**QUICK** START GUIDE

# CATCH A HACKER

## Episode Two: Anatomy of a Lateral Movement Attack

**Created By:** Max Lewis, Mohammad Waqas, Sean Duval, Carlos Buenano, Michal Tzur-Hilleli, Bryan Inman, Matthew Gambold

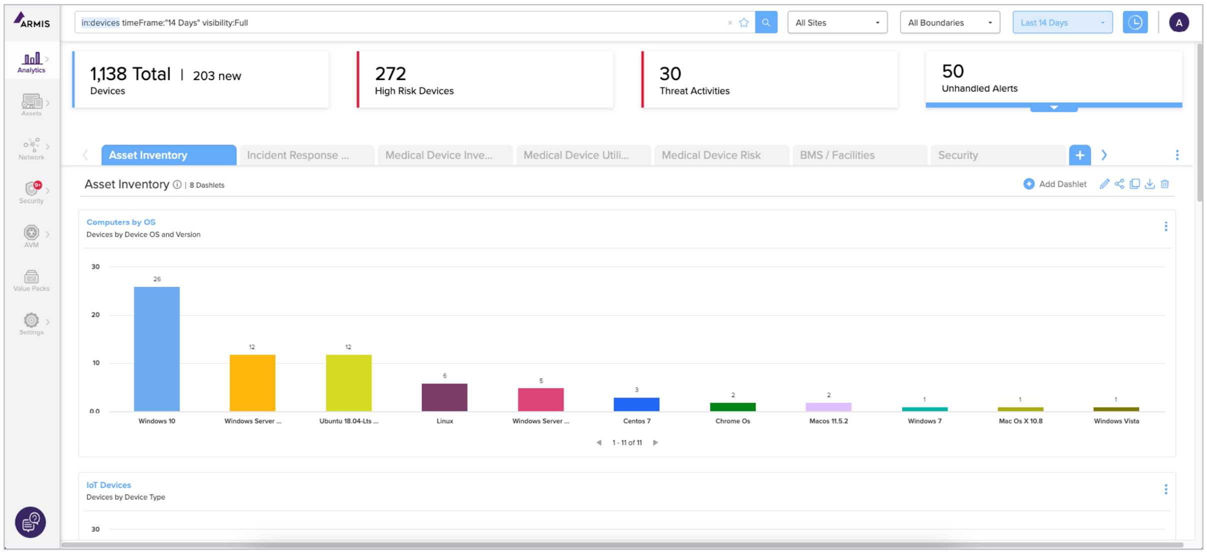
# Labs

# Lab 1: Armis Introduction

**Scenario:** Before we begin the threat hunt, let’s take a few minutes to acclimate ourselves to the Armis console.

## 1 | Login to the Armis console

Login to the Armis console (https://demo-hacker.armis.com). You will be provided with individual credentials from your instructor.



in:devices timeFrame:"14 Days" visibility:Full

All Sites

All Boundaries

Last 14 Days

1,138 Total | 203 new
Devices

272
High Risk Devices

30
Threat Activities

50
Unhandled Alerts

Asset Inventory | 8 Dashlets

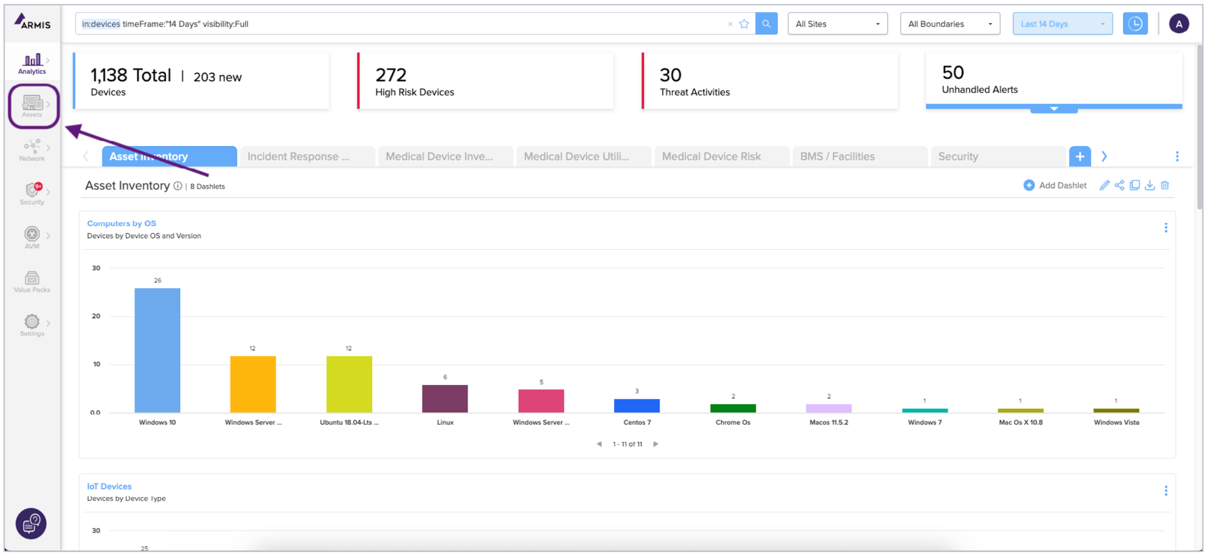
Computers by OS
Devices by Device OS and Version

IoT Devices
Devices by Device Type

This is the main **Dashboards** page, a customizable way to display meaningful Armis device data. We will dive deeper into this in the following labs, but for now, let's navigate to the **Devices** catalog.

## 2 | Navigate to ‘Inventory’

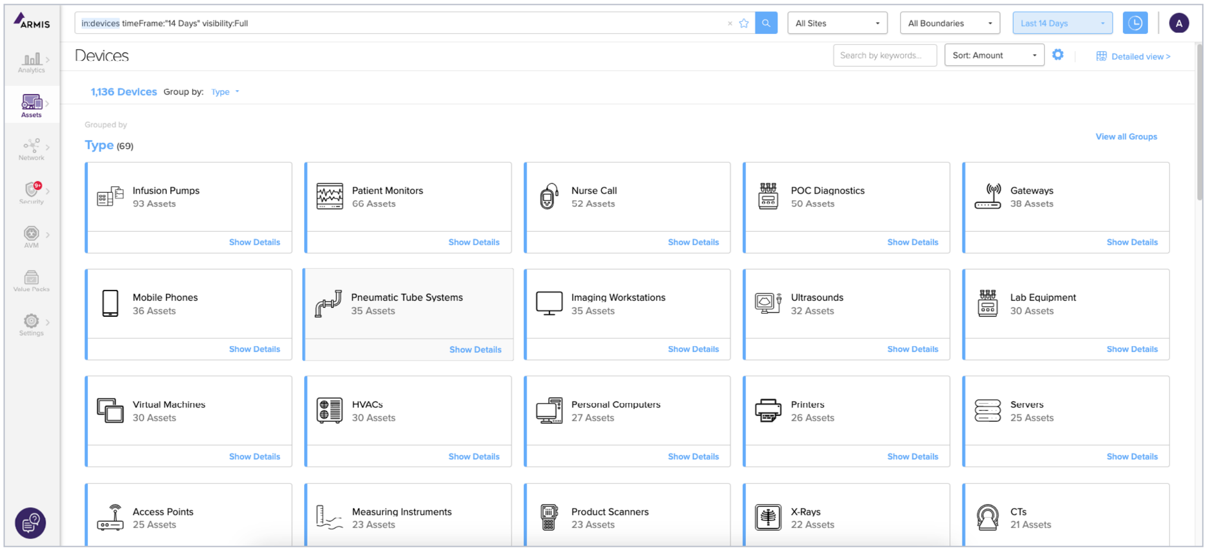
Navigate to **Assets in the top left**, and then select **‘Devices’** to browse all the device categories and models discovered in this environment.



## 3 | Notice the multitude of diverse asset types that are discovered with Armis.

This **“Devices"** catalog view provides a simple and user-friendly breakdown of device types discovered by the Armis platform. Notice that the device types include devices such as:

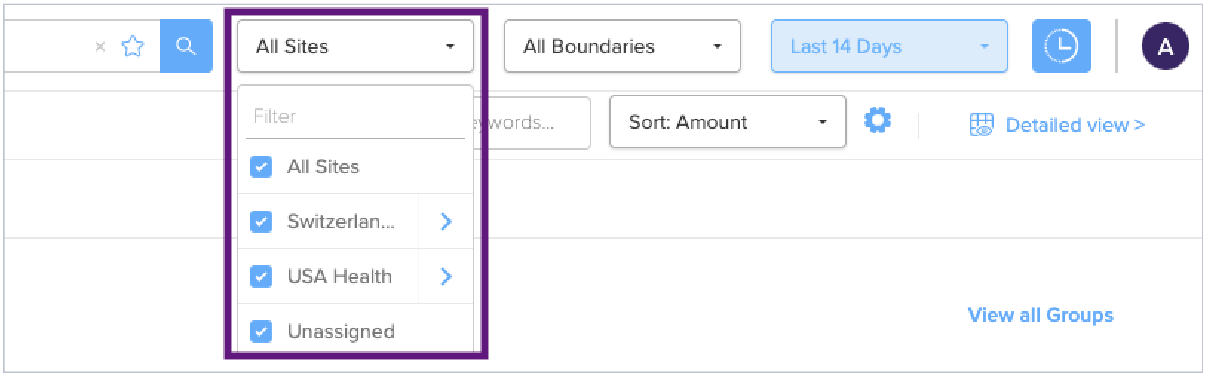
- Traditional IT assets (PCs, Laptops, Servers, Virtual Machines, Firewalls, Routers, etc)
- IoT devices (Cars, Drones, Dash Cams, Cameras, Thermostats, Smart TVs, Lighting, etc)
- IoMT devices (MRI, CT, POC Diagnostics, Infusion Pumps, Pneumatic Tube Systems, etc)



Note: Device type classification is automatic as new devices are discovered by Armis. This environment does not represent all types of devices known to Armis.

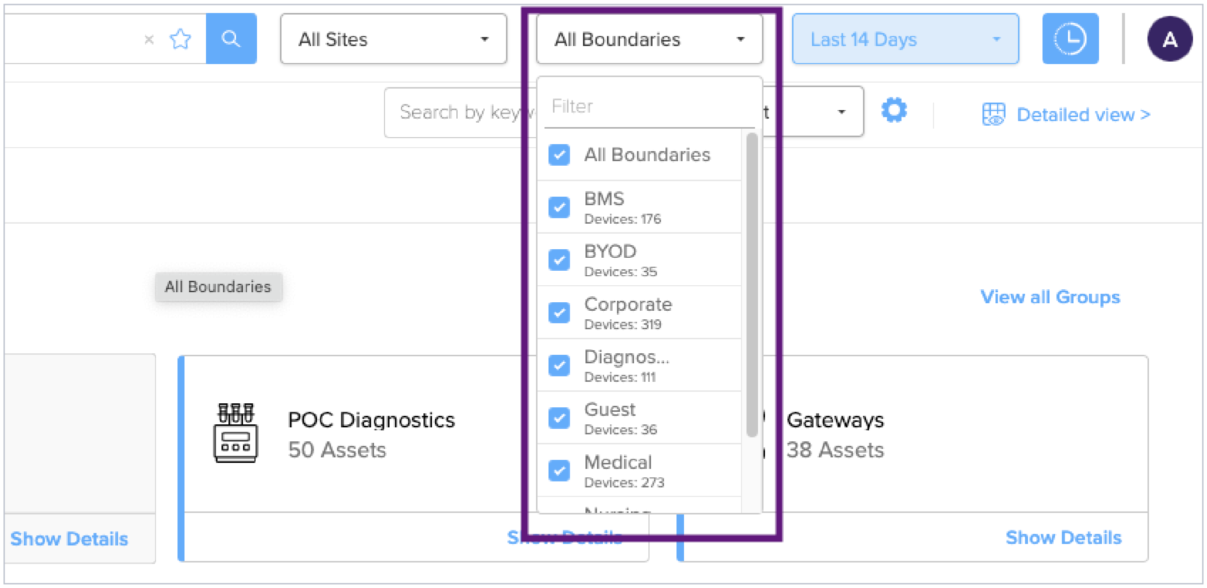
## 4 | Choose and change different physical ‘Sites’

Armis includes the ability to filter the results from any display/query by Site location of devices. In the top right-hand corner is a drop-down menu where you can select the specific site(s) data that you only want to see in the Armis console.



## 5 | Choose and change different logical ‘Boundaries’

An additional way to filter Armis results is by ‘Boundaries’. Boundaries are user-defined and can therefore fit the use cases and definitions for each specific customer. A boundary can be defined by such things as VLANs, subnets, device type, device OS, etc.



## 6 | Return to “Dashboard”

Click the “Analytics / Dashboard” button on the left-hand panel to prepare for the threat hunt scenario.

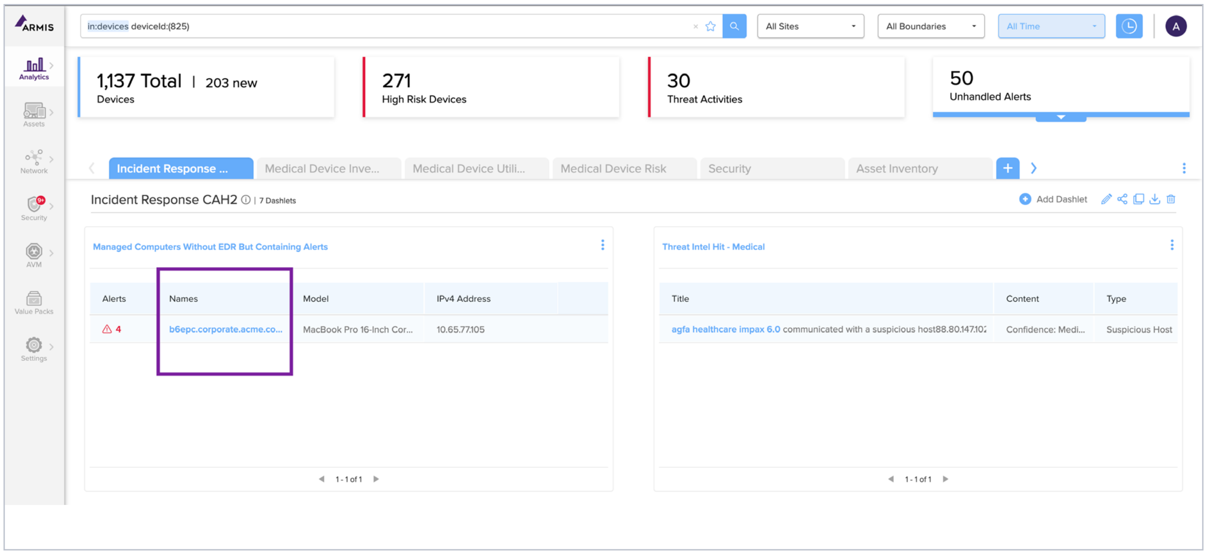
# Lab 2: Anatomy of a Lateral Movement Attack

**Scenario:** You have received several alerts from the Armis platform regarding recent activity inside of your organization's environment. The alerts seem to involve a wide variety of devices in your network: IT devices, Operational Technology and Building Management System (OT/BMS) devices, and Medical devices. This cross-boundary movement could be indicative of an advanced threat actor pivoting laterally through your environment.

Let's take a close look at the affected devices, the associated network activities, and the subsequent alerts generated by Armis.

## 1 | Go to the "Incident Response CAH2" Dashboard

Here we can see some of the dashlets the SOC is using to monitor the environment. Navigate to the Dashlet titled "Managed Computers Without EDR But Containing Alerts''. This dashlet displays key information about devices that have some degree of management (in this case the device is enrolled in JAMF management) yet still presents a risk within the environment due to threat activities and a lack of EDR.



in:devices deviceId:(825)

1,137 Total | 203 new
Devices

271
High Risk Devices

30
Threat Activities

50
Unhandled Alerts

Incident Response CAH2 | 7 Dashlets

Managed Computers Without EDR But Containing Alerts

| Alerts | Names | Model | IPv4 Address |
|---|---|---|---|
| ⚠ 4 | b6epc.corporate.acme.co... | MacBook Pro 16-Inch Cor... | 10.65.77.105 |

Threat Intel Hit - Medical

| Title | Content | Type |
|---|---|---|
| agfa healthcare impax 6.0 communicated with a suspicious host88.80.147.10: | Confidence: Medi... | Suspicious Host |

## 2 | Click on the device with the name "b6epc.corporate.acme.com"

There is one device here that requires further investigation. We can easily pivot into a page with further information on this device by simply clicking on the device name. All dashlets are interactive and data can be displayed in many different custom ways.

Note: This device belongs to a third-party vendor who must access the network to do maintenance and patching on medical devices. This explains why this device is not running the required EDR.

### 3 | Select the “Activities” tab within the device profile

Through passive network traffic inspection, Armis is able to report on activities associated with each device. For example, this device is reporting communication from a suspicious host (185.81.68.180), multiple port scans to various IP addresses, as well as failed ModBus ‘Read Multiple Registers’ requests to a HVAC device within the environment.

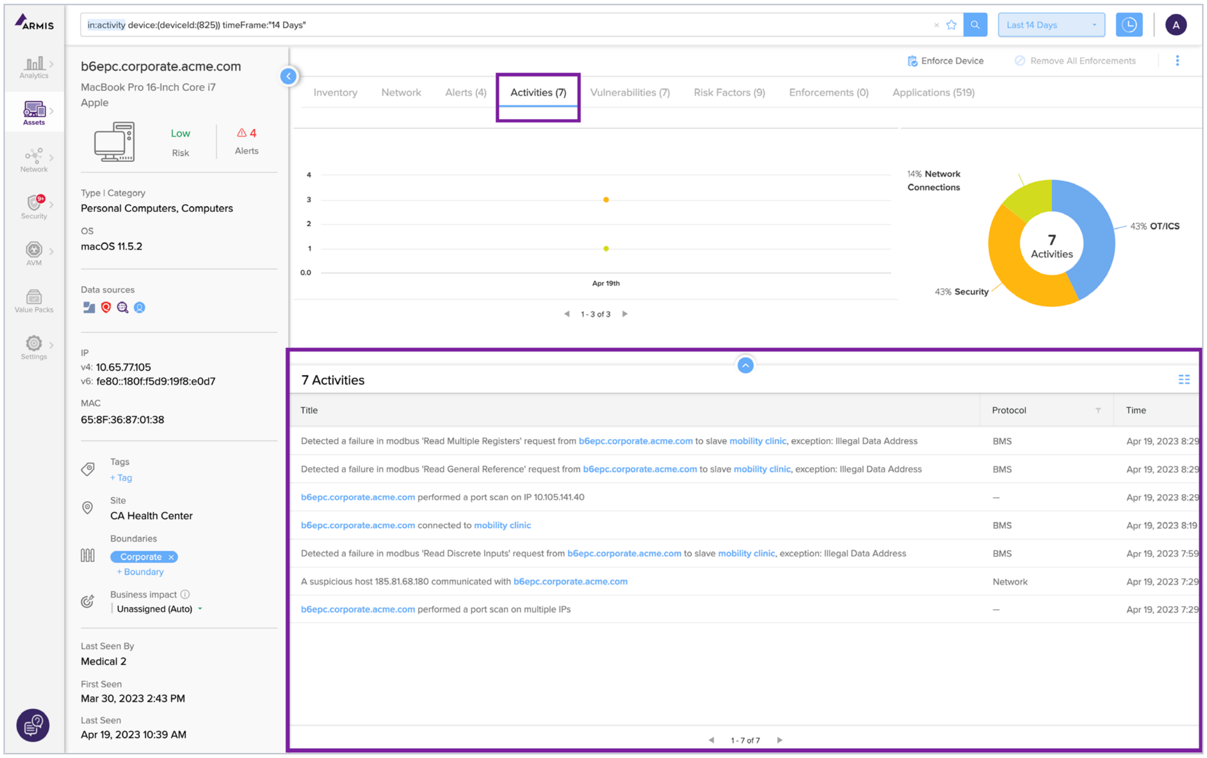
Initially, the threat actor tries to run some ModBus commands but gets error messages. However, the threat actor then makes an attempt with the BACnet protocol and successfully connects to the HVAC system.

Note: All things considered, BACnet is a far more robust protocol than ModBus.

Modbus has become the standard communication protocol for OT. An attacker can use ModBus to send commands, which can be extremely dangerous. However, they would need to first have some understanding of the register mapping to effectively leverage ModBus for malicious activities.

On the other hand, BacNet is very commonly used in Building Management Systems and is designed for interoperability and data sharing across different device types and vendors. An attacker leveraging BacNet is able to do many kinds of Create, Read, Update, Delete (CRUD) operations on supported devices. An attacker could leverage this ability to upload new firmware and configuration options to take full control of a vulnerable BACnet device.

In this case, the attacker is able to leverage BACnet to take control of the HVAC device to move laterally through the environment.



in:activity device:(deviceId:(825)) timeFrame:"14 Days"

b6epc.corporate.acme.com
MacBook Pro 16-Inch Core i7
Apple

Low Risk | 4 Alerts

Type | Category
Personal Computers, Computers

OS
macOS 11.5.2

Data sources

IP
v4: 10.65.77.105
v6: fe80::180f:f5d9:19f8:e0d7

MAC
65:8F:36:87:01:38

Tags
+ Tag

Site
CA Health Center

Boundaries
Corporate ×
+ Boundary

Business impact
Unassigned (Auto)

Last Seen By
Medical 2

First Seen
Mar 30, 2023 2:43 PM

Last Seen
Apr 19, 2023 10:39 AM

7 Activities

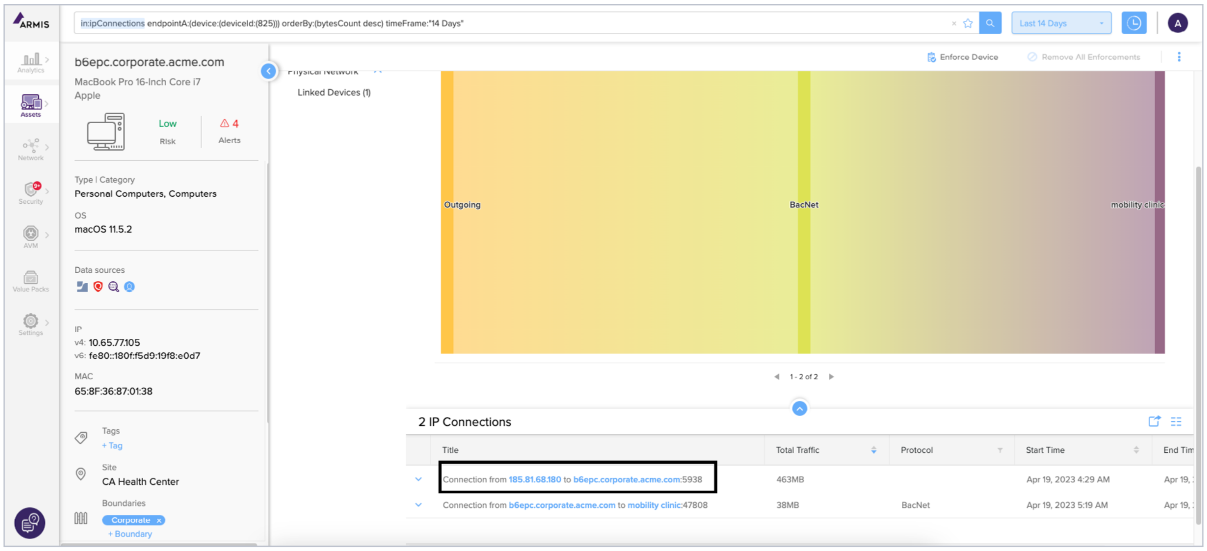
| Title | Protocol | Time |
|---|---|---|
| Detected a failure in modbus 'Read Multiple Registers' request from b6epc.corporate.acme.com to slave mobility clinic, exception: Illegal Data Address | BMS | Apr 19, 2023 8:29 |
| Detected a failure in modbus 'Read General Reference' request from b6epc.corporate.acme.com to slave mobility clinic, exception: Illegal Data Address | BMS | Apr 19, 2023 8:29 |
| b6epc.corporate.acme.com performed a port scan on IP 10.105.141.40 | — | Apr 19, 2023 8:29 |
| b6epc.corporate.acme.com connected to mobility clinic | BMS | Apr 19, 2023 8:19 |
| Detected a failure in modbus 'Read Discrete Inputs' request from b6epc.corporate.acme.com to slave mobility clinic, exception: Illegal Data Address | BMS | Apr 19, 2023 7:59 |
| A suspicious host 185.81.68.180 communicated with b6epc.corporate.acme.com | Network | Apr 19, 2023 7:29 |
| b6epc.corporate.acme.com performed a port scan on multiple IPs | — | Apr 19, 2023 7:29 |

## 4 | Now look at the “Network” tab within the devices

Similar to Activities, Armis can leverage passive network traffic inspection to summarize network sessions by IP Connections, Traffic, and Services. In this case, IP Connections will show us the services being used.

This is where we can clearly see the BacNet connection established.

In this case, when we look at the IP connections, we can see a connection via port 5938. This port is used by the popular but commonly abused remote management tool, TeamViewer.



in:ipConnections endpointA:(device:(deviceId:(825))) orderBy:(bytesCount desc) timeFrame:"14 Days"

b6epc.corporate.acme.com
MacBook Pro 16-Inch Core i7
Apple

Low
Risk

⚠ 4
Alerts

Type | Category
Personal Computers, Computers

OS
macOS 11.5.2

Data sources

IP
v4: 10.65.77.105
v6: fe80::180f:f5d9:19f8:e0d7

MAC
65:8F:36:87:01:38

Tags
+ Tag

Site
CA Health Center

Boundaries
Corporate ×
+ Boundary

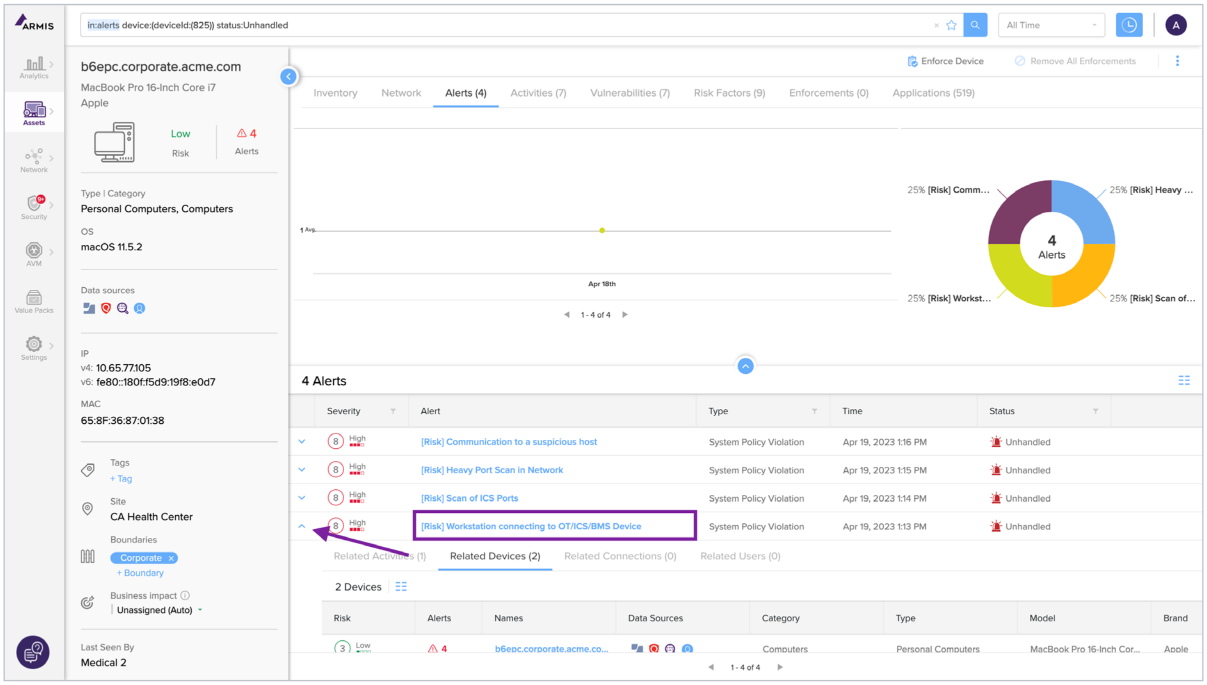
2 IP Connections

| Title | Total Traffic | Protocol | Start Time | End Tim |
|---|---|---|---|---|
| Connection from 185.81.68.180 to b6epc.corporate.acme.com:5938 | 463MB | | Apr 19, 2023 4:29 AM | Apr 19, |
| Connection from b6epc.corporate.acme.com to mobility clinic:47808 | 38MB | BacNet | Apr 19, 2023 5:19 AM | Apr 19, |

## 5 | Now take a look at the “Alerts” tab within the devices

Under Alerts we can see how these different activities and connections are surfaced by Armis into actionable alerts. Alert policies in Armis can be customized and tailored to an organization's requirements and are also able to be forwarded to an existing SIEM.

If you have any questions about Armis alerts and policies, the Armis Engineers present during this session will be happy to dive deeper with you individually.



in:alerts device:(deviceId:(825)) status:Unhandled

b6epc.corporate.acme.com
MacBook Pro 16-Inch Core i7
Apple

Low Risk
4 Alerts

Type | Category
Personal Computers, Computers

OS
macOS 11.5.2

Data sources

IP
v4: 10.65.77.105
v6: fe80::180f:f5d9:19f8:e0d7

MAC
65:8F:36:87:01:38

Tags
+ Tag

Site
CA Health Center

Boundaries
Corporate ×
+ Boundary

Business impact
Unassigned (Auto)

Last Seen By
Medical 2

4 Alerts

| Severity | Alert | Type | Time | Status |
|---|---|---|---|---|
| 8 High | [Risk] Communication to a suspicious host | System Policy Violation | Apr 19, 2023 1:16 PM | Unhandled |
| 8 High | [Risk] Heavy Port Scan in Network | System Policy Violation | Apr 19, 2023 1:15 PM | Unhandled |
| 8 High | [Risk] Scan of ICS Ports | System Policy Violation | Apr 19, 2023 1:14 PM | Unhandled |
| 8 High | [Risk] Workstation connecting to OT/ICS/BMS Device | System Policy Violation | Apr 19, 2023 1:13 PM | Unhandled |

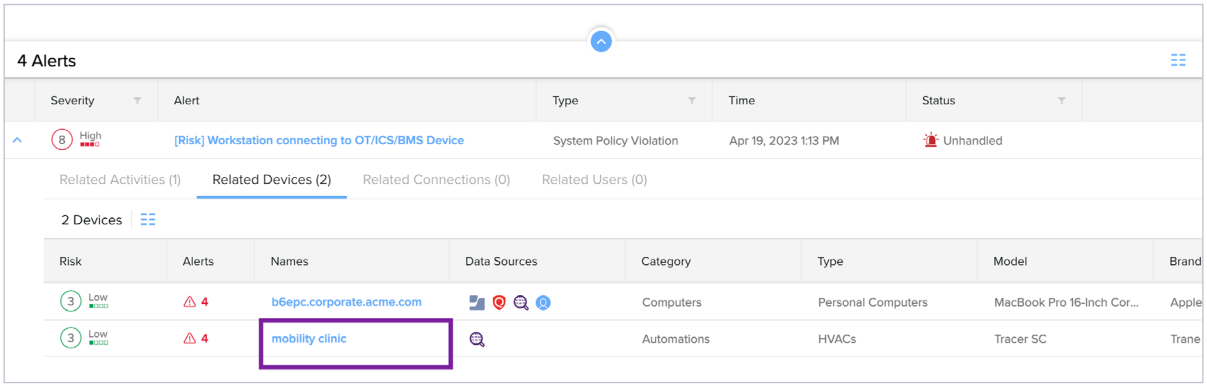
2 Devices

| Risk | Alerts | Names | Data Sources | Category | Type | Model | Brand |
|---|---|---|---|---|---|---|---|
| 3 Low | 4 | b6epc.corporate.acme.co... | | Computers | Personal Computers | MacBook Pro 16-Inch Cor... | Apple |

1 - 4 of 4

## 6 | Select “Related Devices” on the Alert for “Workstation connecting to OT/ICS/BMS Device”

This vendor device has been seen talking to an HVAC system, which is not normal for this organization. If we click the drop-down arrow to the left of this alert we can see some further high-level details to assist in our understanding of the spread and impact of this incident. Each alert has its own alert page. However, we will save that for another day - for now, we can use the drop-down to navigate to “**Related Devices**”.



4 Alerts

| Severity | Alert | Type | Time | Status |
|---|---|---|---|---|
| 8 High | [Risk] Workstation connecting to OT/ICS/BMS Device | System Policy Violation | Apr 19, 2023 1:13 PM | Unhandled |

Related Activities (1) | Related Devices (2) | Related Connections (0) | Related Users (0)

2 Devices

| Risk | Alerts | Names | Data Sources | Category | Type | Model | Brand |
|---|---|---|---|---|---|---|---|
| 3 Low | ⚠ 4 | b6epc.corporate.acme.com | | Computers | Personal Computers | MacBook Pro 16-Inch Cor... | Apple |
| 3 Low | ⚠ 4 | mobility clinic | | Automations | HVACs | Tracer SC | Trane |

## 7 | Explore the device named “Mobility Clinic”

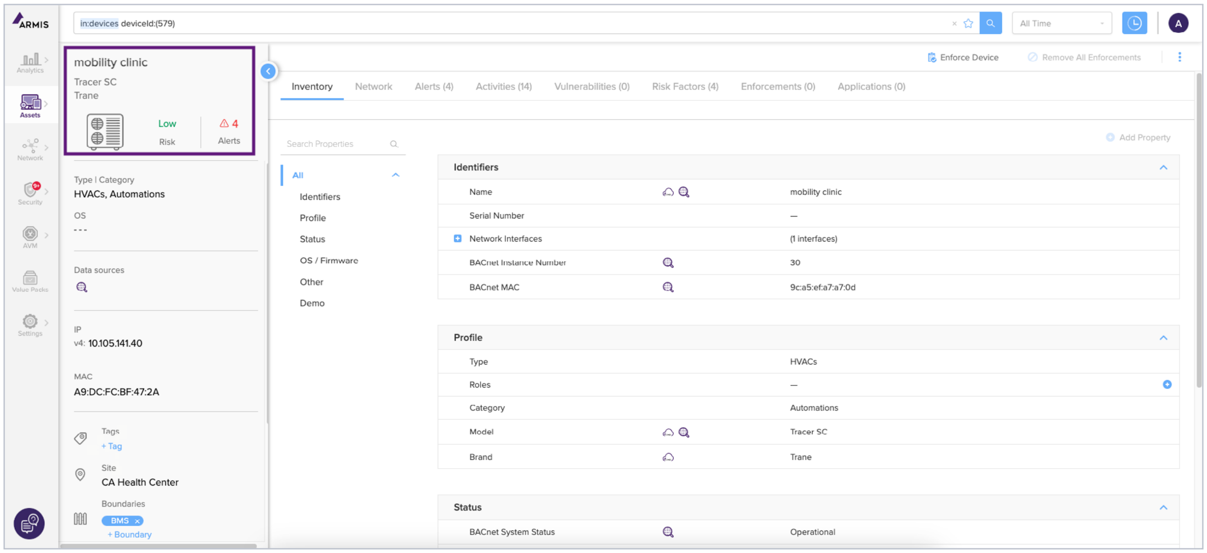
The related device that this third-party vendor’s laptop is talking to is an HVAC system named **Mobility Clinic**. If we click on this device we can now see detailed information on the HVAC.

Take a few moments to look through the relevant tabs on this device.

Note: This is an HVAC (Heating, Ventilation, and Air Conditioning) device. Such devices exist in almost every organization. HVAC systems can present a cybersecurity threat because they are often connected to a building's network and can be used as entry and/or pivot points for attackers to gain access and move laterally through the network. Furthermore, an attacker taking down an HVAC system can pose significant impacts on hospitals and other environments.

HVAC systems are often vulnerable due to being outdated and lack proper security measures. Many HVAC systems run on outdated software, and their control systems are often not designed with security in mind. This makes them an easy target for attackers who can exploit the system to gain control or access to the environment.

Furthermore, HVAC systems are not typically monitored as closely as other critical infrastructure This means that an attack on an HVAC system may go unnoticed for an extended period, giving the attacker time to cause significant damage or steal valuable information.



in:devices deviceId:(579)

mobility clinic
Tracer SC
Trane

Low
Risk

4
Alerts

Type | Category
HVACs, Automations

OS
- - -

Data sources

IP
v4: 10.105.141.40

MAC
A9:DC:FC:BF:47:2A

Tags
+ Tag

Site
CA Health Center

Boundaries
BMS ×
+ Boundary

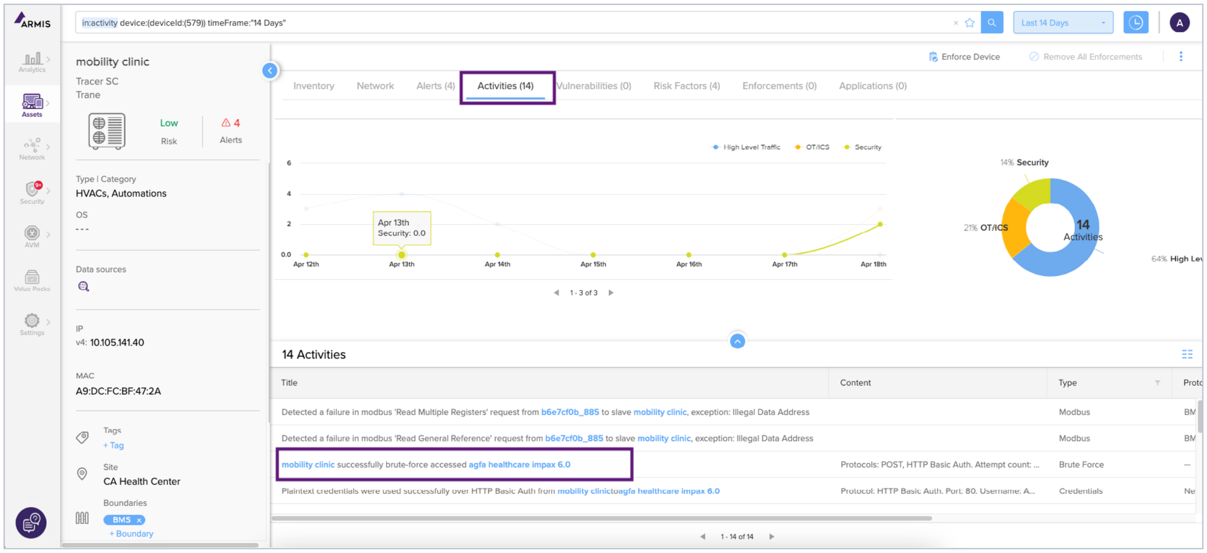
| Identifiers | |
|---|---|
| Name | mobility clinic |
| Serial Number | — |
| Network Interfaces | (1 interfaces) |
| BACnet Instance Number | 30 |
| BACnet MAC | 9c:a5:ef:a7:a7:0d |

| Profile | |
|---|---|
| Type | HVACs |
| Roles | — |
| Category | Automations |
| Model | Tracer SC |
| Brand | Trane |

| Status | |
|---|---|
| BACnet System Status | Operational |

## 8 | Click on the “Activities” Tab to find the Brute Force activity

In ‘Activities’ we can see the attacker has been able to successfully brute force their way onto another device. The ‘Activities’ view provides detailed information on this brute force attack.



in:activity device:(deviceId:(579)) timeFrame:"14 Days"

mobility clinic
Tracer SC
Trane

Low
Risk

4
Alerts

Type | Category
HVACs, Automations

OS
- - -

Data sources

IP
v4: 10.105.141.40

MAC
A9:DC:FC:BF:47:2A

Tags
+ Tag

Site
CA Health Center

Boundaries
BMS
+ Boundary

14 Activities

| Title | Content | Type | Proto |
|---|---|---|---|
| Detected a failure in modbus 'Read Multiple Registers' request from b6e7cf0b_885 to slave mobility clinic, exception: Illegal Data Address | | Modbus | BM |
| Detected a failure in modbus 'Read General Reference' request from b6e7cf0b_885 to slave mobility clinic, exception: Illegal Data Address | | Modbus | BM |
| mobility clinic successfully brute-force accessed agfa healthcare impax 6.0 | Protocols: POST, HTTP Basic Auth. Attempt count: ... | Brute Force | – |
| Plaintext credentials were used successfully over HTTP Basic Auth from mobility clinictoagfa healthcare impax 6.0 | Protocol: HTTP Basic Auth. Port: 80. Username: A... | Credentials | Ne |

1 - 14 of 14

## 9 | Click on the device named “agfa healthcare impax 6.0”

Our investigation has now uncovered that the attacker has been able to move from this HVAC system to a PACS server. From here we can pivot into the affected device named: **agfa healthcare impax 6.0** by simply clicking on the device’s name.

Note: PACS (Picture Archiving and Communication System) server is a computer system that is used to store, retrieve, and share medical images and related patient data in healthcare settings. PACS servers are hard to defend with traditional cybersecurity tools for several reasons:

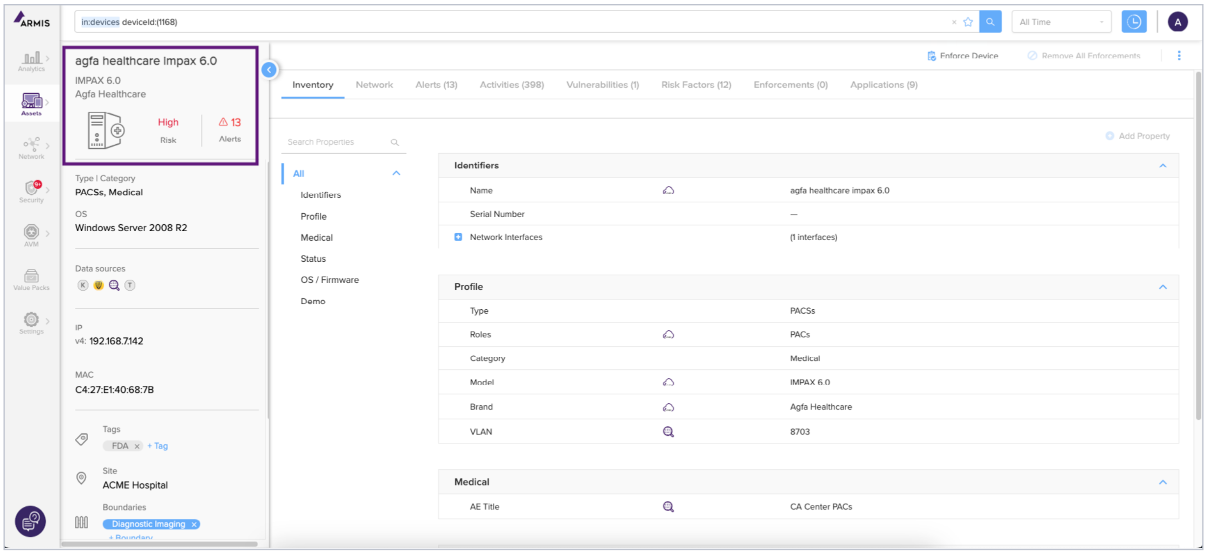
Legacy systems: Many PACS servers are running on legacy systems that may not be compatible with newer security technologies. This makes it difficult to apply modern security measures and tools to protect against cybersecurity threats.

Complexity: PACS servers are complex systems that may have multiple entry points, including web-based interfaces, network connections, and storage devices. This complexity makes it challenging to identify and defend against all potential attack vectors.

Lack of resources: Many healthcare organizations have limited resources to devote to cybersecurity. PACS servers may not receive the same level of attention and investment as other critical systems, leaving them vulnerable to attacks.

Interoperability: PACS servers need to be interoperable with other healthcare systems, such as electronic health records (EHRs) and medical devices. This interoperability can make it difficult to apply security measures that might interfere with the functionality of these systems.

Patient safety concerns: PACS servers hold critical patient data and medical images, and any disruption to these systems can have serious consequences for patient care. This makes it challenging to implement security measures that could potentially impact the availability of these systems.



in:devices deviceId:(1168)

agfa healthcare impax 6.0
IMPAX 6.0
Agfa Healthcare

High
Risk

⚠ 13
Alerts

Type | Category
PACSs, Medical

OS
Windows Server 2008 R2

Data sources
K T

IP
v4: 192.168.7.142

MAC
C4:27:E1:40:68:7B

Tags
FDA × + Tag

Site
ACME Hospital

Boundaries
Diagnostic Imaging ×
+ Boundary

| Identifiers | |
|---|---|
| Name | agfa healthcare impax 6.0 |
| Serial Number | — |
| Network Interfaces | (1 interfaces) |

| Profile | |
|---|---|
| Type | PACSs |
| Roles | PACs |
| Category | Medical |
| Model | IMPAX 6.0 |
| Brand | Agfa Healthcare |
| VLAN | 8703 |

| Medical | |
|---|---|
| AE Title | CA Center PACs |

## 10 | Let's explore this PACS Server and answer the following Scavenger Hunt questions

We will have you quickly assemble some key information about this final device in the following scavenger hunt:

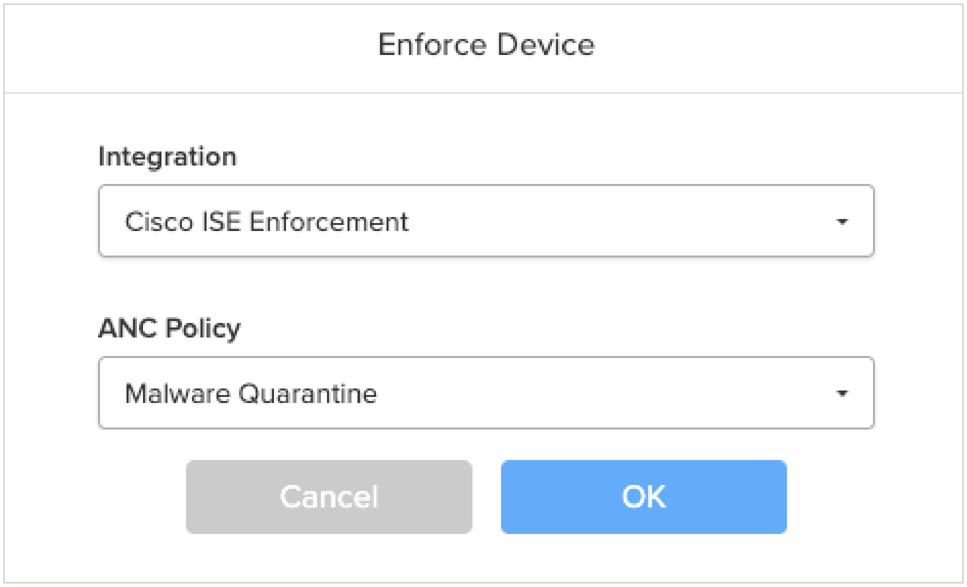
A. What OS does this PACS Server run?
B. How much data was exfiltrated via FTP?
C. What user account was leveraged for this attack?
D. How many total devices are linked to this user?
E. Does the vulnerability associated with this device have any weaponized exploits? (hint: the answer is inside the CVE's record)

## 11 | Use the back button to go back to the PACS server and quarantine the affected host

We can leverage our integration with third-party tools like Firewalls and Network Access Control tools to change the level of access an affected device has on the network or remove it completely.

Armis can also leverage automation to proactively protect the environment via policy-based actions. A task for later could be to create a policy that would automatically quarantine the original laptop before it was able to spread, thus preventing the incident at the first step of the attack chain.

Note: Do **NOT** click on Ok. This could cause an error for other users in the class.



Enforce Device

Integration: Cisco ISE Enforcement

ANC Policy: Malware Quarantine

# Scavenger Hunt Answer Key:

**A.** Windows Server 2008 R2

**B.** 232GB

**C.** William Pearson – Found in “Activities” tab

**D.** 15 devices – Found by clicking “Assets” tab > “Users” > “William Pierson” > “Devices” tab

**E.** Yes –Found by clicking on the CVE under the “Vulnerabilities” tab > “Threat Data” tab under the CVE profile

## Conclusion and Next Steps

Thank you for taking part in the Catch a Hacker exercise. Both the story and the underlying data used in this exercise are based upon real-life incidents with sophisticated Advanced Persistent Threat (APTs) Actors. These threat actors will move laterally across the network and exploit common visibility gaps to reach their target objectives.

Please feel free to keep this guide as this environment will stay online for the next several days. You will soon receive a Credly badge for completing this exercise that will attest to your two hours of Continuing Education credits.

Armis Engineers are present throughout the room, so if you have any questions about how your organization could leverage any of the capabilities you saw today (and more), we are happy to continue the conversation.