



**Huntress** <support@huntress.io>  
to me ▾

12:44 PM (3 hours ago)



# Welcome to Huntress!

You have been invited to join Huntress by Topher Lyons

**Accept**

Cheers,  
The Huntress Team

Huntress Labs  
6021 University Blvd. • Suite 450 • Ellicott City, MD 21043



WELCOME, PLEASE SETUP YOUR ACCOUNT

☐ I accept the [terms of service](#) and [privacy policy](#)

Accept Invitation





WELCOME, PLEASE LOGIN



Enter your e-mail



Enter your password

Login Now

OR

Login with SSO

[Forgot your password?](#)

[Terms](#) | [Privacy](#)

Don't have an account? [Sign up](#)



Help

**Two-Factor Setup**Authenticate ☒What is 2FA? ☐Save Backup Codes ☐Setup TOTP ☐Done ☐

## Setting up Two-Factor Authentication (2FA)

### What is Two-Factor Authentication?

Two-Factor Authentication adds a second component to the normal password authentication process. This means that in addition to entering your email address and password, you will be prompted to provide another piece of secret information to verify your identity. Usually this secret is automatically generated by your phone or a third-party application. This means that even if an attacker is able to steal or guess your password, they still won't be able to login to your account because they don't have your phone or access to your additional secret.

### Why do I have to setup Two-Factor Authentication?

As Huntress continues to add more functionality we're moving towards becoming an all-encompassing security platform, we want to ensure that the service you trust to manage and maintain your IT security is as secure as possible. Enforcing Two-Factor Authentication is another step to improve the overall security of the Huntress Platform.

[Next](#)[Help](#)

## Two-Factor Setup

Authenticate ☒What is 2FA? ☒Save Backup Codes ☐Setup TOTP ☐Done ☐

## Save Backup Codes

Backup codes can be used to access your account in the event you lose access to your device or cannot generate two-factor authentication codes.

 Warning

**Put these in a safe spot.** If you lose your device and don't have the recovery codes you will lose access to your account.

15250915

80755997

32034915

95758835

76279662

78667835

10448735

47644739

85742231

78774333

32949775

10241668

91542604

28730775

60528031

 Download Print Copy

Back

Next

**Two-Factor Setup**Authenticate ☒What is 2FA? ☒Save Backup Codes ☐Setup TOTP ☐Done ☐**Save Backup Codes** ×

This is the last time that you will see these backup codes. Please confirm you have recorded these backup codes. If you lose these backup codes, you or an administrator will need to generate replacement backup codes.

Cancel

☒ Yes, I've saved these backup codes

Save

Backup  
gener

Put

access to your account.

e or cannot

will lose

15250915

95758835

10448735

78774333

91542604

80755997

76279662

47644739

32949775

28730775

32034915

78667835

85742231

10241668

60528031

Download

Print

Copy

Back

Next

**Two-Factor Setup**Authenticate ☒What is 2FA? ☒Save Backup Codes ☒Setup TOTP ☐Done ☐

## Setup Time-based One Time Passcodes (TOTP)

These codes can be generated by many different smart phone apps (Google Authenticator, Microsoft Authenticator, Authy, Duo, etc.) or desktop applications. The code changes every 30 seconds to ensure that attackers can't guess them. To complete the setup you'll need to use your application to scan the QR code or enter the secret key. Finally, enter the 6 digit code in the provided box to confirm the setup.

**1. Download Google Authenticator from your app store:****2. Scan this barcode with your app:**

Scan the image below with the two-factor authentication app on your phone.



Secret Key **EH7R L7NA XCMV 2FJT FG6Y FN9K KEF6 Y5M6**

**3. Enter the six-digit code from the application:**

After scanning the barcode image, the app will display a six-digit code that you can enter below.



## Two-Factor Setup

Authenticate ☒

What is 2FA? ☒

Save Backup  
Codes ☒

Setup TOTP ☒

Done



# Your Two-Factor Authentication is setup!

Congratulations on setting up two-factor authentication for your account. In the future every time you login, you will be prompted to authenticate with a two-factor method to ensure the security of your account.

You may modify these two-factor methods or setup additional two-factor methods from the User preferences view that can be accessed from the menu in the top right corner of the dashboard.

Back

Done



Your Managed EDR trial will end on **2023-02-24**. You have received **3 of 3** High/Critical incident reports during your trial.



There is 1 host currently isolated from its network. See [here](#)



**4**  
Active Incidents

 **1** Critical

 **2** High

 **1** Low

**0**  
Resolved

**0** Month

**0** Quarter

Year

**3**  
Investigations

**3** Month

**3** Quarter

**3** Year




#### Agent Status



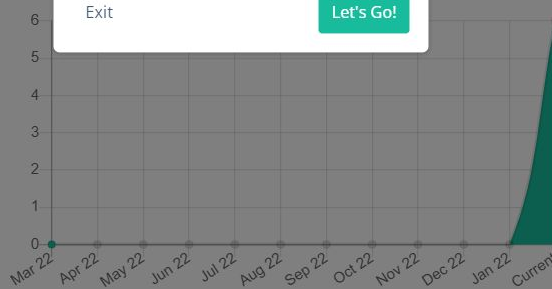
 Total Agents **6**

 Unresponsive **0**

 Outdated **0**

 Isolated **1**

#### System



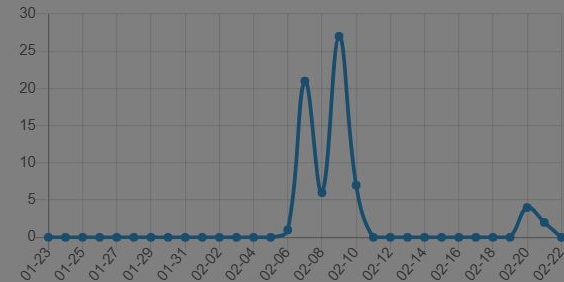
Welcome To Huntress!

Let's take a moment to show you around the dashboard.

Exit

Let's Go!

#### Surveys Per Day (68 Total)



Dashboard

The dashboard presents a high-level overview of the current state of your Huntress account.

ExitPrevNext

Your Managed EDR trial will end on **2023-02-24**. You have received **3 of 3** High

There is 1 host currently isolated from its network. See [here](#)

4

Active Incidents

 1 Critical

 2 High

 1 Low

0

Resolved Incidents

0Month

0Quarter

0Year

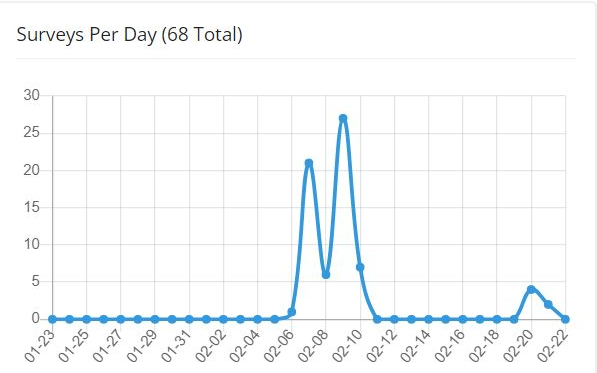
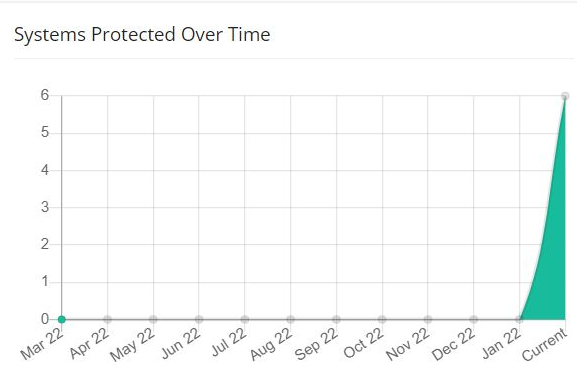
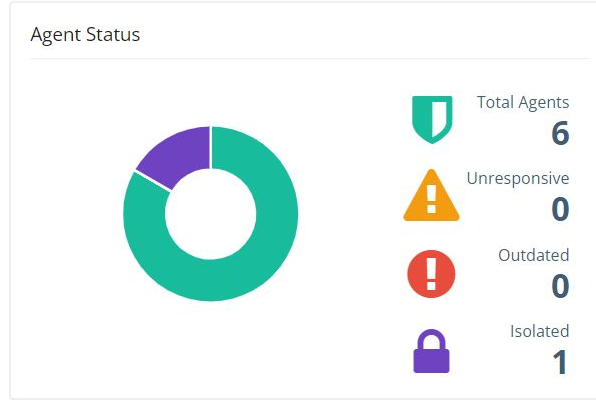
3

Investigations

3Month

3Quarter

3Year



### Organization Menu

You can use this dropdown to switch between **organizations** or return to the account dashboard.

Exit

Prev

Next

4  
Active Incidents

1 Critical

2 High

1 Low

0  
Resolved Incidents

0 Month

0 Quarter

0 Year

3  
Investigations

3 Month

3 Quarter

3 Year

### Agent Status



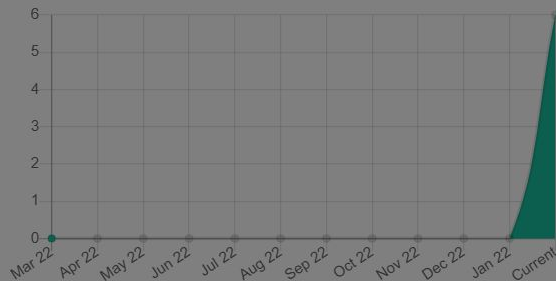
 Total Agents **6**

 Unresponsive **0**

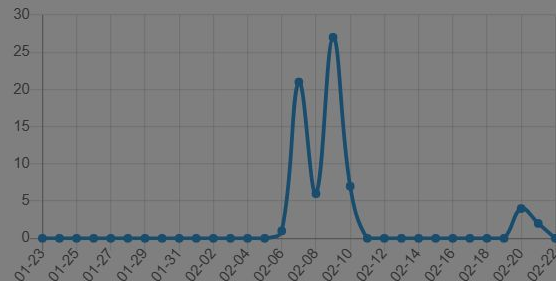
 Outdated **0**

 Isolated **1**

### Systems Protected Over Time



### Surveys Per Day (68 Total)





## ACCOUNT DASHBOARDS

✓ Right of Boom - Huntr...

## ORGANIZATION DASHBOARDS

Olympus

Valhalla

## Organization Menu

This list shows the organizations for your account. Selecting an organization will take you to that organization's dashboard.

Exit

Prev

Next

and on 2023-02-24. You have received 3 of 3 High/Critical incident reports during your trial.

ed from its network. See [here](#) 1 Critical 2 High 1 Low0  
Resolved  
Incidents

0 Month

0 Quarter

0 Year



3  
Investigations

3 Month

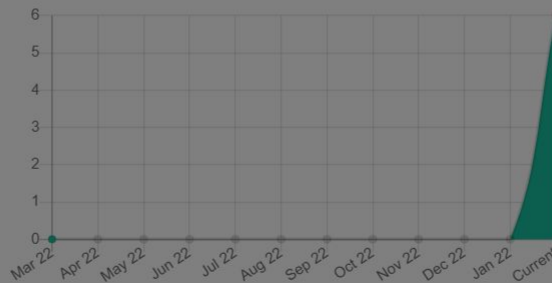
3 Quarter

3 Year

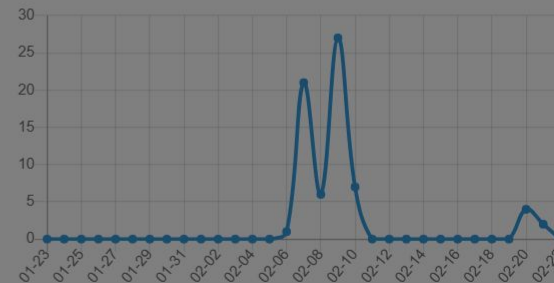
## Agent Status

 Total Agents  
6 Unresponsive  
0 Outdated  
0 Isolated  
1

## Systems Protected Over Time



## Surveys Per Day (68 Total)



Dashboard

Click here to jump back to the dashboard from any page.

ExitPrevNext



02-24. You have received 3 of 3 High/Critical incident reports during your trial.

is network. See [here](#)

4

Active Incidents

 1 Critical

 2 High

 1 Low

0

Resolved Incidents

0 Month

0 Quarter

0 Year

3


Investigations


3 Month


3 Quarter


3 Year


Agent Status



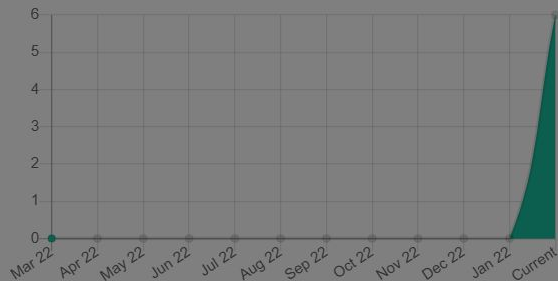
 Total Agents6

 Unresponsive0

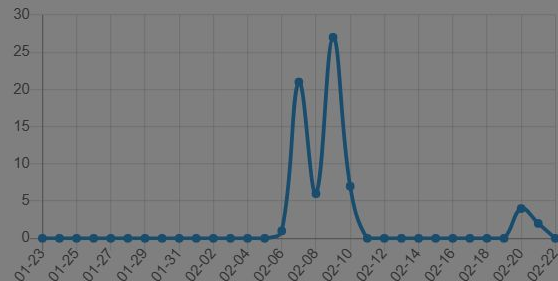
 Outdated0

 Isolated1

Systems Protected Over Time



Surveys Per Day (68 Total)





Your Managed EDR trial will end on **2023-02-24**. You have received **3 of 3** High/Critical incident reports during your trial.



There is 1 host currently isolated from its network. See [here](#)



**4**  
Active Incidents

 **1 Critical**

 **2 High**

 **1 Low**

**0**  
Resolved Incidents

**0** Month

**0** Quarter


**0** Year

**3**  
Investigations




#### Agent Status



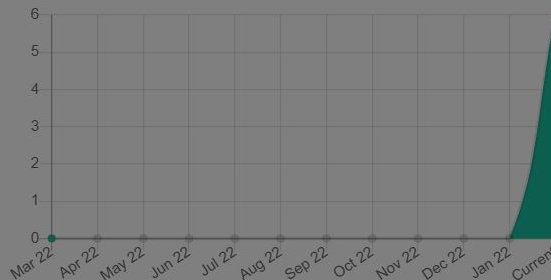
 Total Agents **6**

 Unresponsive **0**

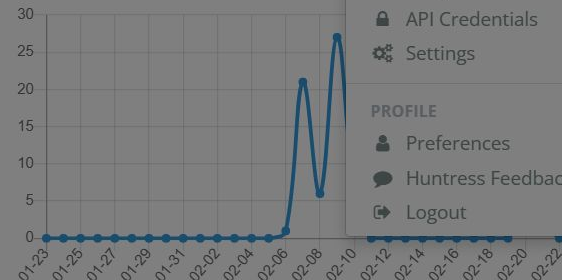
 Outdated **0**

 Isolated **1**

#### Systems Protected Over Time



#### Surveys Per Day (68 Total)




#### Download Agent

To get started download the agent and review the **installation instructions**.

Exit

Prev

Next


 Support & FAQ

 Take The Tour


 Download Agent

#### ACCOUNT

 Dashboard


 Organizations


 Agents

 Escalations


 Incidents


 Investigations


 Reports

 Partner Enablement

 Users

 Integrations


 API Credentials

 Settings

#### PROFILE

 Preferences

 Huntress Feedback

 Logout

Your Managed EDR trial will end on **2023-02-24**. You have received **3** of **3** High/Critical incident reports during your trial.

## Persistent Footholds

1  
Active Incidents

 0 Critical

 0 High

 1 Low

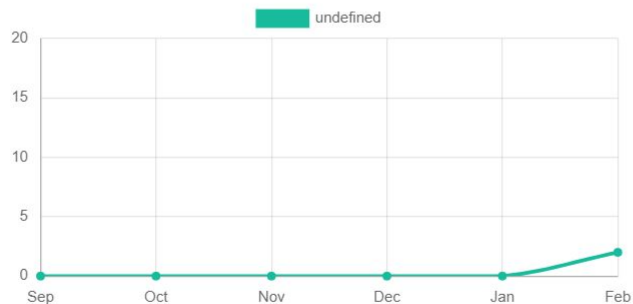
0  
Resolved Incidents

0 Month

0 Quarter

0 Year

Reviewed Autoruns



Reported Footholds



Your Managed EDR trial will end on **2023-02-24**. You have received **3** of **3** High/Critical incident reports during your trial.

## Process Insights

1  
Active Incidents

0 Critical

1 High

0 Low

0  
Resolved Incidents

0 Month

0 Quarter

0 Year

### Process Insights Agent Status

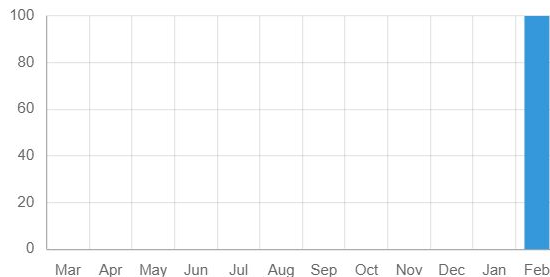


Active  
6

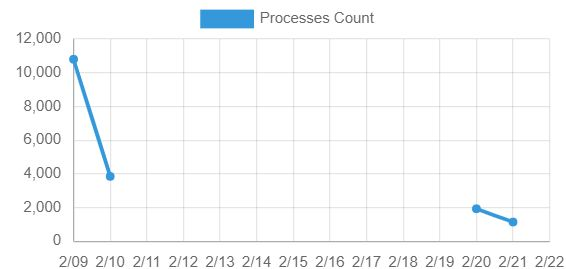


Excluded  
0

### Detections Over Time



### Monitored Processes Over Time



Show 25 entries

Search:

Detected At	Org	Host	Rule	Process	Command Line	Incident(s)
-------------	-----	------	------	---------	--------------	-------------



02-10 17:41:20 UTC

Olympus

Poseidon

Registry Dump of SAM Creds and Secrets

C:\Windows\system32\reg.exe

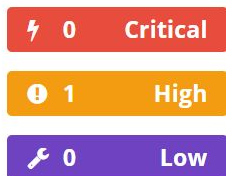
reg save  
HKEY\_LOCAL\_MACHINE\system\curr

931294

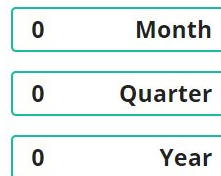
Your Managed EDR trial will end on **2023-02-24**. You have received **3 of 3** High/Critical incident reports during your trial.

## Managed Antivirus

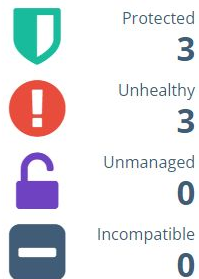
1  
Active Incidents



0  
Resolved Incidents

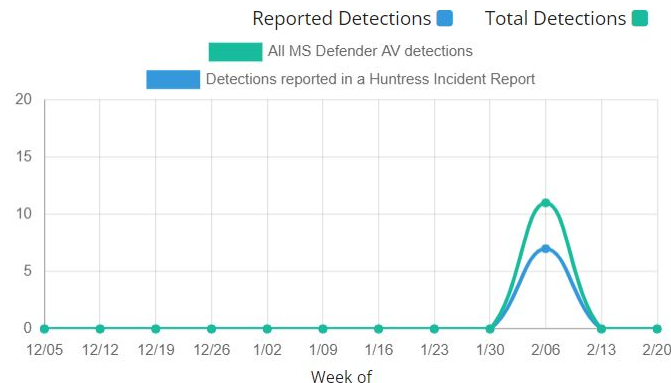


### Microsoft Defender Health



### Defender Detections by Week

[View all Detections](#)



Your Managed EDR trial will end on **2023-02-24**. You have received **3 of 3** High/Critical incident reports during your trial.

## Ransomware Canaries

1

Active Incidents

 1

Critical

 0

High

 0

Low

0

Resolved Incidents

0

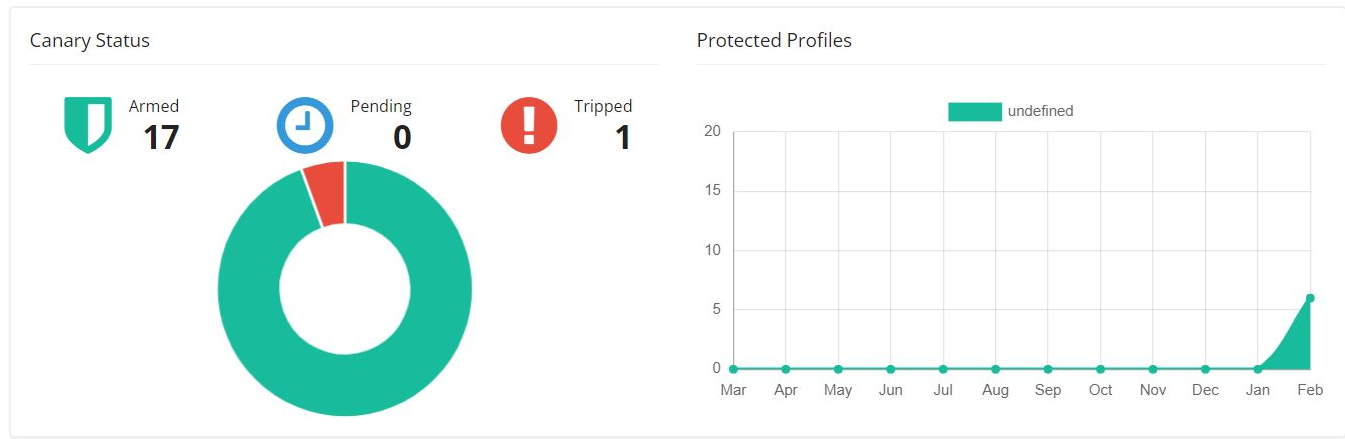
Month

0

Quarter

0

Year



### Ransomware Canary Files

Your Managed EDR trial will end on **2023-02-24**. You have received **3 of 3** High/Critical incident reports during your trial.

## Ransomware Canaries

1

Active Incidents

 1

Critical

 0

High

 0

Low

0

Resolved Incidents

0

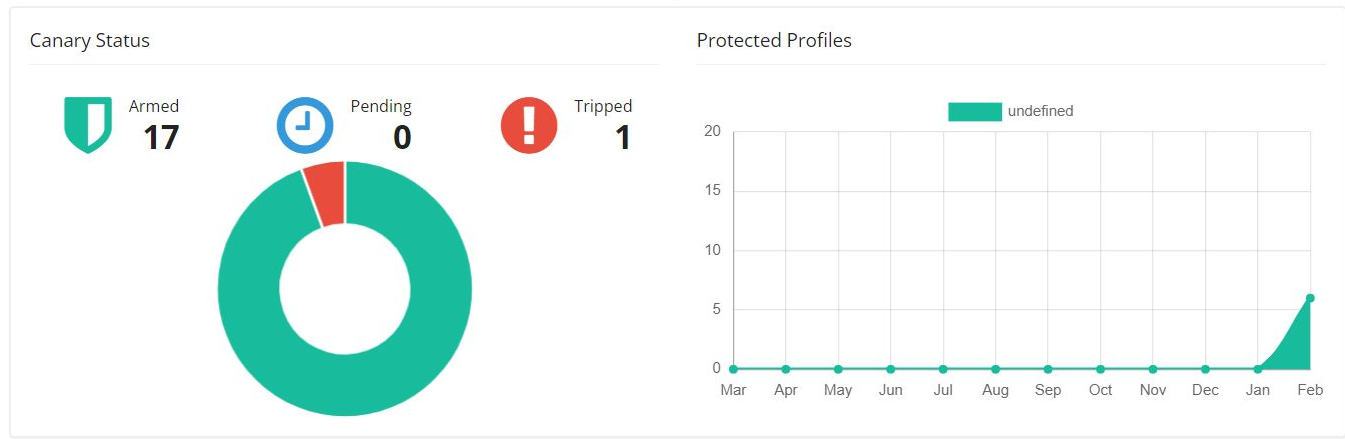
Month

0

Quarter

0

Year



### Ransomware Canary Files





























Your Managed EDR trial will end on **2023-02-24**. You have received **3 of 3** High/Critical incident reports during your trial.

- 
- 
- 
- 
- 
- 
- 
- 
- 

ACCOUNT

- Dashboard
- Organizations
- Escalations
- Agents
- Incidents
- Investigations
- Reports
- Marketing Assets
- Users
- Integrations
- API Credentials
- Settings

Reported Incidents (4)

Service	Severity	State	Sent	Resolved	Organization	Platform	Agent	Subject	Remediations
   	 High	 Active	2023-02-10 17:49	N/A	<a href="#">Olympus</a>		<a href="#">Poseidon</a>	<a href="#">HIGH - Incident on Poseidon (Olympus)</a>	<input type="checkbox"/>
   	 High	 Active	2023-02-09 20:30	N/A	<a href="#">Olympus</a>		<a href="#">Hera</a>	<a href="#">HIGH - Incident on Hera (Olympus)</a>	<input type="checkbox"/>
   	 Critical	 Active	2023-02-08 19:31	N/A	<a href="#">Olympus</a>		<a href="#">Hades</a>	<a href="#">CRITICAL - ISOLATED - Incident on Hades (Olympus)</a>	<input type="checkbox"/>
   	 Low	 Active	2023-02-07 23:23	N/A	<a href="#">Olympus</a>		<a href="#">Zeus</a>	<a href="#">LOW - Incident on Zeus (Olympus)</a>	<input type="checkbox"/>



## ACCOUNT

Dashboard

Organizations

Escalations

Agents

Incidents

Investigations

Reports

Marketing Assets

Users

Integrations

API Credentials

Settings



## ! Incident Report: HIGH - Incident on Hera (Olympus)

**Severity:** High**Status:** Active**Host:** Hera**Organization:** Olympus[Review Remediation Plan](#)[Resolve](#)

Report

Remaining Footholds 0Remediations 11Antivirus Detections 7Process Detections 0

### [WARNING]

Please review this incident report to understand what was identified before remediating. There may be unknown malicious processes, files, or other changes made to the host (and potentially other hosts within the environment) that remain undetected. Restoring from a known good backup or clean OS install is the only way to ensure a complete host-level remediation. While the Assisted Remediation service is an option, it will only remove specific items documented in this report.

Microsoft Defender Antivirus detected the following:

- Meterpreter : Meterpreter is an attack payload that is often used by penetration testers. However, because of its robust feature set, including the ability to execute remote commands, it is used to maintain remote access to a host by threat actors and often used to deploy other malware including ransomware.

Incident Report: [https://rightofboomdemo.huntress.io/org/211850/infection\\_reports/931164](https://rightofboomdemo.huntress.io/org/211850/infection_reports/931164)

Host: Hera - <https://rightofboomdemo.huntress.io/org/211850/agents/5172515>

Organization: Olympus

Tags: None

Security Products: Windows Defender

Remediation Instructions

-----