](#) [Install software](#) [Set up your network](#)

Contact vendor to get a price quote

Purchase an appliance and install software

The solution runs on certified physical and virtual appliances. Acquire an appliance and download the ISO image to install the sensor.

[Identify required appliances](#) [Install software](#) [Set up your network](#)

Select version

22.2.9 (Latest) - recommended

MDS Hash - 5a2dbb762791112af562b643d980920f

Download

Task 2: Upgrade your sensor

1. On the sensor, go to "System Settings" -> "Sensor Management" -> "Software Update".

The screenshot shows the Microsoft Defender for IoT dashboard. On the left, there's a navigation sidebar with sections like Discover, Analyze, and Manage. Under Manage, the 'System settings' option is selected and highlighted with a pink box. In the main content area, under 'Updates', there are two options: 'Software Update' and 'Threat Intelligence'. Both are shown in boxes with a pink border. Below these are sections for 'Subscription & Activation Mode', 'Backup & Restore', 'System Health Check', and 'SNMP MIB Monitoring'.

2. Click on "Upload File" and upload the iso file you downloaded.

This screenshot is identical to the one above, showing the Microsoft Defender for IoT dashboard with the 'System settings' section selected. The 'Software Update' option under the 'Updates' section is highlighted with a pink box.

3. Verify the version on the dashboard.

The screenshot shows the Microsoft Defender for IoT dashboard with the 'Overview' section selected. At the top, it displays 'Microsoft | vishalvadher - 22.2.8'. Below this, there are summary metrics: 0 PPS, 124 Devices, and 32 Alerts. Under 'General Settings', it shows the 'Version:' field containing '22.2.8.20-r-3bd7f37', which is also highlighted with a pink box.

Exercise 4: Simulate Data in your sensor.

Task 1: Enabling the PCAP Player

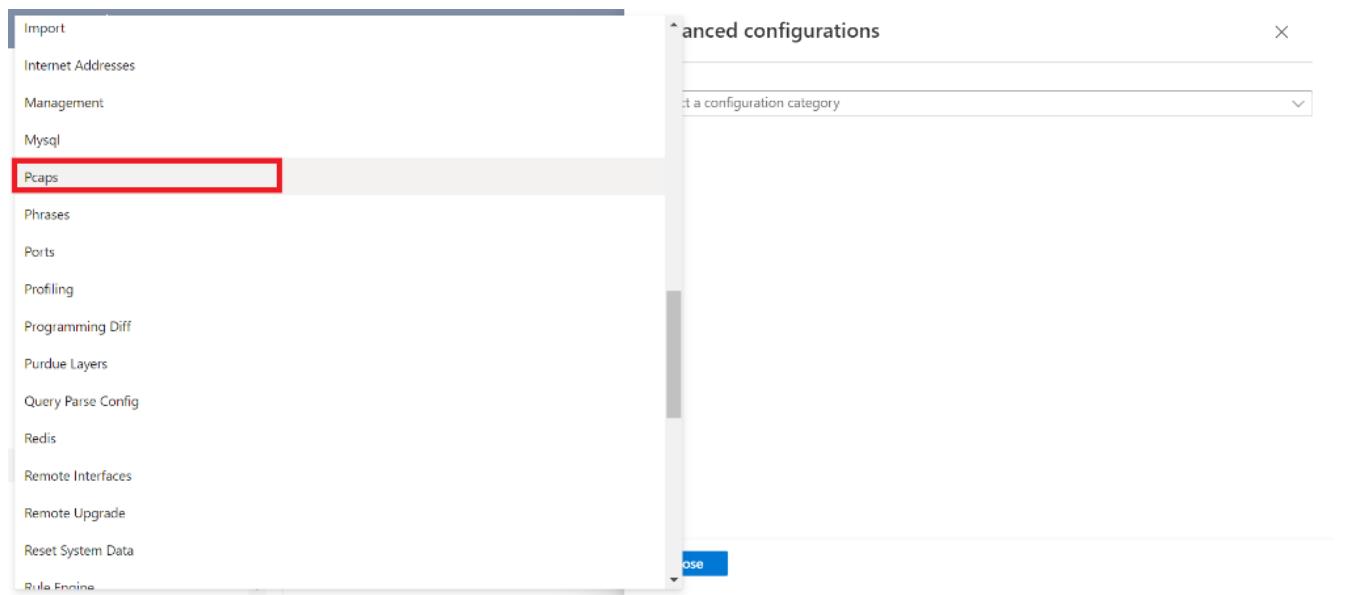
1. The PCAP player needs to be enabled to be visibly available for use in the UI. To do so, please select the "**System settings**" option from the scrolled down left side menu.

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar has a 'System settings' option highlighted with a red box. The main area is titled 'System settings' and contains four cards under 'Sensor Setup': 'Sensor Network Settings', 'Connection to Management Console', 'Time & Region', and 'Subnets'. The 'System settings' link in the sidebar is also highlighted with a red box.

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. The left sidebar has a 'System settings' option highlighted with a red box. The main area is titled 'System settings' and contains four cards under 'Health and troubleshooting': '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.



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 with the 'System settings' page open. The 'Advanced configurations' dialog for 'Pcaps' is overlaid on the main page. The 'enabled' variable is set to 1, and the 'Save' button is highlighted with a red box. The configuration file content is visible in the dialog:

```

cache.should.save.pcap=1
archive.cache.dir=
# 7 GB
filtered.cache.dir.size.megabytes.max=7168
# 3 GB
filtered.cache.dir.size.megabytes.min=3072
filtered.archive.dir.size.megabytes.max=
filtered.archive.dir.size.megabytes.min=
filtered.archive.dir=
player.max_size=1000
player.max_amount=20
player.params=
enabled=1
virtual.lan.hierarchy.depth.support=1

```

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).

Microsoft | Microsoft Defender for IoT - 22.1.3

Home > System settings

Defender for IoT | System settings

Analyze

- Event timeline
- Data mining
- Risk assessment
- Trends & statistics
- Attack vector

Manage

- System settings (highlighted)
- Custom alert rules
- Users
- Forwarding

SSL/TLS Certificate

Manage SSL/TLS certificates installed on this sensor

Play PCAP

Upload and play PCAP files

Sensor management (highlighted)

Network monitoring

Integrations

Import settings

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

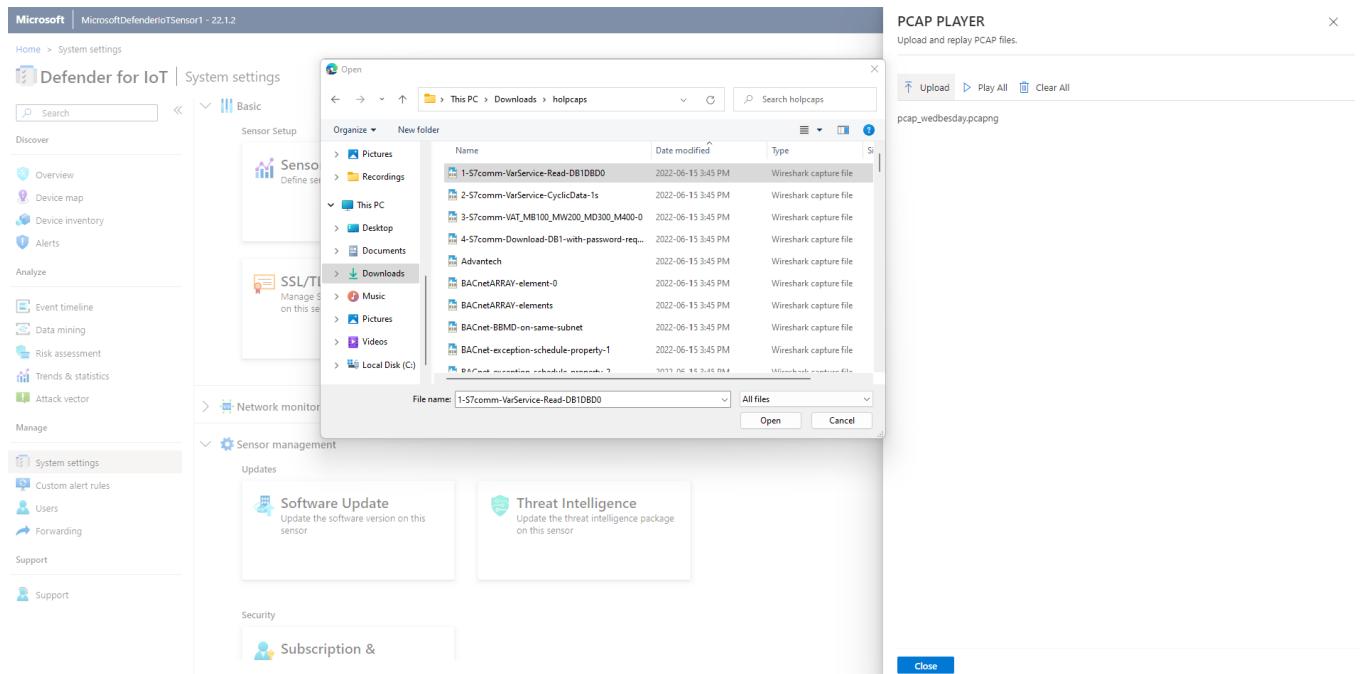
Advanced configurations

Pcaps

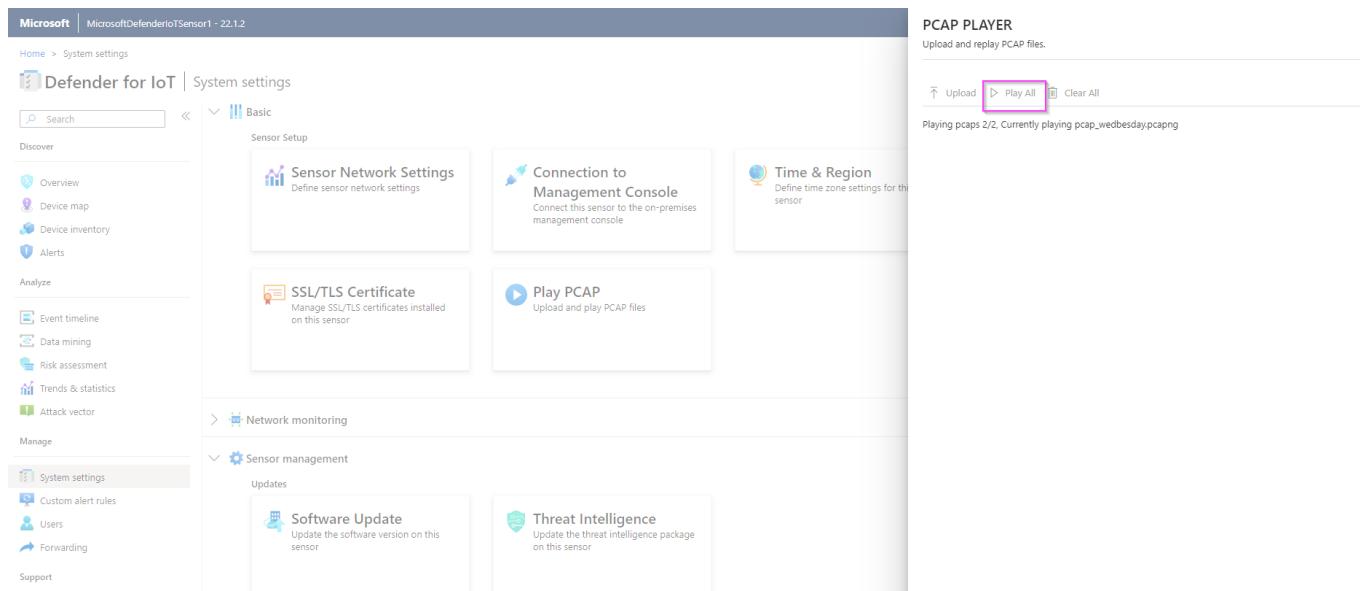
```
size.megabytes.max=44032  
archive.size.megabytes.max=  
size.megabytes.min=17408  
archive.size.megabytes.min=  
cache.should.save.pcap=1  
archive.cache.dir=  
filtered.cache.dir.size.megabytes.max=7168  
filtered.cache.dir.size.megabytes.min=3072  
filtered.archive.dir.size.megabytes.max=  
filtered.archive.dir.size.megabytes.min=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

Save

Close



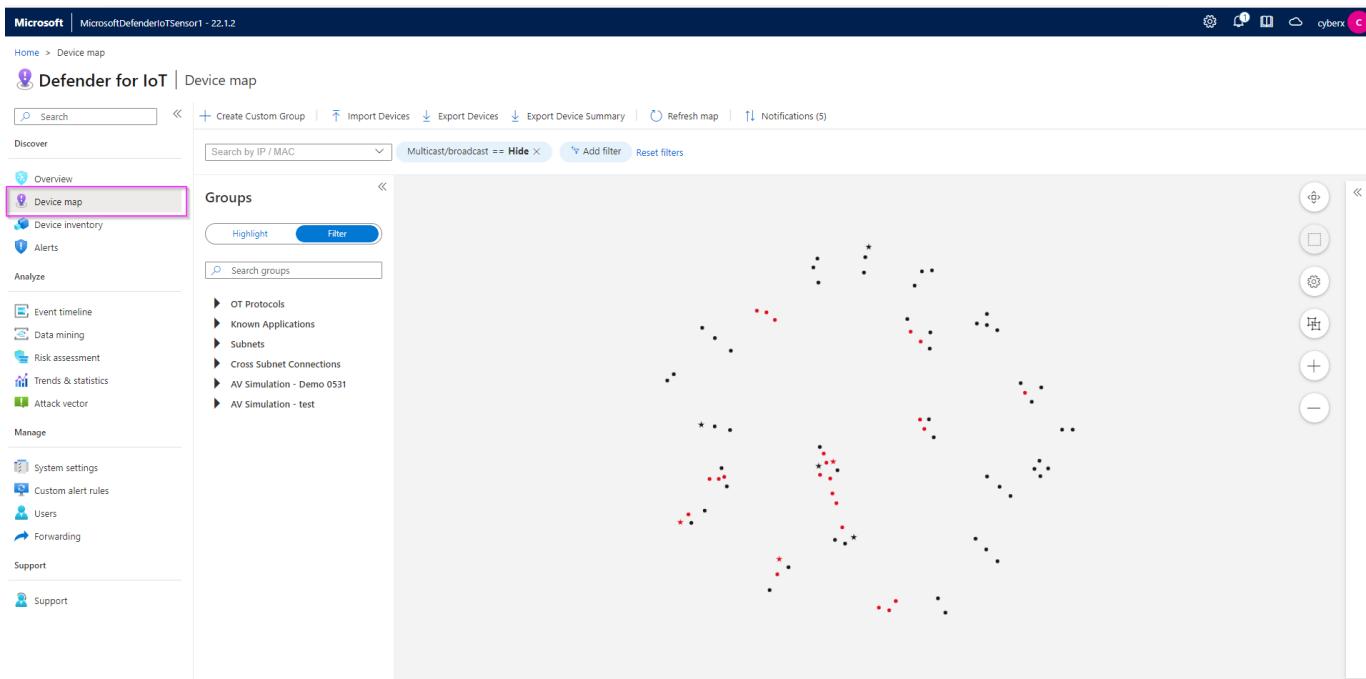
5. Click "Play All" to play the Pcaps.



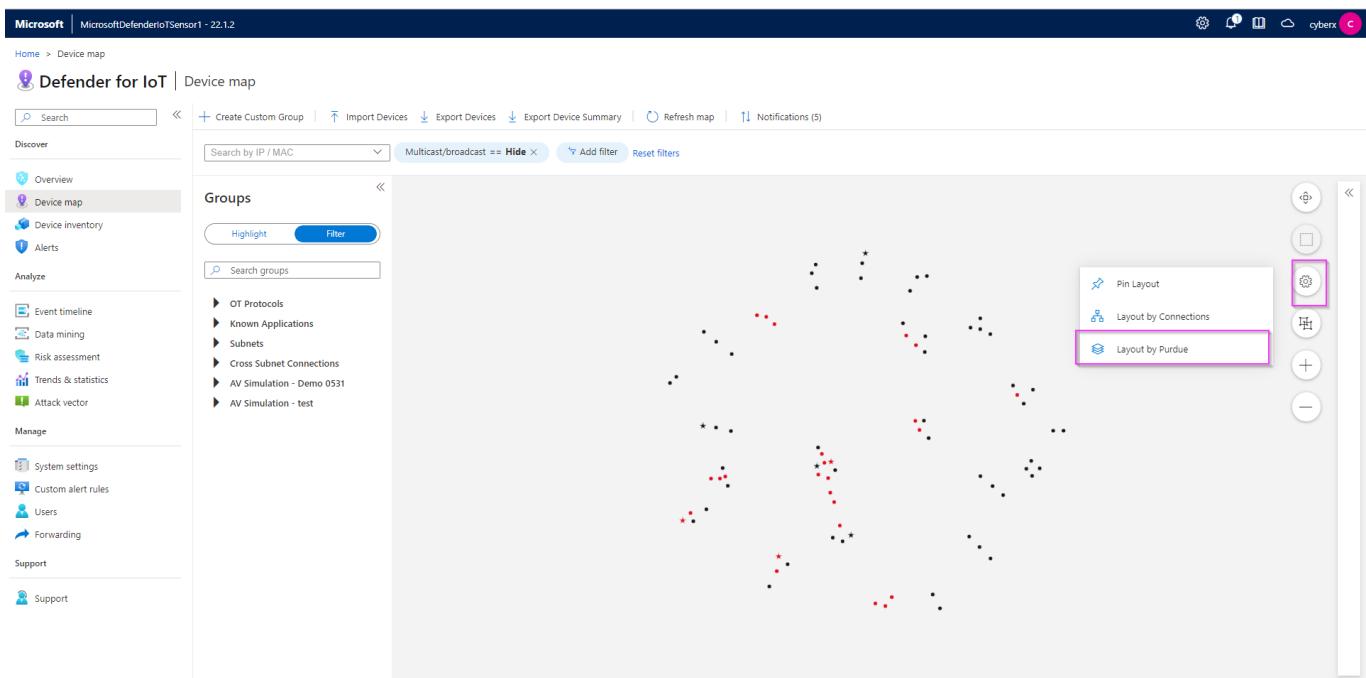
Exercise 5: Analyzing the Data

Task 1: Visualize on the Device Map

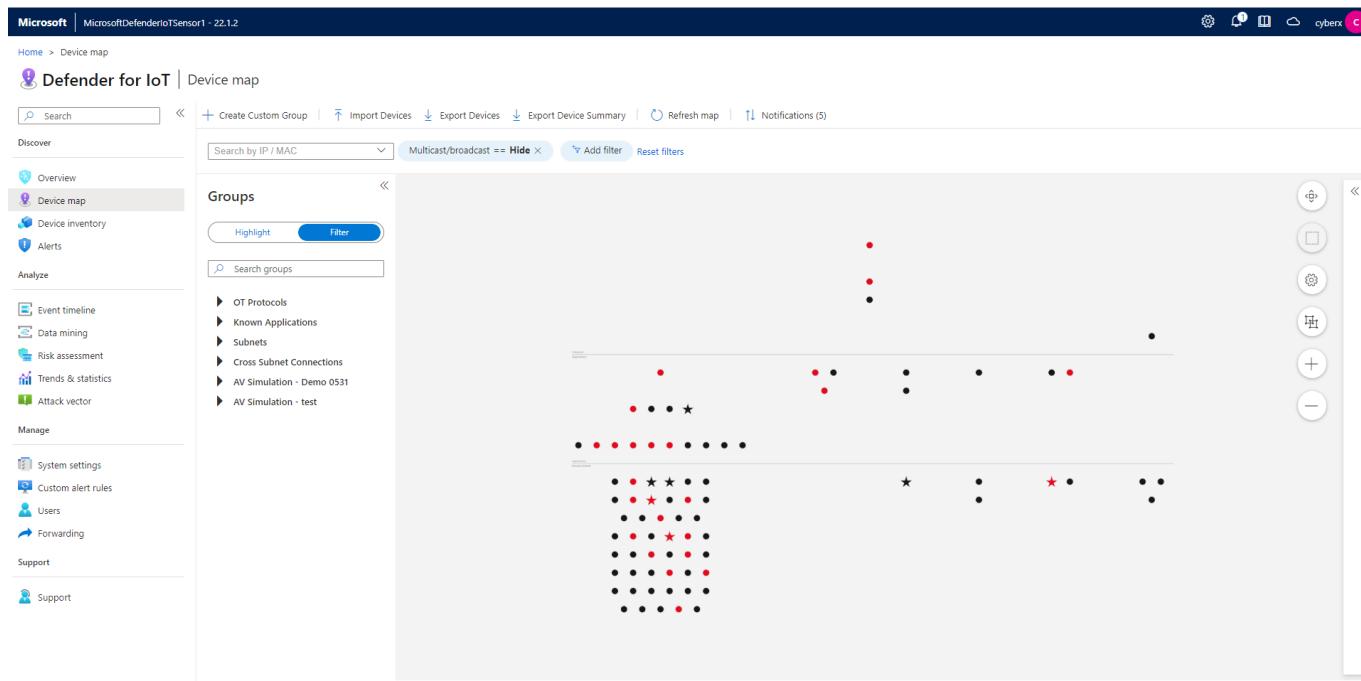
1. Click on “Device Map” from the menu on the left side.



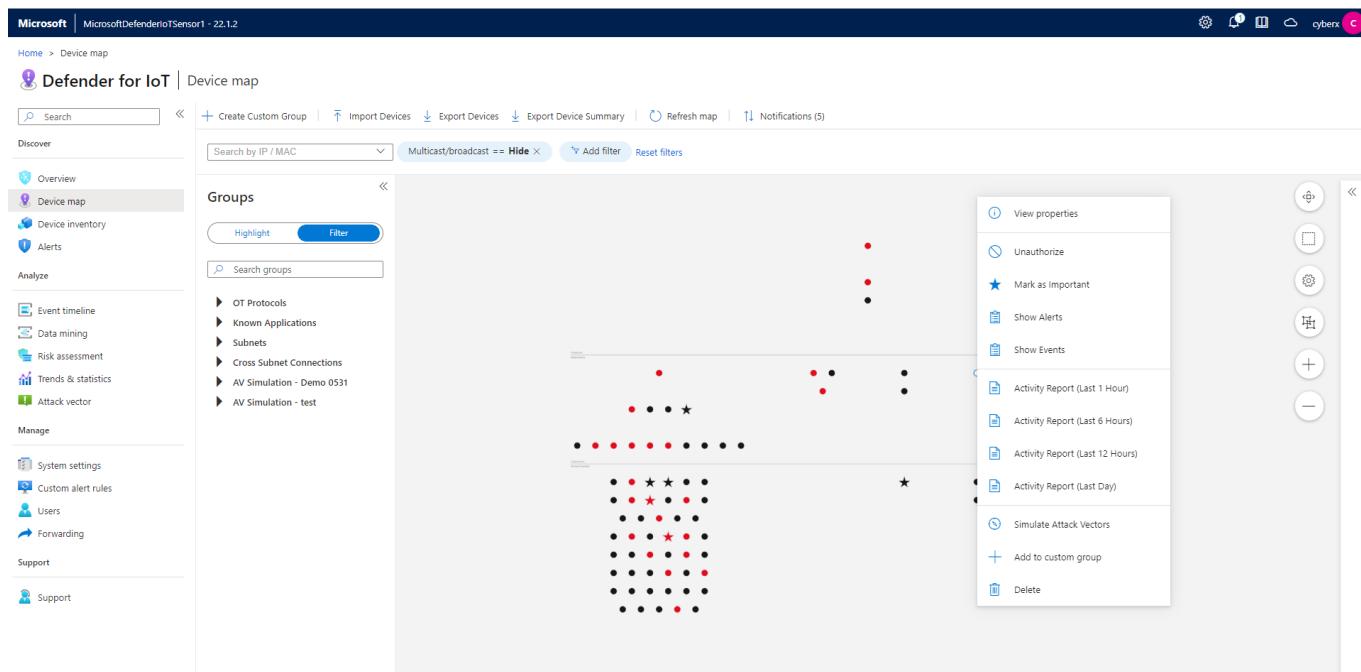
2. Click on the “Settings” option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.



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



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



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

The screenshot shows the Microsoft Defender for IoT Device map interface. On the left, a sidebar lists various categories like Overview, Device map, Device inventory, Alerts, Analyze, Manage, and Support. Under the 'Device map' section, there's a 'Groups' dropdown menu where 'MODBUS' is highlighted with a red box. In the main pane, a network diagram shows three nodes: 192.168.109.1, 192.168.109.21, and 192.168.109.2. The node 192.168.109.1 has a red alert icon. The right side of the interface includes various configuration and monitoring icons.

Task 2: View the associated Alerts

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

This screenshot shows the Microsoft Defender for IoT Device map interface again. The sidebar and network diagram are similar to the previous one, but the context menu for the device 192.168.110.2 is explicitly shown. The 'Show Alerts' option in the context menu is highlighted with a red box. The menu also includes other options like 'View properties', 'Unauthorized', 'Mark as Important', 'Show Events', 'Activity Report (Last 1 Hour)', 'Activity Report (Last 6 Hours)', 'Activity Report (Last 12 Hours)', 'Activity Report (Last Day)', 'Simulate Attack Vectors', 'Add to custom group', and 'Delete'.

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.

This screenshot shows the Microsoft Defender for IoT Device map interface. On the left, there's a sidebar with navigation links like Home, Device map, and Alerts. The main area displays a device card for 'Device | 192.168.110.21'. The card includes sections for General Information (Type: Engineering Station, Vendor: INTEL CORPORATE, Location: Automatic), Network Interfaces (IP: 192.168.110.21, MAC: acfdce:ccbbdd), and Protocols (SSH, EtherNet/IP, TDS, FTP, CIP). Below the card is an 'Edit Properties' button. At the top right, there are tabs for Map View, Alerts (which is selected), and Event Timeline. A search bar and filter options are also present. The main content area shows a table of alerts with columns for Severity, Name, Engine, Detection time, Status, and Source Device. Two alerts are listed: 'Unauthorized Internet Connectivity Detected' (Critical, Policy Violation, 2 weeks ago, New, 192.168.110.21) and 'EtherNet/IP Encapsulation Protocol Command Failed' (Major, Operational, 2 months ago, New, 192.168.110.2). A 'Group by' dropdown menu is visible at the top right of the alert table.

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**”.

This screenshot shows the Microsoft Defender for IoT Alerts page. The left sidebar has links for Discover, Device inventory, Alerts (which is selected), Analyze, Manage, and Support. The main area shows a table of alerts with columns for Severity, Name, Engine, Detection time, Status, and Source Device. Two alerts are listed: 'Unauthorized Internet Connectivity Detected' (Critical, Policy Violation, 2 weeks ago, New, 192.168.110.21) and another identical entry. To the right of the table, a detailed view of the first alert is shown. It includes a summary box with the alert ID (53), status (New), and detection time (2 weeks ago). Below this is a 'Description' section stating: 'A device defined in your internal network is communicating with addresses on the internet. These addresses have not been learned as valid addresses.' It also notes that 'Device 192.168.110.21 communicated with addresses shown in External Addresses. Verify that this device is properly configured.' Further down are sections for 'Related Devices' (Source device: 192.168.110.21, Destination device: Internet (37.142.39.186)) and two buttons at the bottom: 'View full details' and 'Take action'.

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

Showing 22 of 22 alerts

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

Task 3: Device Inventory

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

Showing 100 of 291 items

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

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

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Device inventory

Defender for IoT | Device inventory

Search | Save Filter | Refresh | Edit Columns | Export

Discover

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

Showing 100 of 291 items

	IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmware Version	Model	Operating System	Rack	Slot
<input type="checkbox"/>	192.168.100.8	192.168.100.8	An hour ago	Unknown	DNS, MDNS, Net...	5:14:f3:7d:8:21	INTEL CORPORA...					
<input type="checkbox"/>	192.168.100.1	192.168.100.1	An hour ago	Server	DNS							
<input type="checkbox"/>	192.168.1.11	192.168.1.11	An hour ago	PLC	Siemens S7	0:0:fb:5:4:be:f3	NETGEAR					
<input type="checkbox"/>	192.168.1.180	192.168.1.180	An hour ago	HMI	Siemens S7							
<input type="checkbox"/>	192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	0:30:a7:08:92:c6	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	0:23:ea:49:5a:c2	CISCO SYSTEMS ...					
<input type="checkbox"/>	192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	0:30:a7:08:97:c0	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	0:0cc1:02:09:da	EATON CORPOR...					
<input type="checkbox"/>	192.168.117.7	192.168.117.7	22 hours ago	PLC	Siemens SICAM	0: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	0:0:c2:92:28:38	VMWWARE INC.					
<input type="checkbox"/>	192.168.117.8	192.168.117.8	22 hours ago	PLC	Siemens SICAM	0:e0:a8:01:90:bb	SAT GMBH & CO.	15.01	CPC65 (6065)			
<input type="checkbox"/>	192.168.107.10	FC50507	22 hours ago	DCS Controller	Yokogawa VNet/IP	0:0:0:64:9d:5:d:10	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	0:0:0:64:9d:7:3:d	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	0:0:0:64:9e:84:e5	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1: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	0:0:1: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	0:0:1: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".

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Event timeline

Defender for IoT | Event timeline

Search | Create event | Refresh | Export

User Operations == Hide | Add filter | Reset filters

Discover

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

Event type

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

Load More...

Task 5: Data Mining

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

Create new report

Name * Report name

Description

Send to CM

Choose Category * Category

Order by Activity

Filter by Results within the last 3 minutes

IP address

MAC address

Port

Device group

Save Cancel

2. 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 * PLC Firmware Version

Description Report showing the firmware version of the different PLCs.

Choose Category * Modules and Firmware Versions

Order by Category

Filter by Results within the last 3 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”.

The screenshot shows the Microsoft Defender for IoT interface under the 'Data mining' section. On the left, a sidebar lists various sections like Overview, Device map, Device inventory, Alerts, Event timeline, Data mining (which is selected and highlighted in grey), Risk assessment, Trends & statistics, and Attack vector. In the main area, there's a 'Recommended' section with cards for Programming Commands, Internet Activity, Excluded CVEs, Active Devices (Last 24 Hours), Remote Access, CVEs, and Non Active Devices (Last 7 Days). Below this is a 'My reports' section with a table. The first row in the table, 'PLC Firmware Version', has a description 'Report showing the firmware version of the different PLCs.' and was last modified '2 minutes ago'. This row is also highlighted with a pink box. Other rows in the table include 'ALL' (last modified 4 days ago) and 'test' (last modified 3 months ago).

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

This screenshot shows a detailed view of the 'PLC Firmware Version' report. At the top, there are navigation links: Refresh, Expand all, Collapse all, Export to CSV (highlighted with a pink box), Export to PDF, Snapshots, Manage report, and Edit mode. The report content itself is titled 'PLC Firmware Version' and describes 'Report showing the firmware version of the different PLCs.' Below the title, there's a table with four rows of data. The first row is highlighted with a pink box.

Task 6: Generate a Risk Assessment report

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

This screenshot shows the Microsoft Defender for IoT Risk assessment page. The sidebar on the left is identical to the previous screenshots, with 'Risk assessment' selected. In the main area, there's a 'Generate report' button highlighted with a pink box. Below it is a 'Reports list' table with four entries, each representing a generated risk assessment report. The first three rows of the table are highlighted with a pink box.

Exercise 6: 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. In the top navigation bar, there's a search bar and several icons. Below it, the main title is 'Defender for IoT | Sites and sensors'. A message says 'Trial subscription "BuildEnv" expired. Please contact Microsoft sales.' There are four categories: 'All sensors' (4), 'EIoT' (1), 'OT cloud connected' (2), and 'OT' (1). Under 'Management', 'Sites and sensors' is selected. The table below shows one sensor: 'D4IOT-CxE-Site - D4IOT-CxE-Site'. The 'Onboard OT sensor' button at the top right of the table is highlighted with a pink box.

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

This is a registration form for a sensor. It includes fields for Sensor name, Subscription (with a dropdown menu showing 'Onboard subscription'), and various configuration options like Cloud connected (checked), Automatic Threat Intelligence updates, Sensor version (22.X and above), Site, Resource name, Display name, Tags, and Zone. At the bottom left is a 'Register' button.

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

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

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

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

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

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

Task 3: Verify Cloud connection

1. On the sensor console.

2. On the Cloud management console.

	Sensor name	Sensor type	Zone	Subscription ...	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...	Threa...
<input type="checkbox"/>	Locally managed									
<input type="checkbox"/>	D4IOT-CxE-Site - D4IOT-CxE-Site	EloT	default	BuildEnv		Unavailable	--	-	--	...
<input type="checkbox"/>	D4IOTsensor-TT	OT cloud co...	default	BuildEnv	22.1.3.4162	✗ Disconnected	A month ago	5/25/2022	Automatic	...
<input type="checkbox"/>	sensor-Cyber	OT cloud co...	default	BuildEnv	22.1.3.4162	✓ OK	19 minutes a...	7/11/2022	Automatic	...
<input type="checkbox"/>	test1	OT cloud co...	default	BuildEnv	22.1.3.4162	✓ OK				...

Exercise 7: 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: Manage your devices

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

Device inventory

447 Total devices

78 New devices

Last active time == 03/02/2023 - 03/16/2023 Network location (Preview) == All Add filter

Showing 447 of 447 devices

Group by (Preview) No grouping

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	--	--	--	--
b25eiotlab	192.168.0.17	192.168.0.17	Industrial	PLC	Acuity Brands Lighti	255F T2550 PAC	00:11:00:4E:51:62	--
b25eiotlab	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.

10.140.32.30 Unclassified

Status Authorized 7 days ago Last Seen 0 Alert

PROCURVE NETWORKING BY HP cs-playground | EMEA | Supervisory

Network interfaces

Protocols SNMP

Tags 10.140.32.0/24 10.9.14.0/24-10.140.32.0/24

Site	IPv4 address	Name	Type	Subtype	Vendor	Model
cs-playground	10.140.32.30	10.140.32.30	Unclassified	Unclassified	PROCURVE NETWO	--
cs-playground	10.140.32.165	10.140.32.165	Unclassified	Unclassified	VMWARE INC.	--
cs-playground	10.140.32.32	10.140.32.32	Unclassified	Unclassified	HEWLETT PACKARD	--
cs-playground	10.140.32.63	10.140.32.63	Unclassified	Unclassified	IBM CORP	--
cs-playground	10.140.32.171	10.140.32.171	Unclassified	Unclassified	VMWARE INC.	--
cs-playground	10.140.33.22	10.140.33.22	Unclassified	Unclassified	VMWARE INC.	--
cs-playground	10.140.33.31	10.140.33.31	Unclassified	Unclassified	VMWARE INC.	--
cs-playground	10.140.33.30	10.140.33.30	Unclassified	Unclassified	VMWARE INC.	--
cs-playground	10.140.34.38	10.140.34.38	Unclassified	Unclassified	PRONET GMBH	--
cs-playground	10.140.33.118	10.140.33.118	Unclassified	Unclassified	VMWARE INC.	--
cs-playground	10.140.34.239	10.140.34.239	Unclassified	Unclassified	LANTRONIX	--
cs-playground	10.140.34.41	10.140.34.41	Unclassified	Unclassified	PRONET GMBH	--

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

10.140.32.30

Attributes Vulnerabilities Alerts Recommendations

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

Tags 10.140.32.0/24 10.9.14.0/24-10.140.32.0/24

Name	Value
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
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 screenshot shows the Microsoft Defender for IoT Device inventory page. At the top, there are links for Device inventory, Alerts, Incidents (Preview), Recommendations (Preview), Workbooks, and Firmware inventory (Preview). Below these are sections for Management, Troubleshooting + Support, and Diagnose and solve problems.

Key statistics at the top include 447 Total devices and 76 New devices. A chart titled "Devices by class" shows the distribution: OT (105), Endpoint (86), Network (20), and IoT (6).

The main area displays "Showing 52 groups by vendor". A search bar and filter options ("Last active time == 03/02/2023 - 03/16/2023", "Network location (Preview) == All", "Add filter") are available. A dropdown menu "Group by (Preview)" is set to "Vendor".

A table lists vendor names with counts: 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), and BROCADE COMMUNICATIONS SYSTEMS LLC (1).

Task 2: 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. The left sidebar includes links for Getting started, Device inventory, Alerts (which is selected and highlighted with a pink border), Incidents (Preview), Recommendations (Preview), Workbooks, and Firmware inventory (Preview). Management, Troubleshooting + Support, and Diagnose and solve problems sections are also present.

At the top, three summary boxes show: 584 Open alerts, 584 New alerts, and 0 Active alerts. To the right is a "Open alerts by severity" chart with a legend: High (228), Medium (196), and Low (160).

Filtering options include a search bar, "Last detection == Last month", "Status == 2 selected", and "Add filter". The main area shows "Showing 278 of 278 alerts". A "Group by" dropdown is set to "No grouping".

A detailed table lists individual alerts with columns: Severity, Name, Site, Engine, First detection, Status, Source device, and Tactics. Most alerts are categorized as POLICY_VIOLATION and detected 21 hours ago. Examples include Unauthorized Internet Connectivity, Port Scan Detected, and various PLC programming violations.

2. Click on any alert to see the details.

Showing 278 of 278 alerts

Severity	Name	Site	Engine	First detection	Status
High	Unauthorized Internet Connectivity D	b25eioltab	POLICY_VIOLATION	21 hours ago	
High	Port Scan Detected	b25eioltab	ANOMALY	21 hours ago	
Low	An S7 Stop PLC Command was Sent	b25eioltab	OPERATIONAL	21 hours ago	
High	Unauthorized PLC Programming	b25eioltab	POLICY_VIOLATION	21 hours ago	
Medium	Unauthorized PLC Configuration Writ	b25eioltab	POLICY_VIOLATION	21 hours ago	
Medium	Unauthorized PLC Configuration Writ	b25eioltab	POLICY_VIOLATION	21 hours ago	
High	Unauthorized PLC Programming	b25eioltab	POLICY_VIOLATION	21 hours ago	
High	Unauthorized PLC Programming	b25eioltab	POLICY_VIOLATION	21 hours ago	
High	Unauthorized PLC Programming	b25eioltab	POLICY_VIOLATION	21 hours ago	
Medium	Unauthorized PLC Program Upload	b25eioltab	POLICY_VIOLATION	21 hours ago	
Low	Unauthorized PLC Configuration Rec	b25eioltab	POLICY_VIOLATION	21 hours ago	
Low	Unauthorized PLC Configuration Rec	b25eioltab	POLICY_VIOLATION	21 hours ago	
Low	PLC Operating Mode Changed	b25eioltab	OPERATIONAL	21 hours ago	
Low	PLC Operating Mode Changed	b25eioltab	OPERATIONAL	21 hours ago	

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®

[View full details](#)

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

Techniques: Internet accessible device: T0883

Alert details

Source device	Site	Device IP type
Internet	b25eioltab	Internal
Source device address	Zone	First detection (in the network)
137.220.100.146	default	3/15/2023, 6:08:42 p.m.
Destination device	Sensor	Last detection (in the network)
192.168.0.110	ah1225	3/15/2023, 6:08:42 p.m.
Destination device address	Category	Last activity (manual or automated changes)
192.168.0.110	Internet Access	3/15/2023, 10:18:00 p.m.
	Protocol	
	GENERIC	

Take action

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 584 Open alerts 584 New alerts 0 Active alerts

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)							

Troubleshooting + Support

Diagnose and solve problems New support request (Preview)

Task 3: View your recommendations

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

The screenshot shows the Microsoft Defender for IoT portal interface. On the left, there's a sidebar with various tabs like 'General', 'Alerts', 'Workbooks', etc., with 'Recommendations (Preview)' highlighted. The main area is titled 'Active recommendations' and shows two items:

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

- Click on any recommendation to view full details.

This screenshot shows the details of the 'Review PLC operating mode' recommendation. It includes a summary section with severity (Medium), number of unhealthy devices (16), and last update date (3/20/2023). Below this is a table of 16 unhealthy devices, each with a name, IP, site, and last update time.

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
EIP-Line4	192.168.110.4	muli	3/1/2023

Task 4: Visualize Data by utilizing Workbooks

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

The screenshot shows the Microsoft Defender for IoT Workbooks Gallery. On the left, there's a sidebar with categories: General (Getting started, Device inventory, Alerts, Recommendations (Preview), Workbooks - highlighted with a pink box), Management (Sites and sensors, Plans and pricing, Settings (Preview)), Troubleshooting + Support (Diagnose and solve problems), and Sensors (Sensor health, Alerts, Devices, Vulnerabilities). At the top, there's a search bar, a 'New' button, and links for Refresh, Feedback, Help, Community Git repo, and Browse across galleries. Below the sidebar, there are sections for Quick start, Recently modified workbooks (8), and Defender for IoT (4). Each item has a thumbnail, name, and a brief description.

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

Sensors

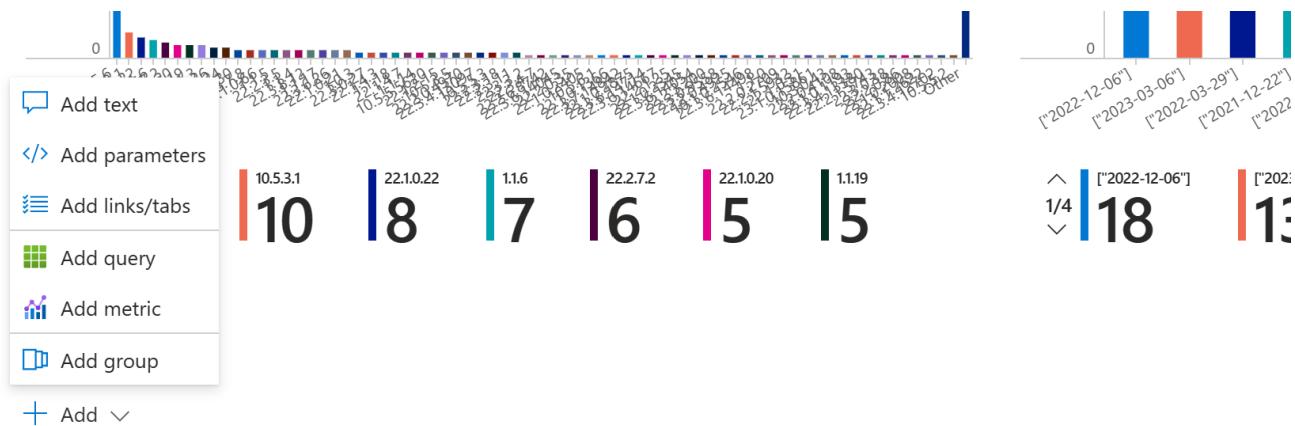
This report consolidates data regarding your sensors' health.

The screenshot shows the Sensor health - Overview page. It includes a donut chart with the following data: Unavailable (842), Disconnected (313), and Ok (18). Below the chart are two line charts: 'Sensor version' and 'TI version'. The 'Sensor version' chart shows a high count of sensors (~150) with a small number of others. The 'TI version' chart shows a distribution of TI versions from ~0.06 to ~0.17.

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

The screenshot shows the top ribbon of the Microsoft Defender for IoT interface. The buttons visible are: Workbooks, Edit (highlighted with a pink box), Refresh, Feedback, Help, Auto refresh: Off.

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



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

Exercise 8: Integrate with Microsoft Sentinel

Task 1: Create a Log Analytics Workspace

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

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

- 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](#)

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 *	CS-playground
Resource group *	CS-playground
	Create new

Instance details

Name *	VishakhaSentinel
Region *	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.

Add Microsoft Sentinel to a workspace

+ Create a new workspace ⏪ Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
DemoTogether	centralus	demotogether	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.

The screenshot shows the Microsoft Sentinel News & guides interface. At the top, it says "Selected workspace: 'handsonlab'". Below that is a search bar and a documentation link. The navigation menu includes "General", "Overview", "Logs", and "News & guides", with "News & guides" being the active tab. The main content area features the heading "A cloud-native SIEM to h".

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

The screenshot shows the Microsoft Sentinel Content Hub. On the left is a sidebar with "General", "Threat management", "Content management", and "Configuration" sections. The "Content hub (Preview)" option under "Content management" is selected. In the center, there's a search bar with "Defender for IoT" typed in. A detailed view of the "Microsoft Defender for IoT" solution is shown on the right, including its provider (Microsoft), support (Microsoft Support), version (2.0.2), and a brief description. The "Install" button is highlighted with a pink box.

3.Click on “Create”.

The screenshot shows the Microsoft Defender for IoT solution creation page. It features a "Microsoft Defender for IoT solution for Microsoft Sentinel" title, a "Plan" dropdown set to "Microsoft Defender for IoT", and a prominent "Create" button. The "Create" button is highlighted with a pink box.

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 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 one row: 'Microsoft Defender for IoT' by Microsoft, which is connected. There are filters for 'Status', 'Connector name', 'Providers', 'Data Types', and 'Status'.

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			
	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 displays three counts: 917 Open incidents, 917 New incidents, and 0 Active incidents. Below these are filters for Severity (All), Status (2 selected), and a Product name dropdown. The Product name dropdown is open, showing a list of products with checkboxes. The 'Microsoft Defender for IoT' checkbox is checked. A red box highlights this dropdown. To the right of the grid, there's a summary chart titled 'Open incidents by severity' with categories: High (121), Medium (458), Low (338), and Informational (0). A large red box also highlights the entire right-hand pane where the summary chart and incident details would be displayed.

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 right side features a detailed view of a specific incident. The incident details pane includes:

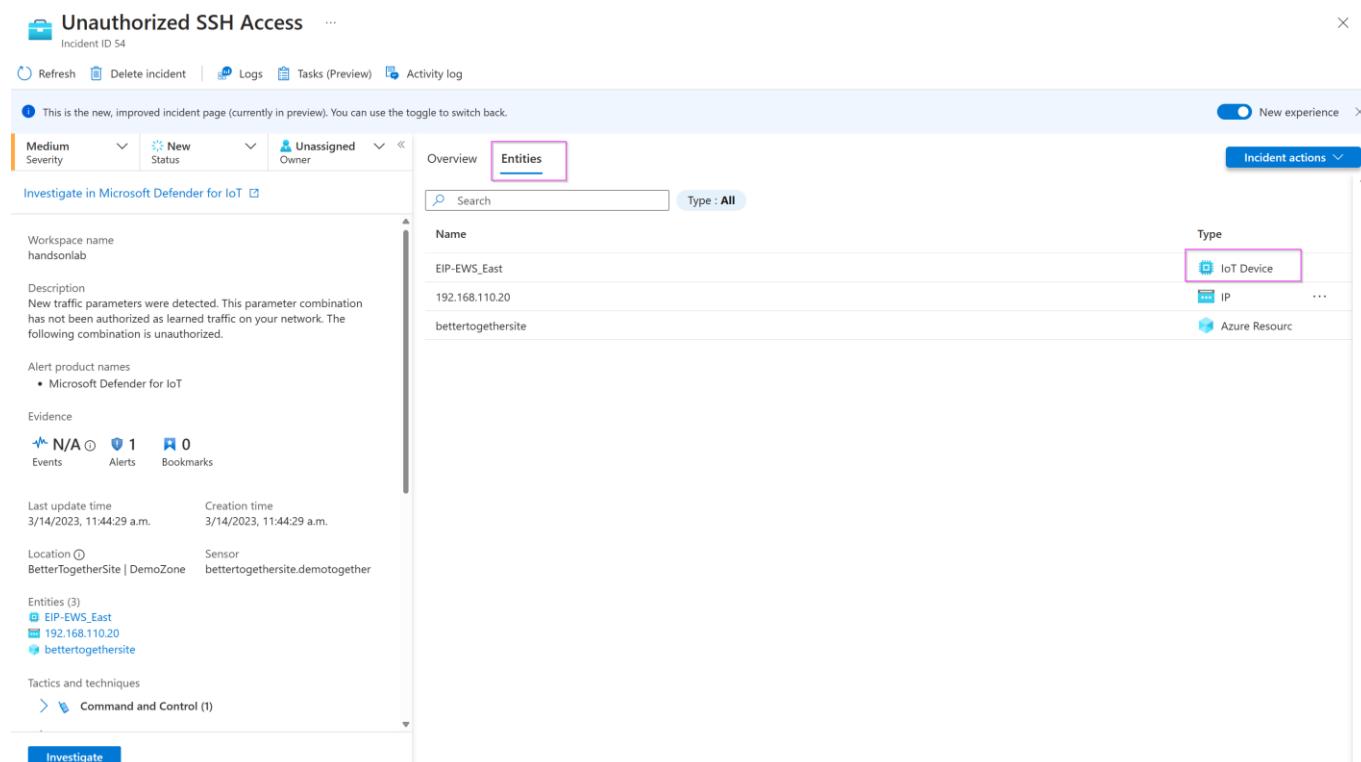
- Incident Summary:** Malicious Domain Name Request, Incident ID: 107793, Status: New, Owner: Unassigned.
- Description:** Suspicious network activity was detected. This activity may be associated with an attack exploiting a method used by known malware.
- Alert product names:** Microsoft Defender for IoT.
- Evidence:** 1 Event, 0 Alerts, 0 Bookmarks.
- Last update time:** 09/22/22, 10:36 AM.
- Creation time:** 09/22/22, 03:05 AM.
- Entities:** 1 (192.168.42.23), with a link to 'View full details'.
- Tactics and techniques:** Command and Control (1), Initial Access (0).
- Links:** Incident workbook, Incident Overview.

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 (Events: N/A, Alerts: 1, Bookmarks: 0), 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 9: 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 10: 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.