DEFENDER HANDS ON LAB

Contents

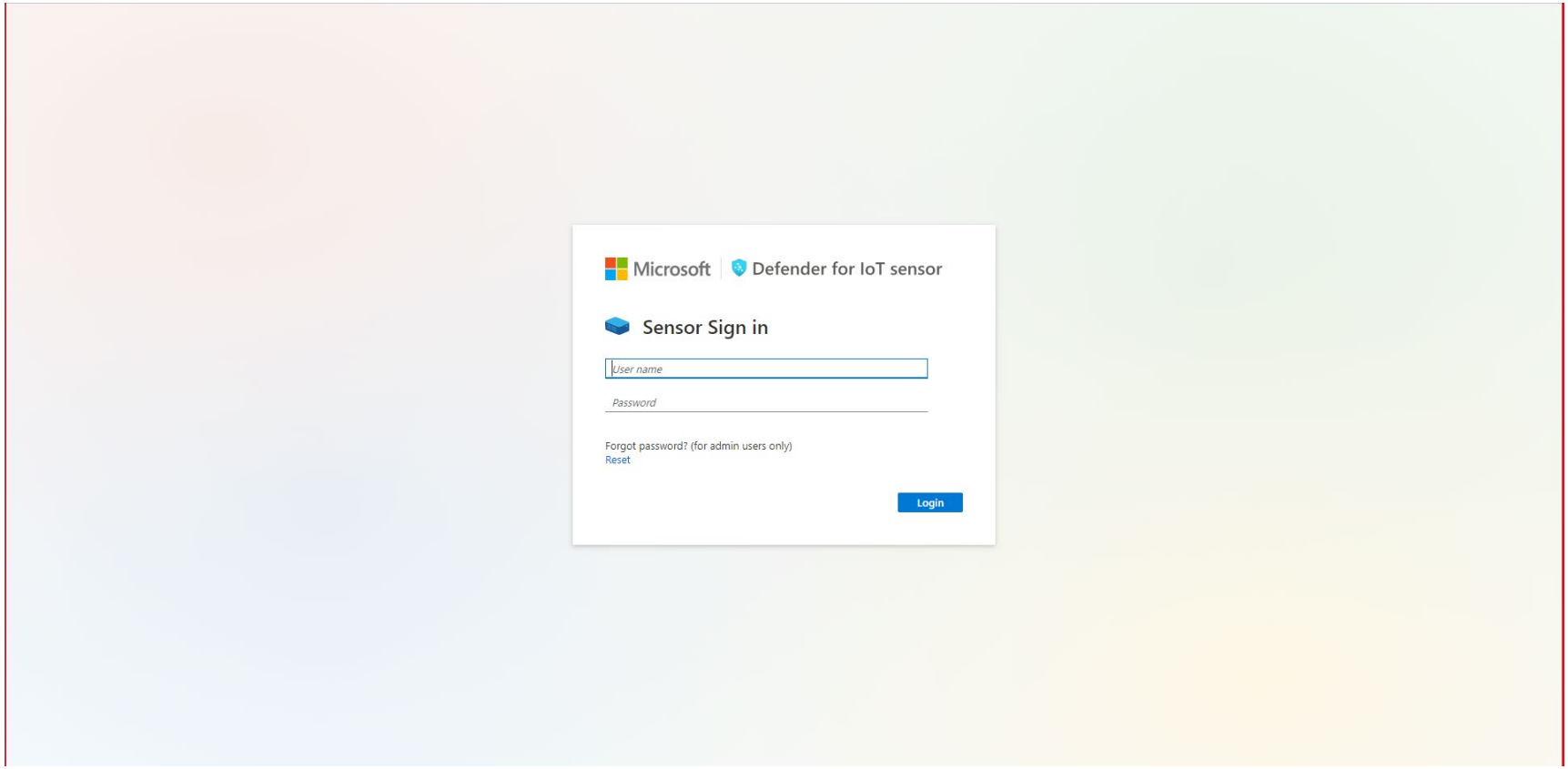
Class Objective:

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

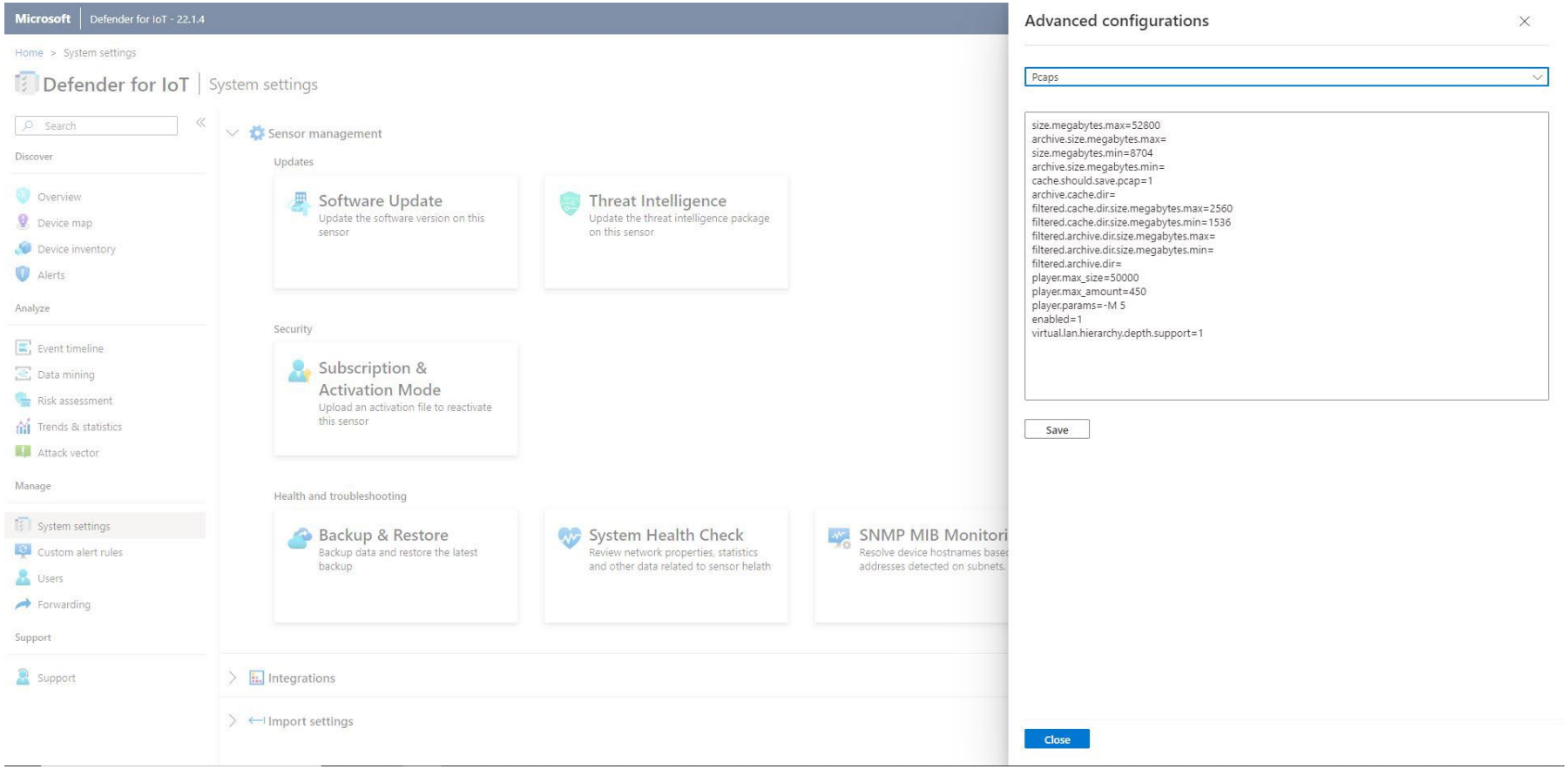
Exercise 1- Setting sensor environment for class

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



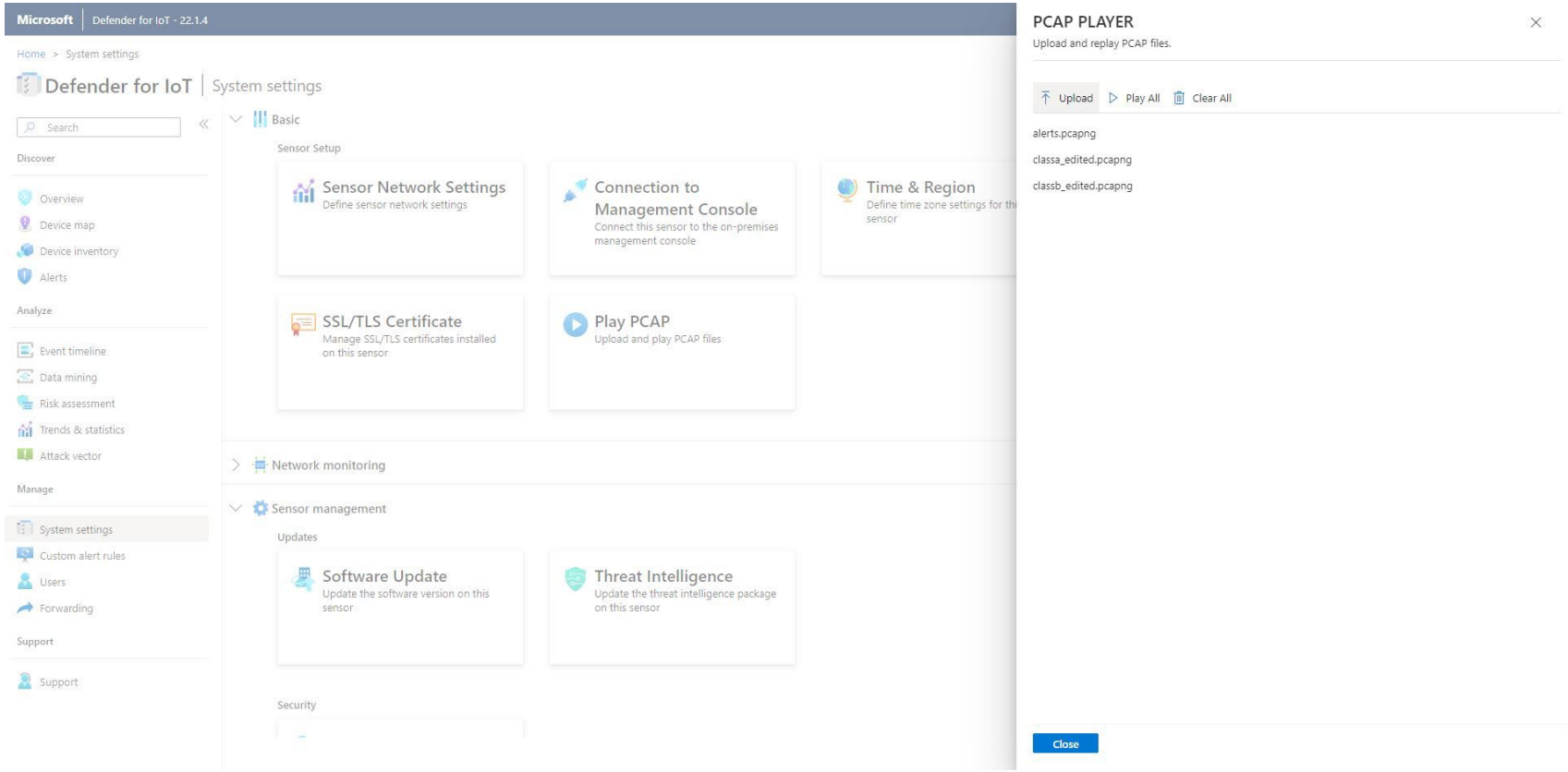
Step 1

Edit System Properties to enable pcap player



Step 2

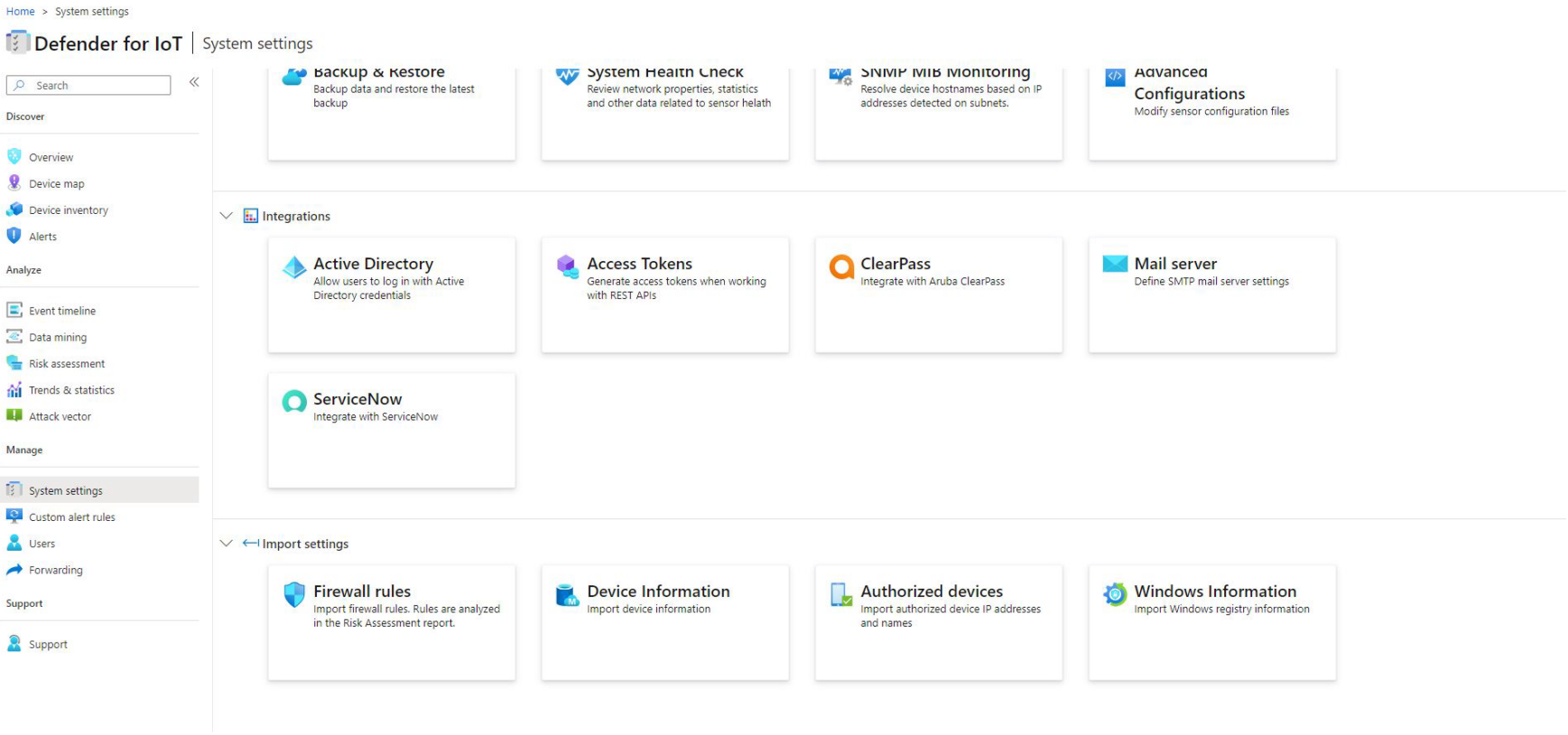
Upload pcaps

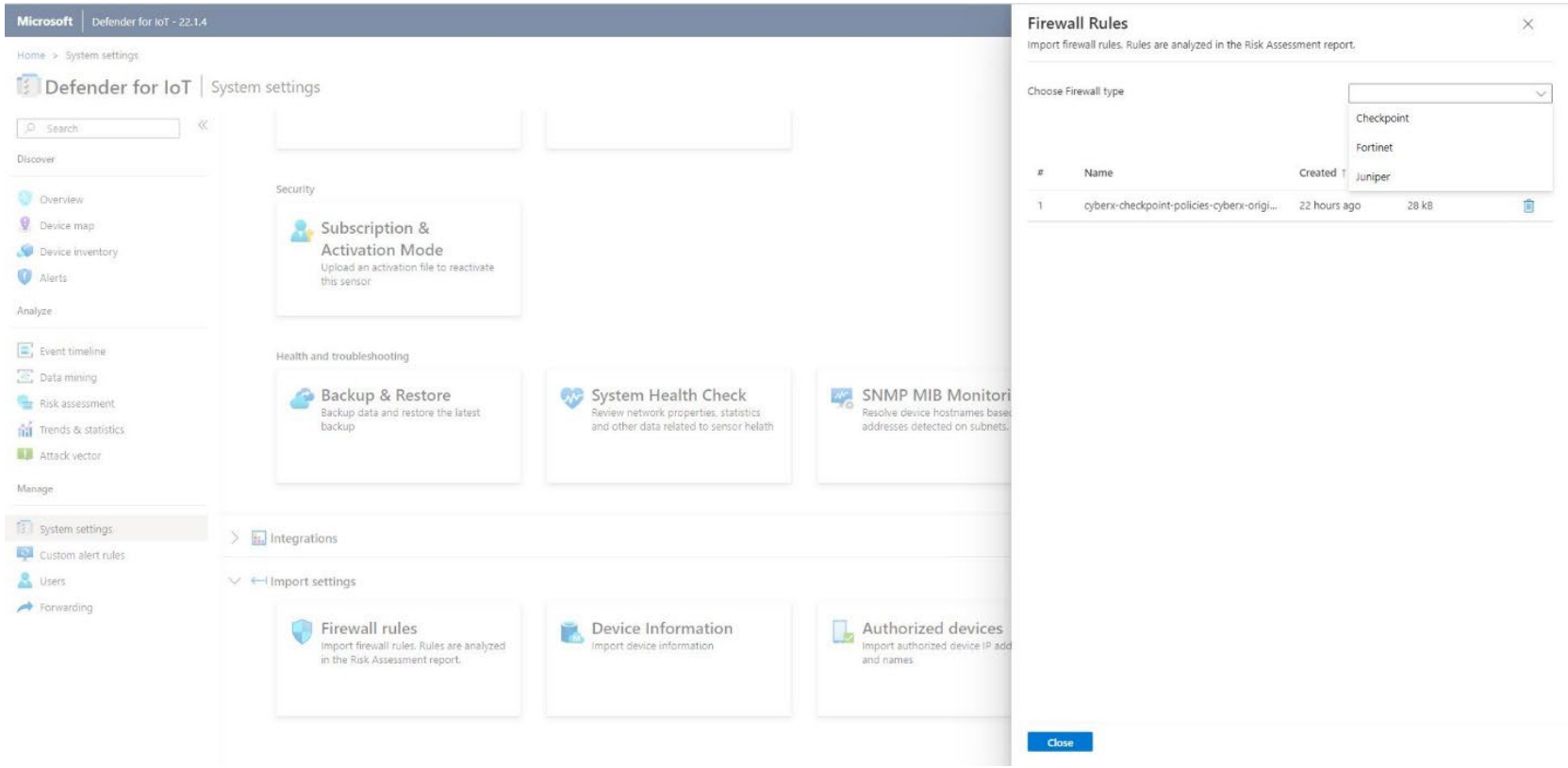


Step 3

Import firewall rules from the System Settings -> Firewall Rules

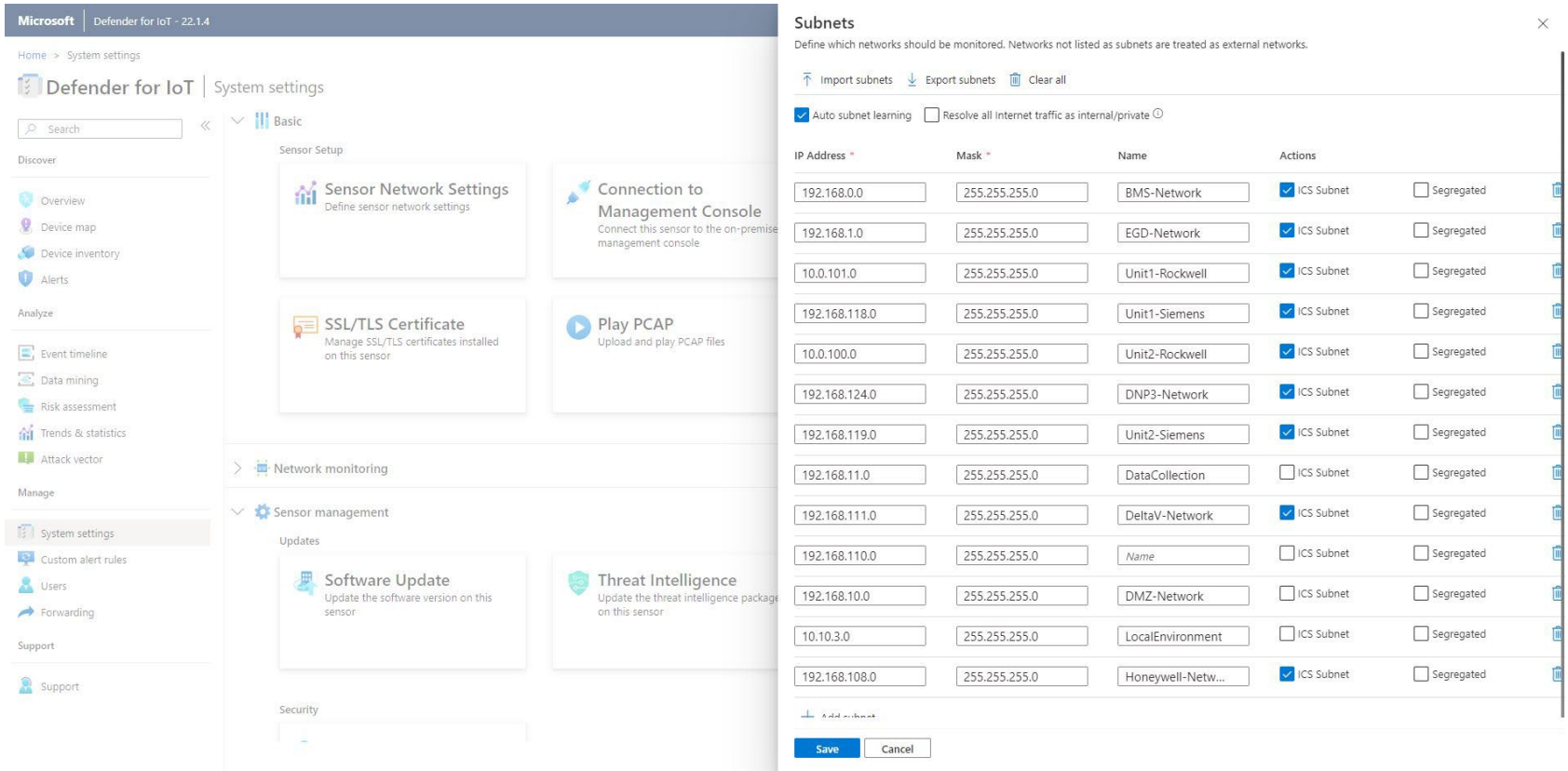
Select file


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 helath
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
Custom alert rules
Users
Forwarding
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 helath
SNMP MIB Monitori
Integrations
Import settings
Firewall rules
Import firewall rules. Rules are analyzed in the Risk Assessment report.
Device Information
Import device information
Authorized devices
Firewall Rules
Import firewall rules. Rules are analyzed in the Risk Assessment report.
Choose Firewall type
Checkpoint
Fortinet
Juniper
Name Created 28 kB
1 cyberx-checkpoint-policies-cyberx-origi... 22 hours ago
Close

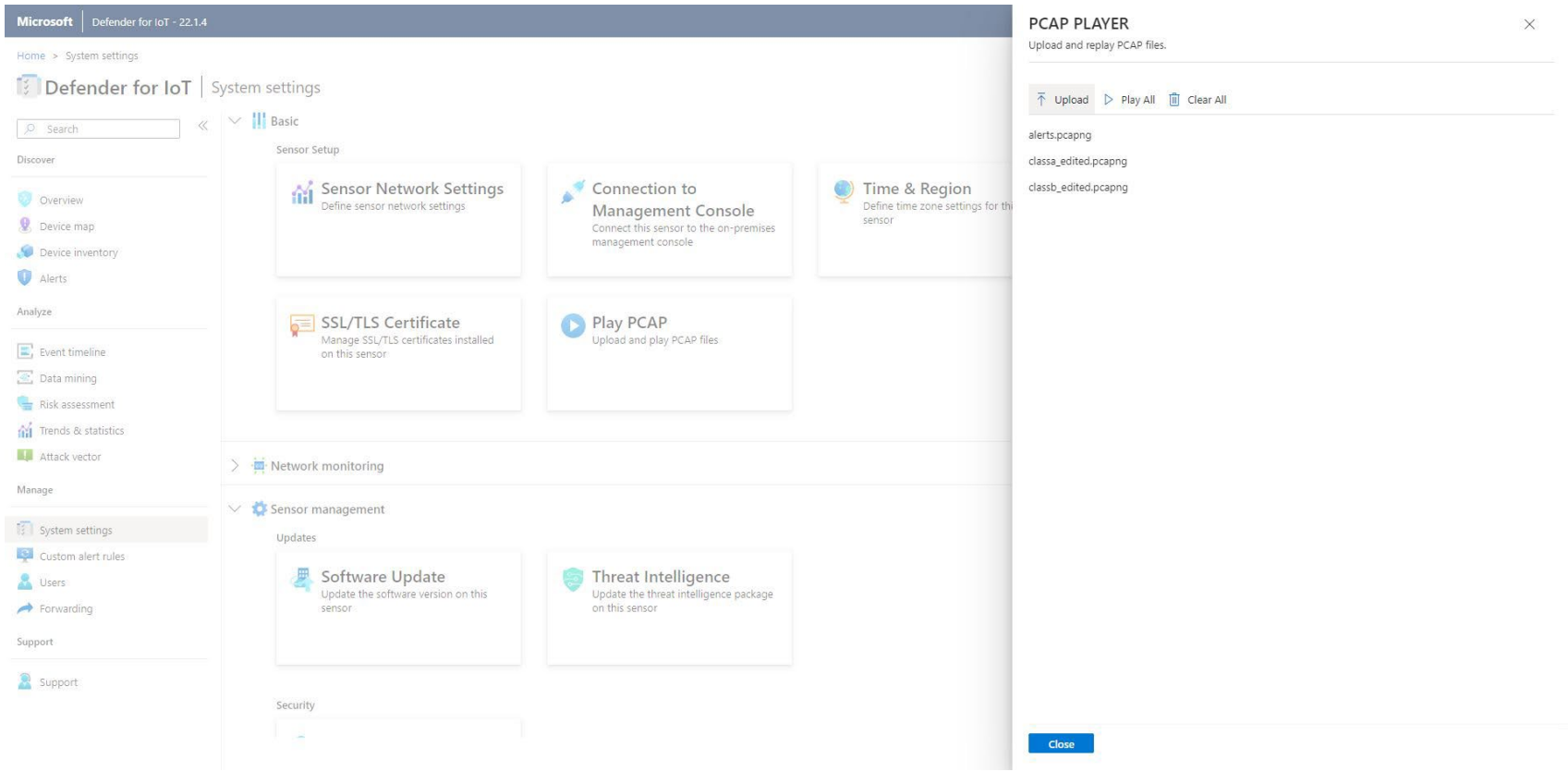
Step 4
Import subnets

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



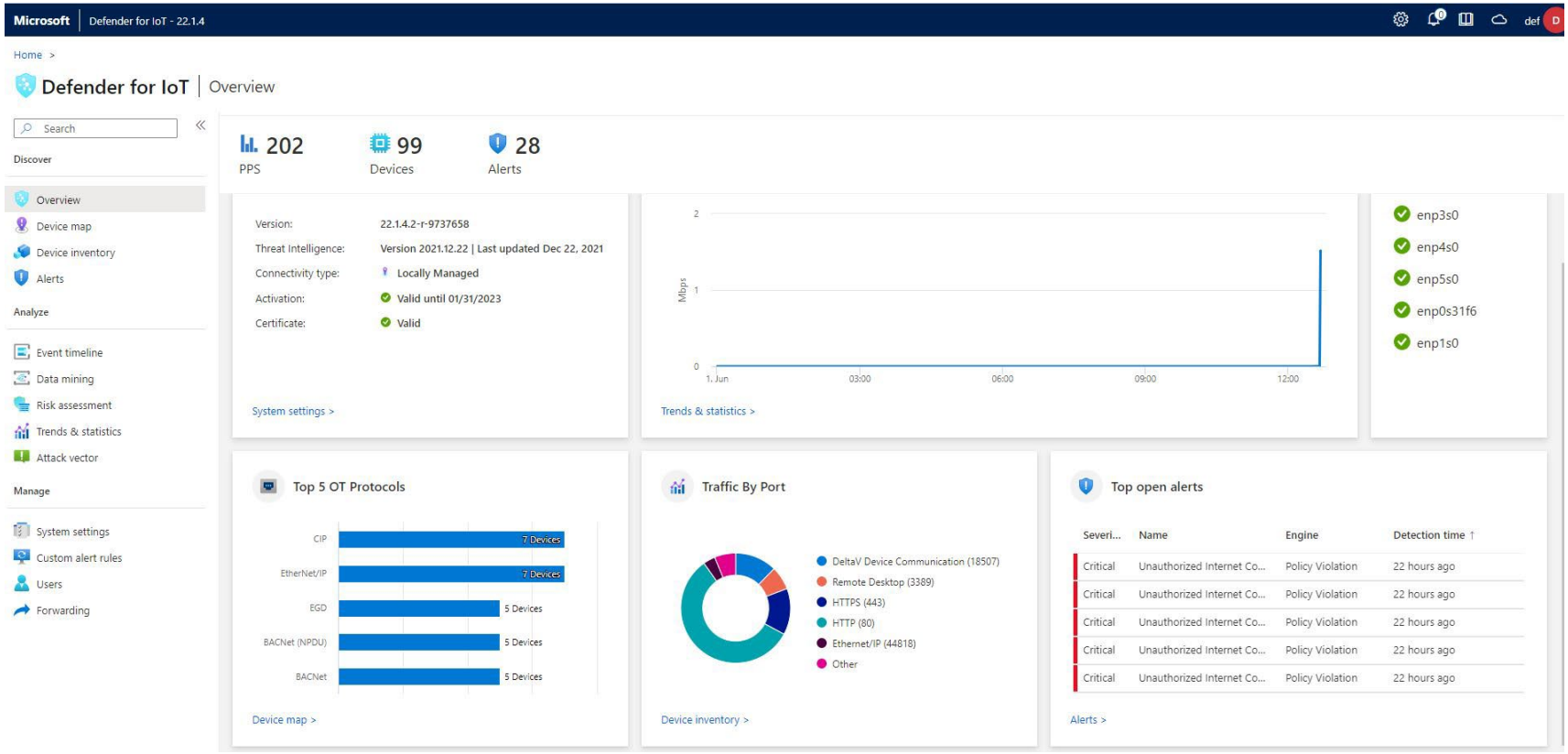
Step 5

Play pcaps by hitting **Play All**



Step 6

Verify data collection



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

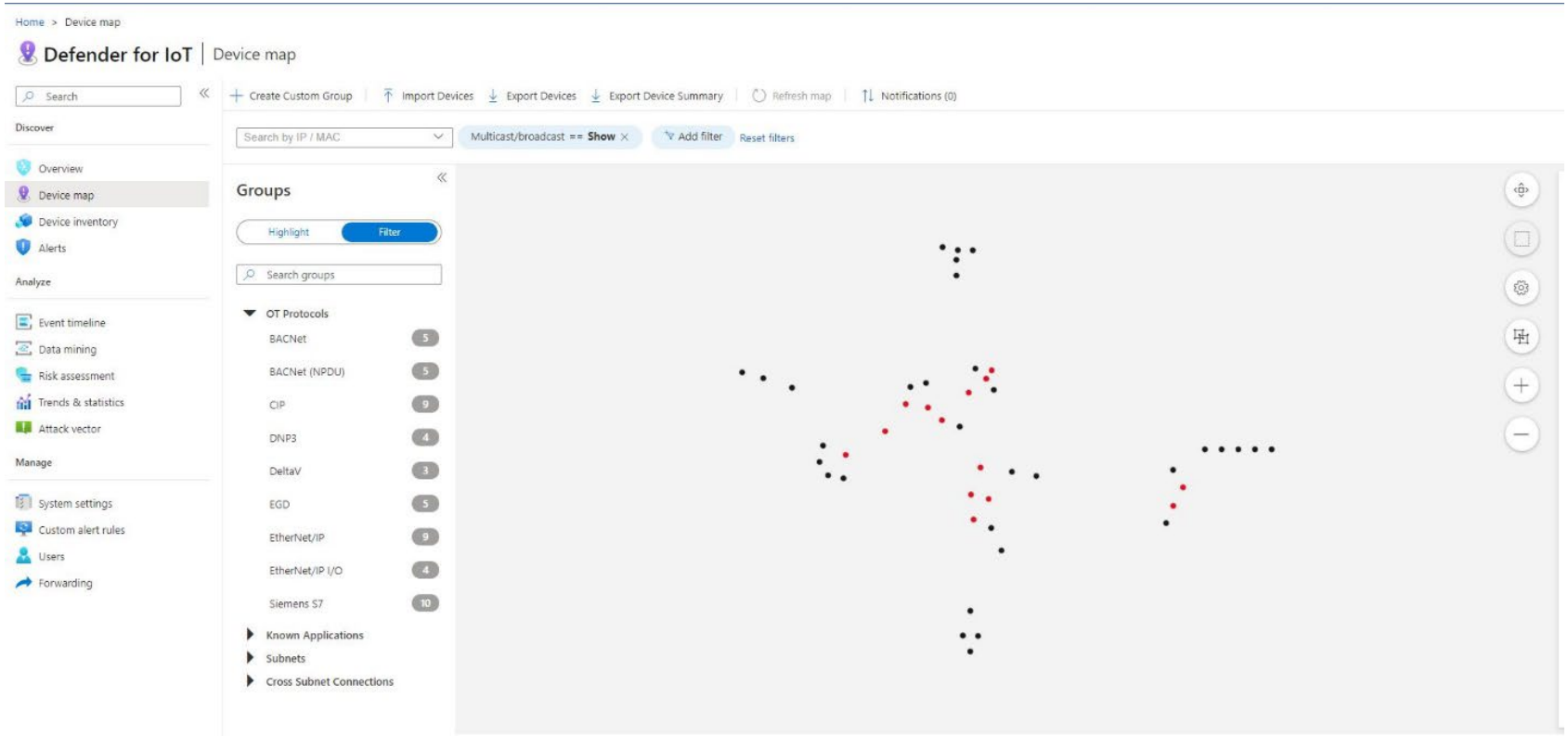
-Link to Alerts

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**

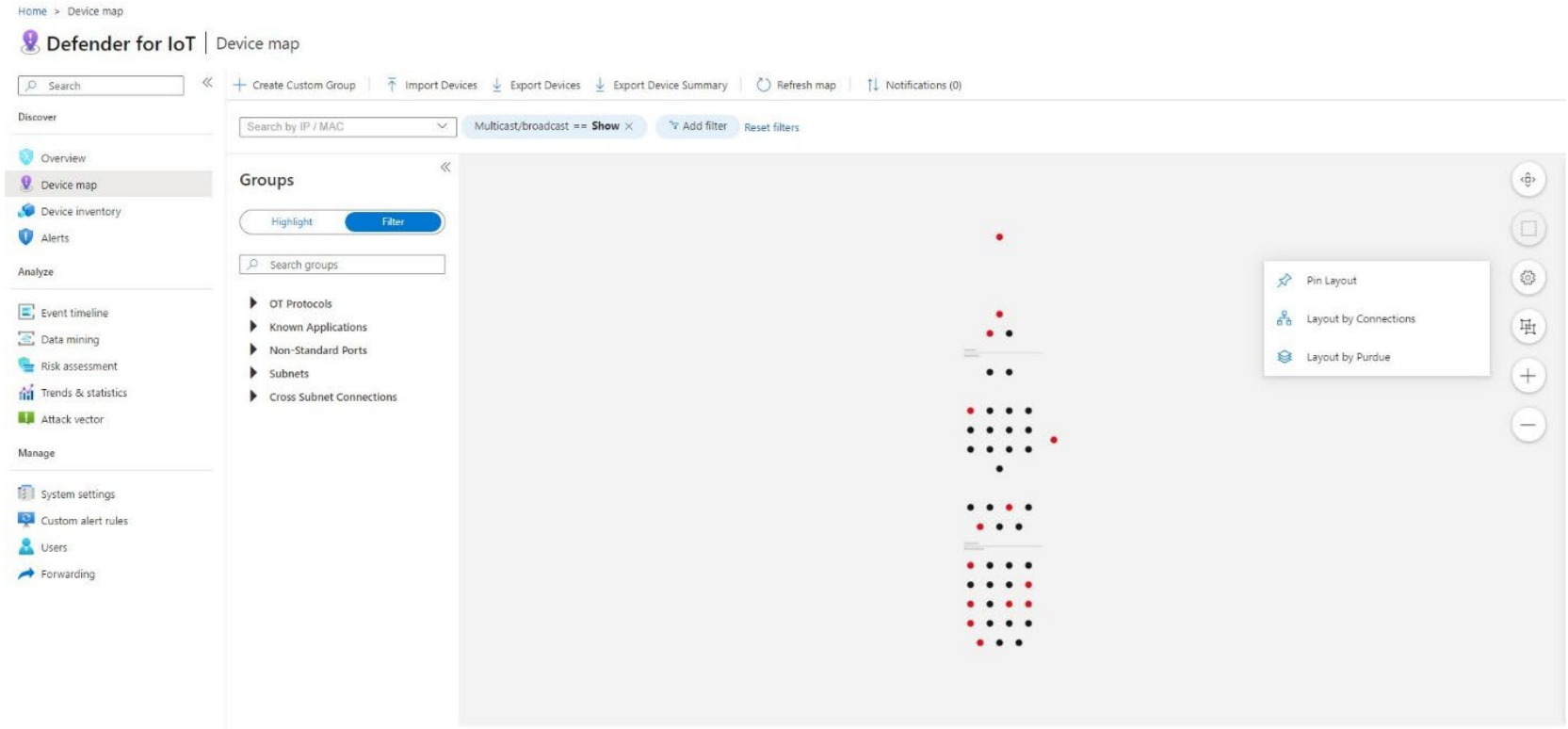


Default view is by connections,

Step 2

Lay out map with Perdue Model and confirm

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



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

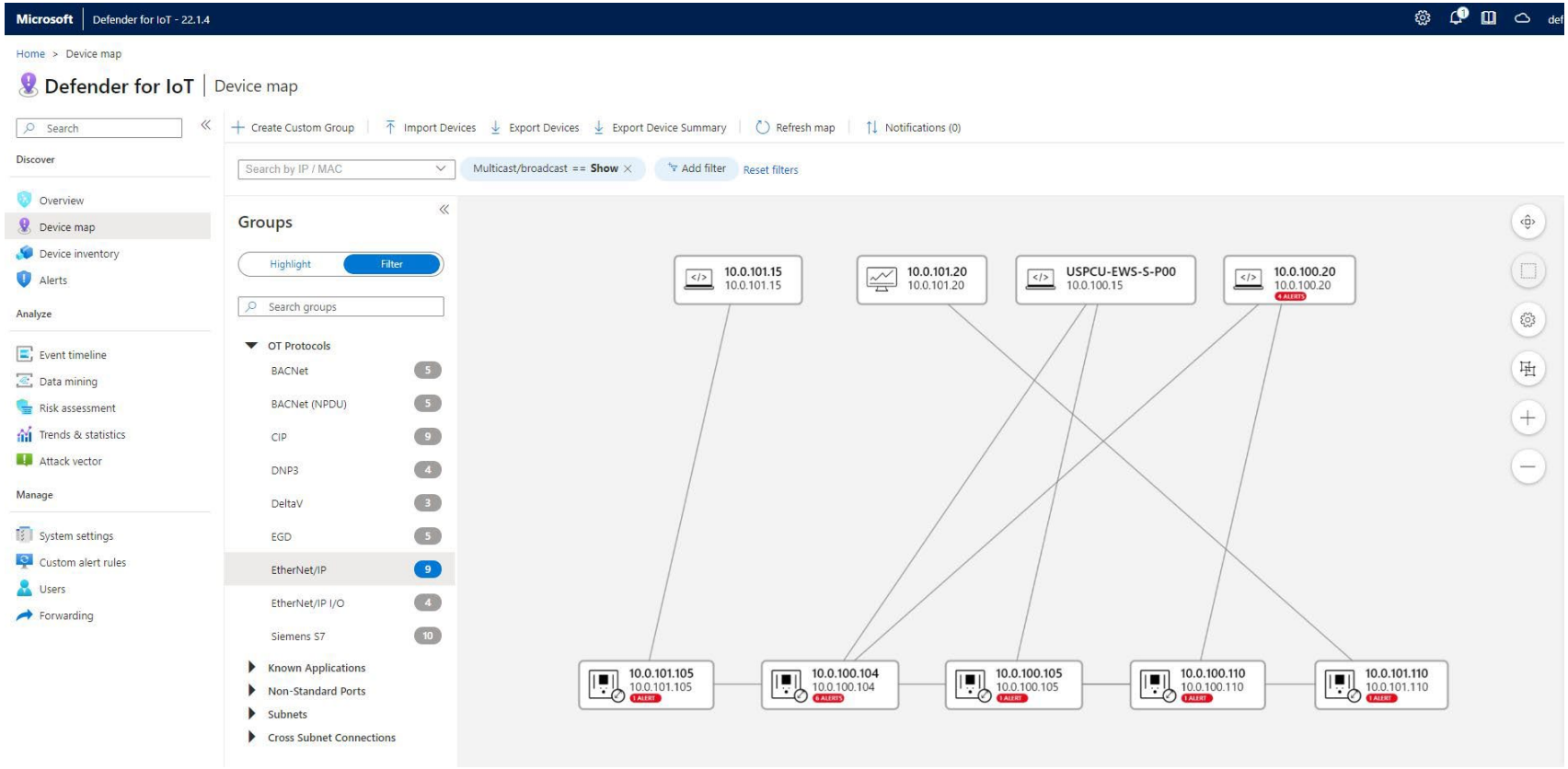
Cross Subnet Connections

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



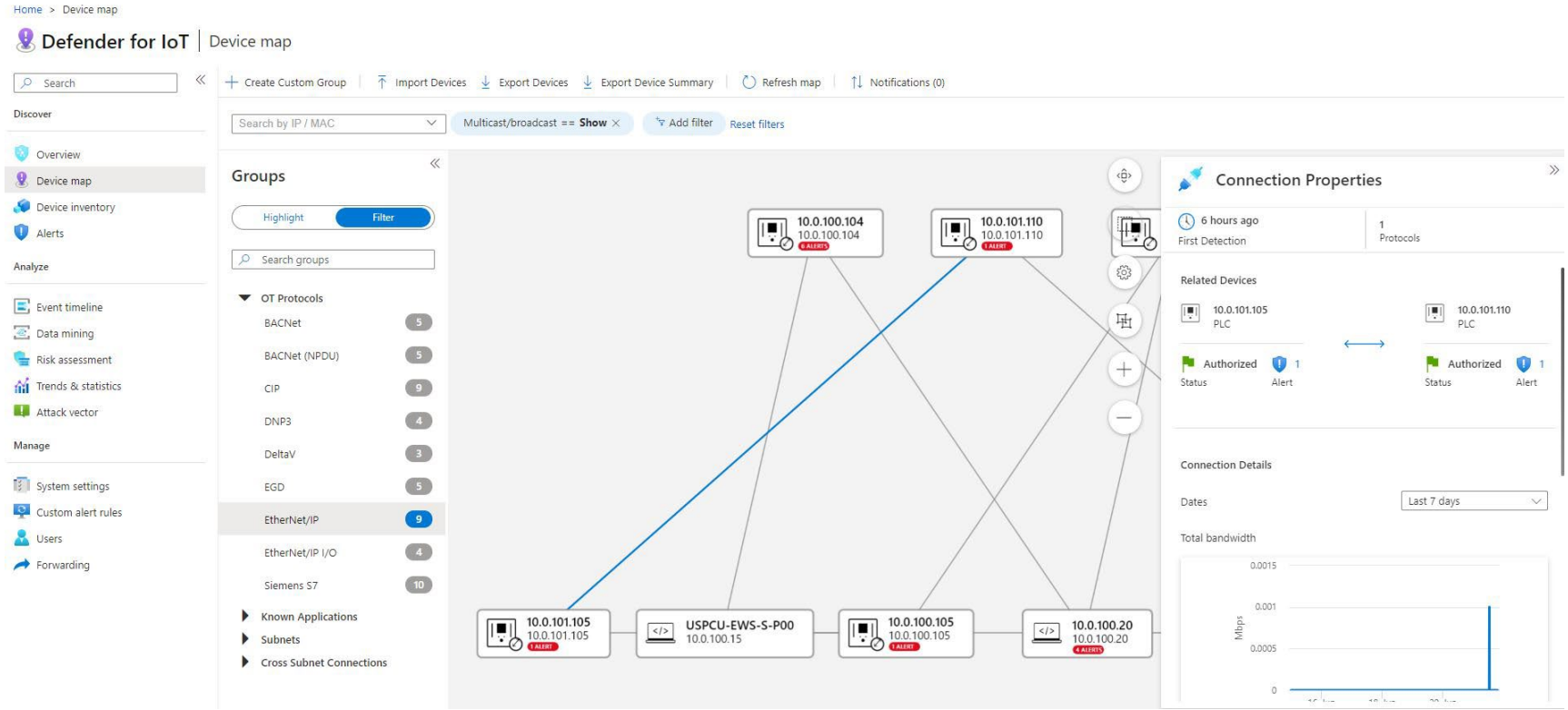
Observe in the field to the right that the icons are now larger, and we can see the connections they have with one another.

Step 4

Connection details

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

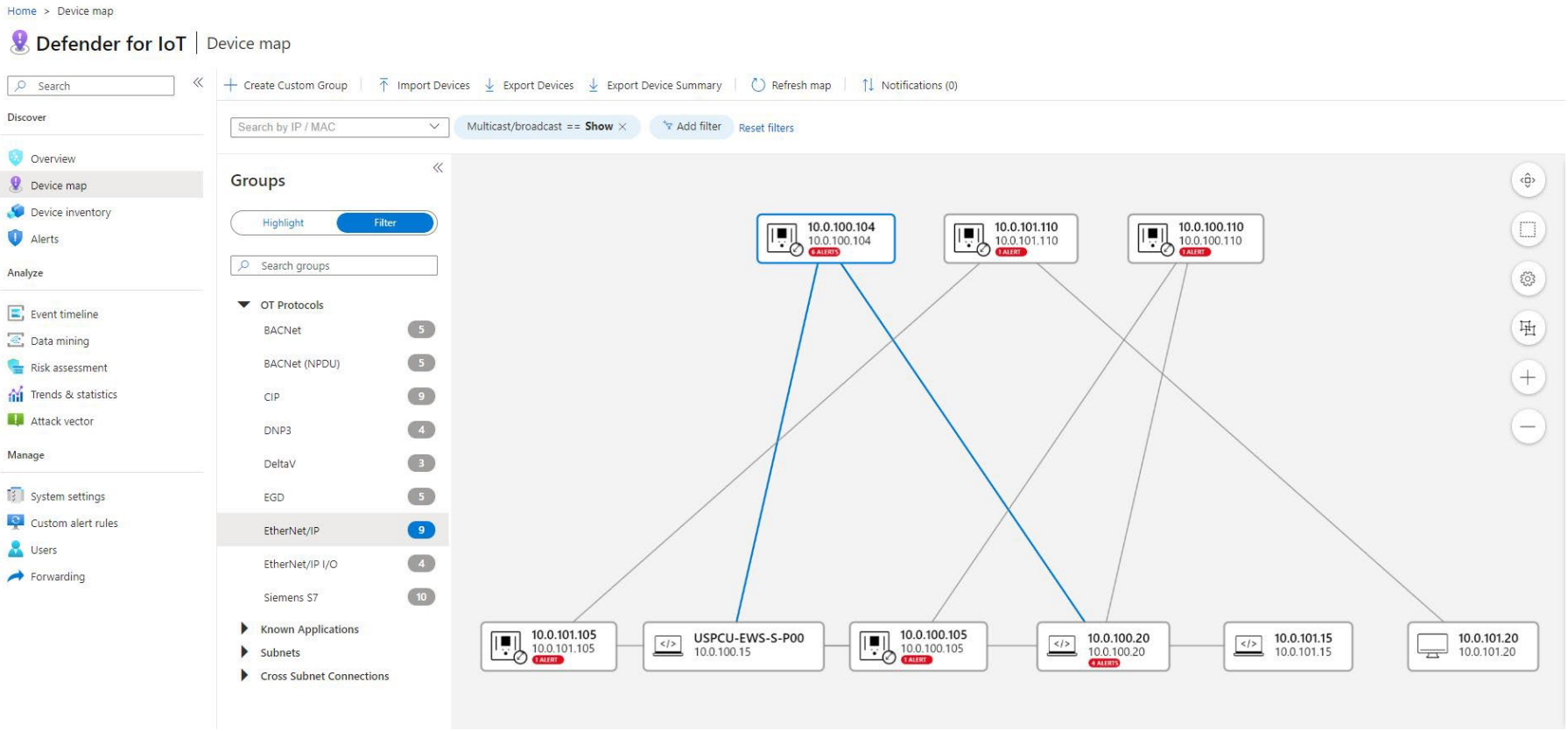
This will show the two devices that are connected, authorization status, when and how the communicate.



Step 4

Select 10.0.100.104

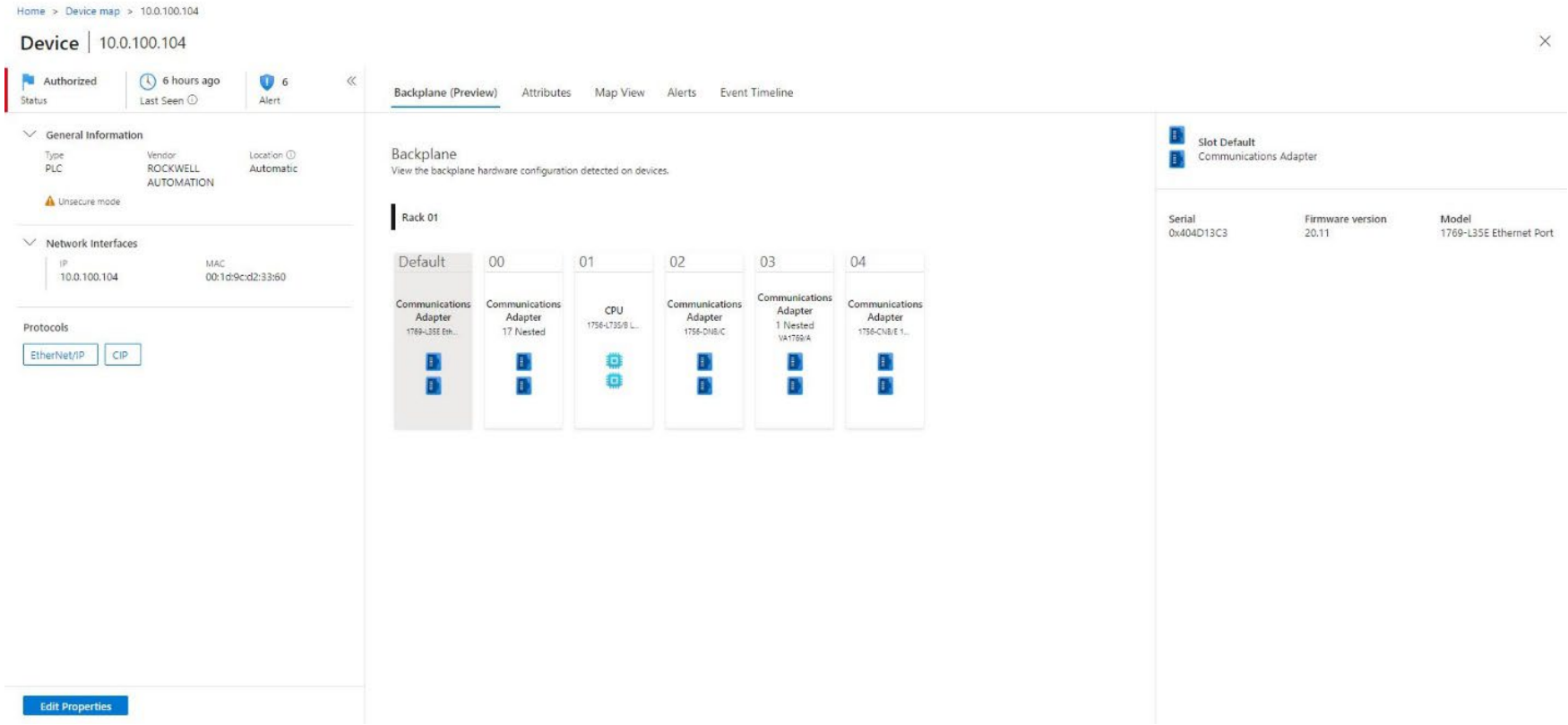
the device will be outlined in blue and the connections it has to other devices will also change to blue.



Step 5

Device Properties

Right click on the item and select “view properties”



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:

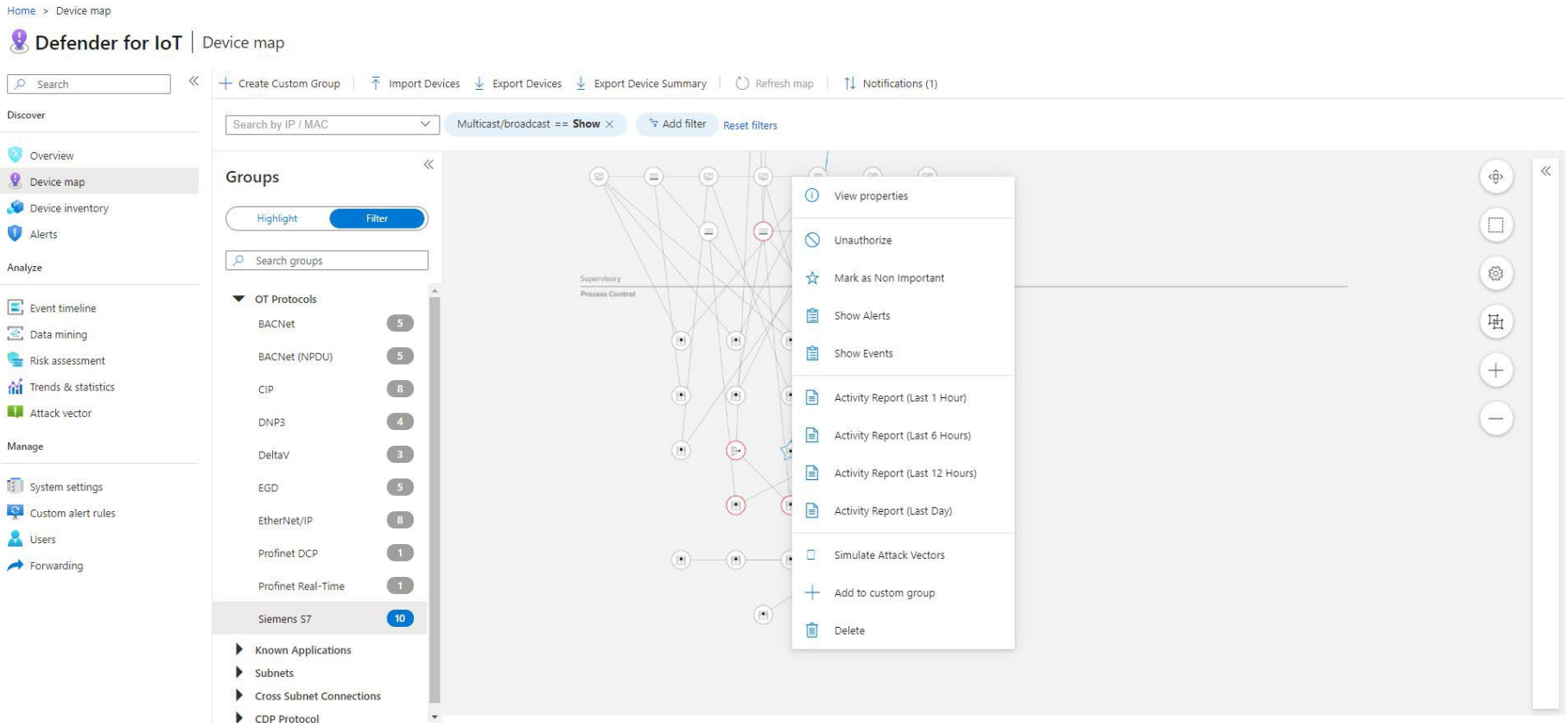
CPUs, Communication Adapters, Analog I/O, Digital I/O

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,

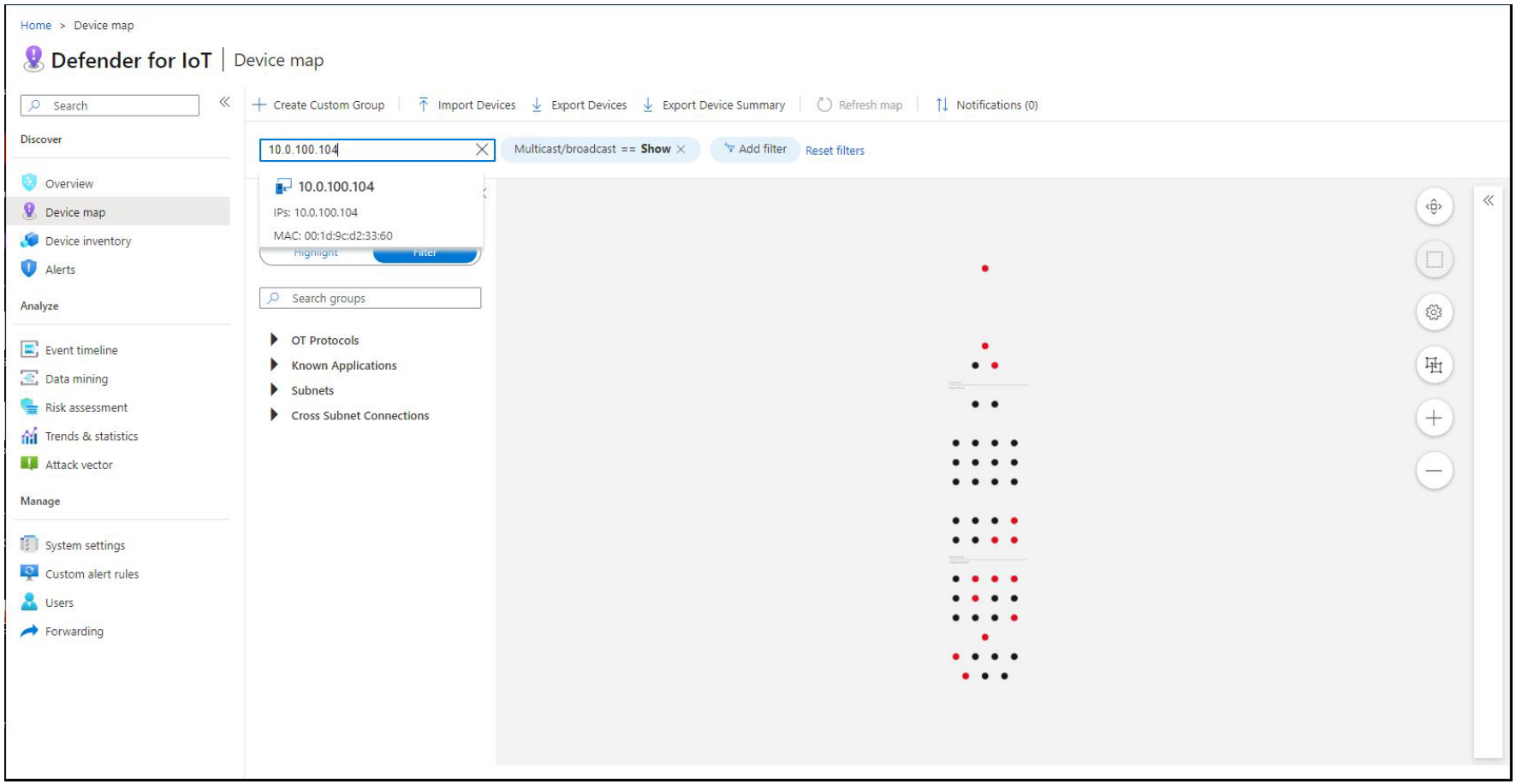
Right click on any device and explore its properties, alerts, events, activity. You can add devices to custom groups, simulate attack vectors, mark things important, unauthorize, and even delete from the map.



Step 6

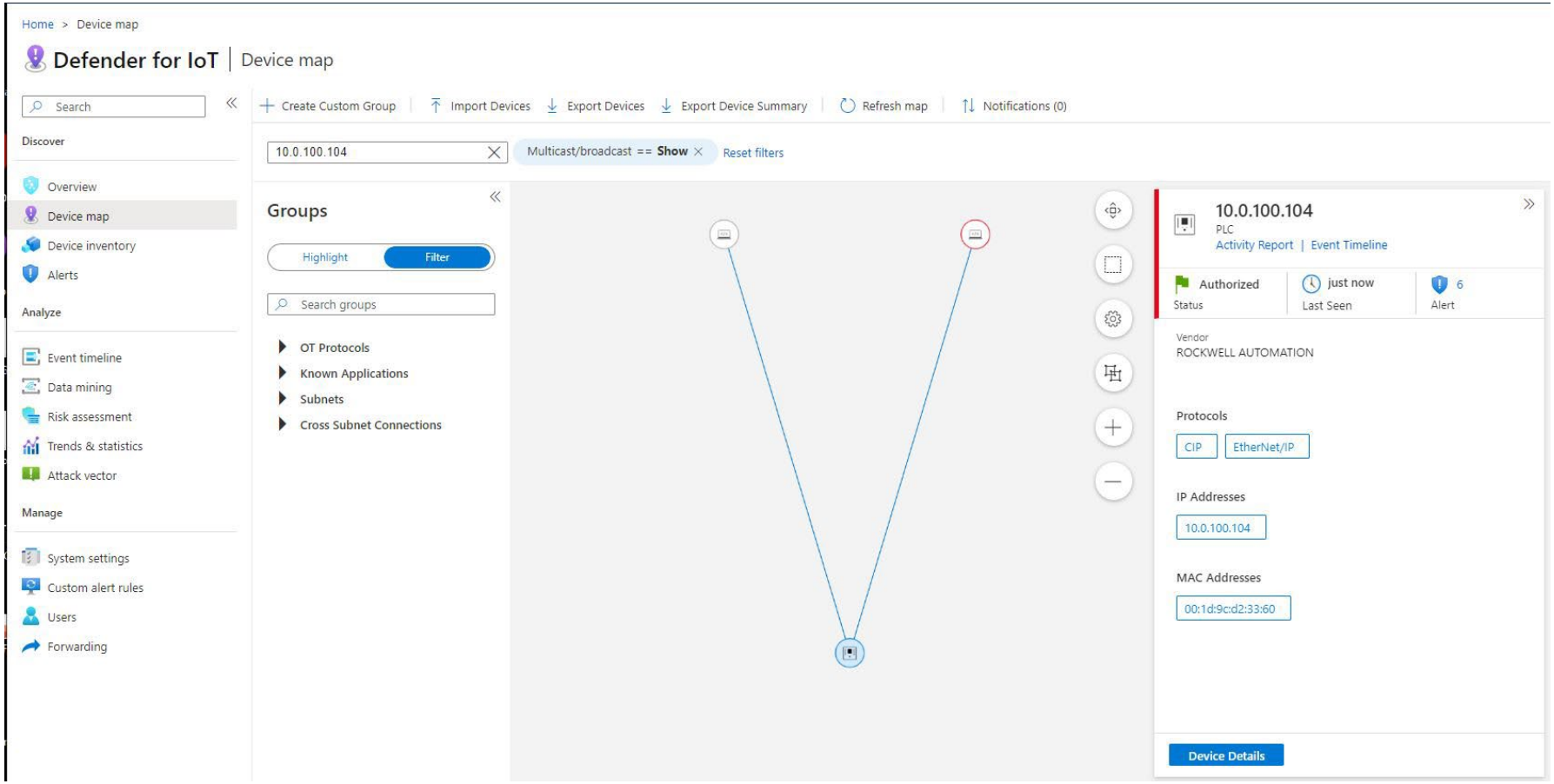
Device Search

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

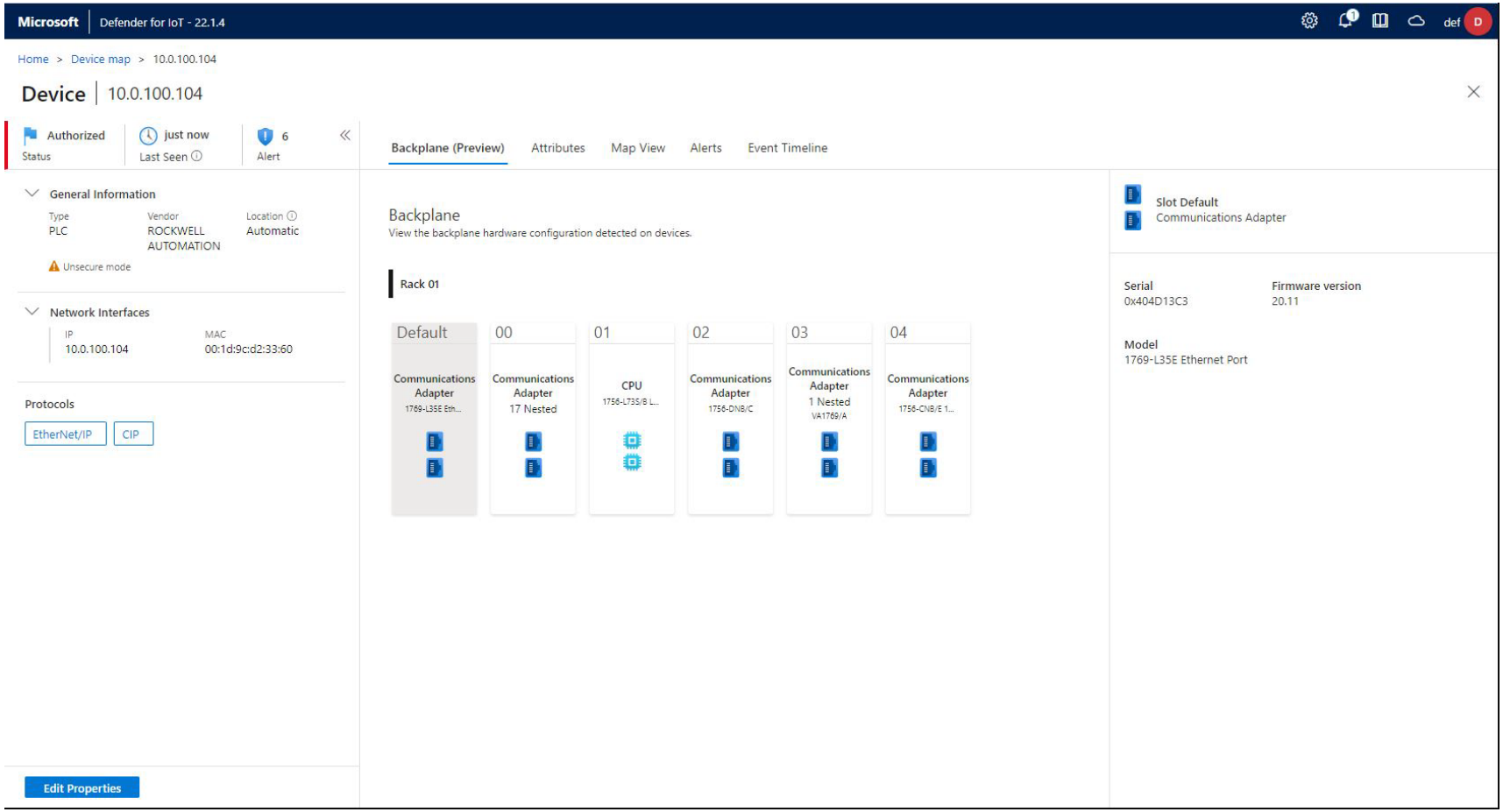


Look at 10.0.100.104

Here you see the connections it has to other devices:



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

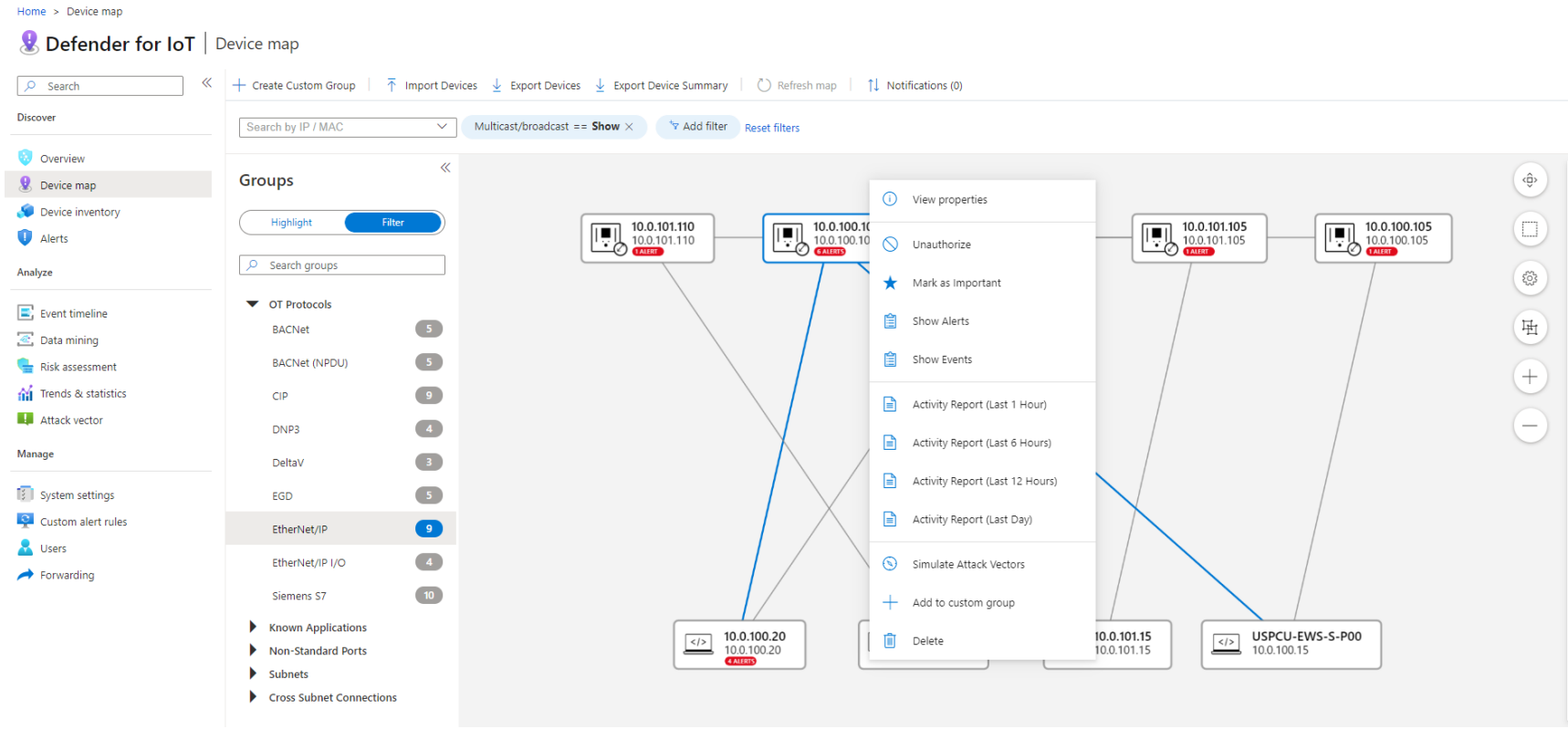

Microsoft
Defender for IoT - 22.1.4
def D
Home > Device map > 10.0.100.104
Device | 10.0.100.104
Authorized
Status
just now
Last Seen
6
Alert
Backplane (Preview)
Attributes
Map View
Alerts
Event Timeline
General Information
Type
PLC
Vendor
ROCKWELL AUTOMATION
Location
Automatic
Unsecure mode
Network Interfaces
IP
10.0.100.104
MAC
00:1d:9c:d2:33:60
Protocols
EtherNet/IP
CIP
Edit Properties
Backplane
View the backplane hardware configuration detected on devices.
Rack 01
Default
Communications Adapter
1769-L35E Eth...
00
Communications Adapter
17 Nested
01
CPU
1756-L73S/B L...
02
Communications Adapter
1756-DNB/C
03
Communications Adapter
1 Nested
VA1769/A
04
Communications Adapter
1756-CNB/E 1...
Slot Default
Communications Adapter
Serial
0x404D13C3
Firmware version
20.11
Model
1769-L35E Ethernet Port

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

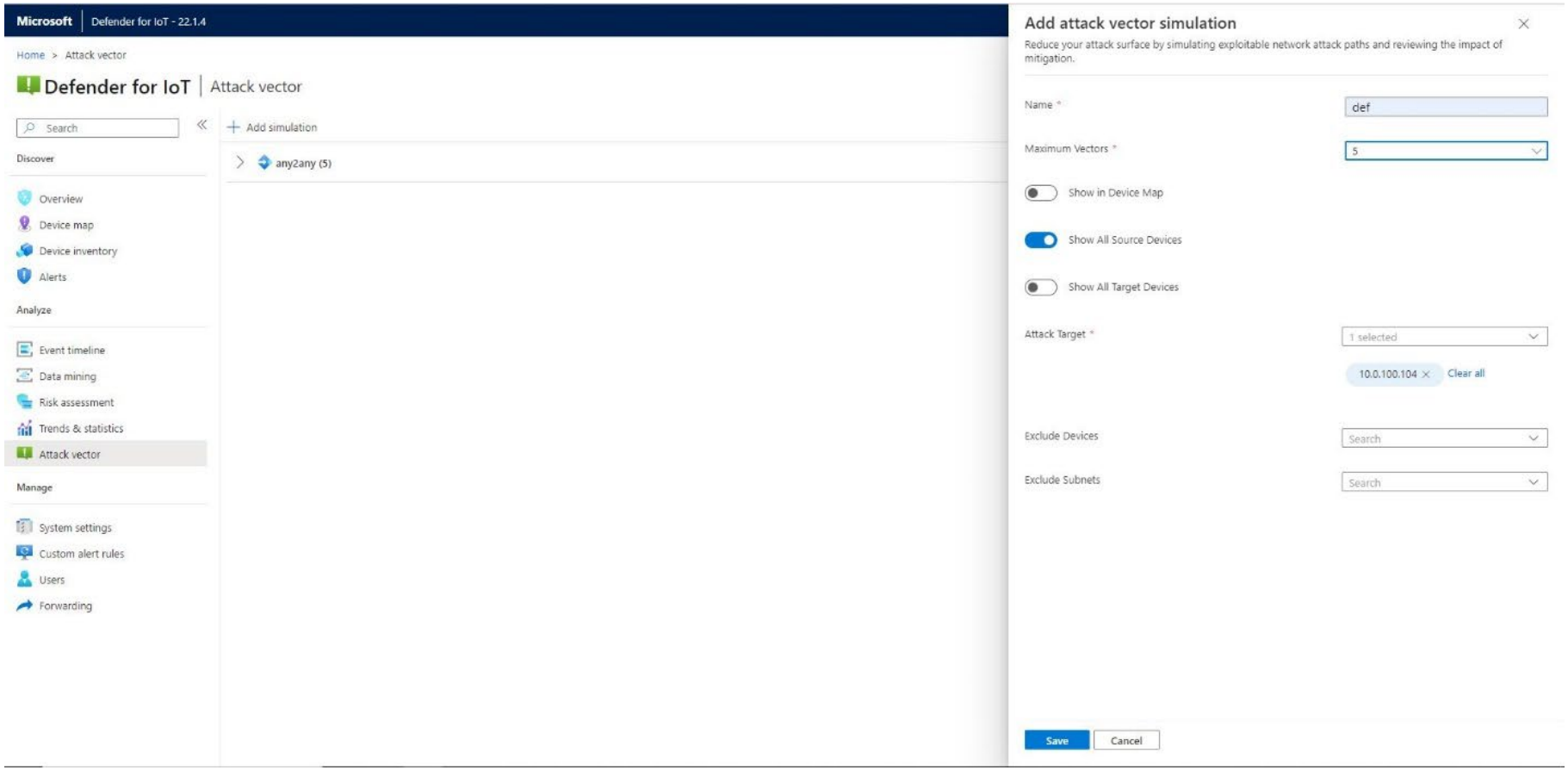


Step 2

Select “Simulate Attack Vectors

Step 3

Name simulation



Step 4

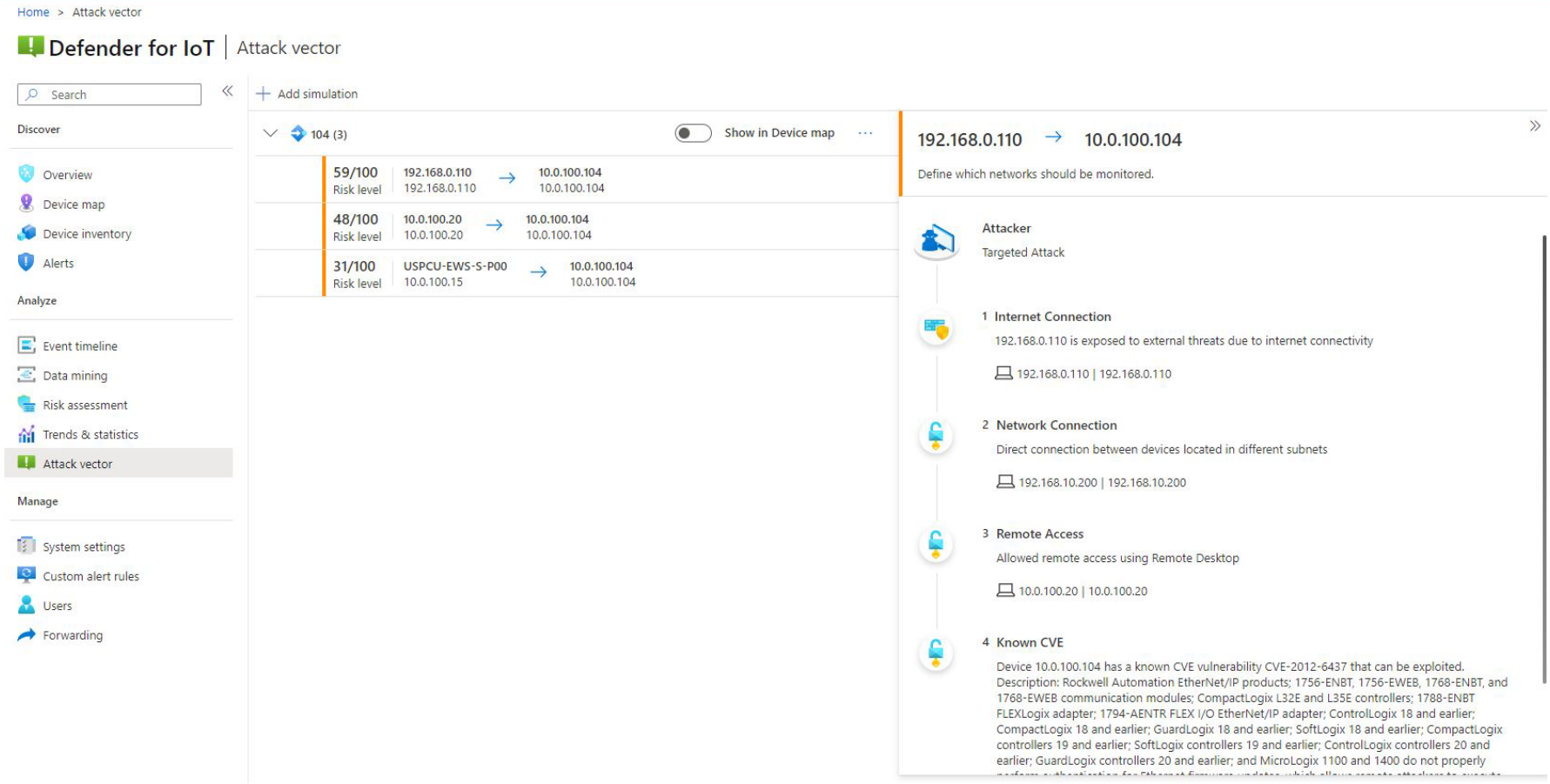
Select the maximum number of vectors

Step 6

select “Run”

Step 5

Inspect Results



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

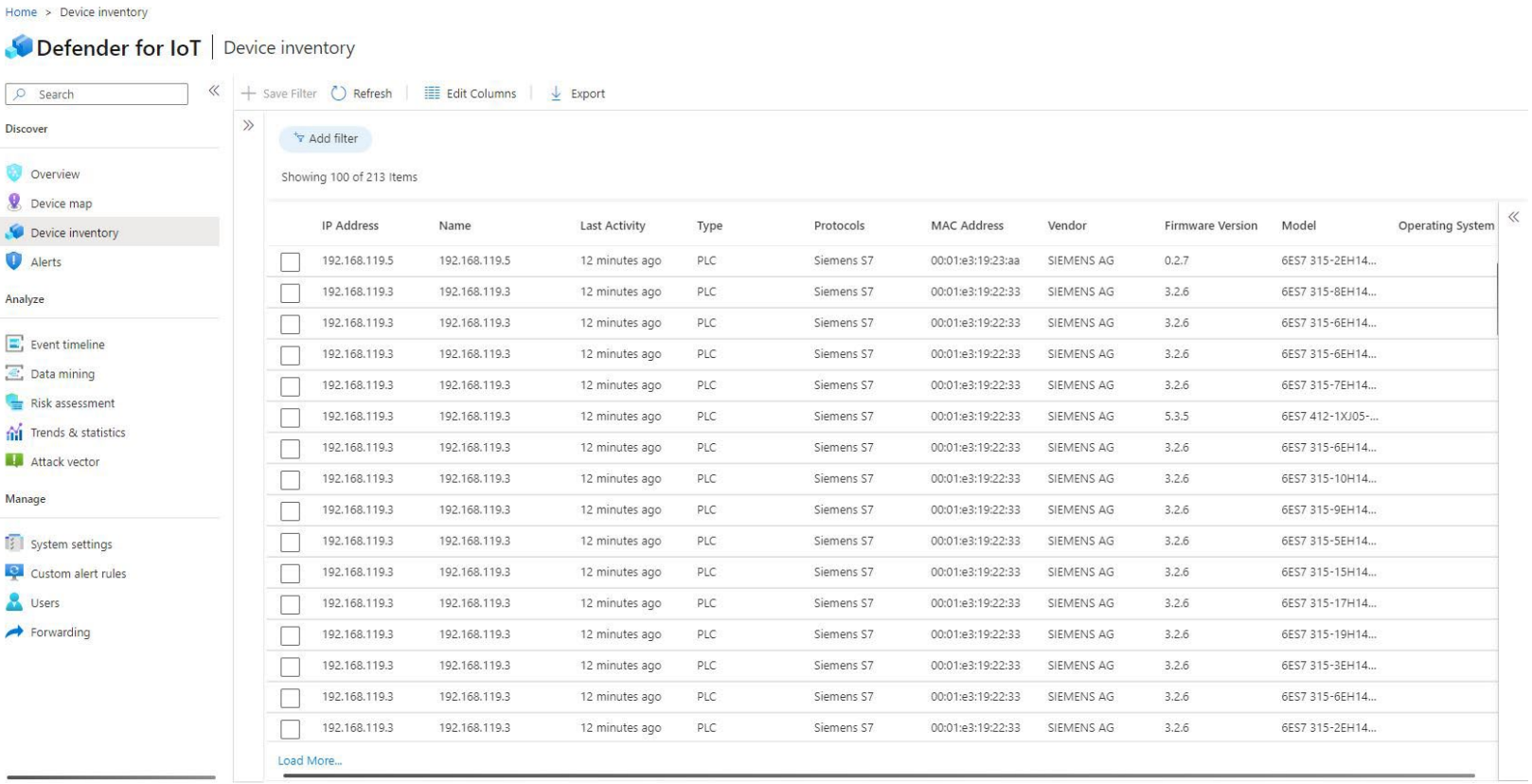
Internet connections.

Exercise 4 Inventory

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

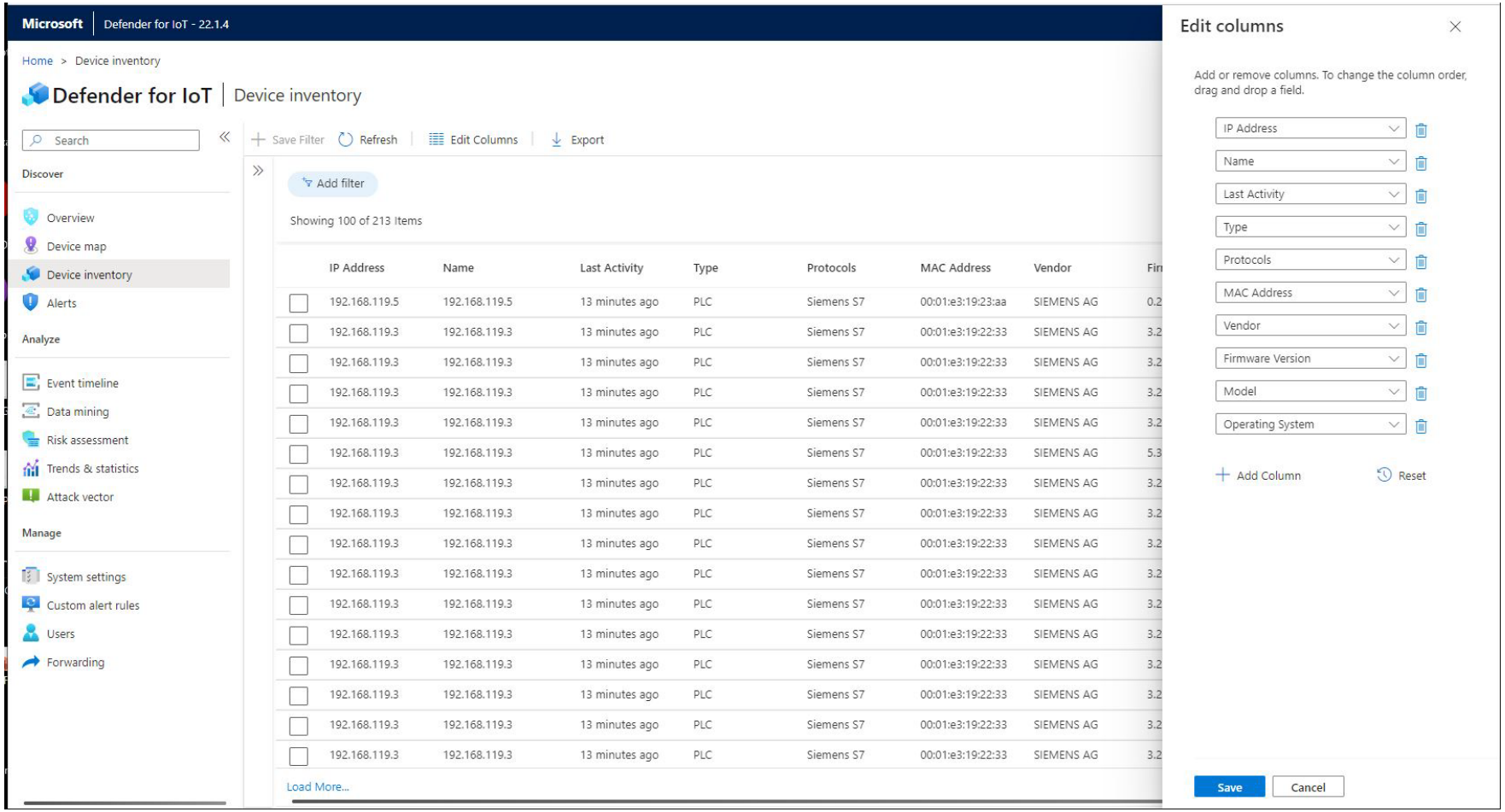
Step 1

Select “Inventory”


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
Add filter
Showing 100 of 213 Items
IP Address
Name
Last Activity
Type
Protocols
MAC Address
Vendor
Firmware Version
Model
Operating System
192.168.119.5 192.168.119.5 12 minutes ago PLC Siemens S7 00:01:e3:19:23:aa SIEMENS AG 0.2.7 6ES7 315-2EH14...
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 6ES7 315-8EH14...
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 6ES7 315-6EH14...
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 6ES7 315-6EH14...
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 6ES7 315-7EH14...
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 6ES7 412-1XJ05-...
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 6ES7 315-6EH14...
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 6ES7 315-10H14...
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 6ES7 315-9EH14...
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 6ES7 315-5EH14...
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 6ES7 315-15H14...
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 6ES7 315-17H14...
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 6ES7 315-19H14...
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 6ES7 315-3EH14...
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 6ES7 315-6EH14...
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 6ES7 315-2EH14...
Load More...

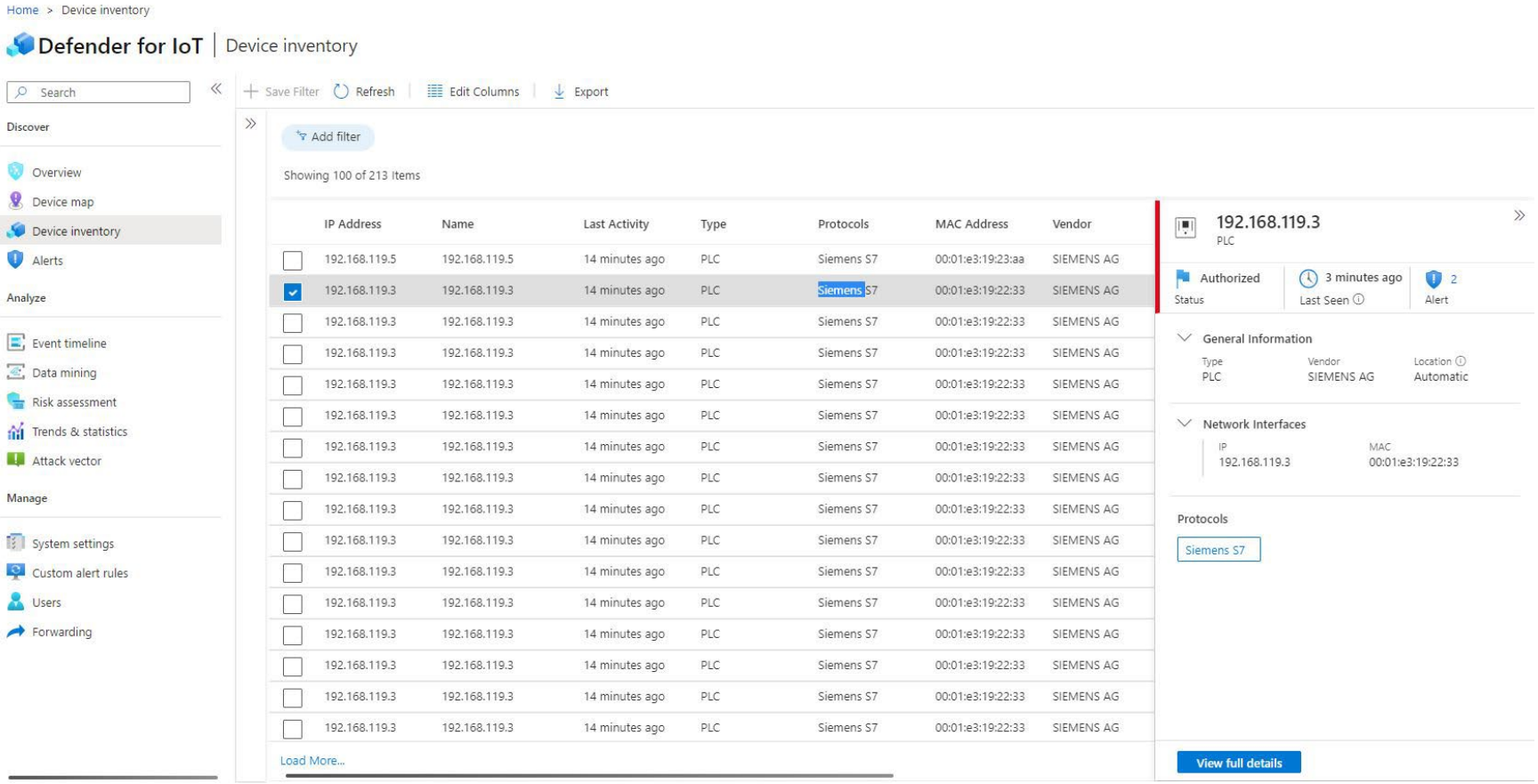
Step 2

Edit Columns



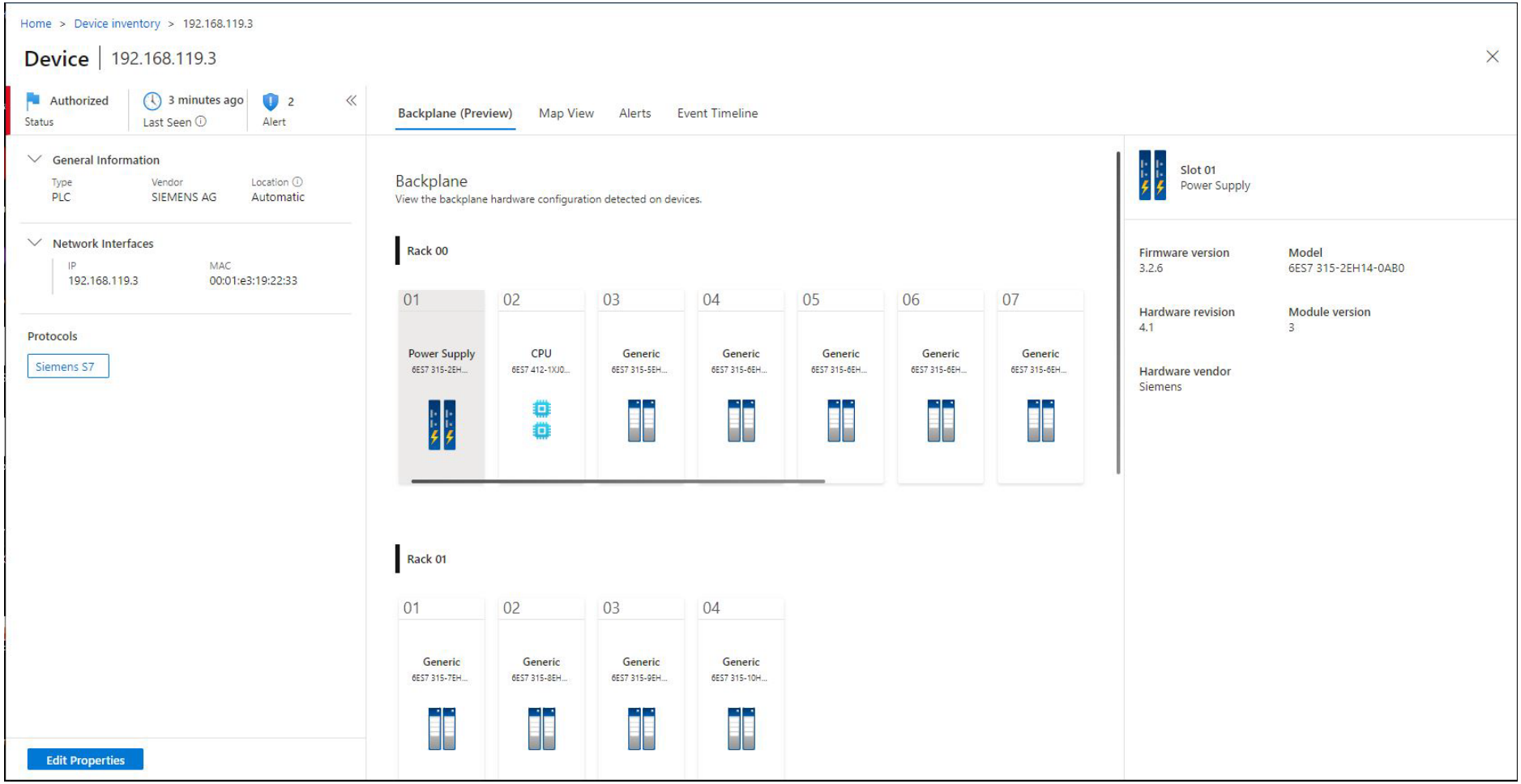
Step 3 select

192.168.119.3



Step 4

“View full details”

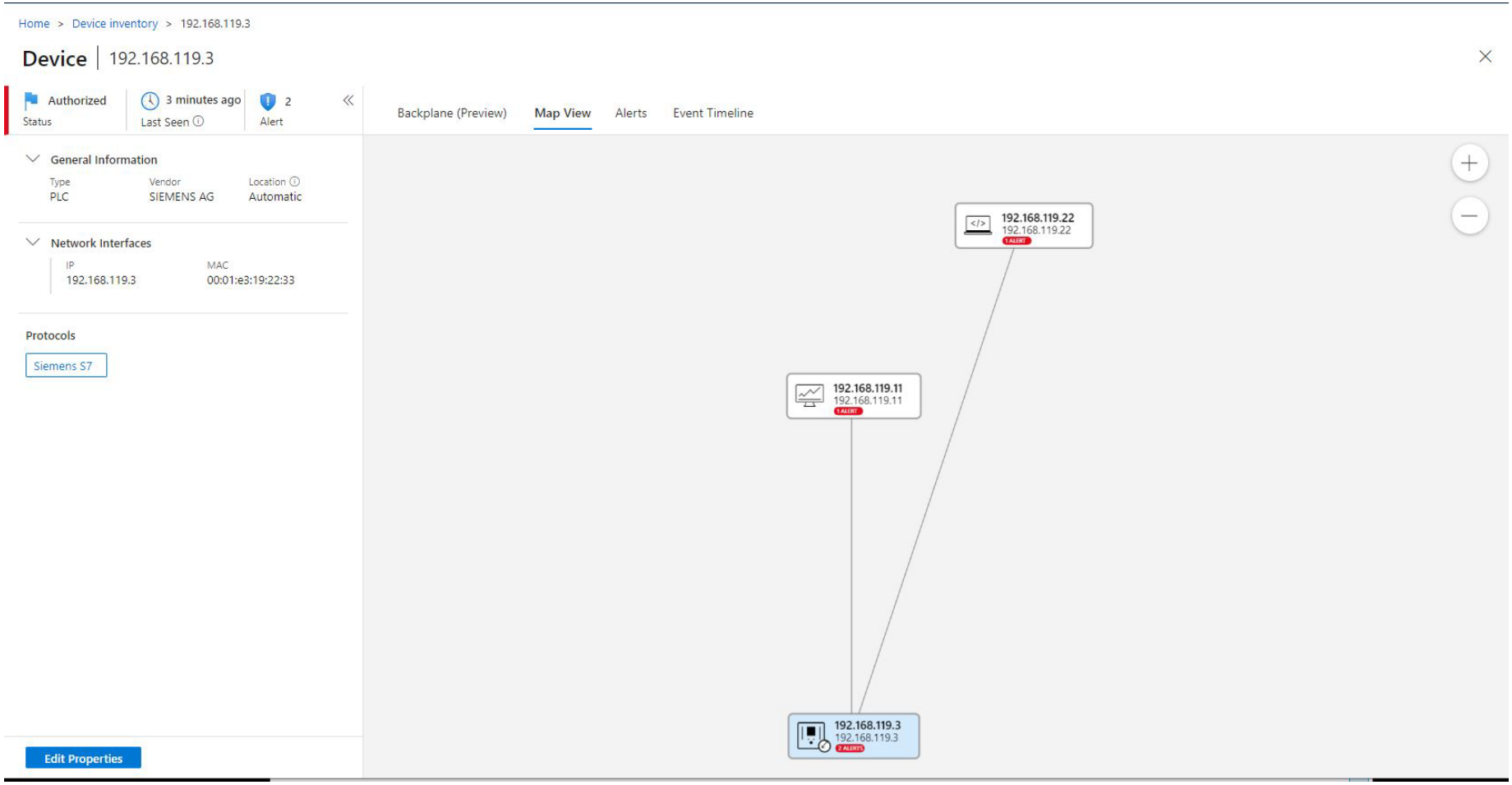


Notice that this is an even more complex PLC, Multiple Racks and each with their populated slots.

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

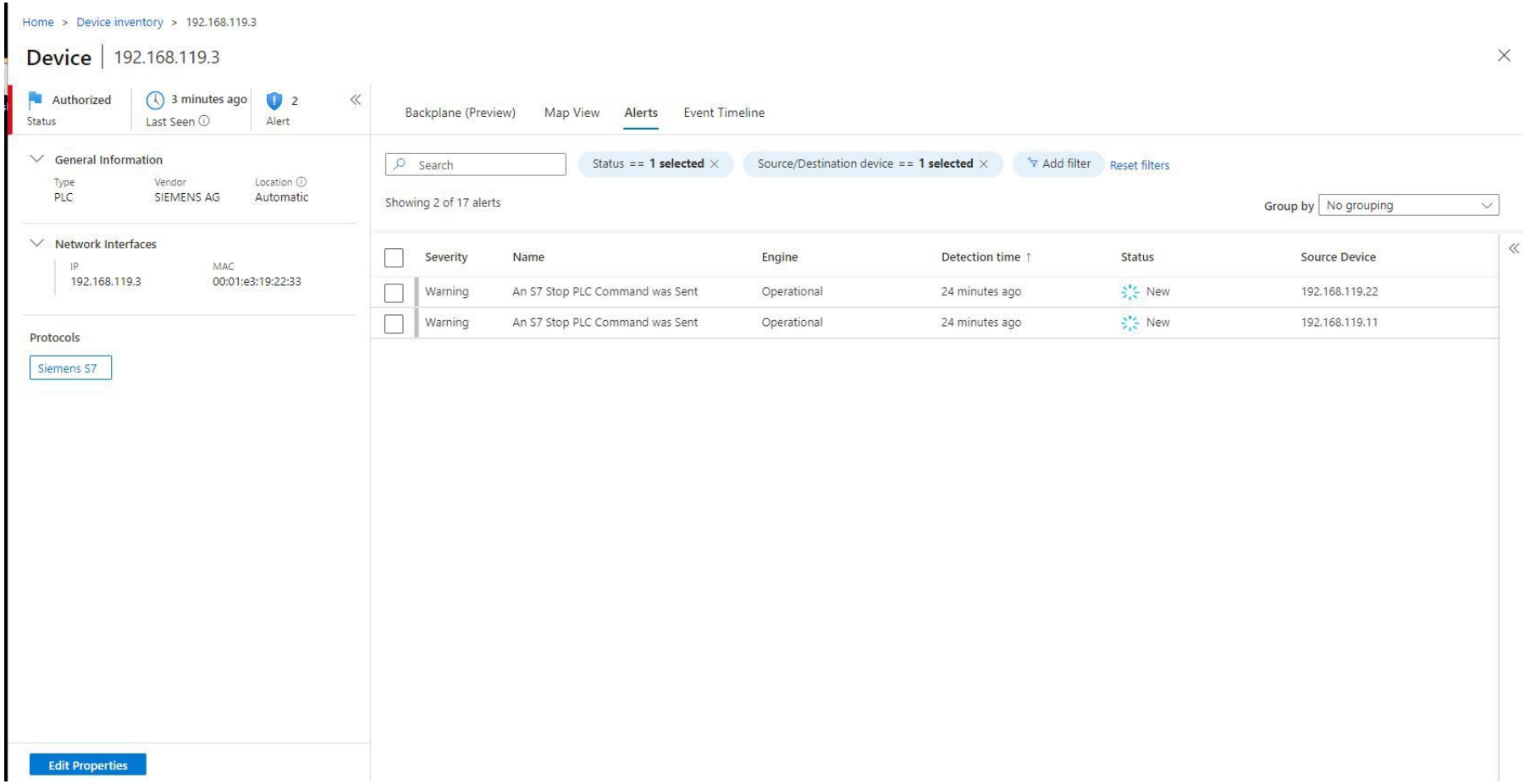
Step 5

Click on Map View



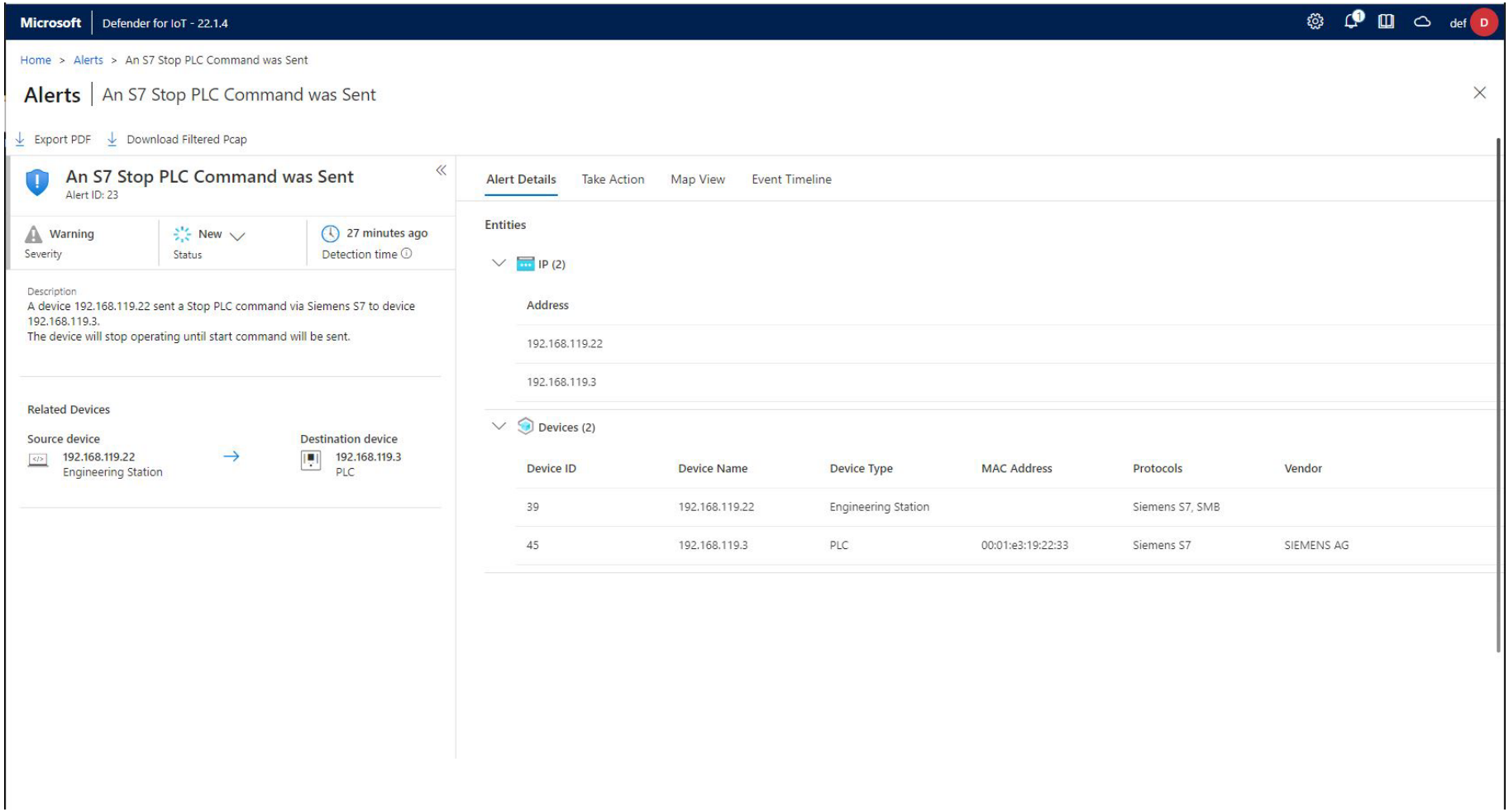
Step 6

Click the Alerts tab



Step 7

Highlight an alert and “get full details”



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

Take Action>mute

Map view

Download filtered pcap

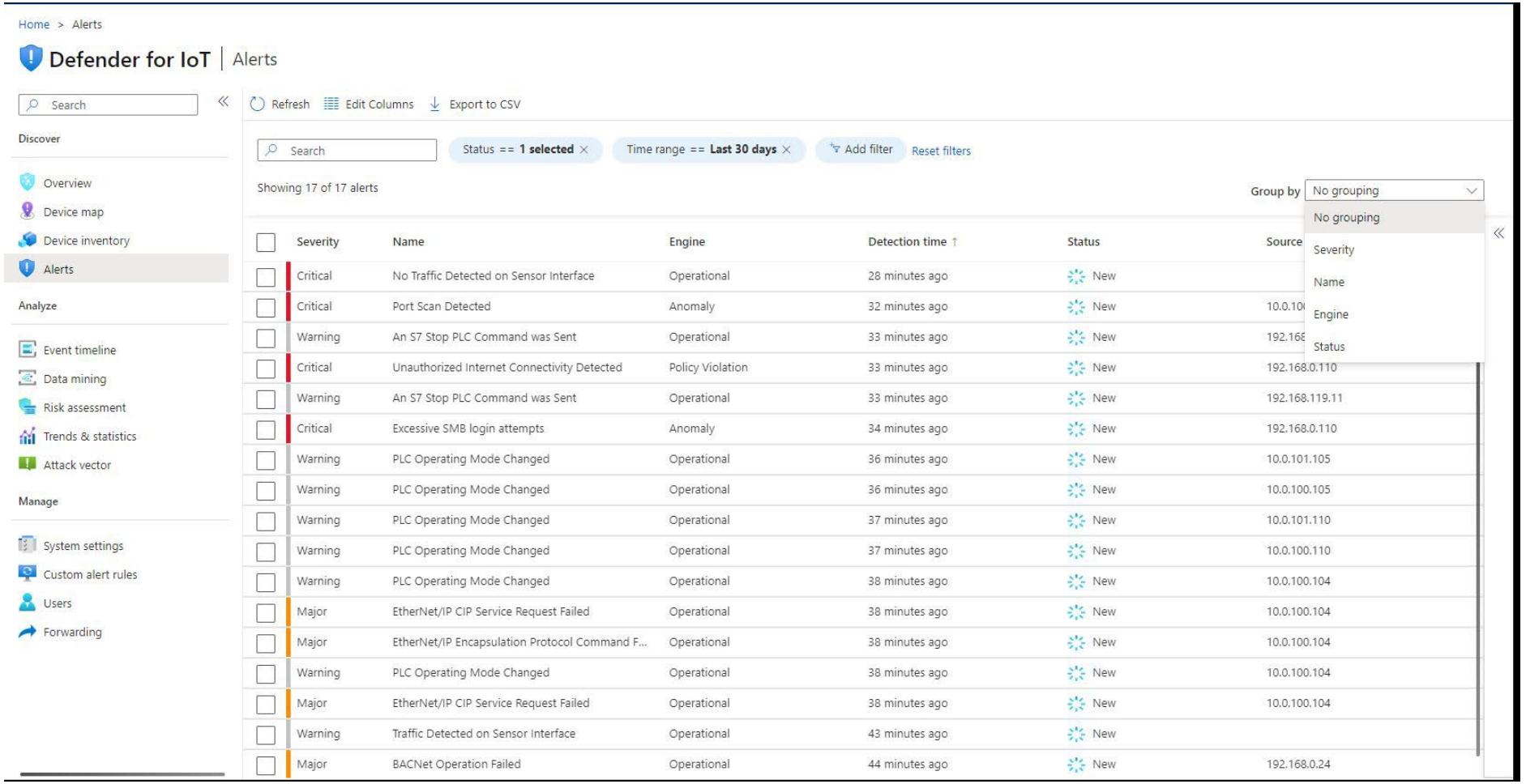
Event Timeline

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



Step 2

Grouping Option

Sort this list by different groupings

- Severity

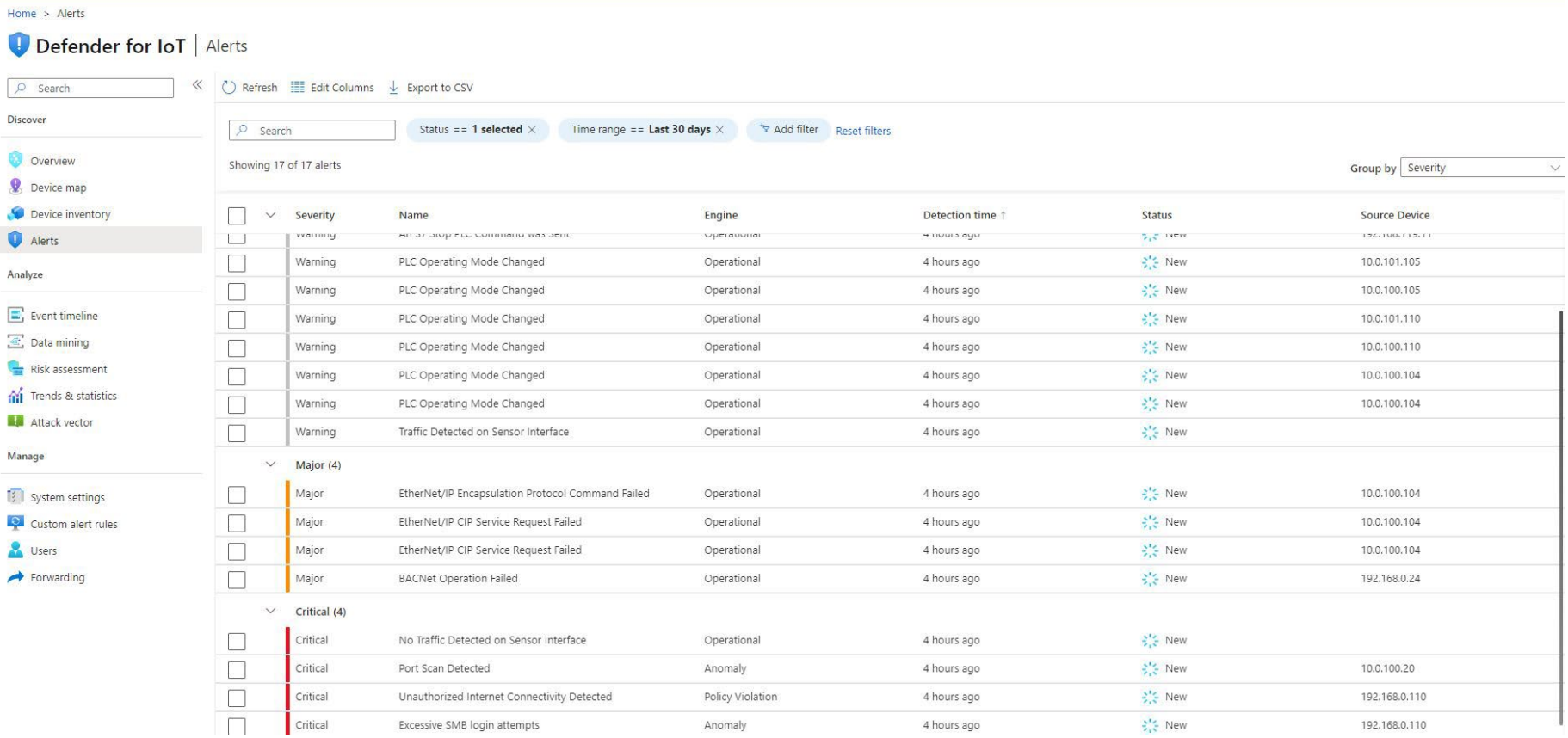
Name

Engine

Status

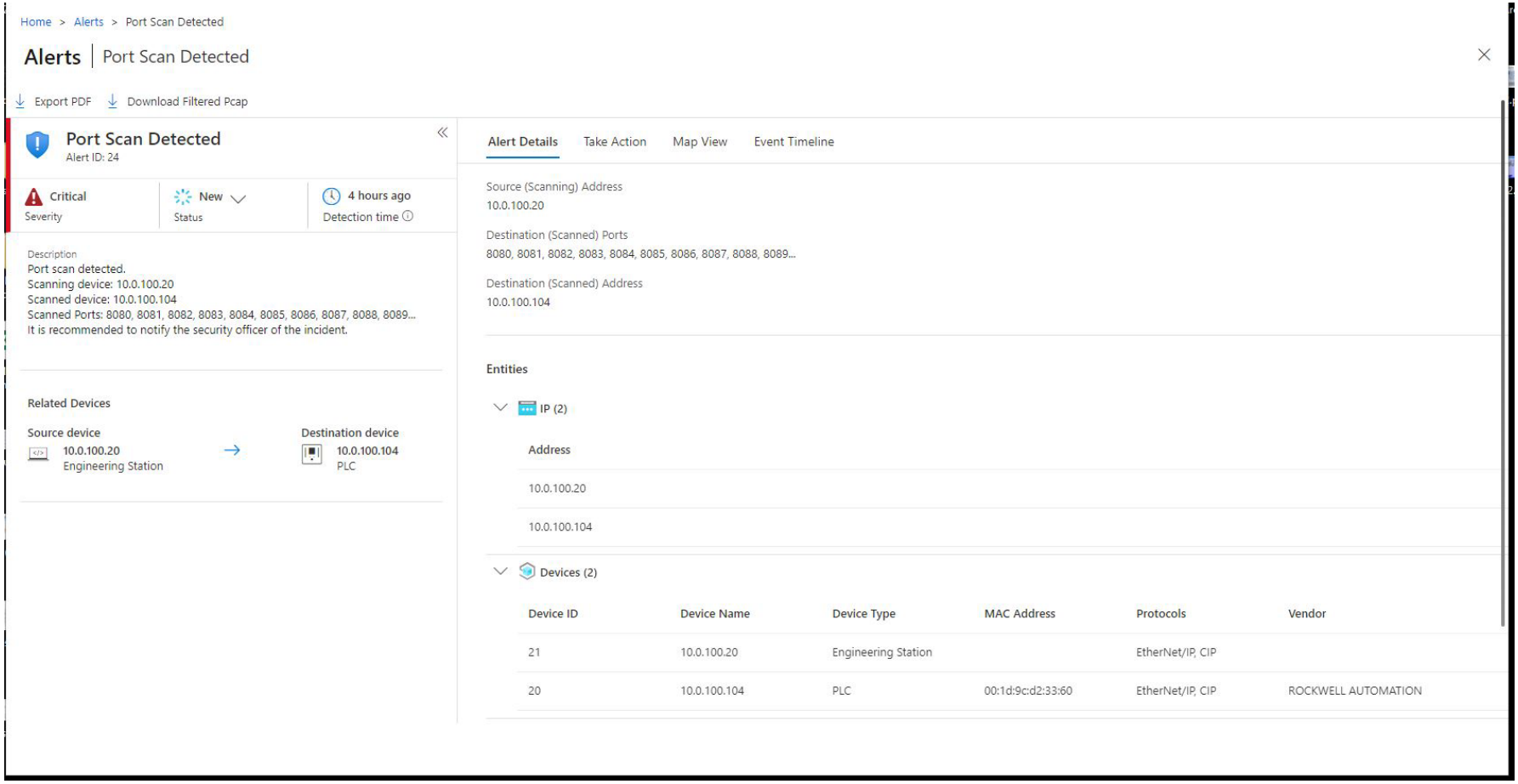
Step 3

Group the alerts by Severity and scroll down to the bottom



Step 4

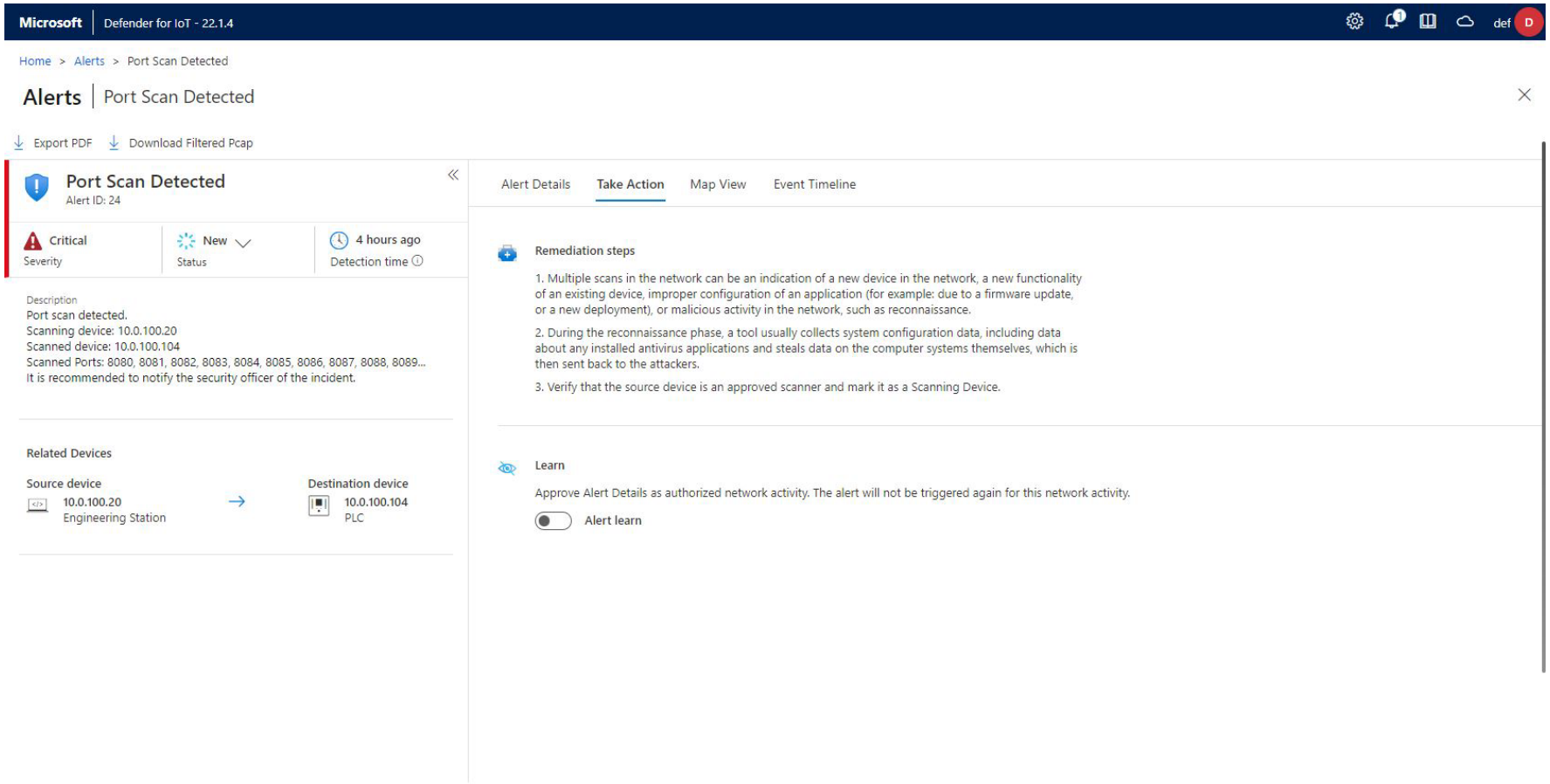
Select Critical “Port Scan Detected” and then “View Full Details”



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



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.

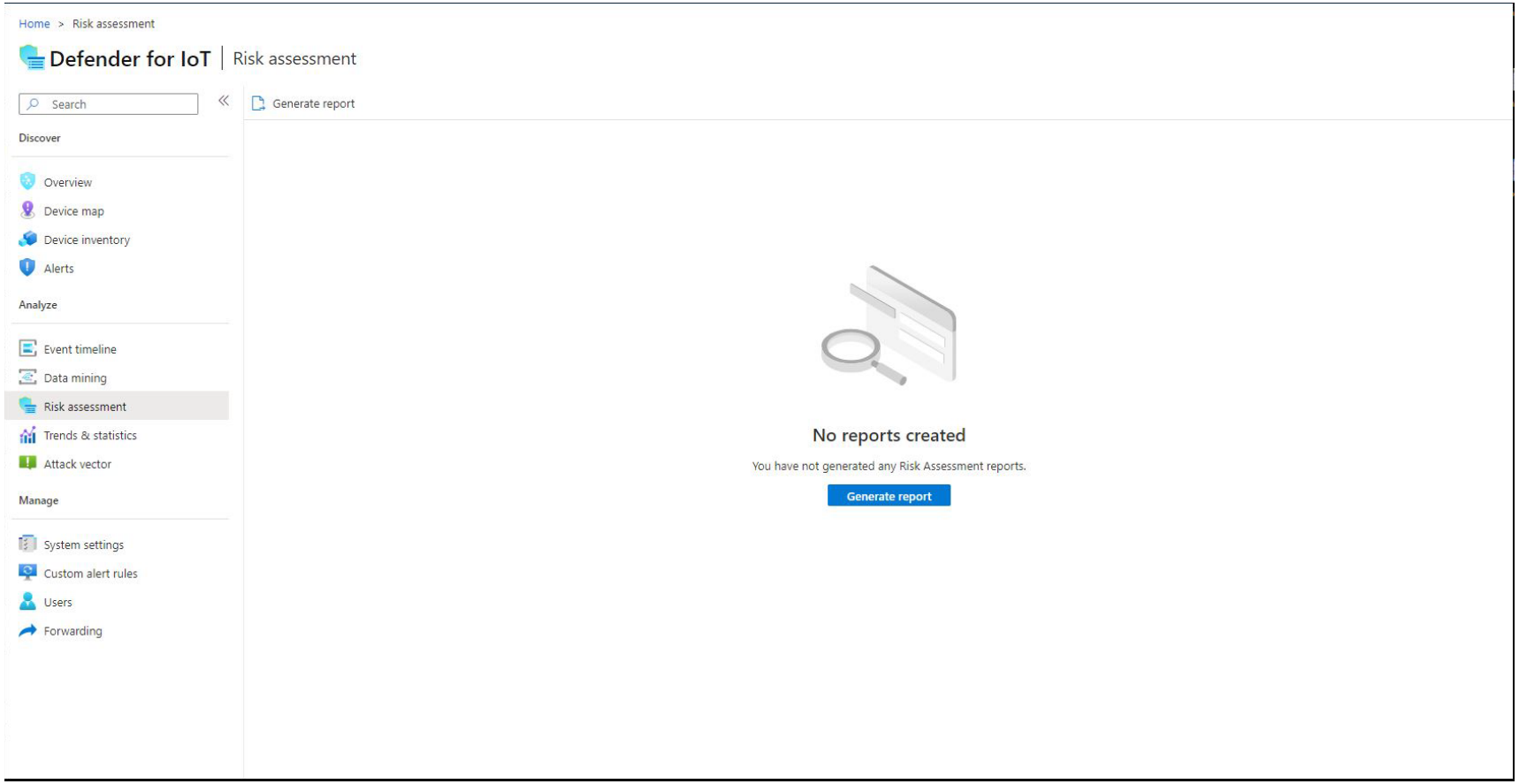
Exercise 6 Risk Assessment

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

Step 1,

Select Risk Assessment from Menu

Step 2 Generate Report



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 is says and how it can be leveraged.

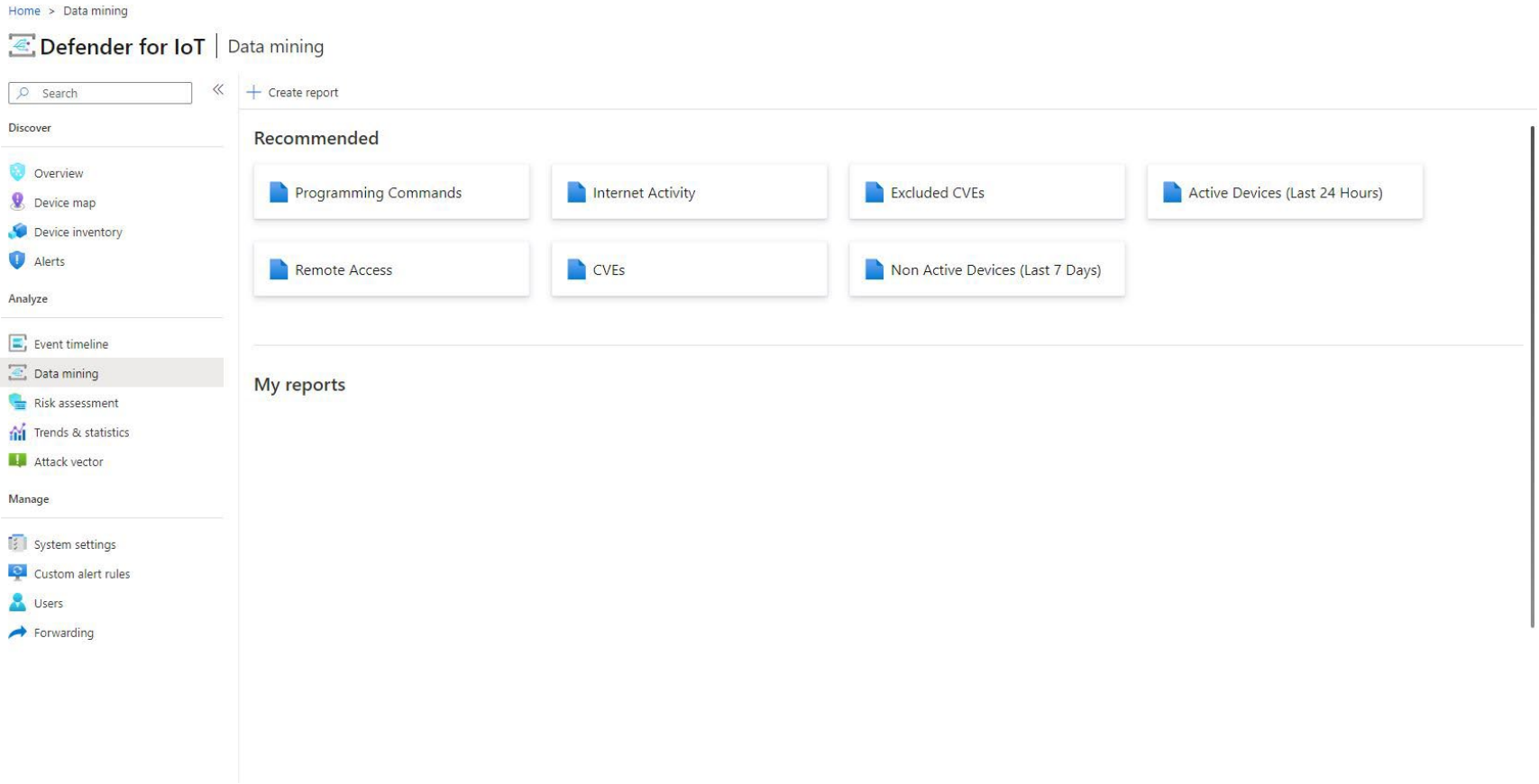
Exercise 7 Data Mining

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

Step 1
select “Data Mining”

Step 2

Review the “recommended” reports



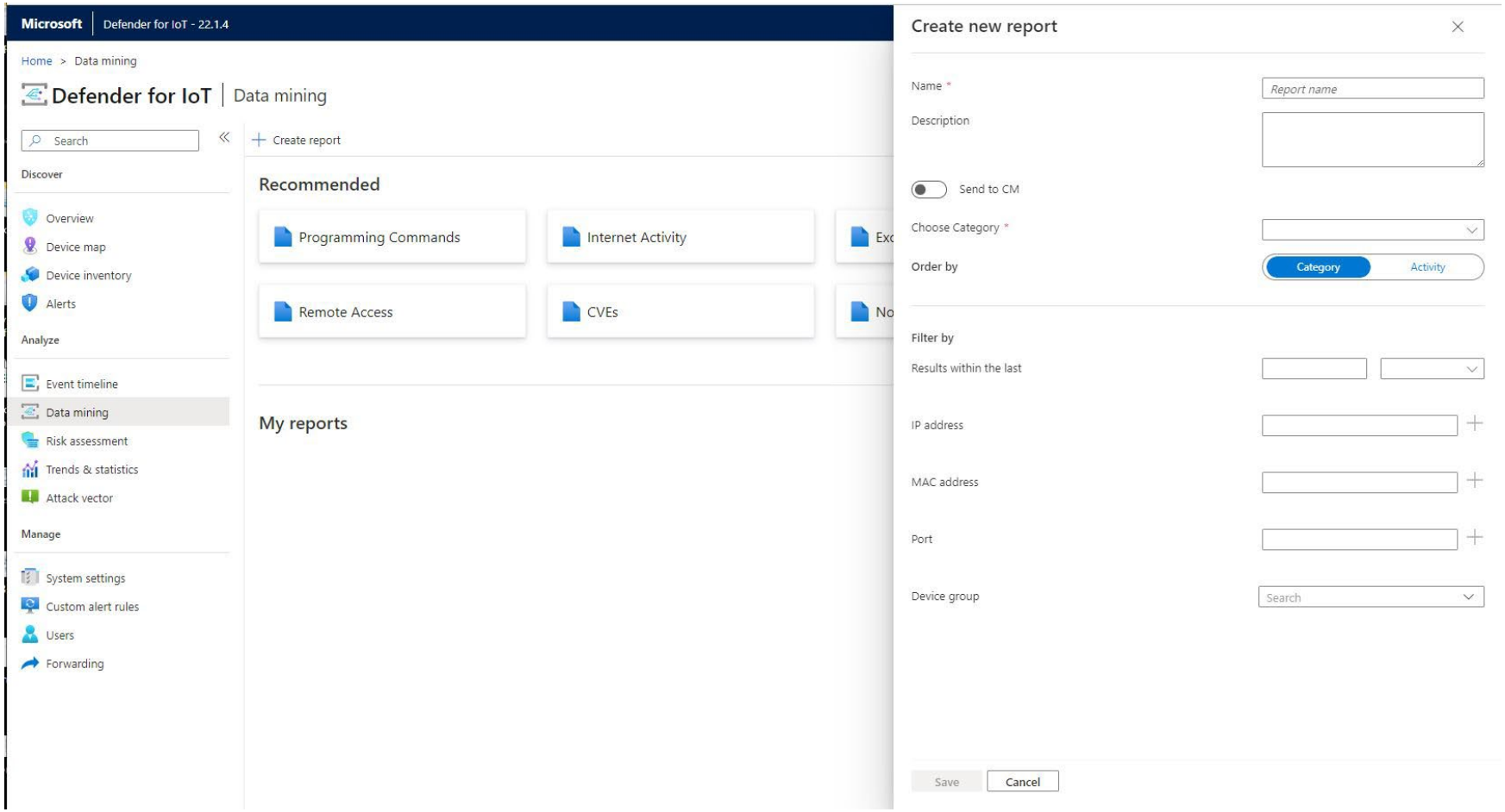
Step 3

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

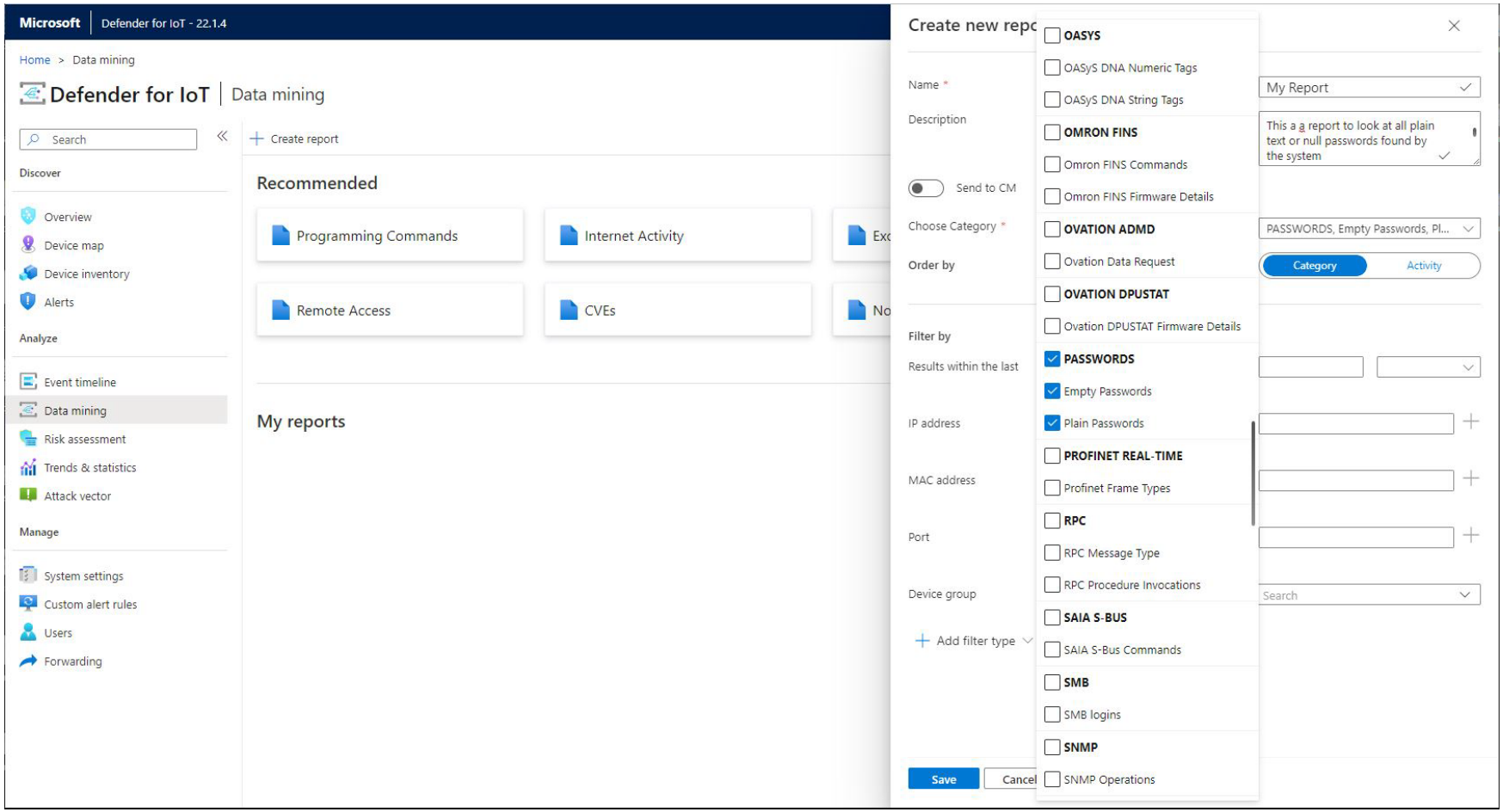
Select the “Create Report”



Here you are present 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

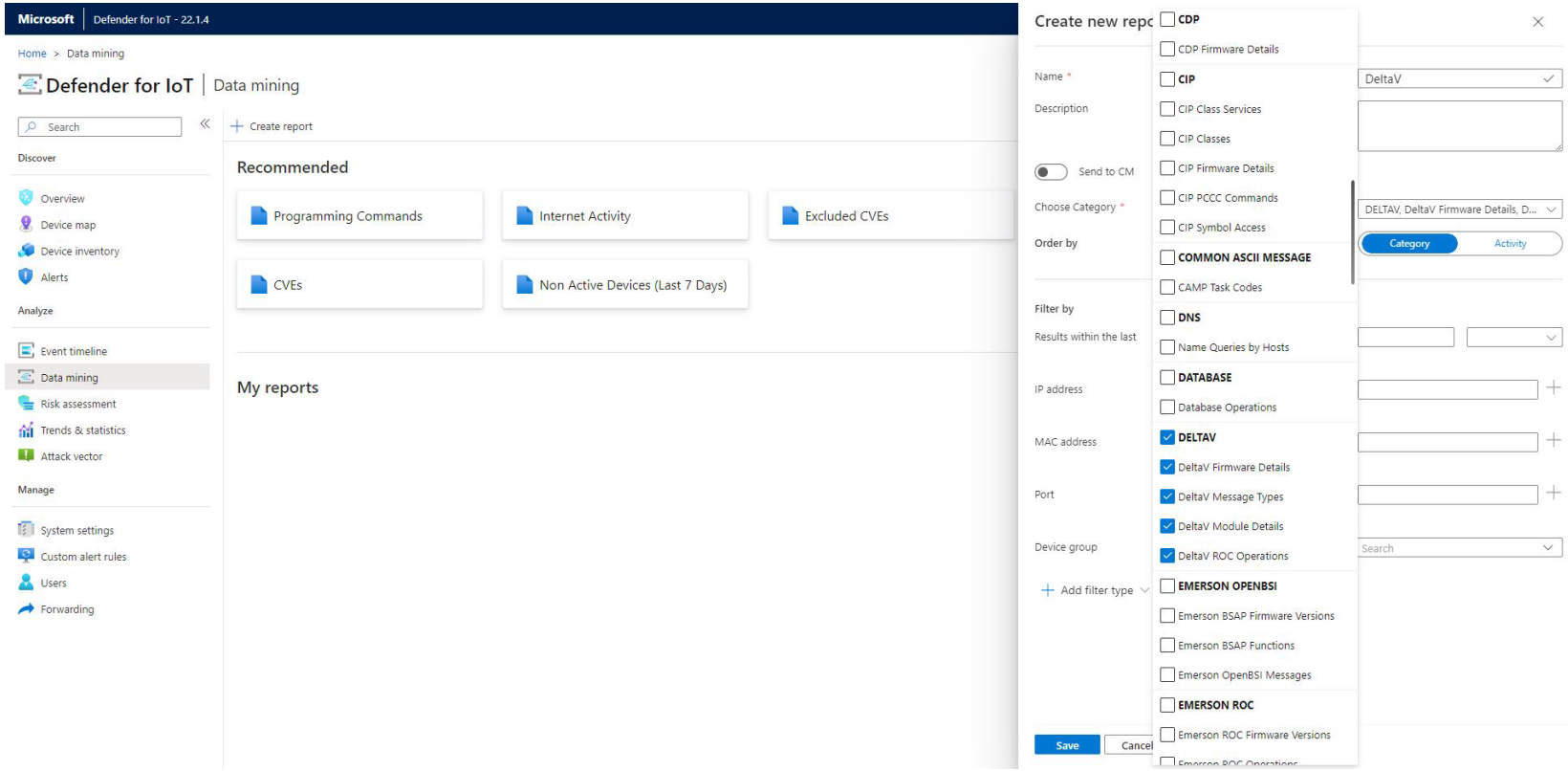


Step 6

Build another report

Name it DeltaV

Select DeltaV from the dropdown list

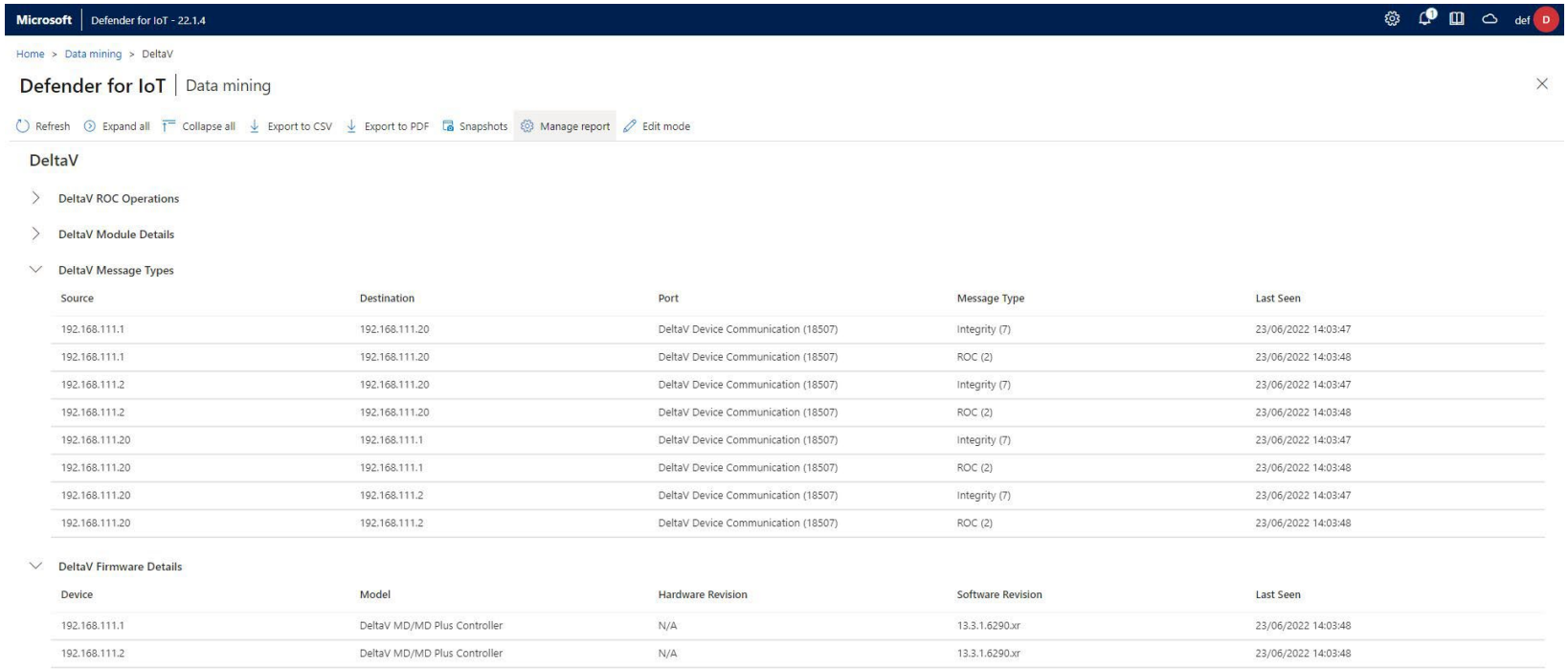


Step 7

Save the report and open it.

Step 8

Expand each sub catagory



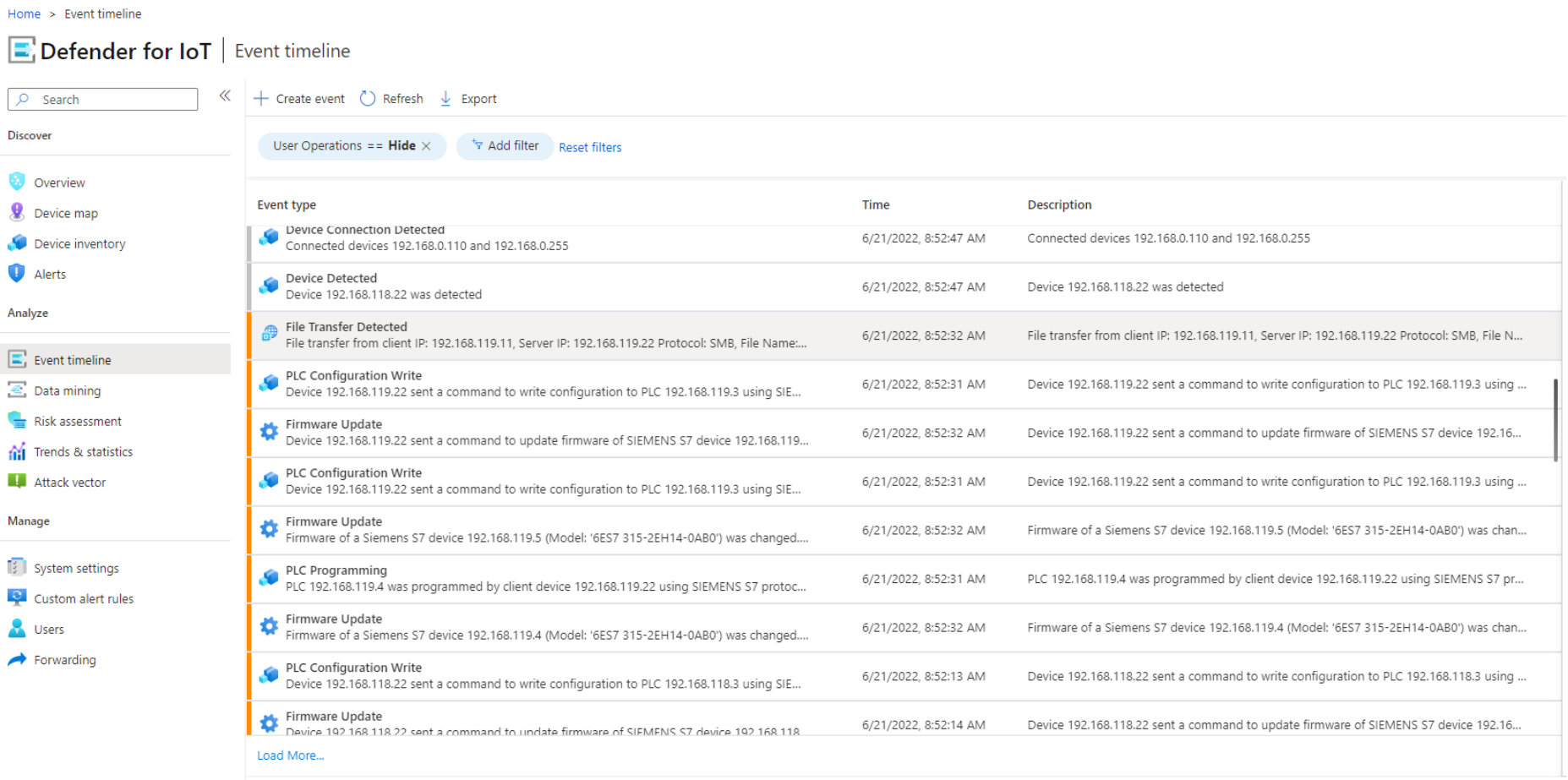
Take some time and explore the variety of reports you can generate and think of who would; benefit from this extensive data

Exercise 8 Event Timeline

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

Step 1

Select “Event Timeline”



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

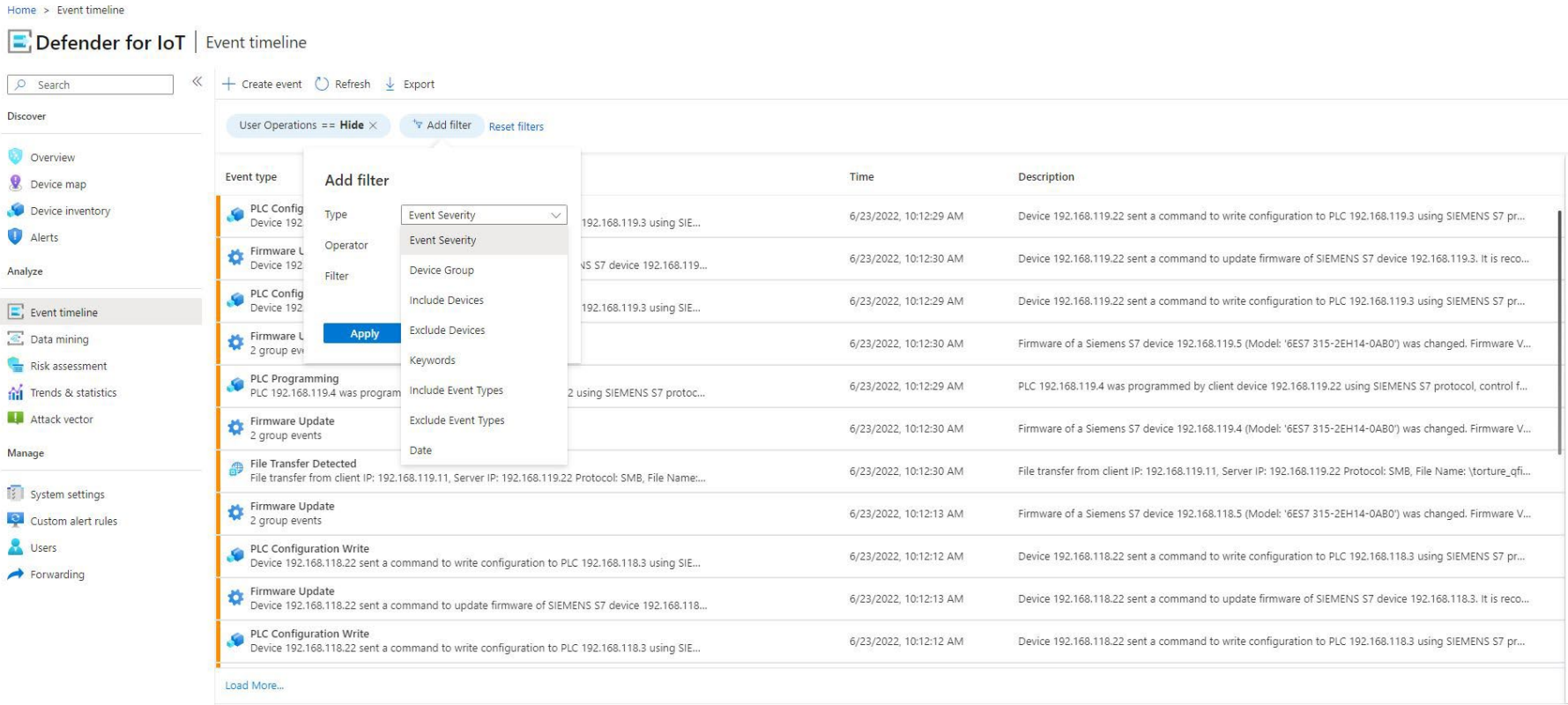
Essentially what you have is an auditable timeline of every action in the system, including user activity on the system itself.

Step 3

Select Add Filter

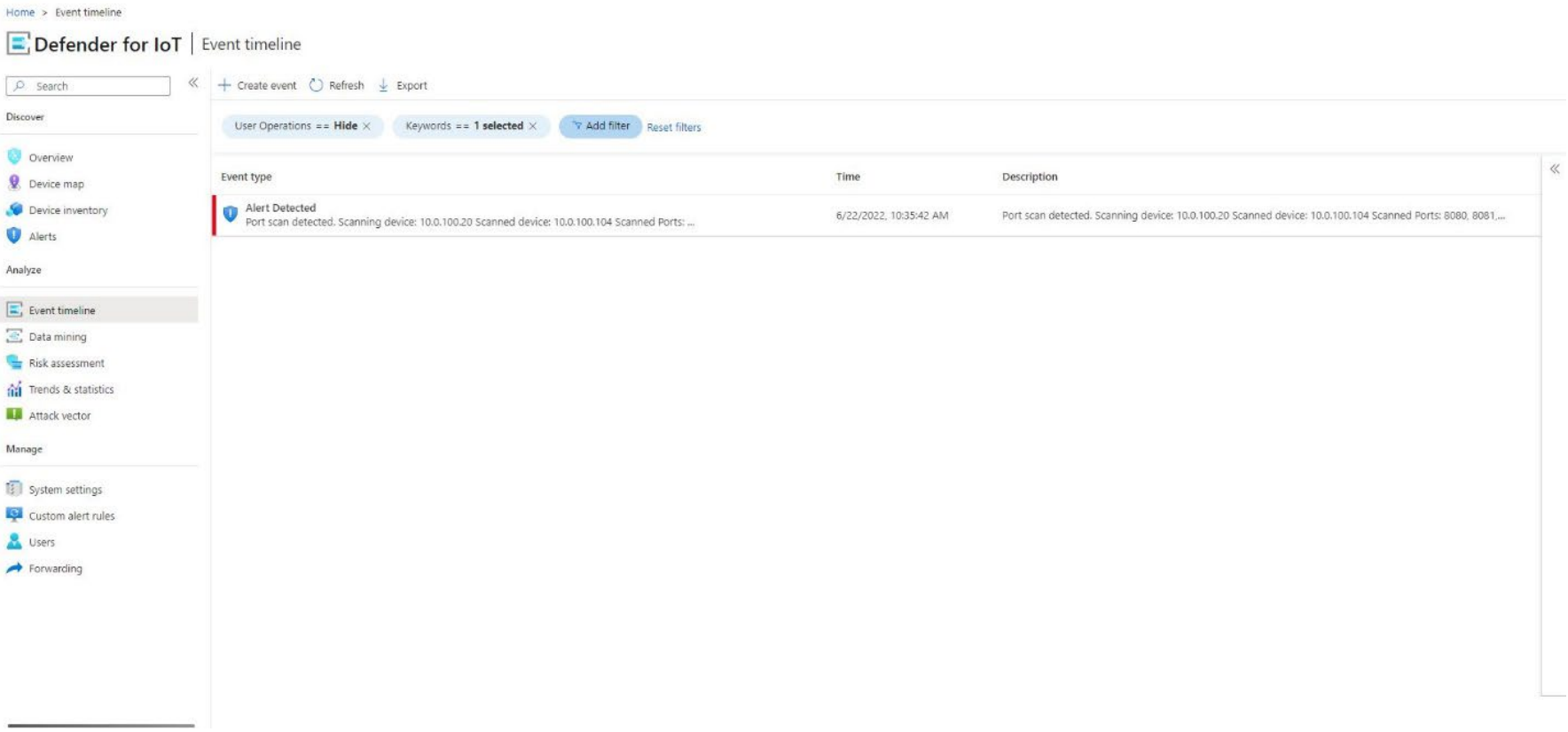
Type = Keyword

Filter = Port



Step 4

Apply Filter and Review

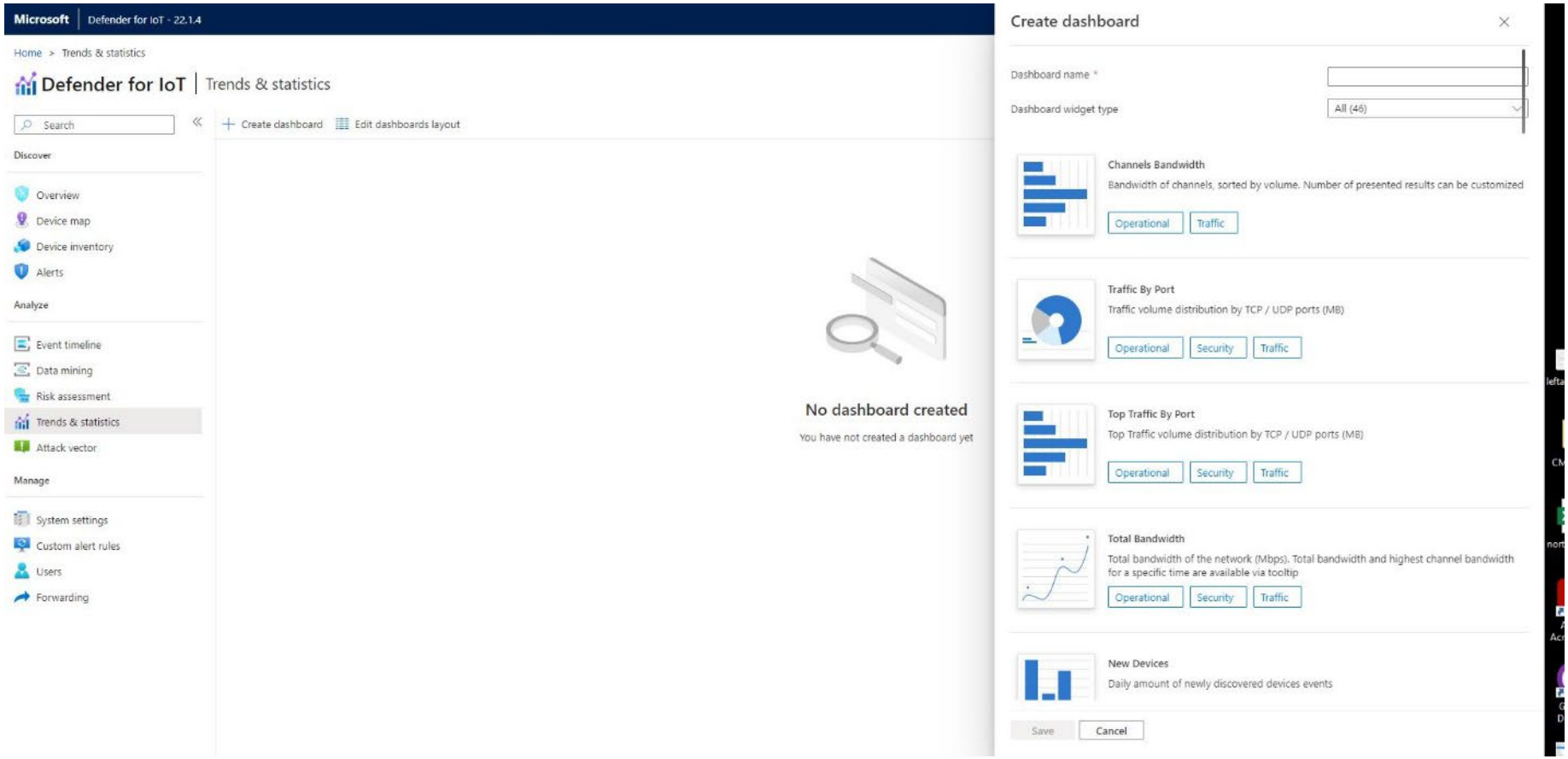


Exercise 9 Trends and Statistics

- Trends and Statistic
- Dashboard Creation
- Add Widgets

Step 1

Select Trends and Statistics then “create dashboard”

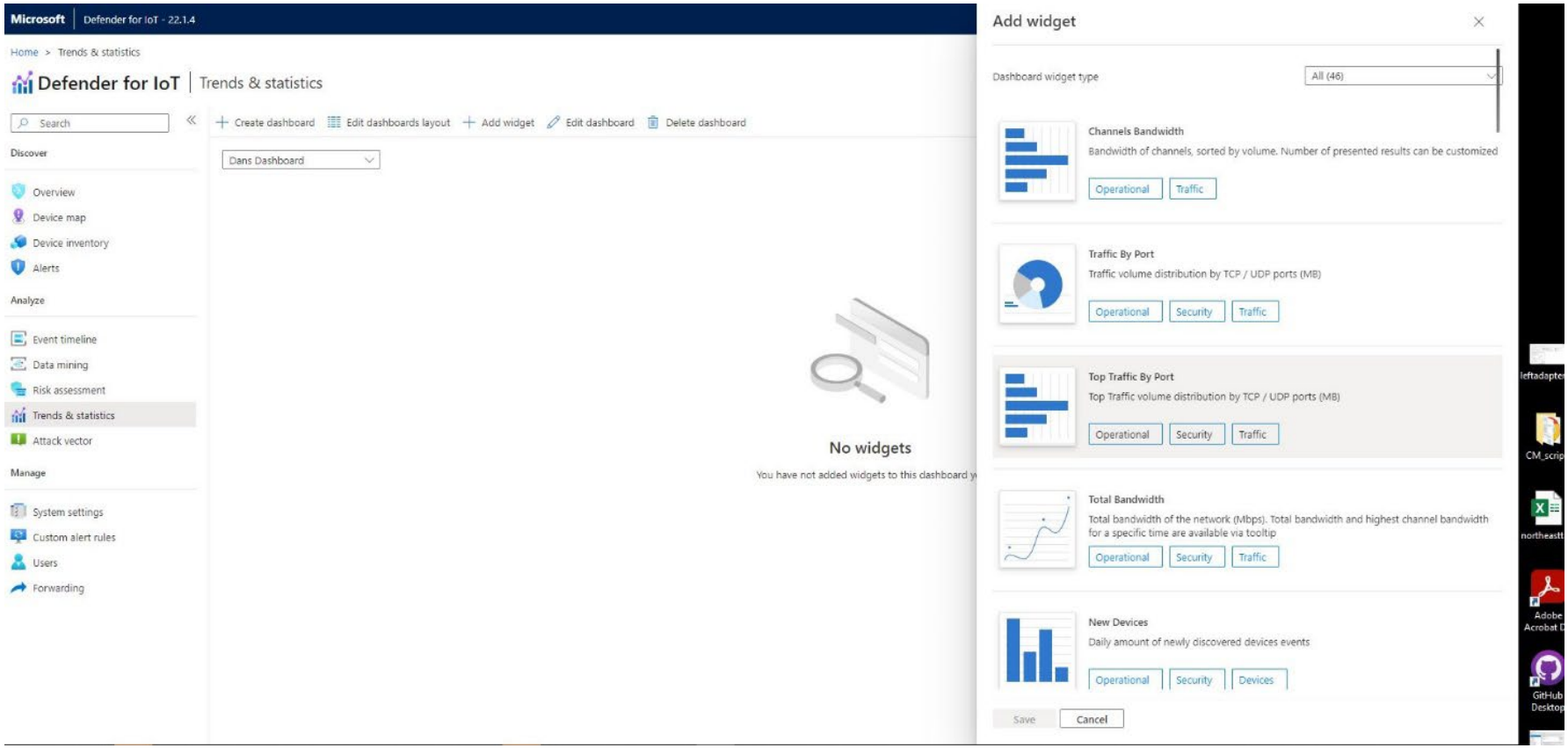


Step 2

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

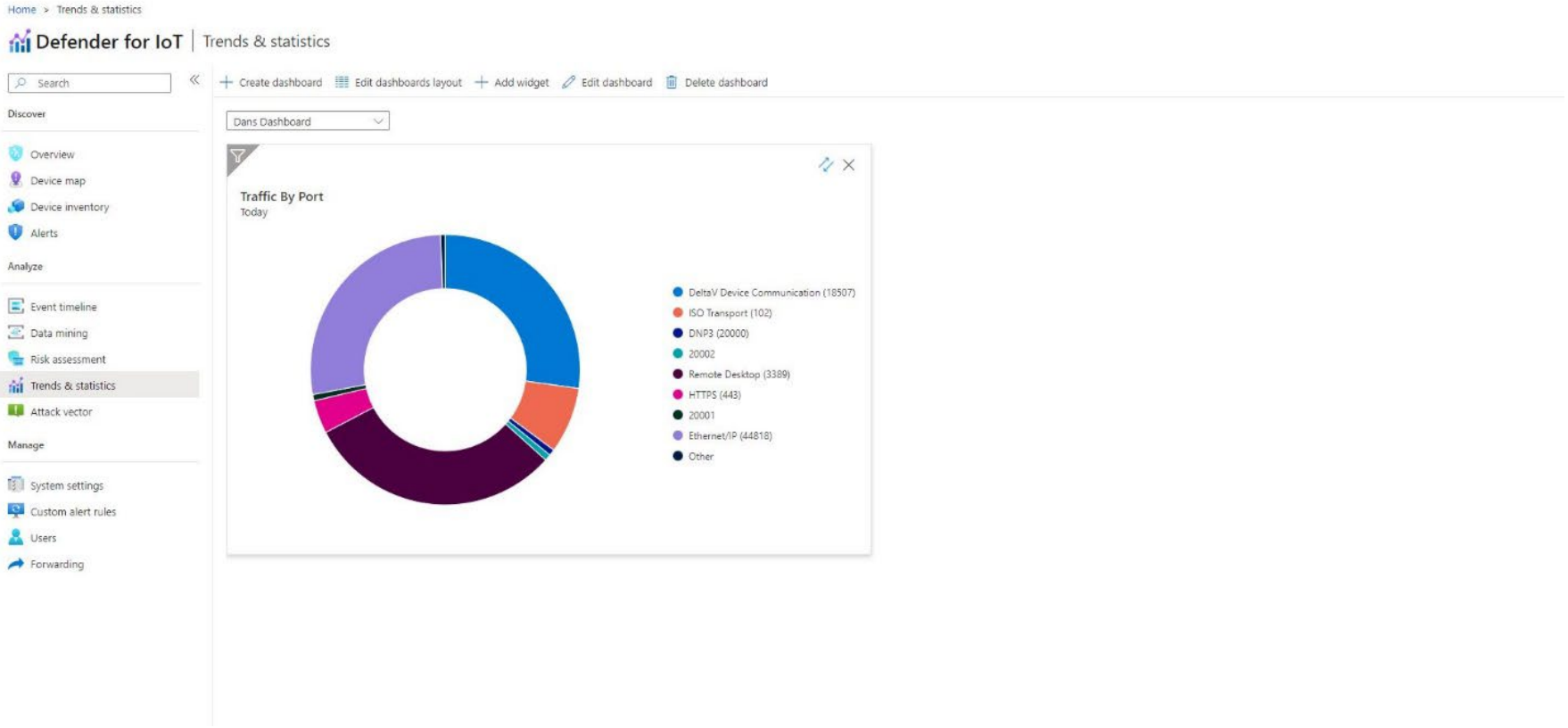
Step 3

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



Step 4

Chose “Traffic by Port”



Step 5

Add other widgets, experiment with the page layout,