
DEFENDER HANDS ON LAB

Contents

Class Objective:	8
OT/ICS Security Overview	8
Hands on Experience with Defender for IoT	8
Understanding security challenges and using D4IOT data to gain insights	8
Understanding security technologies and the Microsoft Platform	8
Exercises	8
Exercise 1- Setting sensor environment for class.....	8
• Import firewall rules	8
• Import subnet list	8
• Play pcap file(s).....	8
• Verify data collection	8
Step 1	9
Edit System Properties to enable pcap player	9
Step 2	10
Upload pcaps.....	10
Step 3	11
Import firewall rules from the System Settings -> Firewall Rules	11
Step 4	14
Import subnets	14
Step 5	15
Play pcaps by hitting Play All	15
Step 6	16
Verify data collection	16

Exercise 2: Device Map	18
• Device Map.....	18
• Layout by Perdue Model	18
• Select Ethernet/IP.....	18
• Connection Details.....	18
• Device Connections.....	18
• Device Properties.....	18
• Search for device	18
Step 1	18
Select Device Map.....	18
Step 2	19
Lay out map with Perdue Model and confirm.....	19
Step 3	21
Select Ethernet/IP.....	21
Step 4	22
Connection details.....	22
Step 4	23
Select 10.0.100.104	23
Step 5	24
Device Properties.....	24
Step 6	27
Device Search	27
Exercise 3: Attack Vectors.....	31
• Select Device	31

• Select Simulate Attack Vectors.....	31
• Name Simulation	31
• Select Maximum Number of Vectors.....	31
• Run Simulation.....	31
• Inspect Results.....	31
Step 1	32
Right click on 10.0.100.104	32
Step 2	32
Select “Simulate Attack Vectors	32
Step 3	32
Name simulation	32
Step 4	33
Select the maximum number of vectors.....	33
Step 6	33
select “Run”.....	33
Step 5	34
Exercise 4 Inventory.....	35
• Inventory	36
• Column Editing	36
• Device selection.....	36
• Device Details	36
• Device Map View	36
• Device Alerts.....	36

• Device Details	36
Step 1	36
Select “Inventory”.....	36
Step 2	38
Edit Columns.....	38
Step 3 select	39
192.168.119.3.....	39
Step 4	39
“View full details”	39
Step 5	41
Click on Map View	41
Step 6	42
Click the Alerts tab.....	42
Step 7	43
Highlight an alert and “get full details”.....	43
Exercise 5 Alerts.....	46
• Select Alerts from menu.....	46
• View Grouping Options.....	46
• Group By Severity	46
• Investigate Port Scan and details.....	46
• Take Action.....	46
Step 1	46
Select Alerts from menu	46
Step 2	47

Grouping Option.....	47
Step 3	48
Group the alerts by Severity and scroll down to the bottom	48
Step 4	49
Select Critical “Port Scan Detected” and then “View Full Details”	49
Step 5	51
“Take Action” tab.....	51
Exercise 6 Risk Assessment	53
• Select Risk Assessment	53
• Create Report	53
• Download File.....	53
• Open File	53
• Review.....	53
Step 1,.....	53
Select Risk Assessment from Menu.....	53
Step 2 Generate Report	53
Step 3 Download and Open.....	54
Exercise 7 Data Mining.....	56
• Open Data Mining.....	56
• Open each Recommended Reports	56
• Create Report	56
Step 1	56
select “Data Mining”	56
Step 2	57

Review the “recommended” reports.....	57
Step 3	57
Open each of them and see what they contain.	57
Step 4	58
Select the “Create Report”.....	58
Step 5	59
Step 6	60
Build another report	60
Step 7	61
Save the report and open it.	61
Step 8	61
Expand each sub catagory.....	61
Exercise 8 Event Timeline.....	62
• Open Event Timeline.....	62
• Review types of notifications provided.....	62
• Search for event.....	62
• View Event.....	62
Step 1	62
Select “Event Timeline”.....	62
Step 2	63
Scroll through these different events and the info provided.....	63
Step 3	64
Step 4	65
Exercise 9 Trends and Statistics.....	66

• Trends and Statistic.....	66
• Dashboard Creation	66
• Add Widgets	66
Step 1	67
Select Trends and Statistics then “create dashboard”	67
Step 2	68
Create a dashboard by giving it a name, and then hit “save”	68
Step 3	68
“Add Widget” and select from the list that appears on the right hand side.....	68
Step 4	69
Chose “Traffic by Port”	69
Step 5	69
Add other widgets, experiment with the page layout,.....	69

Class Objective:

OT/ICS Security Overview

Hands on Experience with Defender for IoT

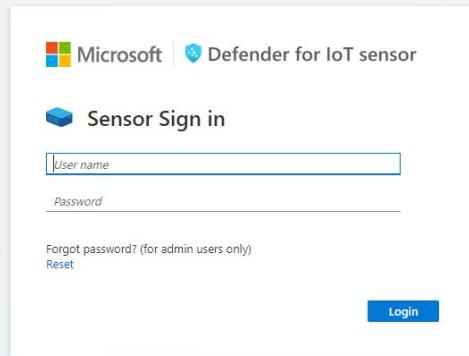
Understanding security challenges and using D4IOT data to gain insights

Understanding security technologies and the Microsoft Platform

Exercises

Exercise 1- Setting sensor environment for class

- Login
- Import firewall rules
- Import subnet list
- Play pcap file(s)
- Verify data collection



Step 1

Edit System Properties to enable pcap player

Microsoft | Defender for IoT - 22.1.4

Home > System settings

Defender for IoT | System settings

Search:

Sensor management

Updates

- Software Update**
Update the software version on this sensor
- Threat Intelligence**
Update the threat intelligence package on this sensor

Security

- Subscription & Activation Mode**
Upload an activation file to reactivate this sensor

Health and troubleshooting

- Backup & Restore**
Backup data and restore the latest backup
- System Health Check**
Review network properties, statistics and other data related to sensor health
- SNMP MIB Monitor**
Resolve device hostnames based on addresses detected on subnets.

Integrations

Import settings

Advanced configurations

Pcaps

```
size.megabytes.max=52800  
archive.size.megabytes.max=  
size.megabytes.min=8704  
archive.size.megabytes.min=  
cache.should.save.pcap=1  
archive.cache.dir=  
filtered.cache.dir.size.megabytes.max=2560  
filtered.cache.dir.size.megabytes.min=1536  
filtered.archive.dir.size.megabytes.max=  
filtered.archive.dir.size.megabytes.min=  
filtered.archive.dir=  
player.max_size=50000  
player.max_amount=450  
player.params=-M 5  
enabled=1  
virtual.lan.hierarchy.depth.support=1
```

Save

Close

The screenshot shows the Microsoft Defender for IoT system settings page. On the left, there's a sidebar with categories like Discover, Analyze, Manage, and Support. Under Manage, 'System settings' is selected. The main area has sections for Sensor management, Security, and Health and troubleshooting. A 'Sensor management' section contains 'Software Update' and 'Threat Intelligence' options. The 'Security' section has a 'Subscription & Activation Mode' option. The 'Health and troubleshooting' section includes 'Backup & Restore', 'System Health Check', and 'SNMP MIB Monitor'. At the bottom, there are 'Integrations' and 'Import settings' links. On the right, a modal window titled 'Advanced configurations' is open, showing a configuration for 'Pcaps' with a large block of JSON-like configuration code. There are 'Save' and 'Close' buttons at the bottom of the modal.

Step 2

Upload pcaps

The screenshot shows the Microsoft Defender for IoT - 22.1.4 interface. The left sidebar includes sections for Discover, Analyze, Manage, and Support. Under Manage, 'System settings' is selected. The main content area displays 'Basic' configuration options under 'Sensor Setup', such as Sensor Network Settings, Connection to Management Console, SSL/TLS Certificate, and Play PCAP. A 'Network monitoring' section is partially visible. On the right, a modal window titled 'PCAP PLAYER' is open, showing uploaded files: alerts.pcapng, classa_edited.pcapng, and classb_edited.pcapng. Buttons for Upload, Play All, and Clear All are present.

Step 3

Import firewall rules from the **System Settings -> Firewall Rules**

Select file

Home > System settings

Defender for IoT | System settings

- Search
- 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

Backup & Restore

Backup data and restore the latest backup

System Health Check

Review network properties, statistics and other data related to sensor health

SNMP MIB Monitoring

Resolve device hostnames based on IP addresses detected on subnets.

Advanced Configurations

Modify sensor configuration files

Integrations

Active Directory

Allow users to log in with Active Directory credentials

Access Tokens

Generate access tokens when working with REST APIs

ClearPass

Integrate with Aruba ClearPass

Mail server

Define SMTP mail server settings

ServiceNow

Integrate with ServiceNow

Import settings

Firewall rules

Import firewall rules. Rules are analyzed in the Risk Assessment report.

Device Information

Import device information

Authorized devices

Import authorized device IP addresses and names

Windows Information

Import Windows registry information

Microsoft | Defender for IoT - 22.1.4

Home > System settings

Defender for IoT | System settings

Search

Discover

- Overview
- Device map
- Device inventory
- Alerts

Analyze

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

Manage

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

Subscription & Activation Mode
Upload an activation file to reactivate this sensor

Health and troubleshooting

- Backup & Restore
Backup data and restore the latest backup
- System Health Check
Review network properties, statistics and other data related to sensor health
- SNMP MIB Monitor
Resolve device hostnames based on addresses detected on subnets

Integrations

- Firewall rules
Import firewall rules. Rules are analyzed in the Risk Assessment report.
- Device Information
Import device information
- Authorized devices
Import authorized device IP addresses and names

Firewall Rules

Import firewall rules. Rules are analyzed in the Risk Assessment report.

Choose Firewall type

Checkpoint

Fortinet

Juniper

#	Name	Created	Size	Action
1	cyberx-checkpoint-policies-cyberx-origin...	22 hours ago	28 kB	

Close

Step 4

Import subnets

This will assign names to some of the subnets that we will encounter during the exercise

The screenshot shows the Microsoft Defender for IoT interface version 22.1.4. The left sidebar includes sections for Overview, Device map, Device inventory, Alerts, Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector, System settings (selected), Custom alert rules, Users, Forwarding, Support, and Security.

The main area displays the "Basic" configuration under "System settings". It features several cards: "Sensor Network Settings" (Define sensor network settings), "Connection to Management Console" (Connect this sensor to the on-premise management console), "SSL/TLS Certificate" (Manage SSL/TLS certificates installed on this sensor), "Play PCAP" (Upload and play PCAP files), "Network monitoring" (indicated by a right-pointing arrow), "Sensor management" (with "Updates" sub-section containing "Software Update" and "Threat Intelligence" cards), and "Security" (indicated by a right-pointing arrow).

A modal window titled "Subnets" is open on the right. It contains instructions: "Define which networks should be monitored. Networks not listed as subnets are treated as external networks." Below are buttons for "Import subnets" (with an upward arrow icon), "Export subnets" (with a downward arrow icon), and "Clear all" (with a trash bin icon). A checkbox for "Auto subnet learning" is checked, and an unchecked checkbox for "Resolve all Internet traffic as internal/private" is present. The main table lists 15 subnets:

IP Address *	Mask *	Name	Actions
192.168.0.0	255.255.255.0	BMS-Network	<input checked="" type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
192.168.1.0	255.255.255.0	EGD-Network	<input checked="" type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
10.0.101.0	255.255.255.0	Unit1-Rockwell	<input checked="" type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
192.168.118.0	255.255.255.0	Unit1-Siemens	<input checked="" type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
10.0.100.0	255.255.255.0	Unit2-Rockwell	<input checked="" type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
192.168.124.0	255.255.255.0	DNP3-Network	<input checked="" type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
192.168.119.0	255.255.255.0	Unit2-Siemens	<input checked="" type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
192.168.11.0	255.255.255.0	DataCollection	<input type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
192.168.111.0	255.255.255.0	DeltaV-Network	<input checked="" type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
192.168.110.0	255.255.255.0	Name	<input type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
192.168.10.0	255.255.255.0	DMZ-Network	<input type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
10.10.3.0	255.255.255.0	LocalEnvironment	<input type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated
192.168.108.0	255.255.255.0	Honeywell-Netw...	<input checked="" type="checkbox"/> ICS Subnet <input type="checkbox"/> Segregated

At the bottom of the modal are "Save" and "Cancel" buttons.

Step 5

Play pcaps by hitting **Play All**

The screenshot shows the Microsoft Defender for IoT - 22.1.4 interface. The left sidebar includes sections for Home, Discover, Analyze, and Manage. Under Manage, the 'System settings' option is selected. The main content area displays various configuration cards under 'Basic' and 'Sensor Setup'. A 'PCAP PLAYER' overlay is open on the right, titled 'Upload and replay PCAP files.' It contains a file list with 'alerts.pcapng', 'classa_edited.pcapng', and 'classb_edited.pcapng', along with buttons for 'Upload', 'Play All', and 'Clear All'.

Step 6

Verify data collection

Microsoft | Defender for IoT - 22.1.4

Home > **Defender for IoT | Overview**

Search

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

202 PPS

99 Devices

28 Alerts

Version: 22.1.4.2-r-9737658

Threat Intelligence: Version 2021.12.22 | Last updated Dec 22, 2021

Connectivity type: Locally Managed

Activation: Valid until 01/31/2023

Certificate: Valid

System settings >

Trends & statistics >

Top 5 OT Protocols

Protocol	Devices
CIP	7 Devices
EtherNet/IP	7 Devices
EGD	5 Devices
BACNet (NPDU)	5 Devices
BACNet	5 Devices

Device map >

Traffic By Port

Device inventory >

Top open alerts

Severity	Name	Engine	Detection time
Critical	Unauthorized Internet Co...	Policy Violation	22 hours ago
Critical	Unauthorized Internet Co...	Policy Violation	22 hours ago
Critical	Unauthorized Internet Co...	Policy Violation	22 hours ago
Critical	Unauthorized Internet Co...	Policy Violation	22 hours ago
Critical	Unauthorized Internet Co...	Policy Violation	22 hours ago

Alerts >

enp3s0
enp4s0
enp5s0
enp0s31f6
enp1s0

Observe the following are populating as the pcap plays

- PPS rate
- Devices
- Alerts

In this screen there is a great deal of information available about the sensor and what it is observing

Look at each of these fields and what they tell you

General Settings

Version

Threat Intelligence

Connection Type

Interfaces (collecting data)

Traffic Monitor- Histogram of traffic presented to sensor, measured in Mb/s

-Link to Trends and Statistics page

Top OT Protocols- Top 5 displayed

-Link to Device Map

Traffic by Port

-Link to Device Inventory

Top Open Alerts

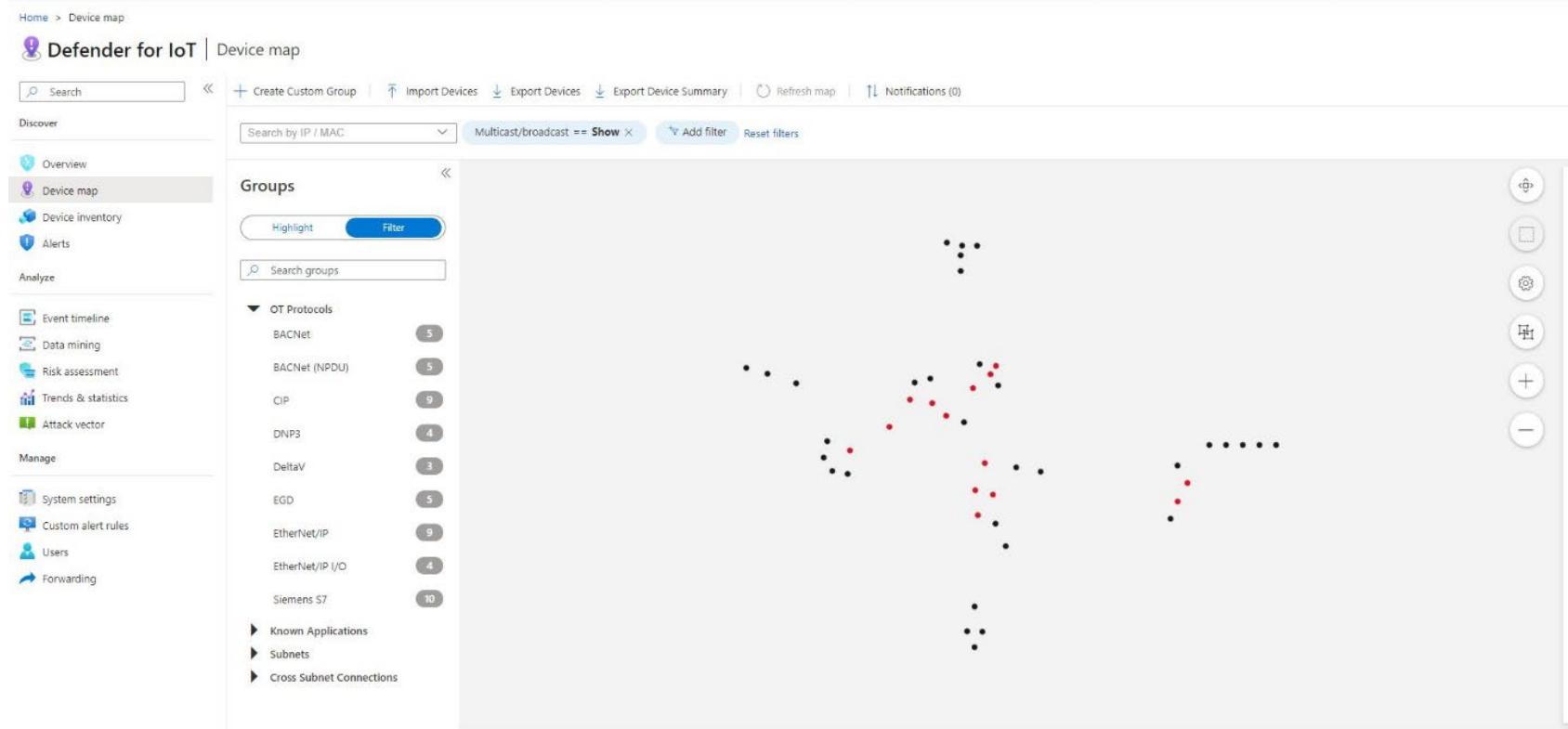
-Link to Alerts

Exercise 2: Device Map

- Device Map
- Layout by Perdue Model
- Select Ethernet/IP
- Connection Details
- Device Connections
- Device Properties
- Search for device

Step 1

Select **Device Map**



Default view is by connections,

Step 2

Lay out map with Perdue Model and confirm

Click **gear** icon and select **Layout by Perdue** option and **confirm**.

Defender for IoT | Device map

Search | Create Custom Group | Import Devices | Export Devices | Export Device Summary | Refresh map | Notifications (0)

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

Groups

Highlight Filter

Search groups

Multicast/broadcast == Show Add filter Reset filters

OT Protocols
Known Applications
Non-Standard Ports
Subnets
Cross Subnet Connections

Pin Layout
Layout by Connections
Layout by Purdue

Each dot represents an asset discovered by the sensor. Those colored Red have an alarm associated with them.

These are laid out in the Perdue Model

Enterprise Traffic at the top.

IT type traffic, Mail, VOIP, TEAM, Web, etc

Supervisory Traffic in the middle

Typically, Human Machine Interfaces and Engineering Workstations

Process Control on the bottom

Programable Logic Controller and Remote Terminal Units

On the left of the screen, you will see groupings by like attributes including:

OT Protocols

Known Applications

Subnets

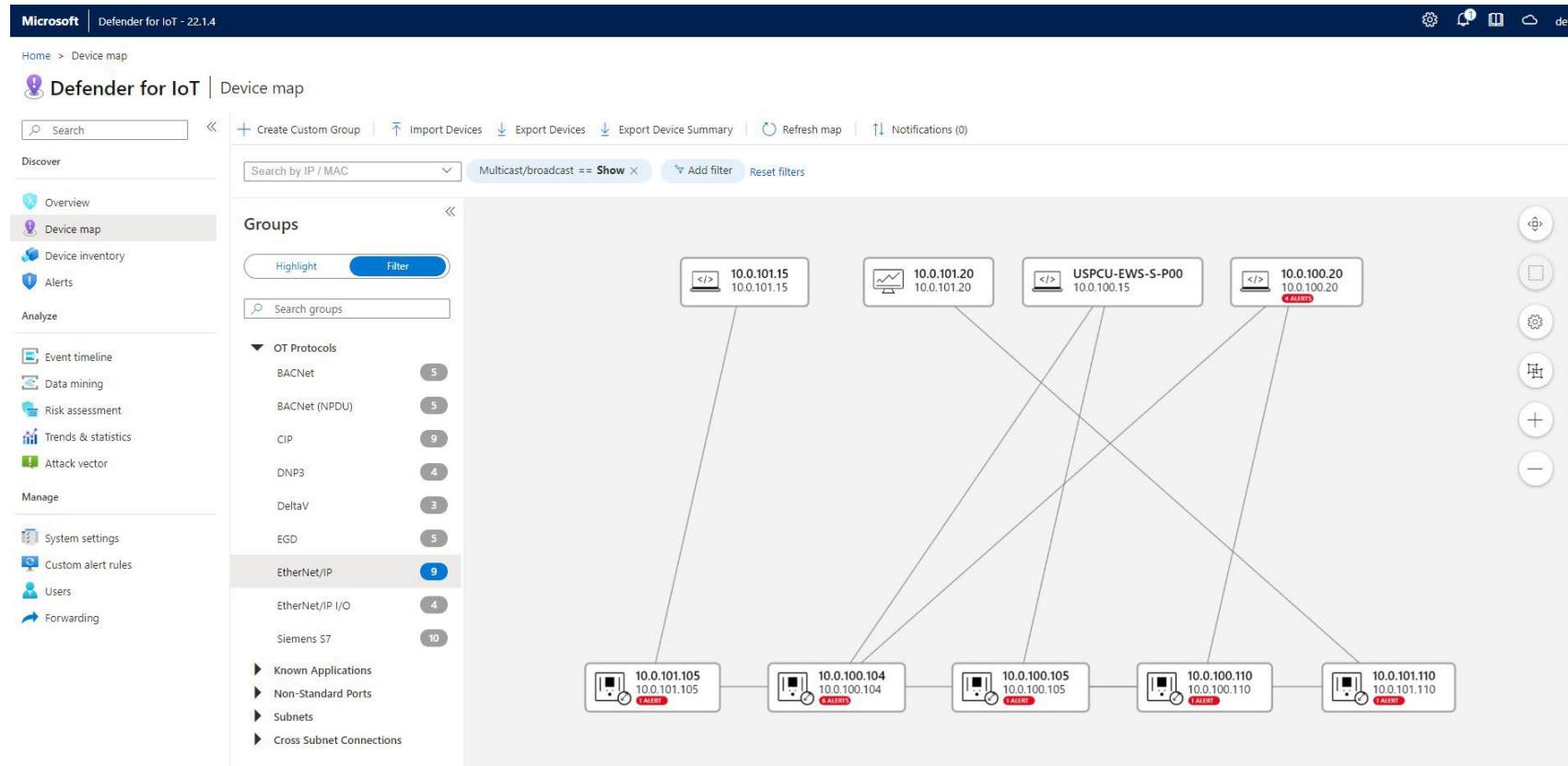
Cross Subnet Connections

Each group allows you to click on the right arrow and expand, showing the groups and the number of assets in each

Step 3

Select Ethernet/IP

Select **Ethernet/IP** as the OT protocol and **Filter** the view to only show those devices that have been observed communicating with Ethernet/IP



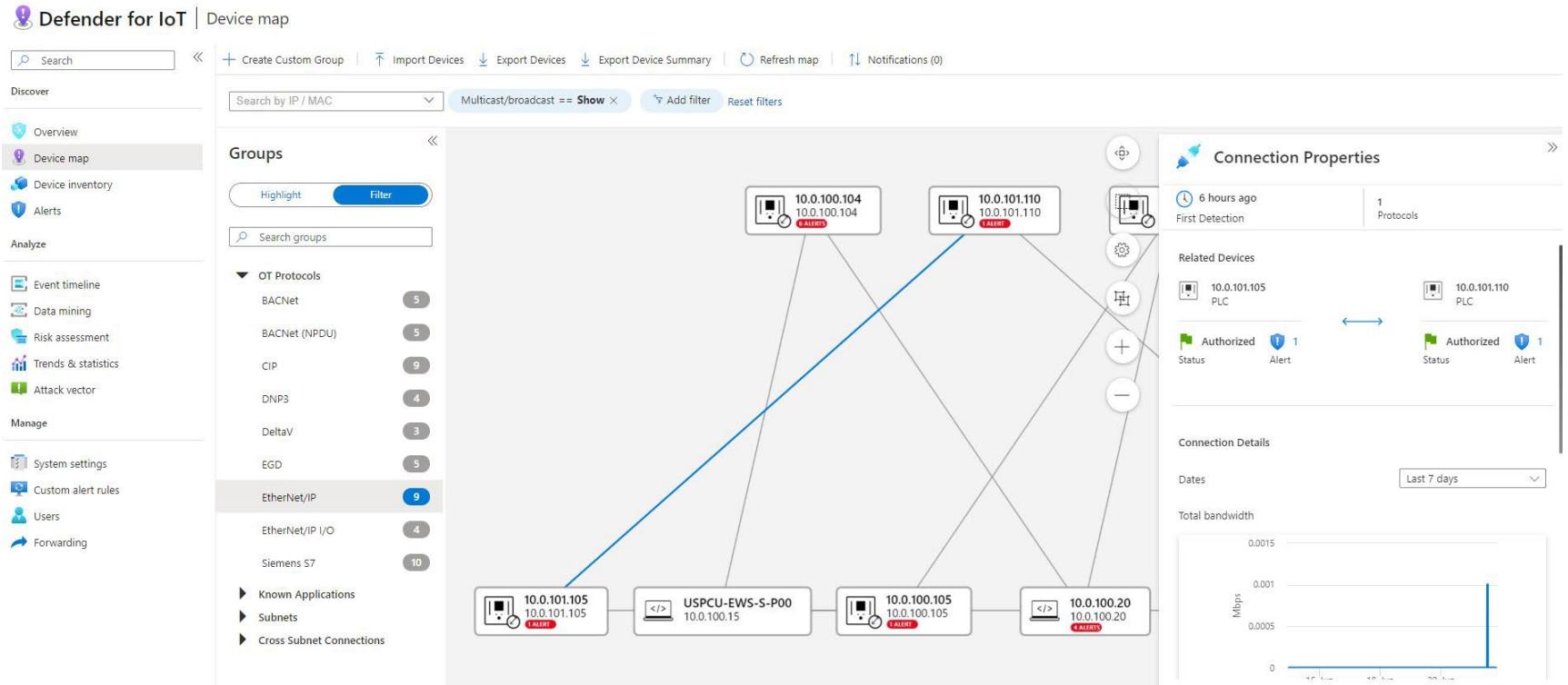
Observe in the field to the right that the icons are now larger, and we can see the connections they have with one another.

Step 4

Connection details

Click a line connecting two devices, then open the “properties” panel on the right.

This will show the two devices that are connected, authorization status, when and how they communicate.



Step 4

Select 10.0.100.104

the device will be outlined in blue and the connections it has to other devices will also change to blue.



Step 5

Device Properties

Right click on the item and select “view properties”

Device | 10.0.100.104



Authorized Status | 6 hours ago | 6 Alert | <<

Backplane (Preview) Attributes Map View Alerts Event Timeline

General Information

- Type: PLC
- Vendor: ROCKWELL AUTOMATION
- Location: Automatic

Network Interfaces

IP: 10.0.100.104	MAC: 00:1d:9c:d2:33:60
------------------	------------------------

Protocols

- EtherNet/IP
- CIP

Backplane
View the backplane hardware configuration detected on devices.

Rack 01

Slot	00	01	02	03	04
Default	Communications Adapter 1769-L35E Eth...	Communications Adapter 17 Nested	CPU 1756-L735B L...	Communications Adapter 1756-DN8/C	Communications Adapter 1 Nested 1756-A

Slot Default
Communications Adapter

Serial: 0x404D13C3 | Firmware version: 20.11 | Model: 1769-L35E Ethernet Port

Edit Properties

In this screen you will observe the following bits of information including:

Authorization Status

When it was last seen communicating

Type, Vendor, IP, and MAC addresses.

Look at the backplane and notice what devices are filling the slots. You will see:

CPU, Communication Adapters, Analog I/O, Digital I/O

As each of those is selected the field to the right will populate with:

Slot number, Serial Number, Firmware Version, and Model

Navigate through the different options available in the Map section, including other protocols, subnets,

Right click on any device and explore its properties, alerts, events, activity. You can add devices to custom groups, simulate attack vectors, mark things important, unauthorize, and even delete from the map.

Defender for IoT | Device map

Search

Create Custom Group Import Devices Export Devices Export Device Summary Refresh map Notifications (1)

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

Groups

Highlight Filter

Search groups

OT Protocols

- BACNet (5)
- BACNet (NPDU) (5)
- CIP (8)
- DNP3 (4)
- DeltaV (3)
- EGD (5)
- EtherNet/IP (8)
- Profinet DCP (1)
- Profinet Real-Time (1)
- Siemens S7 (10)

Known Applications Subnets Cross Subnet Connections CDP Protocol

Multicast/broadcast == Show Add filter Reset filters

Supervisory Process Control

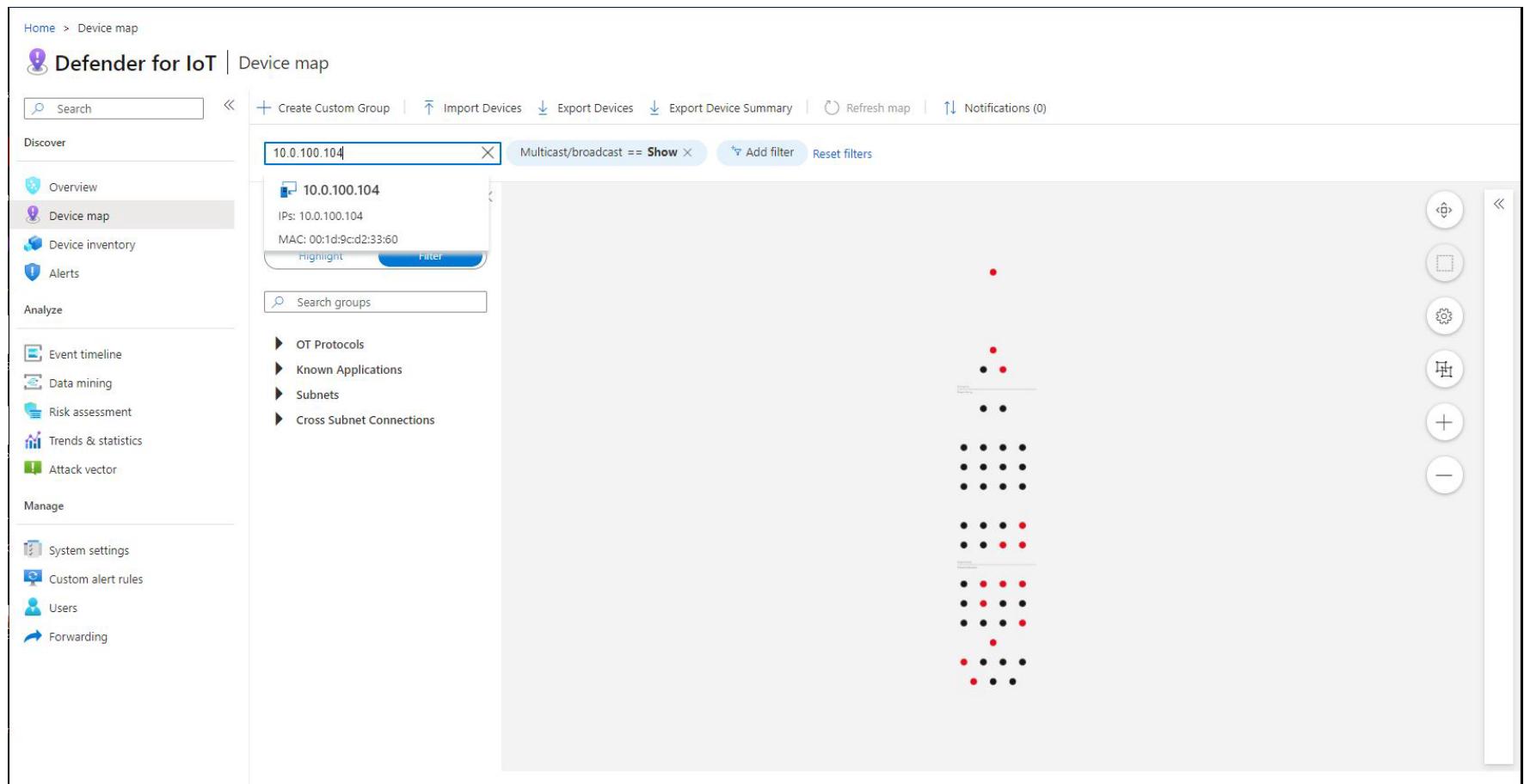
View properties Unauthorized Mark as Non important Show Alerts Show Events Activity Report (Last 1 Hour) Activity Report (Last 6 Hours) Activity Report (Last 12 Hours) Activity Report (Last Day) Simulate Attack Vectors Add to custom group Delete

Device map

Step 6

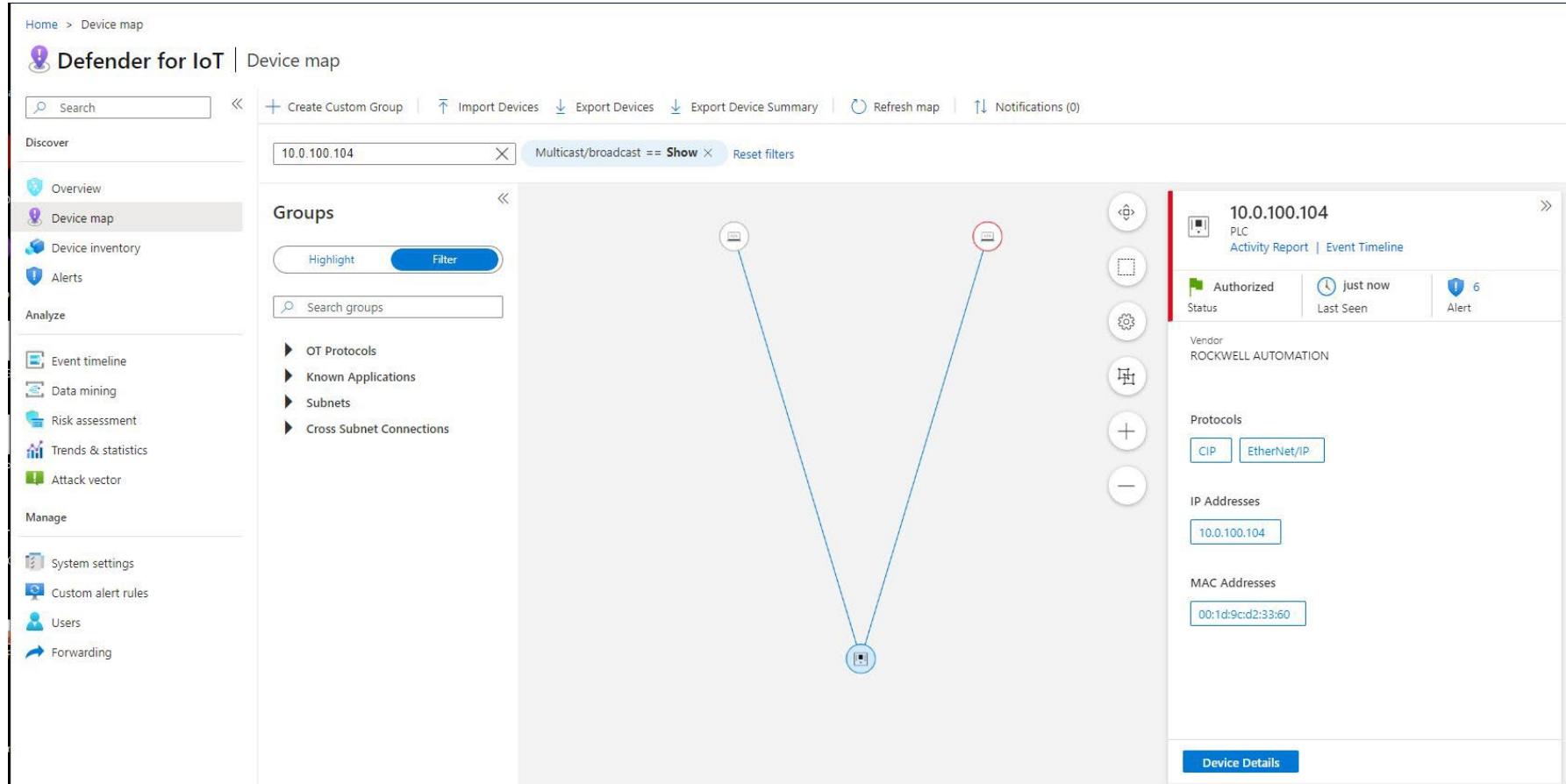
Device Search

Using the Search feature within the Device Map, look for 10.0.100.104



Look at 10.0.100.104

Here you see the connections it has to other devices:



and when you click “device details” you will see the following:

Microsoft | Defender for IoT - 22.1.4

Home > Device map > 10.0.100.104

Device | 10.0.100.104

Authorized Status | just now Last Seen | 6 Alert

General Information

Type PLC	Vendor ROCKWELL AUTOMATION	Location Automatic
⚠️ Unsecure mode		

Network Interfaces

IP 10.0.100.104	MAC 00:1d:9c:d2:33:60
-----------------	-----------------------

Protocols

EtherNet/IP CIP

Backplane (Preview) Attributes Map View Alerts Event Timeline

Backplane

View the backplane hardware configuration detected on devices.

Rack 01

Slot	00	01	02	03	04
Default	Communications Adapter 1769-L35E Eth...	Communications Adapter 17 Nested	CPU 1756-L735/B L...	Communications Adapter 1756-DNB/C	Communications Adapter 1 Nested VAI769/A

Slot Default Communications Adapter

Serial 0x404D13C3 Firmware version 20.11

Model 1769-L35E Ethernet Port

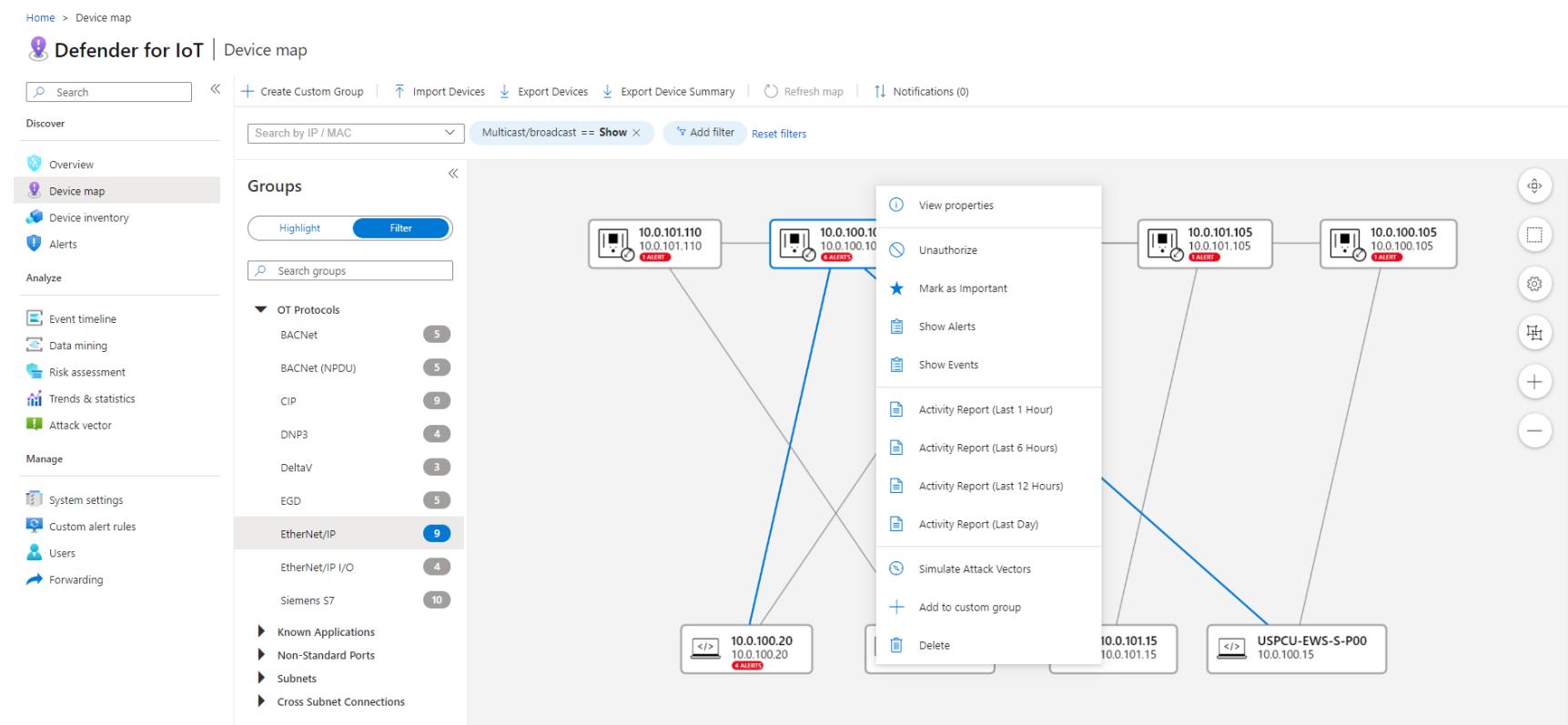
Edit Properties

Exercise 3: Attack Vectors

- Select Device
- Select Simulate Attack Vectors
- Name Simulation
- Select Maximum Number of Vectors
- Run Simulation
- Inspect Results

Step 1

Right click on 10.0.100.104



Step 2

Select "Simulate Attack Vectors"

Step 3

Name simulation

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar has sections for Discover (Overview, Device map, Device inventory, Alerts), Analyze (Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector), and Manage (System settings, Custom alert rules, Users, Forwarding). The 'Attack vector' section is selected. The main area shows a tree view with 'any2any (5)' expanded. On the right, a modal window titled 'Add attack vector simulation' is open, asking to 'Reduce your attack surface by simulating exploitable network attack paths and reviewing the impact of mitigation.' It contains fields for 'Name *' (def), 'Maximum Vectors *' (5), and several toggle switches: 'Show in Device Map' (off), 'Show All Source Devices' (on), and 'Show All Target Devices' (off). Below these are dropdowns for 'Attack Target *' (1 selected: 10.0.100.104) and 'Exclude Devices' (Search). At the bottom are 'Save' and 'Cancel' buttons.

Step 4

Select the maximum number of vectors

Step 6

select "Run"

Step 5

Inspect Results

Home > Attack vector

Defender for IoT | Attack vector

Search Add simulation

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

104 (3)

Risk level	Source IP	Target IP
59/100	192.168.0.110	→ 10.0.100.104
48/100	10.0.100.20	→ 10.0.100.104
31/100	USPCU-EWS-S-P00	→ 10.0.100.104

Show in Device map

192.168.0.110 → 10.0.100.104

Define which networks should be monitored.

Attacker Targeted Attack

1 Internet Connection
192.168.0.110 is exposed to external threats due to internet connectivity
192.168.0.110 | 192.168.0.110

2 Network Connection
Direct connection between devices located in different subnets
192.168.10.200 | 192.168.10.200

3 Remote Access
Allowed remote access using Remote Desktop
10.0.100.20 | 10.0.100.20

4 Known CVE
Device 10.0.100.104 has a known CVE vulnerability CVE-2012-6437 that can be exploited.
Description: Rockwell Automation EtherNet/IP products: 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 do not properly

Select each of the vectors the system has found.

Start looking from the bottom of this vector.

Notice that the PLC 10.0.100.104 has a CVE associated with it, this is based upon the information we learned about it Manufacturer, Model, and Firmware.

So this device has a known exploit, but if someone cannot reach it the concern is huge (perhaps it can be upgraded later)

The other concerns are above that in the chain.

Remote Access

Network Connections

Internet connections.

[Exercise 4 Inventory](#)

- Inventory
- Column Editing
- Device selection
- Device Details
- Device Map View
- Device Alerts
- Device Details

Step 1

Select “Inventory”

Defender for IoT | Device inventory

Search | Save Filter | Refresh | Edit Columns | Export

Add filter

Showing 100 of 213 Items

	IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmware Version	Model	Operating System
<input type="checkbox"/>	192.168.119.5	192.168.119.5	12 minutes ago	PLC	Siemens S7	00:01:e3:19:23:aa	SIEMENS AG	3.2.7	6EST 315-2EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-8EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-6EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-6EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-7EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	5.3.5	6EST 412-1XJ05...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-6EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-10H14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-9EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-5EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-15H14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-17H14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-19H14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-3EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-6EH14...	
<input type="checkbox"/>	192.168.119.3	192.168.119.3	12 minutes ago	PLC	Siemens S7	00:01:e3:19:22:33	SIEMENS AG	3.2.6	6EST 315-2EH14...	

Load More...

Step 2

Edit Columns

Step 3 select

192.168.119.3

Home > Device inventory

Defender for IoT | Device inventory

The screenshot shows the 'Device inventory' section of the Defender for IoT web interface. On the left, a sidebar lists categories: Discover (Overview, Device map, Device inventory selected), Analyze (Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector), and Manage (System settings, Custom alert rules, Users, Forwarding). The main area displays a table of 100 items from 213 total. The table columns are: IP Address, Name, Last Activity, Type, Protocols, MAC Address, and Vendor. A row for '192.168.119.3' is highlighted with a blue selection box around its IP address. To the right, a detailed view panel for '192.168.119.3' shows the following information:

	192.168.119.3	PLC
Status	Authorized	Last Seen 3 minutes ago
Alerts 2		
General Information		
Type	Vendor	Location
PLC	SIEMENS AG	Automatic
Network Interfaces		
IP	MAC	
192.168.119.3	00:01:e3:19:22:33	
Protocols		
Siemens S7		

A 'View full details' button is located at the bottom right of the detailed view panel.

Step 4

"View full details"

Home > Device inventory > 192.168.119.3

Device | 192.168.119.3

Authorized Status
Last Seen 3 minutes ago
Alert 2

Backplane (Preview)
Map View
Alerts
Event Timeline

General Information

Type	PLC	Vendor	SIEMENS AG	Location	Automatic
------	-----	--------	------------	----------	-----------

Network Interfaces

IP	192.168.119.3	MAC	00:01:e3:19:22:33
----	---------------	-----	-------------------

Protocols

- Siemens S7

Backplane
View the backplane hardware configuration detected on devices.

Rack 00

Slot	Module Type	Model
01	Power Supply	6E57 315-2EH...
02	CPU	6E57 412-1XJ0...
03	Generic	6E57 315-5EH...
04	Generic	6E57 315-6EH...
05	Generic	6E57 315-6EH...
06	Generic	6E57 315-6EH...
07	Generic	6E57 315-6EH...

Rack 01

Slot	Module Type	Model
01	Generic	6E57 315-7EH...
02	Generic	6E57 315-8EH...
03	Generic	6E57 315-9EH...
04	Generic	6E57 315-10H...

Slot 01
Power Supply

Firmware version 3.2.6

Hardware revision 4.1

Hardware vendor Siemens

Model 6E57 315-2EH14-0AB0

Module version 3

[Edit Properties](#)

Notice that this is an even more complex PLC, Multiple Racks and each with their populated slots.

Some manufacturers offer , in addition to model/firmware, extra data In this case Module and Hardware revision.

Step 5

Click on Map View

Home > Device inventory > 192.168.119.3

Device | 192.168.119.3

Status | Authorized | 3 minutes ago | Last Seen | Alert | << | Backplane (Preview) | Map View | Alerts | Event Timeline

General Information

Type PLC	Vendor SIEMENS AG	Location Automatic
-------------	----------------------	-----------------------

Network Interfaces

IP 192.168.119.3	MAC 00:01:e3:19:22:33
---------------------	--------------------------

Protocols

- Siemens S7

Edit Properties

```
graph TD; A[192.168.119.22] --- B[192.168.119.11]; B --- C[192.168.119.3]
```

Step 6

Click the Alerts tab

Device | 192.168.119.3

The screenshot shows a device monitoring interface for a PLC at 192.168.119.3. The top navigation bar includes links for Home, Device inventory, and the specific device address. Below the navigation is a header with status indicators: Authorized (green), Last Seen (3 minutes ago), and Alert (2). The main content area is divided into sections: General Information, Network Interfaces, and Protocols. The General Information section shows Type (PLC), Vendor (SIEMENS AG), and Location (Automatic). The Network Interfaces section lists IP (192.168.119.3) and MAC (00:01:e3:19:22:33). The Protocols section lists Siemens S7. On the right, the Alerts tab is selected, showing a table of 17 alerts. The table columns are Severity, Name, Engine, Detection time, Status, and Source Device. Two rows are visible:

Severity	Name	Engine	Detection time	Status	Source Device
Warning	An S7 Stop PLC Command was Sent	Operational	24 minutes ago	New	192.168.119.22
Warning	An S7 Stop PLC Command was Sent	Operational	24 minutes ago	New	192.168.119.11

At the bottom left of the main content area is a blue "Edit Properties" button.

Step 7

Highlight an alert and “get full details”

Microsoft | Defender for IoT - 22.1.4

Home > Alerts > An S7 Stop PLC Command was Sent

Alerts | An S7 Stop PLC Command was Sent

[Export PDF](#) [Download Filtered Pcap](#)

An S7 Stop PLC Command was Sent

Alert ID: 23

Severity: Warning **Status**: New **Detection time**: 27 minutes ago

Description: A device 192.168.119.22 sent a Stop PLC command via Siemens S7 to device 192.168.119.3. The device will stop operating until start command will be sent.

Related Devices

Source device: 192.168.119.22 Engineering Station → **Destination device**: 192.168.119.3 PLC

Entities

IP (2)

Address
192.168.119.22
192.168.119.3

Devices (2)

Device ID	Device Name	Device Type	MAC Address	Protocols	Vendor
39	192.168.119.22	Engineering Station		Siemens S7, SMB	
45	192.168.119.3	PLC	00:01:e3:19:22:33	Siemens S7	SIEMENS AG

Explore this interface and see what you can do such as:

Take Action>mute

Map view

Download filtered pcap

Event Timeline

Exercise 5 Alerts

- Select Alerts from menu
- View Grouping Options
- Group By Severity
- Investigate Port Scan and details
- Take Action

Step 1

Select Alerts from menu

Defender for IoT | Alerts

<input type="checkbox"/>	Severity	Name	Engine	Detection time	Status	Source
<input type="checkbox"/>	Critical	No Traffic Detected on Sensor Interface	Operational	28 minutes ago	New	
<input type="checkbox"/>	Critical	Port Scan Detected	Anomaly	32 minutes ago	New	10.0.101.100
<input type="checkbox"/>	Warning	An S7 Stop PLC Command was Sent	Operational	33 minutes ago	New	192.168.0.168
<input type="checkbox"/>	Critical	Unauthorized Internet Connectivity Detected	Policy Violation	33 minutes ago	New	192.168.0.110
<input type="checkbox"/>	Warning	An S7 Stop PLC Command was Sent	Operational	33 minutes ago	New	192.168.119.11
<input type="checkbox"/>	Critical	Excessive SMB login attempts	Anomaly	34 minutes ago	New	192.168.0.110
<input type="checkbox"/>	Warning	PLC Operating Mode Changed	Operational	36 minutes ago	New	10.0.101.105
<input type="checkbox"/>	Warning	PLC Operating Mode Changed	Operational	36 minutes ago	New	10.0.100.105
<input type="checkbox"/>	Warning	PLC Operating Mode Changed	Operational	37 minutes ago	New	10.0.101.110
<input type="checkbox"/>	Warning	PLC Operating Mode Changed	Operational	37 minutes ago	New	10.0.100.110
<input type="checkbox"/>	Warning	PLC Operating Mode Changed	Operational	38 minutes ago	New	10.0.100.104
<input type="checkbox"/>	Major	EtherNet/IP CIP Service Request Failed	Operational	38 minutes ago	New	10.0.100.104
<input type="checkbox"/>	Major	EtherNet/IP Encapsulation Protocol Command F...	Operational	38 minutes ago	New	10.0.100.104
<input type="checkbox"/>	Warning	PLC Operating Mode Changed	Operational	38 minutes ago	New	10.0.100.104
<input type="checkbox"/>	Major	EtherNet/IP CIP Service Request Failed	Operational	38 minutes ago	New	10.0.100.104
<input type="checkbox"/>	Warning	Traffic Detected on Sensor Interface	Operational	43 minutes ago	New	
<input type="checkbox"/>	Major	BACNet Operation Failed	Operational	44 minutes ago	New	192.168.0.24

Step 2**Grouping Option**

Sort this list by different groupings

Severity

Name

Engine

Status

Step 3

Group the alerts by Severity and scroll down to the bottom

Defender for IoT | Alerts

<th data-cs="7" data-kind="parent"> <input type="text" value="Search"/> <input type="button" value="Refresh"/> <input type="button" value="Edit Columns"/> <input type="button" value="Export to CSV"/> </th> <th data-kind="ghost"></th> <th data-kind="ghost"></th> <th data-kind="ghost"></th> <th data-kind="ghost"></th> <th data-kind="ghost"></th> <th data-kind="ghost"></th>	<input type="text" value="Search"/> <input type="button" value="Refresh"/> <input type="button" value="Edit Columns"/> <input type="button" value="Export to CSV"/>						
<input type="text" value="Search"/> Status == 1 selected <input type="button" value="Time range == Last 30 days"/> <input type="button" value="Add filter"/> <input type="button" value="Reset filters"/>							
<input type="button" value="Discover"/> <input type="button" value="Analyze"/> <input type="button" value="Manage"/>							
<input type="button" value="Overview"/> <input type="button" value="Device map"/> <input type="button" value="Device inventory"/> <input type="button" value="Alerts"/>							
<p>Showing 17 of 17 alerts</p>							
Severity	Name	Engine	Detection time	Status	Source Device	Group by	
Warning	PLC Stop PLC Command was Sent	Operational	4 hours ago	New	10.0.101.121	Severity	
Warning	PLC Operating Mode Changed	Operational	4 hours ago	New	10.0.101.105		
Warning	PLC Operating Mode Changed	Operational	4 hours ago	New	10.0.100.105		
Warning	PLC Operating Mode Changed	Operational	4 hours ago	New	10.0.101.110		
Warning	PLC Operating Mode Changed	Operational	4 hours ago	New	10.0.100.110		
Warning	PLC Operating Mode Changed	Operational	4 hours ago	New	10.0.100.104		
Warning	PLC Operating Mode Changed	Operational	4 hours ago	New	10.0.100.104		
Warning	Traffic Detected on Sensor Interface	Operational	4 hours ago	New	192.168.0.24		
Major (4)							
Major	EtherNet/IP Encapsulation Protocol Command Failed	Operational	4 hours ago	New	10.0.100.104		
Major	EtherNet/IP CIP Service Request Failed	Operational	4 hours ago	New	10.0.100.104		
Major	EtherNet/IP CIP Service Request Failed	Operational	4 hours ago	New	10.0.100.104		
Major	BACNet Operation Failed	Operational	4 hours ago	New	192.168.0.24		
Critical (4)							
Critical	No Traffic Detected on Sensor Interface	Operational	4 hours ago	New	10.0.100.20		
Critical	Port Scan Detected	Anomaly	4 hours ago	New	192.168.0.110		
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	4 hours ago	New	192.168.0.110		
Critical	Excessive SMB login attempts	Anomaly	4 hours ago	New	192.168.0.110		

Step 4

Select Critical “Port Scan Detected” and then “View Full Details”

Home > Alerts > Port Scan Detected

Alerts | Port Scan Detected

[Export PDF](#) [Download Filtered Pcap](#)

Port Scan Detected

Alert ID: 24

Critical Severity **New** Status **4 hours ago** Detection time ⓘ

Description
Port scan detected.
Scanning device: 10.0.100.20
Scanned device: 10.0.100.104
Scanned Ports: 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089...
It is recommended to notify the security officer of the incident.

Related Devices

Source device 10.0.100.20 Engineering Station → Destination device 10.0.100.104 PLC

Alert Details Take Action Map View Event Timeline

Source (Scanning) Address
10.0.100.20

Destination (Scanned) Ports
8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089...

Destination (Scanned) Address
10.0.100.104

Entities

IP (2)

Address
10.0.100.20
10.0.100.104

Devices (2)

Device ID	Device Name	Device Type	MAC Address	Protocols	Vendor
21	10.0.100.20	Engineering Station		EtherNet/IP, CIP	
20	10.0.100.104	PLC	00:1d:9c:d2:33:60	EtherNet/IP, CIP	ROCKWELL AUTOMATION

In this view we can see the source of the scan, the destination or target of the scan , the ports that have been scanned. Keep in mind this alert was generated by one of the Machine Learning engine within the product. The alert was raised because scanning of devices or ports in an OT environment may be an indication of compromise, essentially the reconnaissance phase of an attack

Step 5

"Take Action" tab

The screenshot shows the Microsoft Defender for IoT interface. At the top, it displays "Microsoft" and "Defender for IoT - 22.1.4". Below the header, the navigation path is "Home > Alerts > Port Scan Detected". The main title is "Alerts | Port Scan Detected". On the left, there's a summary card for the "Port Scan Detected" alert (Alert ID: 24), showing a critical severity (red shield icon), a new status (blue circle with a checkmark), and a detection time of 4 hours ago. The alert description states: "Port scan detected. Scanning device: 10.0.100.20. Scanned device: 10.0.100.104. Scanned Ports: 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089... It is recommended to notify the security officer of the incident." Below this, a "Related Devices" section shows a source device "10.0.100.20 Engineering Station" connected to a destination device "10.0.100.104 PLC". The central pane is titled "Take Action" and contains sections for "Remediation steps" and "Learn". The "Remediation steps" section lists three numbered steps: 1. Multiple scans in the network can be an indication of a new device in the network, a new functionality of an existing device, improper configuration of an application (for example: due to a firmware update, or a new deployment), or malicious activity in the network, such as reconnaissance. 2. During the reconnaissance phase, a tool usually collects system configuration data, including data about any installed antivirus applications and steals data on the computer systems themselves, which is then sent back to the attackers. 3. Verify that the source device is an approved scanner and mark it as a Scanning Device. The "Learn" section contains a note: "Approve Alert Details as authorized network activity. The alert will not be triggered again for this network activity." and a toggle switch labeled "Alert learn" which is currently off.

Here you will see two heading. The first is a list of remediation step suggested by the system telling you why the alert was trigger, what may be happening, and to investigate what is going on (also available is a pcap of this alert to be used during the investigation).

If after the investigation it is found that this particular scanning is indeed appropriate and not a hazard to the system, you are given the ability to "learn" this behavior. This essentially adjust the baseline so this particular behavior will no longer trigger an alarm.

Now spend some time investigating the alerts and getting familiar with what type of data it is providing you.

Exercise 6 Risk Assessment

- Select Risk Assessment
- Create Report
- Download File
- Open File
- Review

Step 1,

Select Risk Assessment from Menu

Step 2 Generate Report

Home > Risk assessment

 Defender for IoT | Risk assessment

<< Generate report

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



No reports created

You have not generated any Risk Assessment reports.

Generate report

Step 3 Download and Open

After a minute or so the system will generate a “risk-assessment-report.pdf”

It will look like this:



At this point I will share the report and go over what it says and how it can be leveraged.

Exercise 7 Data Mining

- Open Data Mining
- Open each Recommended Reports
- Create Report

Step 1

select “Data Mining”

Step 2

Review the “recommended” reports

The screenshot shows the 'Defender for IoT | Data mining' interface. On the left, there's a navigation sidebar with sections for Discover, Analyze, and Manage. Under 'Discover', 'Data mining' is selected. Under 'Analyze', 'Event timeline' and 'Data mining' are also listed. The main content area is titled 'Recommended' and contains six cards: 'Programming Commands', 'Internet Activity', 'Excluded CVEs', 'Active Devices (Last 24 Hours)', 'Remote Access', and 'CVEs'. Below this, there's a section titled 'My reports' which is currently empty.

Step 3

Open each of them and see what they contain.

Think of how each of these can be used to help secure the OT network.

Step 4

Select the “Create Report”

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, and Manage. Under Analyze, 'Data mining' is selected. In the main area, there's a 'Recommended' section with tiles for Programming Commands, Internet Activity, Remote Access, and CVEs. Below that is a 'My reports' section which is currently empty. To the right, a modal window titled 'Create new report' is open. It has fields for 'Name *' (Report name), 'Description', and a toggle switch for 'Send to CM'. There are dropdown menus for 'Choose Category *' (set to 'Category') and 'Order by'. Below that are sections for 'Filter by' (Results within the last, IP address, MAC address, Port) and 'Device group' (with a search dropdown). At the bottom of the modal are 'Save' and 'Cancel' buttons.

Here you are presented with the extensive data the system has in its database. These reports can be anything from Module and Firmware version to passwords the system has seen.

Step 5

Create a password report using the selections made in the image below

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a sidebar with sections like Discover, Analyze, and Manage. Under Analyze, 'Data mining' is selected. In the main area, there's a 'Recommended' section with cards for Programming Commands, Internet Activity, Remote Access, and CVEs. Below that is a 'My reports' section which is currently empty. A modal window titled 'Create new report' is open on the right. It has fields for 'Name *' (set to 'My Report'), 'Description' (a note about looking for plain text or null passwords), and 'Send to CM' (unchecked). There are tabs for 'Category' (selected) and 'Activity'. The 'Category' tab shows several device types with checkboxes: OASYS, OMRON FINS, OVATION ADMD, OVATION DPUSTAT, PROFINET REAL-TIME, RPC, SAIA S-BUS, SMB, and SNMP. Under 'Category', 'PASSWORDS' is checked. Under 'Activity', 'Empty Passwords' and 'Plain Passwords' are checked. There are also dropdowns for IP address, MAC address, Port, and Device group, each with a '+' button to add filters. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Step 6

Build another report

Name it DeltaV

Select DeltaV from the dropdown list

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a sidebar with various navigation options like Overview, Device map, Device inventory, Alerts, Event timeline, Data mining (which is selected), Risk assessment, Trends & statistics, Attack vector, System settings, Custom alert rules, Users, and Forwarding. The main area has sections for Recommended (Programming Commands, Internet Activity, Excluded CVEs, CVEs, Non Active Devices (Last 7 Days)) and My reports. A modal window titled 'Create new repc' is open on the right, containing fields for Name (DeltaV), Description, Send to CM (unchecked), Choose Category (set to COMMON ASCII MESSAGE), Order by, Filter by (Results within the last 7 days), IP address, MAC address (with DeltaV checked), Port, Device group, and a plus sign for Add filter type. Under 'Add filter type', there are checkboxes for EMERSON OPENBSI, EMERSON ROC, and other Emerson-related items. At the bottom of the modal are Save and Cancel buttons.

Step 7

Save the report and open it.

Step 8

Expand each sub category

The screenshot shows the Microsoft Defender for IoT - 22.1.4 interface. The top navigation bar includes 'Home', 'Data mining', and 'DeltaV'. The main title is 'Defender for IoT | Data mining'. Below the title are various navigation and action buttons: Refresh, Expand all, Collapse all, Export to CSV, Export to PDF, Snapshots, Manage report, and Edit mode. The main content area is titled 'DeltaV' and contains two expandable sections: 'DeltaV ROC Operations' and 'DeltaV Message Types'. The 'DeltaV Message Types' section is expanded, showing a table with columns: Source, Destination, Port, Message Type, and Last Seen. The table lists 10 rows of network traffic data. The 'DeltaV Firmware Details' section is also expanded, showing a table with columns: Device, Model, Hardware Revision, Software Revision, and Last Seen. The table lists 2 rows of device information. The interface has a dark theme with red highlights for certain buttons and sections.

Source	Destination	Port	Message Type	Last Seen
192.168.111.1	192.168.111.20	DeltaV Device Communication (18507)	Integrity (7)	23/06/2022 14:03:47
192.168.111.1	192.168.111.20	DeltaV Device Communication (18507)	ROC (2)	23/06/2022 14:03:48
192.168.111.2	192.168.111.20	DeltaV Device Communication (18507)	Integrity (7)	23/06/2022 14:03:47
192.168.111.2	192.168.111.20	DeltaV Device Communication (18507)	ROC (2)	23/06/2022 14:03:48
192.168.111.20	192.168.111.1	DeltaV Device Communication (18507)	Integrity (7)	23/06/2022 14:03:47
192.168.111.20	192.168.111.1	DeltaV Device Communication (18507)	ROC (2)	23/06/2022 14:03:48
192.168.111.20	192.168.111.2	DeltaV Device Communication (18507)	Integrity (7)	23/06/2022 14:03:47
192.168.111.20	192.168.111.2	DeltaV Device Communication (18507)	ROC (2)	23/06/2022 14:03:48

Device	Model	Hardware Revision	Software Revision	Last Seen
192.168.111.1	DeltaV MD/MD Plus Controller	N/A	13.3.1.6290.xr	23/06/2022 14:03:48
192.168.111.2	DeltaV MD/MD Plus Controller	N/A	13.3.1.6290.xr	23/06/2022 14:03:48

Take some time and explore the variety of reports you can generate and think of who would benefit from this extensive data

Exercise 8 Event Timeline

- Open Event Timeline
- Review types of notifications provided
- Search for event
- View Event

Step 1

Select “Event Timeline”

Defender for IoT | Event timeline

Search Create event Refresh Export

User Operations == Hide X Add filter Reset filters

Event type	Time	Description
Device Connection Detected Connected devices 192.168.0.110 and 192.168.0.255	6/21/2022, 8:52:47 AM	Connected devices 192.168.0.110 and 192.168.0.255
Device Detected Device 192.168.118.22 was detected	6/21/2022, 8:52:47 AM	Device 192.168.118.22 was detected
File Transfer Detected File transfer from client IP: 192.168.119.11, Server IP: 192.168.119.22 Protocol: SMB, File Name:...	6/21/2022, 8:52:32 AM	File transfer from client IP: 192.168.119.11, Server IP: 192.168.119.22 Protocol: SMB, File N...
PLC Configuration Write Device 192.168.119.22 sent a command to write configuration to PLC 192.168.119.3 using SIE...	6/21/2022, 8:52:31 AM	Device 192.168.119.22 sent a command to write configuration to PLC 192.168.119.3 using ...
Firmware Update Device 192.168.119.22 sent a command to update firmware of SIEMENS S7 device 192.168.119...	6/21/2022, 8:52:32 AM	Device 192.168.119.22 sent a command to update firmware of SIEMENS S7 device 192.16...
PLC Configuration Write Device 192.168.119.22 sent a command to write configuration to PLC 192.168.119.3 using SIE...	6/21/2022, 8:52:31 AM	Device 192.168.119.22 sent a command to write configuration to PLC 192.168.119.3 using ...
Firmware Update Firmware of a Siemens S7 device 192.168.119.5 (Model: '6ES7 315-2EH14-0AB0') was changed....	6/21/2022, 8:52:32 AM	Firmware of a Siemens S7 device 192.168.119.5 (Model: '6ES7 315-2EH14-0AB0') was chan...
PLC Programming PLC 192.168.119.4 was programmed by client device 192.168.119.22 using SIEMENS S7 protoc...	6/21/2022, 8:52:31 AM	PLC 192.168.119.4 was programmed by client device 192.168.119.22 using SIEMENS S7 pr...
Firmware Update Firmware of a Siemens S7 device 192.168.119.4 (Model: '6ES7 315-2EH14-0AB0') was changed....	6/21/2022, 8:52:32 AM	Firmware of a Siemens S7 device 192.168.119.4 (Model: '6ES7 315-2EH14-0AB0') was chan...
PLC Configuration Write Device 192.168.118.22 sent a command to write configuration to PLC 192.168.118.3 using SIE...	6/21/2022, 8:52:13 AM	Device 192.168.118.22 sent a command to write configuration to PLC 192.168.118.3 using ...
Firmware Update Device 192.168.118.22 sent a command to update firmware of SIEMENS S7 device 192.168.118...	6/21/2022, 8:52:14 AM	Device 192.168.118.22 sent a command to update firmware of SIEMENS S7 device 192.16...

[Load More...](#)

Step 2

Scroll through these different events and the info provided.

What you see is a list of all event and alarms that the system has generated.

While we already know how we can leverage and respond to alerts, let's look at some of the other information being presented.

Device Connections

File Transfers

PLC Configuration Write/Read

Firmware Updates

Firmware Uploads or Downloads

PLC programming

Essentially what you have is an auditable timeline of every action in the system, including user activity on the system itself.

Step 3

Select Add Filter

Type = Keyword

Filter = Port

Defender for IoT | Event timeline

Search Create event Refresh Export

User Operations == Hide [Add filter](#) [Reset filters](#)

Event type	Add filter	Time	Description
PLC Config Device 192	Type Event Severity	6/23/2022, 10:12:29 AM	Device 192.168.119.22 sent a command to write configuration to PLC 192.168.119.3 using SIEMENS S7 pr...
Firmware L Device 192	Operator Device Group	6/23/2022, 10:12:30 AM	Device 192.168.119.22 sent a command to update firmware of SIEMENS S7 device 192.168.119.3. It is reco...
PLC Config Device 192	Filter Include Devices	6/23/2022, 10:12:29 AM	Device 192.168.119.22 sent a command to write configuration to PLC 192.168.119.3 using SIEMENS S7 pr...
Firmware L 2 group evi	Exclude Devices	6/23/2022, 10:12:30 AM	Firmware of a Siemens S7 device 192.168.119.5 (Model: '6ES7 315-2EH14-0AB0') was changed. Firmware V...
PLC Programming PLC 192.168.119.4 was program	Keywords Include Event Types	6/23/2022, 10:12:29 AM	PLC 192.168.119.4 was programmed by client device 192.168.119.22 using SIEMENS S7 protocol, control f...
Firmware Update 2 group events	Exclude Event Types	6/23/2022, 10:12:30 AM	Firmware of a Siemens S7 device 192.168.119.4 (Model: '6ES7 315-2EH14-0AB0') was changed. Firmware V...
File Transfer Detected	Date File transfer from client IP: 192.168.119.11, Server IP: 192.168.119.22 Protocol: SMB, File Name:...	6/23/2022, 10:12:30 AM	File transfer from client IP: 192.168.119.11, Server IP: 192.168.119.22 Protocol: SMB, File Name: '\torture_qfi...
Firmware Update 2 group events		6/23/2022, 10:12:13 AM	Firmware of a Siemens S7 device 192.168.118.5 (Model: '6ES7 315-2EH14-0AB0') was changed. Firmware V...
PLC Configuration Write Device 192.168.118.22 sent a command to write configuration to PLC 192.168.118.3 using SIE...		6/23/2022, 10:12:12 AM	Device 192.168.118.22 sent a command to write configuration to PLC 192.168.118.3 using SIEMENS S7 pr...
Firmware Update Device 192.168.118.22 sent a command to update firmware of SIEMENS S7 device 192.168.118...		6/23/2022, 10:12:13 AM	Device 192.168.118.22 sent a command to update firmware of SIEMENS S7 device 192.168.118.3. It is reco...
PLC Configuration Write Device 192.168.118.22 sent a command to write configuration to PLC 192.168.118.3 using SIE...		6/23/2022, 10:12:12 AM	Device 192.168.118.22 sent a command to write configuration to PLC 192.168.118.3 using SIEMENS S7 pr...

[Load More...](#)

Step 4

Apply Filter and Review

Defender for IoT | Event timeline

Search Create event Refresh Export

User Operations == Hide Keywords == 1 selected Add filter Reset filters

Event type	Time	Description
Alert Detected Port scan detected. Scanning device: 10.0.100.20 Scanned device: 10.0.100.104 Scanned Ports: ...	6/22/2022, 10:35:42 AM	Port scan detected. Scanning device: 10.0.100.20 Scanned device: 10.0.100.104 Scanned Ports: 8080, 8081, ...

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

Exercise 9 Trends and Statistics

- Trends and Statistic
- Dashboard Creation
- Add Widgets

Step 1

Select Trends and Statistics then “create dashboard”

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, and Manage. Under Analyze, the 'Trends & statistics' option is selected and highlighted. The main area is titled 'Trends & statistics' and displays a message 'No dashboard created' with a magnifying glass icon. To the right, a modal window titled 'Create dashboard' is open. It has fields for 'Dashboard name' (with a placeholder 'Untitled') and 'Dashboard widget type' (set to 'All (46)'). Below these are five widget options: 'Channels Bandwidth', 'Traffic By Port', 'Top Traffic By Port', 'Total Bandwidth', and 'New Devices'. Each widget has a preview image, a title, a description, and three category buttons: 'Operational', 'Security', and 'Traffic'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Step 2

Create a dashboard by giving it a name, and then hit “save”

Step 3

“Add Widget” and select from the list that appears on the right hand side

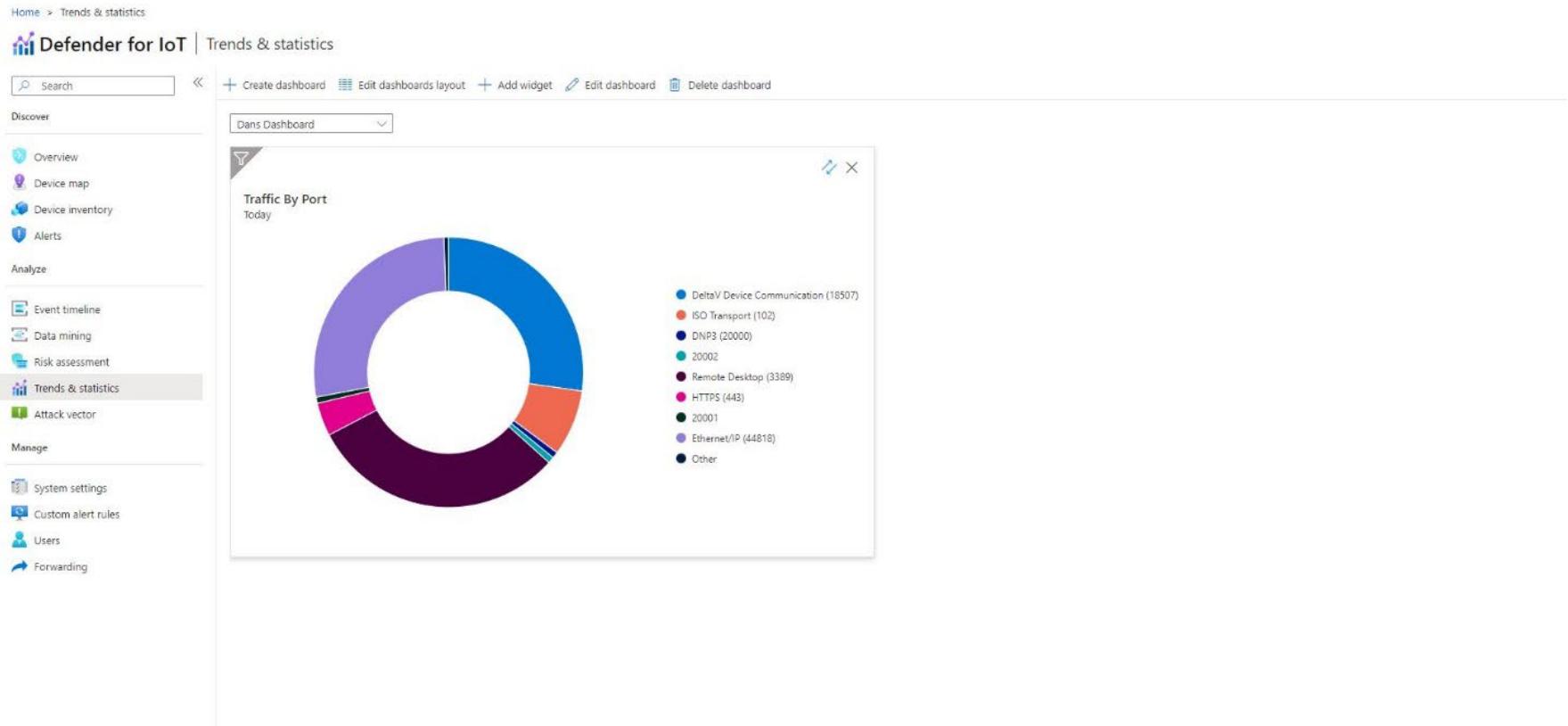
The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a sidebar with categories like Discover, Analyze, and Manage. Under Analyze, 'Trends & statistics' is selected. In the main area, a dashboard titled 'Dans Dashboard' is shown with a message 'No widgets'. To the right, an 'Add widget' modal is open, displaying a list of 46 available dashboard widget types. The first few items in the list are:

- Channels Bandwidth**: Bandwidth of channels, sorted by volume. Number of presented results can be customized. Categories: Operational, Traffic.
- Traffic By Port**: Traffic volume distribution by TCP / UDP ports (MB). Categories: Operational, Security, Traffic.
- Top Traffic By Port**: Top Traffic volume distribution by TCP / UDP ports (MB). Categories: Operational, Security, Traffic.
- Total Bandwidth**: Total bandwidth of the network (Mbps). Total bandwidth and highest channel bandwidth for a specific time are available via tooltip. Categories: Operational, Security, Traffic.
- New Devices**: Daily amount of newly discovered devices events. Categories: Operational, Security, Devices.

At the bottom of the modal are 'Save' and 'Cancel' buttons.

Step 4

Chose "Traffic by Port"



Step 5

Add other widgets, experiment with the page layout,