Netradyne Standard Operating procedure
Crowdstrike

v1.0

Internal and Confidential

netradyne

TABLE OF CONTENTS

Document Control

Document ID	NDCS2022001
Document Name	Netradyne Standard Operating procedure Crowdstrike
Document Status	Released

Document Released Date	29-Jun-2022
Document Author	Prathamesh Padoskar
Document Content Contributors	Gautam Kumar; Hemchand Tellakula
Document Signatory	Saravanan Sankaran
Document Owner	Infosec
Document Version	v1.0
Information Classification	Internal

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised By
V1.0	29-Jun-2022	First Draft	Infosec

Document Review/Approval

Date	Signatory Name	Organization/Signatory Title	Comments
29-Jun-2022	Saravanan Sankaran	Sr. Director IT & Infosec	

Distribution of Final Document

Name	Organization/Title

1 Overview

How to monitor alerts and steps to take necessary actions against the alert/incidents.

The crowd strike solution build on extensible platform that provide customers with complete end point protection leveraging crowdstrike lightweight agent and event telemetry.

As cloud native solution deployment is easy. With no requirement of on-site hardware or consoles, the single light weight agent can be installed in seconds in physical and virtual and cloud deliver workloads with support of windows, Mac, linux and mobile devices.

By design crowdstrike solution detects and prevents malicious activities. The main dashboard highlights what threats has been blocked with immediate access to supporting details.

2 Scope

How to monitor alerts and steps to take necessary actions against the alert/incidents.

Devices are integrated with Crowdstrike solution. Based on activities / processes on devices alerts are generated as per severity Critical, High, Medium, Low, Informational. Currently Linux devices are integrated with crowdstrike. Also, emails are triggered once per day for each detection at medium severity level or incident at 1.0 and above.

You can monitor alert through email or proactively by logging on Crowdstrike console and navigating to detection dashboard.

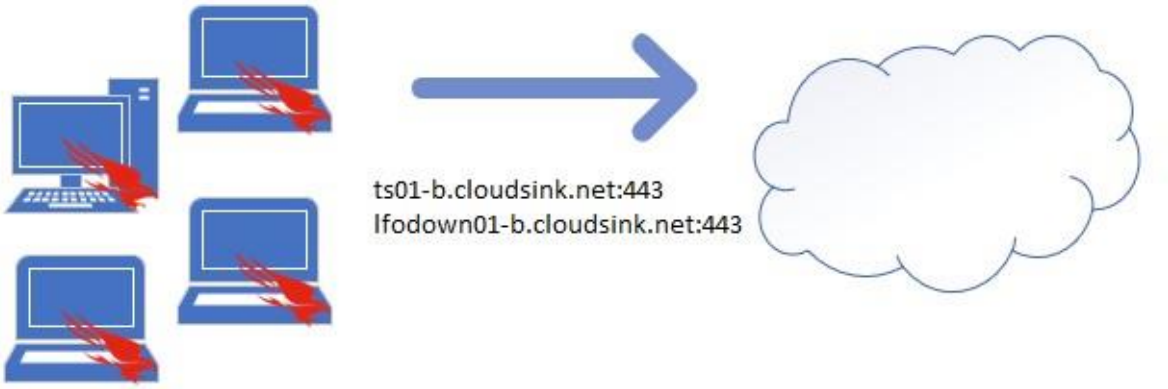
3 Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

Role	***Responsibilities***
Owner	• Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. • Is the point of contact for the document. • Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process.
Reviewers/Stakeholders	Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality)
Approvers	The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead.
Document Release	Document Owner/team to work with repository administrator to make release version available.

4 Architecture

CrowdStrike is an agent-based sensor that can be installed on Windows, Mac, or Linux operating systems for desktop or server platforms. These platforms rely on a cloud-hosted SaaS Solution, to manage policies, control reporting data, manage, and respond to threats.



CrowdStrike Falcon Sensors communicate directly to the cloud by two primary URLs:

ts01-b.cloudsink.net

lfodown01-b.cloudsink.net

These URLs are leveraged for agent updates, data sync, and threat uploads.

CrowdStrike can work offline or online to analyze files as they attempt to run on the endpoint. This is done using:

- Predefined Prevention Hashes
- Behavioral Indicator of Attacks
- Known Malware
- Exploit Mitigation

5 Pre-requisites / Assumptions

Only authorized users have credentials to access https://falcon.us-2.crowdstrike.com/login/ crowdstrike UI. Below are the listed users who have access to Netradyne crowdstrike with the level of access defined.

No.	Name	Access Level
1	Chethan Gangaraju	Admin access with 2FA
2	Thambi Durai	Admin access with 2FA
3	Blaize Mathews	Admin access with 2FA
4	Ramesh Babu	Admin access with 2FA
5	Mauricio Taxman	Admin access with 2FA
6	Gautam Kumar	Admin access with 2FA
7	Tellakula Hemchand	Admin access with 2FA

6 Monthly Device reconciliation process

Netradyne SOC publishes all the list of devices integrated with EDR on monthly basis in order to perform device reconciliation and track pending devices for EDR integration.

7 Crowdstrike Console Overview

7.1 Accessing the falcon console

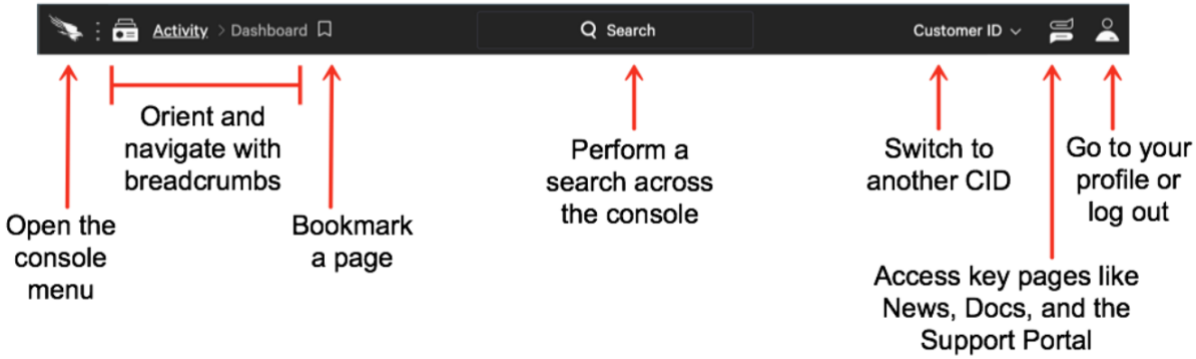
Netradyne SOC publishes all the list of devices integrated with EDR on monthly basis in order to perform device reconciliation and track pending devices for EDR integration.

Google Chrome is the only supported browser for the Falcon console.

- Go to your Falcon console URL. The URL depends on which cloud your organization uses. If you're not sure, refer to the initial setup instructions sent by CrowdStrike.
  - US-1: https://falcon.crowdstrike.com
  - US 2: https://falcon.us-2.crowdstrike.com
  - US 2: https://falcon.us-2.crowdstrike.com
  - US 2: https://falcon.us-2.crowdstrike.com
- Enter your credentials on the login screen.
- On the next screen, enter your 2FA token. The first time you sign in, you're prompted to set up a 2FA token. Common 2FA providers include Duo Mobile, winauth, JAuth, and GAuth Authenticator.

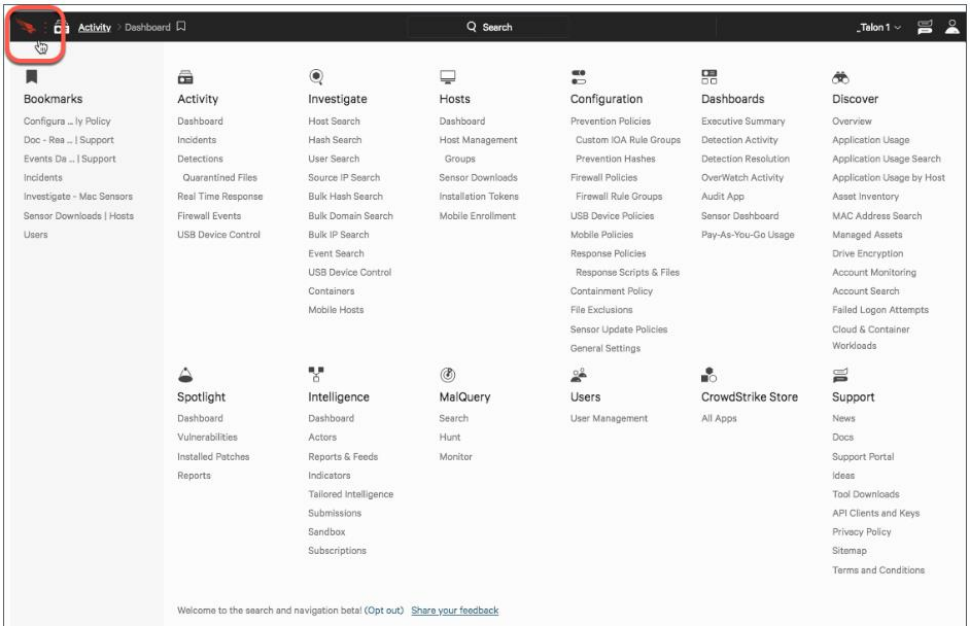
7.2 Falcon console navigation

- Navigation bar easily access the console menu, perform searches, switch customer IDs (CIDs), and more from the navigation bar.



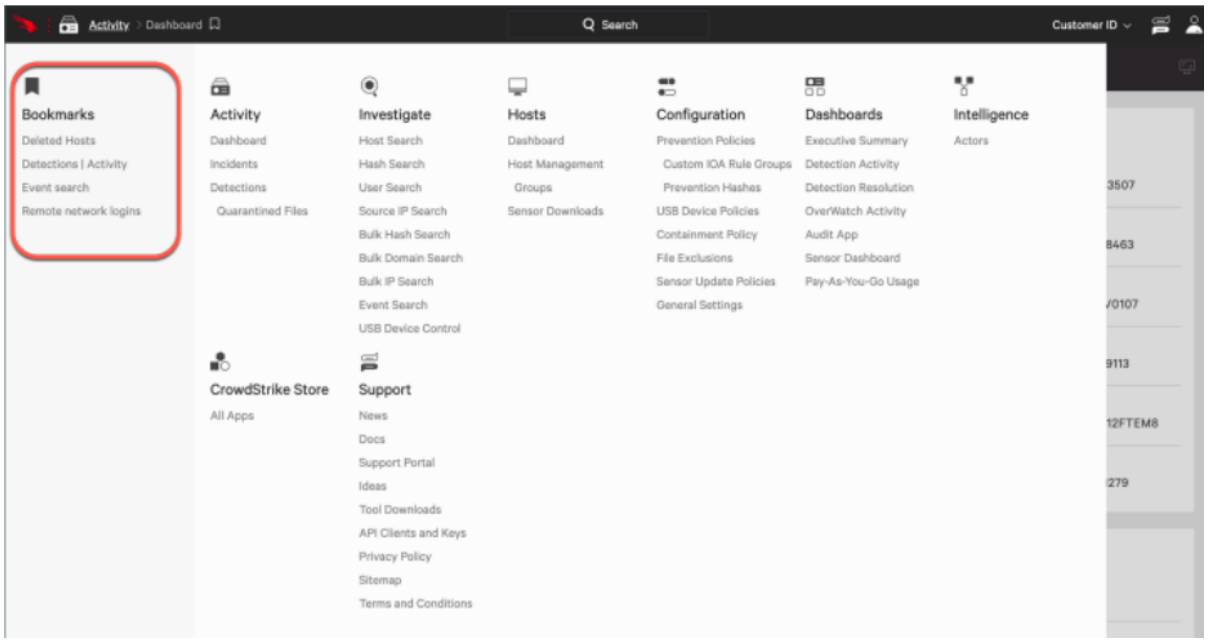
7.2 Falcon console menu

Click the Falcon icon in the navigation bar to open the menu. To close the menu, click outside of the menu or press ESC.



7.3 Falcon console bookmarks

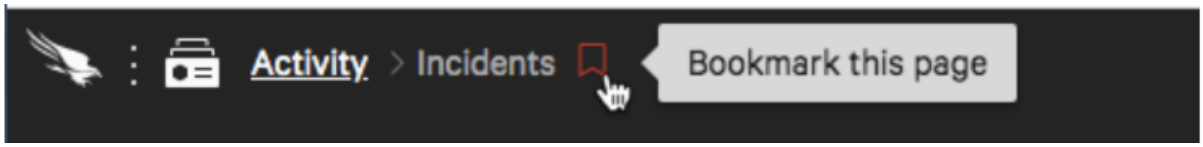
Build and manage your own list of bookmarks to easily navigate the Falcon console pages you visit most, including specific search results and pages with filters applied. Your bookmarks are available in the menu.



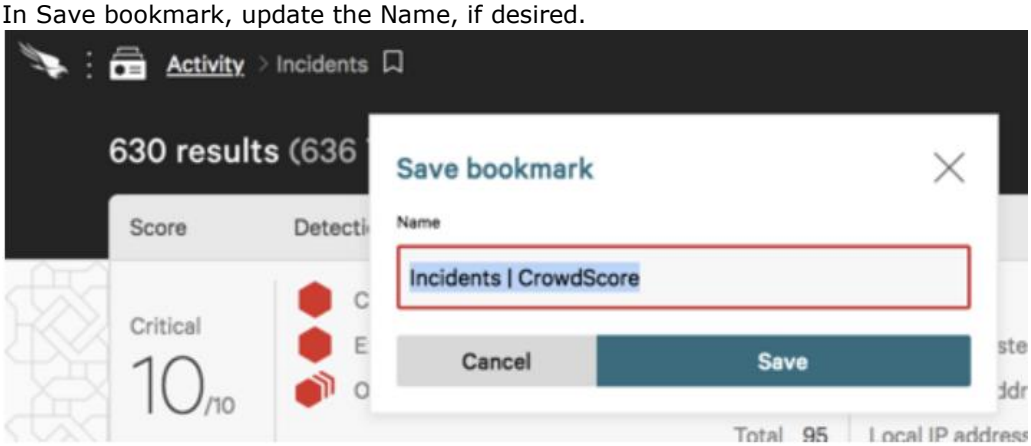
7.4 Creating bookmark

Create bookmarks for specific console pages, including any applied filters.

- Go to the page you want to bookmark.
- Click the bookmark icon.



- In Save bookmark, update the Name, if desired.

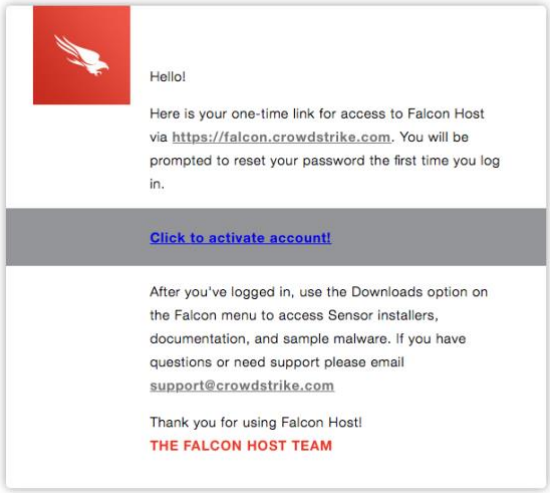


- Save

8 Crowdstrike Agent Integration Process Installation Steps

Step 1: Activate the account

After purchasing CrowdStrike Falcon or starting a product trial, look for the following email to begin the activation process.



The activation process includes:

1) Setting up a password
2) Establishing a method for 2-factor authentication

In a Chrome browser go to your Falcon console URL (Google Chrome is the only supported browser for the Falcon console).

The URL depends on which cloud your organization uses. If you're not sure, refer to the initial setup instructions sent by CrowdStrike.

US-1: https://falcon.crowdstrike.com

US 2: https://falcon.us-2.crowdstrike.com

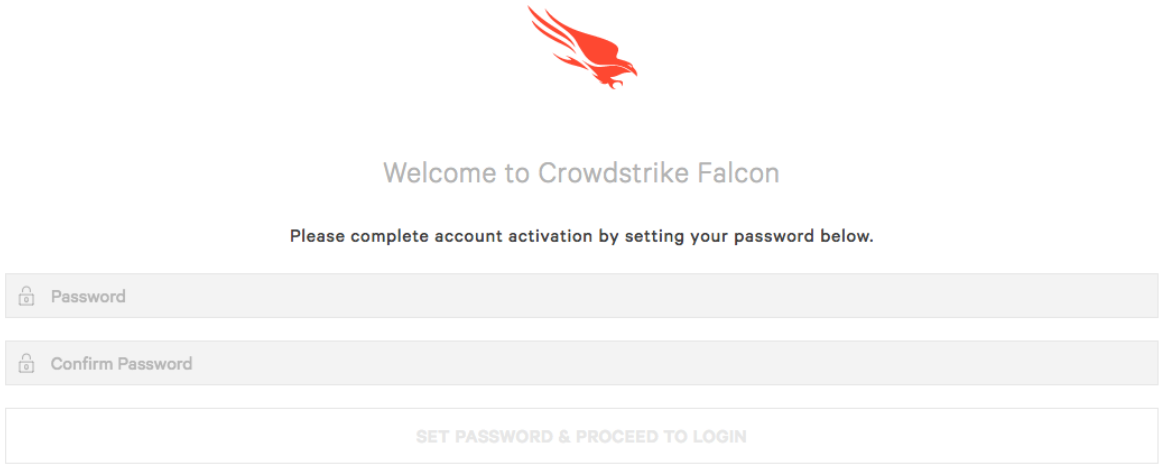
US-GOV-1: https://falcon.laggar.gcw.crowdstrike.com

EU-1: https://falcon.eu-1.crowdstrike.com

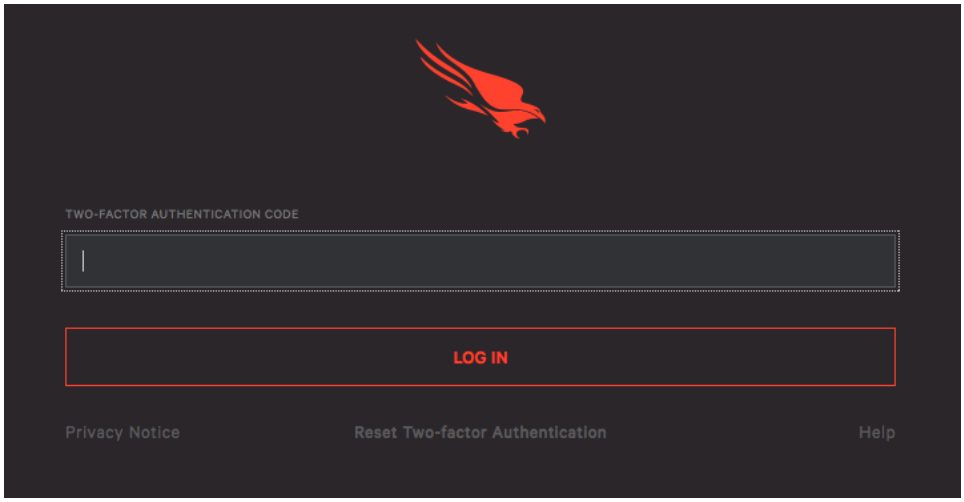
8.1 Windows

In Google Chrome:

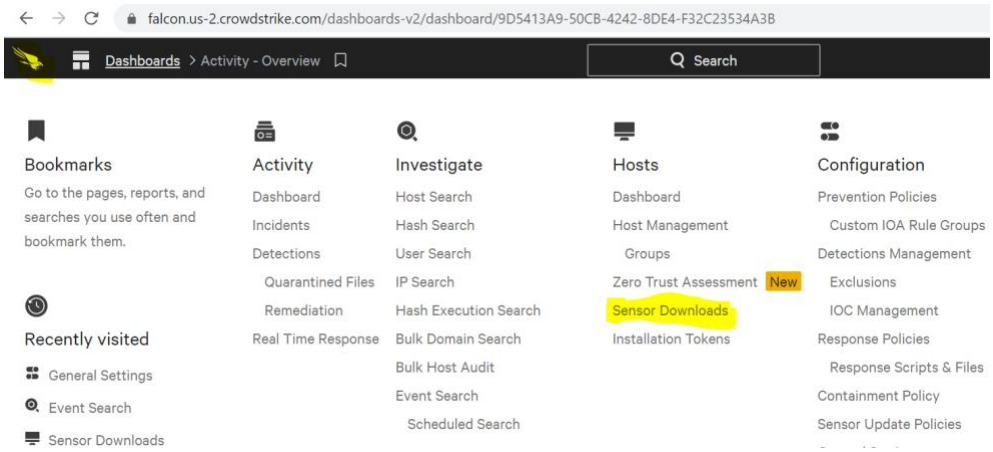
1) Enter your credentials on the login screen.

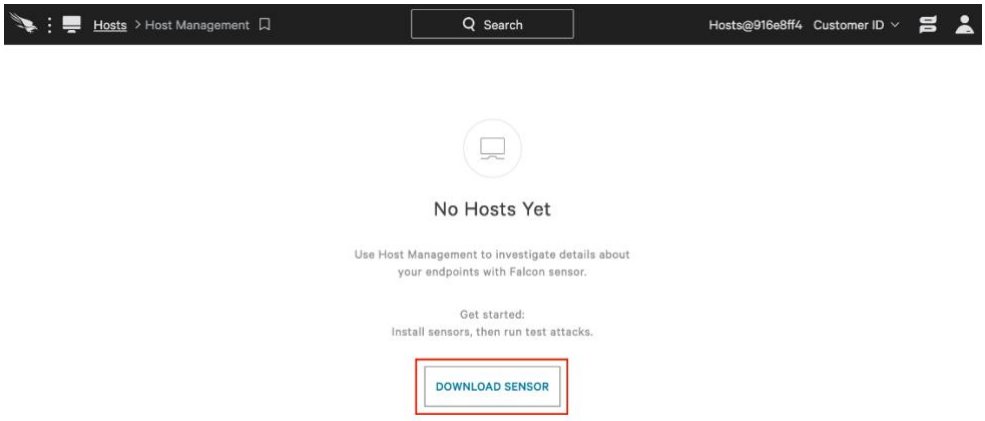


2) On the next screen, enter your 2FA token. The first time you sign in, you're prompted to set up a 2FA token. Common 2FA providers include Duo Mobile, winauth, JAuth, and GAuth Authenticator. The password screen appears first, followed by the screen where you select a method of 2-factor authentication.

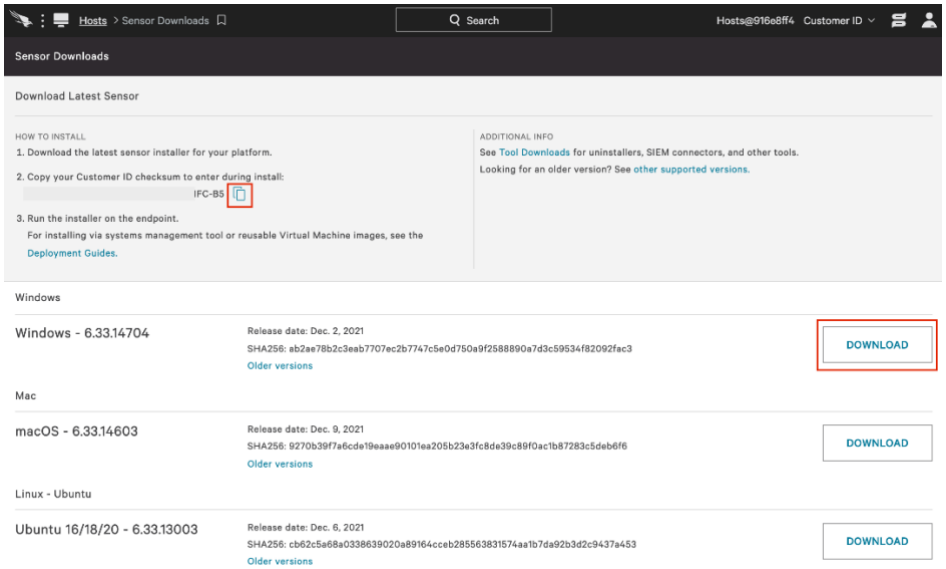


3) Download and install the agent.
Upon verification, the Falcon UI will open to the Activity App. Click the "Download Sensor" button. Also you can click on falcon icon on dashboard and select download sensor option under Host menu.





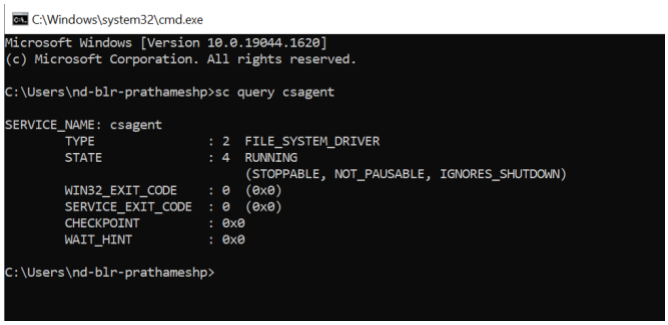
The downloads page consists of the latest available sensor versions. Select the correct sensor version for your OS by clicking on the download link to the right. At the top of the downloads page is a Customer ID, you will need to copy this value as it is used later in the install process.



Next, obtain admin privileges. Run the installer for your platform.

4) Confirm that the sensor is running
Unlike legacy endpoint security products, Falcon does not have a user interface on the endpoint. There are no icons in the Windows System Tray or on any status or menu bars.

From the windows command prompt, run the following command to ensure that "STATE" is "RUNNING": $ sc query csagent



8.2 Linux

1) Download and install the agent.
Same as windows follow steps to download falcon sensor. Copy your Customer ID Checksum (CID), displayed on Sensor Downloads.

NOTE: For Linux installations the kernel version is important. See the Linux Deployment Guide in the support section of the Falcon user interface for kernel version support.

8.3 Mac

1) Download and install the agent.
Same as windows follow steps to download falcon sensor. Copy your Customer ID Checksum (CID), displayed on Sensor Downloads.

2) Run the sensor installer on your device in one of these ways:
i) Double-click the .pkg file.
ii) Run this command at a terminal, replacing <installer .pkg> with the path and file name of your installer package.
sudo installer -verboseR -package <installer_filename> -target /

3) Change in System Preferences

- When prompted, enter administrative credentials for the installer.
    - For macOS Mojave 10.14 through macOS Catalina 10.15, after entering the credential for installation, you're asked to approve the kernel extension on each host. The Apple message on the host identifies the CrowdStrike kernel extension as a blocked system extension signed by CrowdStrike Inc.

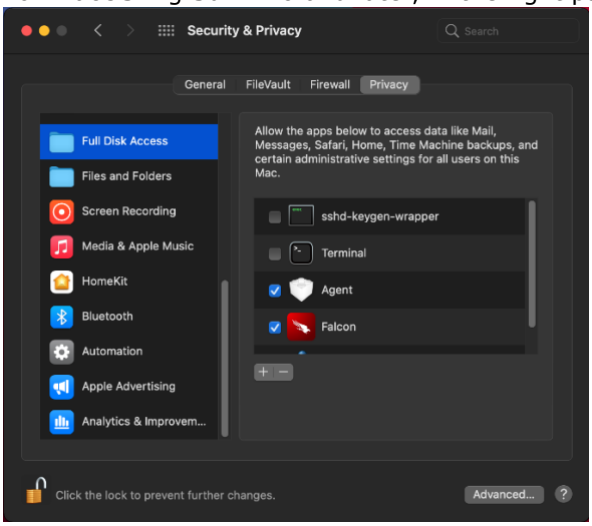
  - In the message, click Open Security Preferences. If the message no longer appears on the host, click the Apple icon and open System Preferences, then click Security & Privacy.
  - On the General tab, click Allow to allow the CrowdStrike kernel extension.
- Run falconctl, installed with the Falcon sensor, to provide your customer ID checksum (CID).
  - This command is slightly different if you're installing with password protection (see documentation).
  - In this example, replace 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX with your CID.

    sudo /Applications/Falcon.app/Contents/Resources/falconctl license 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX

- For macOS Big Sur 11.0 and later, after providing your CID with the license command, you will be asked to approve the system extension on each host:
  - In the message, when asked to filter network content, click Allow.
  - When the System Extension Blocked message appears, click Open Security Preferences.
  - On the General tab, click Allow to allow the Falcon system extension. You may need to click the lock icon to enable you to make security changes. If you do not approve the Falcon system extension when prompted on the host, run the falconctl load command to load Falcon again and show the prompts on the host for approval:

    sudo /Applications/Falcon.app/Contents/Resources/falconctl load
- Grant Full Disk Access (detailed instructions in product guide) – Beginning with macOS Catalina, Apple requires full disk access to be granted to CrowdStrike Falcon in order to work properly. This is a Catalina requirement by Apple for files and folders containing personal data. This requirement is applicable to all 3rd-party software which need to access files across all users of the machine (e.g. backup software).

  - Click the Apple icon and open System Preferences, then click Security & Privacy.
  - On the Privacy tab, if privacy settings are locked, click the lock icon and specify the password.
  - In the left pane, select Full Disk Access.
  - For macOS Big Sur 11.0 and later, in the right pane, select the Agent check box:



- For all macOS versions, in the right pane, click the plus icon.

- In finder, find Falcon in the list of applications (no "Agent" is required).

- Click Open and then click Quit Now:
- Click the lock icon to re-lock privacy settings.

After installation, the sensor runs silently. To confirm that the sensor is running, run this command at a terminal:

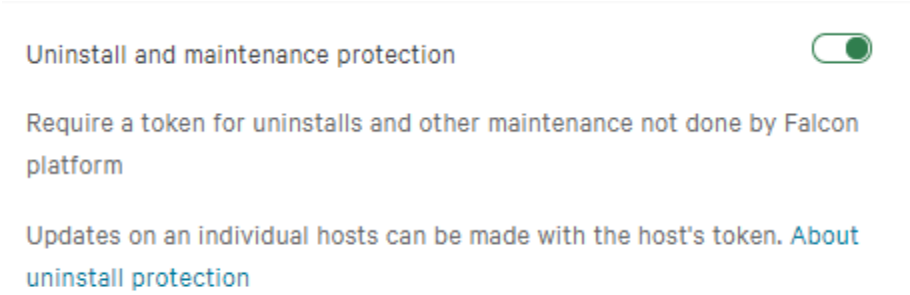
sudo /Applications/Falcon.app/Contents/Resources/falconctl stats

The output shows a list of details about the sensor, including its agent ID (AID), version, customer ID, and more.

9 Agent Removal Process

Uninstall Protection Policy

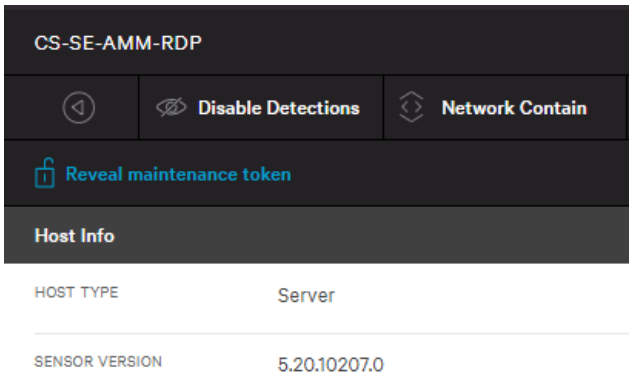
Within the Falcon Update Policy, Sensor Uninstall Protection is configurable (Configuration > Sensor Update Policies > [Policy] > Sensor Protection). With this policy applied to our devices, an uninstall will now require a token to complete.

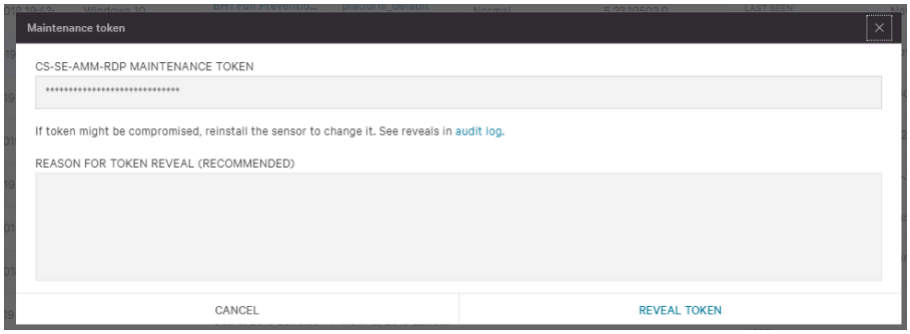


Falcon Uninstall Workflow with Protection Enabled

To simplify the management of protected Falcon Agent installations, maintenance tokens can be accessed from the Hosts app. Navigate to Host App > Host Management, then select the host of interest and click "Reveal maintenance token" and you are presented with the one-time maintenance token, which can be given to the end-user/technician updating or uninstalling the Falcon Agent.

Even if the device is offline, the token will allow the uninstall/update to proceed.

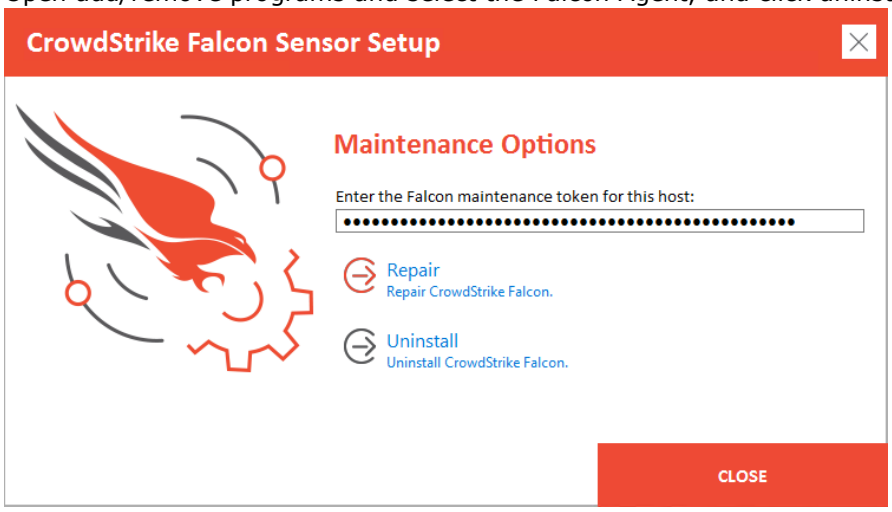




When Uninstall Protection is enabled and an uninstall is initiated, users are presented with the setup dialog and are required to input the token obtained from the Falcon UI.

9.1 Windows

Open add/remove programs and select the Falcon Agent, and click uninstall:



9.2 Mac

Launch Terminal Application:
Uninstall Falcon Agent

sudo /Applications/Falcon.app/Contents/Resources/falconctl uninstall --maintenance-token INPUT_YOUR_TOKEN

9.3 Linux

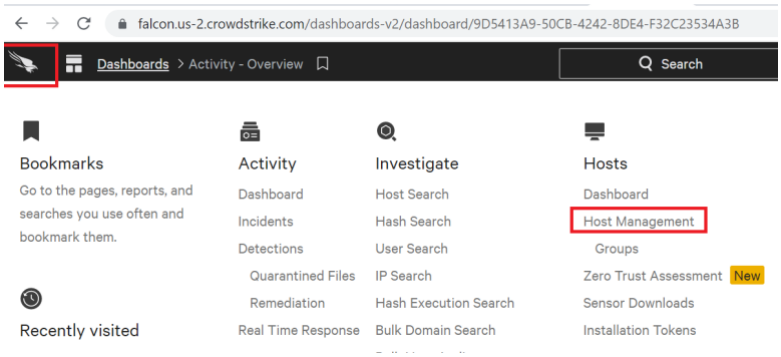
To uninstall CrowdStrike manually on a Linux system, run one of the following commands based upon your Linux distribution:

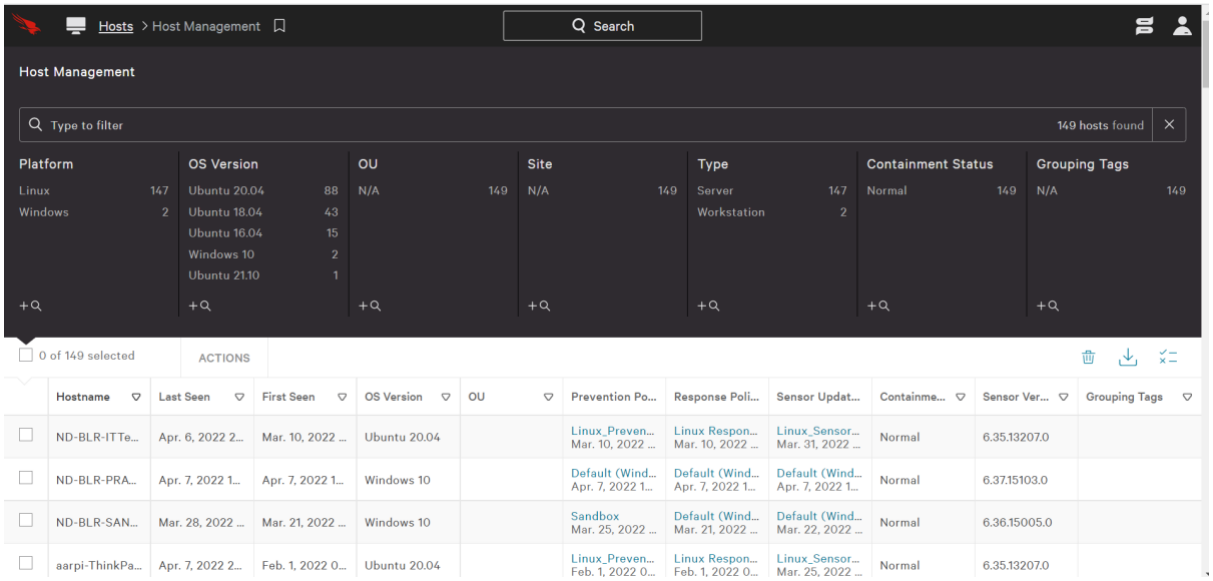
- Ubuntu : sudo apt-get purge falcon-sensor
- RHEL, CentOS, Amazon Linux: sudo yum remove falcon-sensor
- SLES: sudo zypper remove falcon-sensor

10 Managing Host

10.1 Navigating the Host Management page

On the Host Management page, view information about each host including OS, host type, the prevention policy applied to the host, and a host's containment status and sensor version.





From this page, you can see which prevention policy is applied to a host. The Prevention Policy column can have the following values:

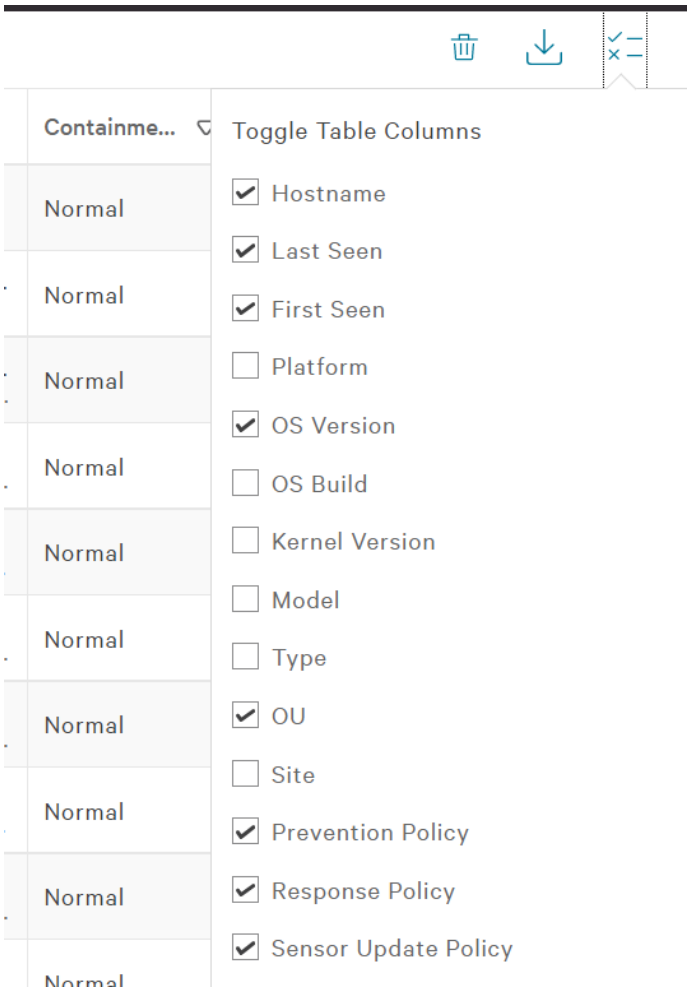
- "No Policy" - Used if the host recently had a Falcon sensor installed on it, and either the cloud has not yet evaluated which policy is appropriate or the host is no longer active.
- "{Policy Name}" & "{Applied Date}" - Name of the policy that has been pushed down to the host and the date and time at which the host received the policy.
- "{Policy Name}" & "Changes pending" - Name of the policy that will be pushed down to the host.
- "Policy Deleted" & "Changes pending" - The host has a policy that has been deleted and the cloud has yet to determine which new policy the sensor should receive. During this transitional period, the host will continue to use the policy that was previously applied to it as it waits to receive the new policy from the cloud.

10.2 Find Host

The Host Management page lets you filter, search, and customize the columns you see to help you find and manage your hosts.

Use the filter bar at the top to search for a specific host or click the default filters to view a more targeted list.

Choose the columns that appear on the Host Management page by clicking the column selection button on the right side of the screen.



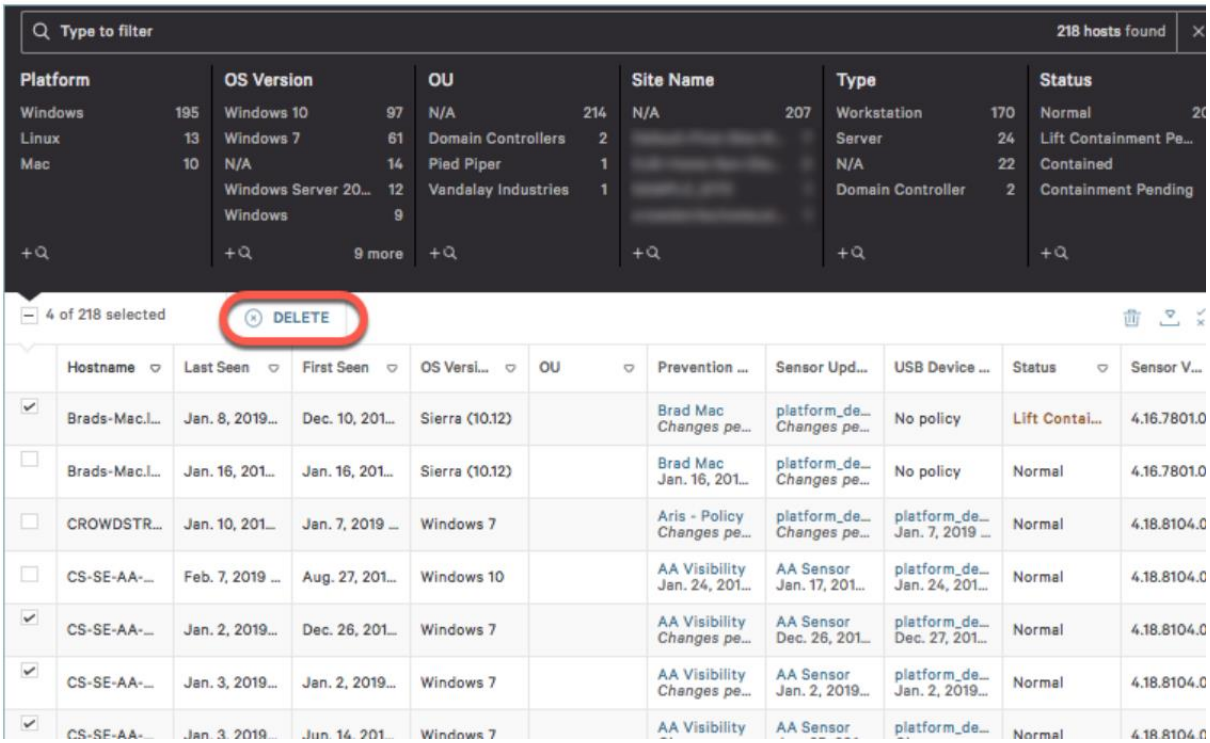
10.3 Deleting Host

Users with the Falcon Admin role can clean up inactive or duplicate hosts by deleting them.

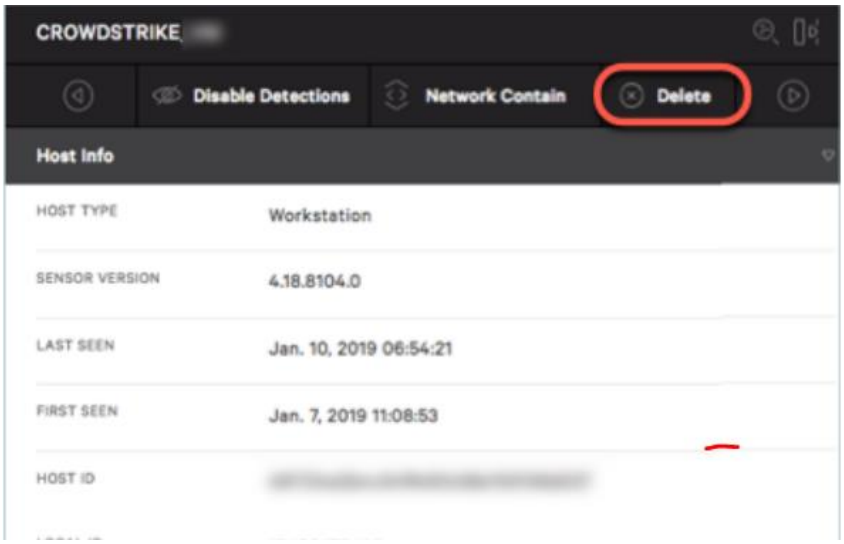
- A host becomes inactive when its sensor doesn't send a heartbeat back to the cloud for two minutes. Inactive hosts are identified by their Last Seen time.
- Duplicate hosts typically appear when machines are reimaged. After being reimaged, the Hostname stays the same, but the sensor gets a new Host ID.

10.4 How to delete host

In Hosts > Host Management, select one or more hosts to show the Delete button. Click Delete to move selected hosts to the trash. Up to 100 hosts can be deleted in bulk at one time.



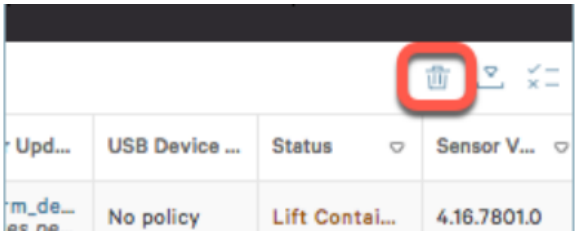
The host summary panel also includes an option to delete a host.



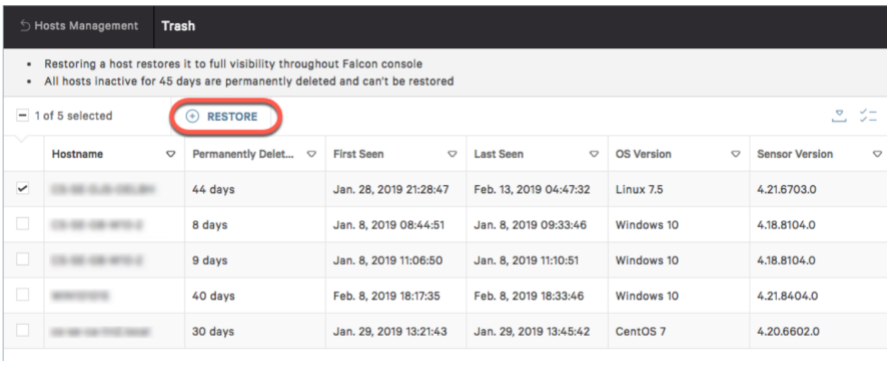
10.5 Restoring a host

Active Windows, Mac, and Linux hosts that are deleted can be restored. Deleted mobile hosts cannot.

If you accidentally delete an active Windows, Mac, or Linux host and need to restore it, click the trash can icon to reach your deleted hosts that have been moved to the trash.



On the Host Management > Trash page, select one or more hosts to enable the Restore button. Click Restore, and your selected hosts will have detections re-enabled and they will re-appear throughout the console.



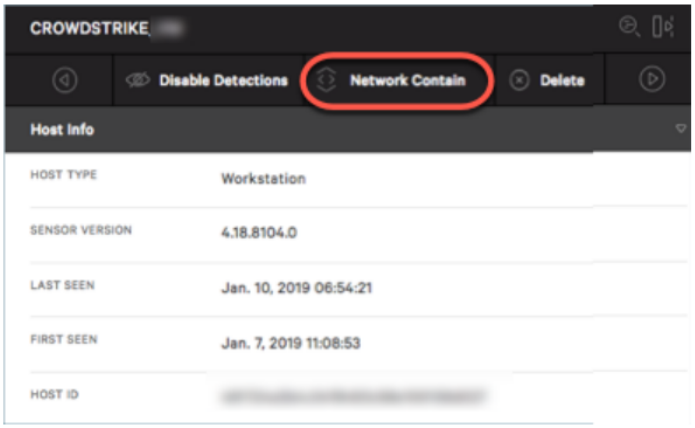
If you accidentally delete an iOS or Android host, It is truly deleted, and will not remain active or appear on Host Management > Trash page where it could be restored. You must send a new invite to the associated user so they can re-enroll.

10.6 Changing a host's containment status

From a host's summary panel, you can network contain a Windows, Mac, or Linux host to isolate it from all network activity.

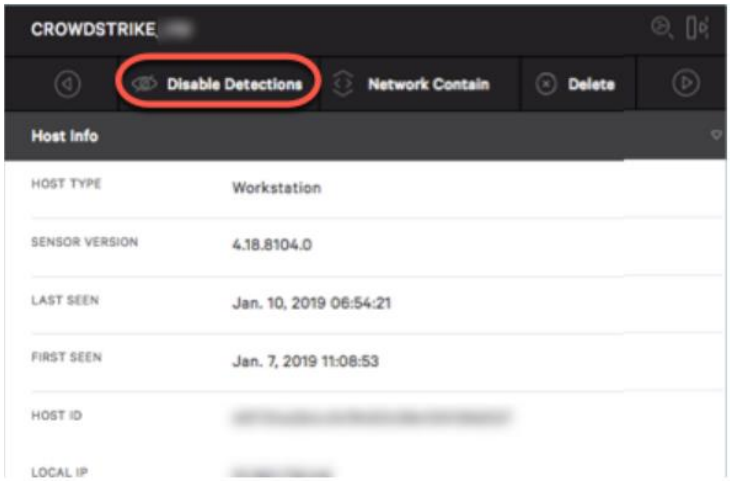
To change a host's containment status, click the network containment option in the host's summary panel:

- Network Contain - click to contain an un-contained host
- Lift Containment - click to un-contain a contained host
- Lift Containment Pending - status is in the process of moving from contained to un-contained
- Lift Containment Pending - status is in the process of moving from contained to un-contained



10.7 Disabling detections on a host

To disable detections on a host, click Disable Detections. This is helpful for users who want to set up hosts to test detections in the Falcon console and who later want to remove those old test detections from the console.



When active, this feature only suppresses detections for the host. The feature does not disable the sensor or interfere with the sensor's ability to protect the host. Consider the behavior explained below.

- The sensor continues to operate normally except those detections for the host do not appear in the Activity > Detections feed or in any related email alerts
- Activity related to the host is still factored into Activity > Incidents.
- Configurations such as prevention toggles that are applied to the host from Prevention Policies, prevention hash rules (set in IOC Management), Custom IOA Rule Groups, Exclusion rules, and so on are still processed normally.

When a user disables detections:

- Falcon console impact: The detections for that host are removed from the console immediately. No new detections will display in the console going forward unless detections are enabled.
- API impact: The DetectionSummaryEvent stops getting sent to the Streaming API for that host.
- Event Search impact: Even after disabling detections, the data for all existing detections prior to disabling detections will still be in Event Search.

To re-enable detections, click Enable Detections, which appears instead of "Disable Detections" when a host's detections are currently disabled.

When a user enables detections:

- Falcon console impact: New detections will start appearing in the console immediately. Previous detections will not be restored to the console for that host.
- API impact: The DetectionSummaryEvent starts getting sent to the Streaming API for that host.
- Event Search impact: Detections will start to appear in Event Search. No detections will be available for the period of time when detections were disabled. The data for any detections for that host that existed prior to disabling detections will remain in Event Search.

10.8 Managing Host group

Host groups allow you to assign policy settings, sensor upgrades, file path exclusions, and more to one or more hosts. Hosts can belong to multiple groups so you can tailor policy and other configuration settings to the needs of your environment.

There are two types of host groups — dynamic and static. The group type is selected when you create it and can't be changed later.

- **Dynamic host groups**: These are empty upon initial creation. To add hosts, define filters based on attributes such as grouping tags, IP/CIDR range, OS version, Active Directory OU, or hostname prefix or suffix. When hosts match the assignment rule for a dynamic group, they are automatically added to the group. When a host no longer matches the assignment rule for the group, it's automatically removed. We recommend dynamic groups in most cases.

- **Static host groups**: These are defined manually. Static groups are useful for hosts in static environments, such as QA or testing, or for when dynamic group filters are insufficient. There is a limit of adding 1,000 hosts to a static group at a time.

  When creating a static host group, you must select whether to add hosts by hostname or host ID (also known as agent ID). This selection can't be changed later. You can add hosts to a static group using any of these methods:
  - By selecting hosts using filters in the Falcon console
  - By manually entering hosts in the Falcon console
  - By uploading a text file containing a list of hosts

When creating dynamic or static host groups for containers, use these fields to create the filter specific to pods:

- Pod Name
- Pod Namespace
- Pod ID
- Pod Labels

10.9 Planning dynamic host groups
Dynamic groups are flexible so you can tailor your group structure to the specific needs of your environment. You'll use these groups to assign policies to your hosts, so consider different ways you can identify hosts to sort them into the correct groups. Groups can be based on standard attributes, grouping tags, or a combination.

- Using standard attributes
  Standard attributes are existing traits that can be used as filters to organize hosts. Attributes include IP address/CIDR block, hostname, and Active Directory OU. Possible use cases include:
  - Apply more restrictive policies for hosts in your Finance department by creating a dynamic group that filters Hostnames that start with "FIN*".
  - Disable cloud updating in an office with bandwidth limits by creating a dynamic group assignment rule using the IP/CIDR filter to select only hosts on that office's subnet.

  You can add multiple filters to your assignment rule to be more specific about which hosts belong to that group. For example, if you're remediating a suspected incident on hosts in a single department at one office location, you might add multiple criteria to your assignment rule so that the target group is made up of hosts that both:

  - belong to a specific departmental OU
  - are in the Site Name impacted

10.10 Creating Host group

- Go to Hosts > Groups.
- Click Add New Group.

- Enter a name, description, and platform. Allowed characters are:
  - a-z
  - A-Z
  - 0-9
  - - (hyphen)
  - _ (underscore)
  - :
  - ;
  - .
  - !
  - spaces

10.11 Assigning hosts to a host group

You assign hosts using different processes, depending on the group's type.

- Dynamic group: Assign hosts by creating an assignment rule.
- Dynamic group: Assign hosts by creating an assignment rule.

10.12 Assigning Host to dynamic group

- Dynamic group: Assign hosts by creating an assignment rule.
- Select the dynamic group you want to add hosts to.
- Select Edit in the top right of the Assignment Rule bar.
- In the filter bar, add criteria by selecting or typing filter names.
- Select Save to save and apply this assignment rule.

10.13 Assigning Host to static group

You can assign hosts to a static group by selecting existing hosts in the console or by uploading a list of host IDs or hostnames. Whether you upload hosts by ID or name depends on the type of group created (Static by host ID or Static by hostname).

When uploading hosts by hostname, Falcon checks that submitted hostnames match hosts that currently exist in the Falcon console. If you want to add hosts to a group before deploying sensors, you can disable validation.

Note: You can assign up to 1,000 hosts to a static host group at a time.

- Go to Hosts > Groups.
- Locate the static group to add hosts to and click Edit Group ().
- Select one of these options:
  - Upload a file or enter hosts manually:
    - Select Upload Hosts.
    - Add hosts by their IDs or by their hostnames. Enter the hosts one per line, or select a TXT file that contains only host IDs or only hostnames separated by new lines. Example using IDs:
      host-ID1, host-ID2, host-ID3
    - If you're adding hosts by hostname that are not currently in Falcon, select Disable Hostname Validation.
    - Click Next.
    - Click Upload.
  - Select hosts in the Falcon console:

- Select Add Hosts.
- Select the checkbox near the hosts you want to assign. Use the filter bar to reduce the list of displayed hosts.
- Select Done in the upper-right corner to assign all selected hosts.

When you return to your static group, you can see the hosts assigned to the group.

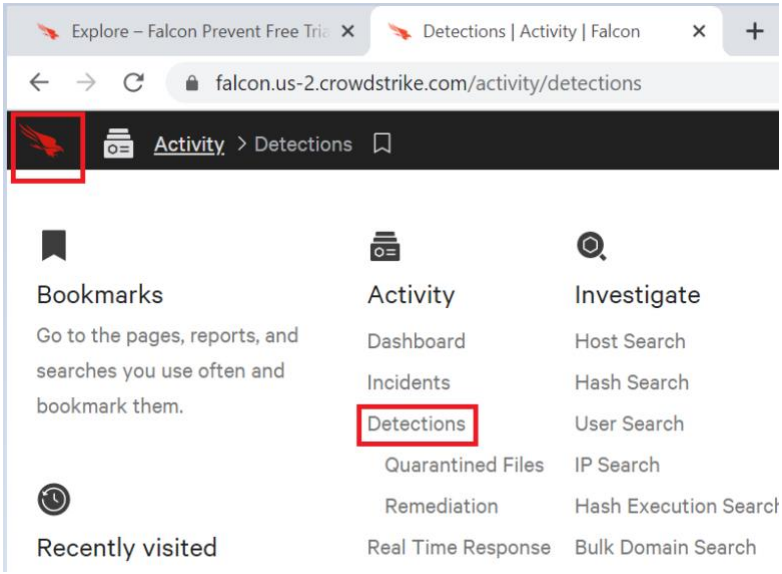
10.14 Deleting a host group

- Go to Hosts > Groups.
- Select the group you want to delete.
- Click Delete in the upper-right corner.
- When prompted, click Delete Group to permanently delete this group.

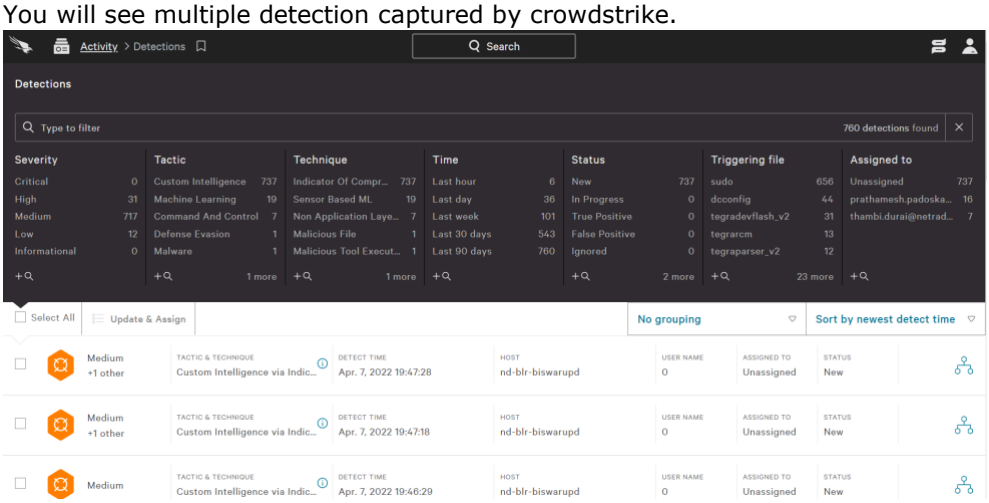
11 Sample detection and testing

11.1 Viewing Detection

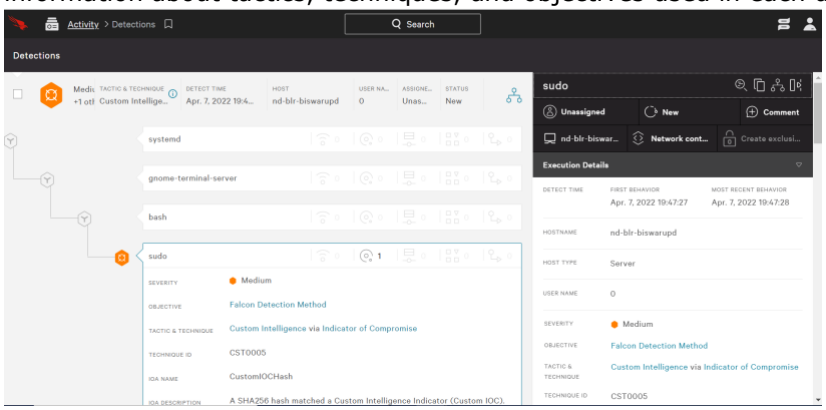
- Open detection dashboard by clicking falcon Icon and select Detection under activity tab.



- You will see multiple detection captured by crowdstrike.



- Learn more by clicking any of the detections. When you do so, an Executions Details Panel appears on the right and an expanded view of all processes involved in the detection shows in the main window.
- In Execution Details, you can learn about the specific detection. Falcon also provides information about tactics, techniques, and objectives used in each detection.

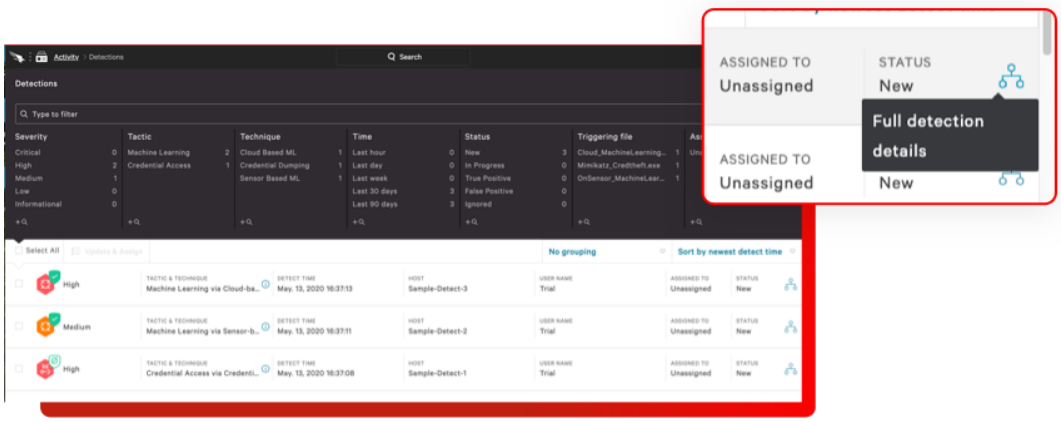


- You can also see what prevention actions Falcon took, plus get details about the commands, executables, and files involved. By default, Execution Details displays information about the final process in the detection.

11.2 Process Views

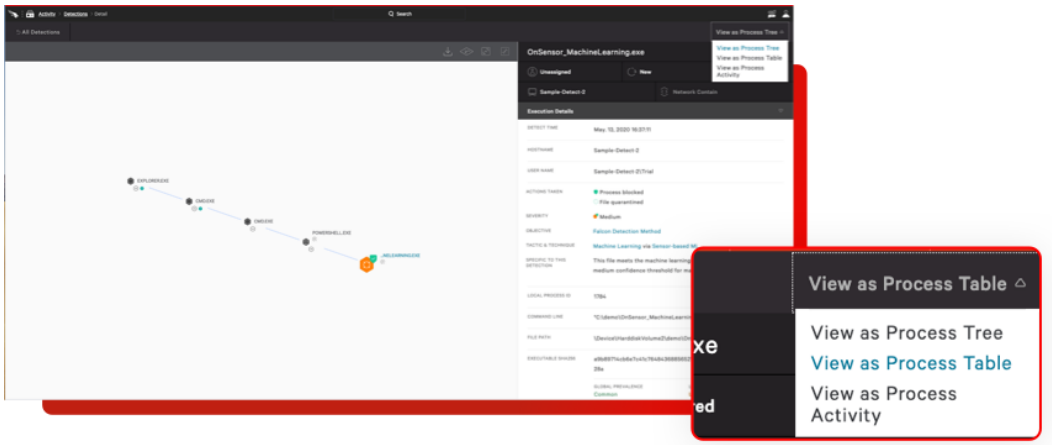
- Falcon provides three process views to help you visualize a detection.

- Click the  Full Detections details icon in any detection row to expose the View as drop-down menu in the Detections page's upper right corner.

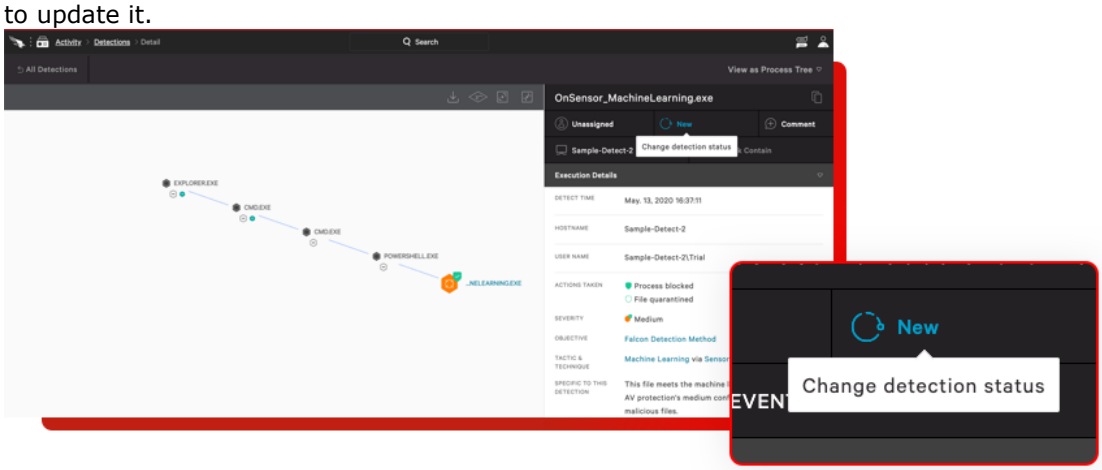


11.3 Viewing Options

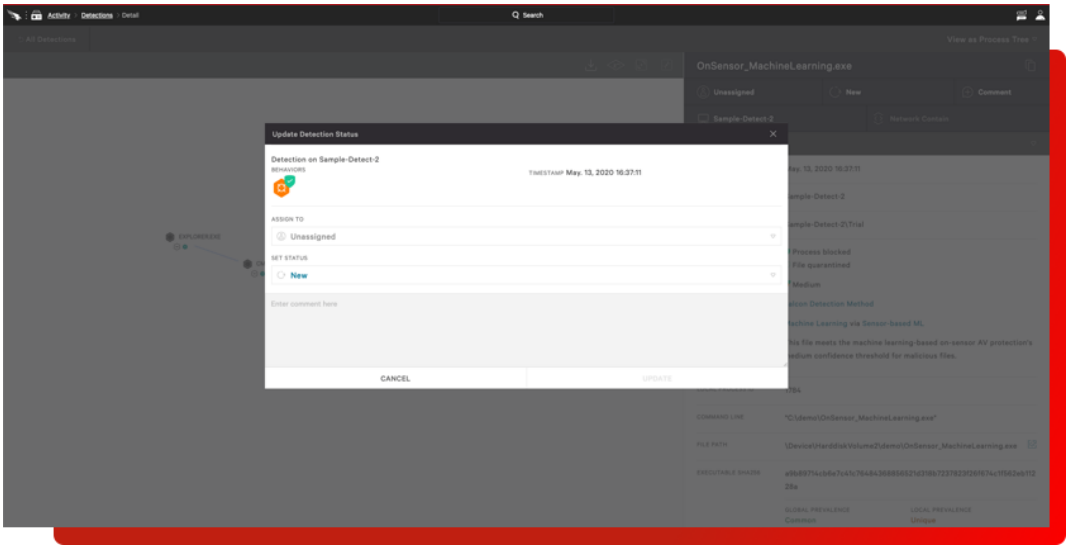
Further above you can switch to other viewing options from the View as dropdown. Select View as Process Tree, View as Process Table, or View as Process.



- After you have reviewed the detection, you can optionally change its status. Click on New to update it.



- A dialogue window will open. Change the status and click Update. Also assign to yourself or user who will handle detection.



12 Hunting and Investigation

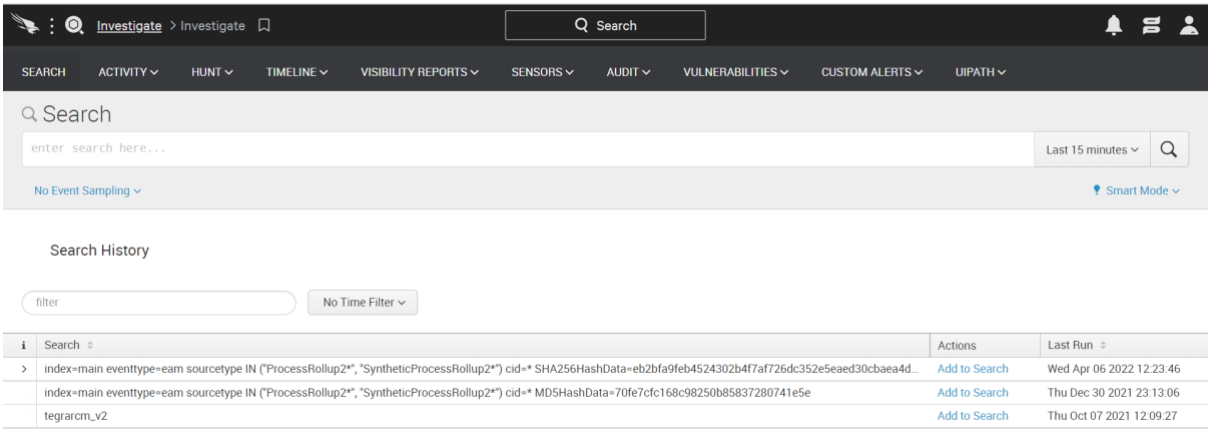
12.1 Introduction

The Hunting Guide for Windows teaches you how to hunt for adversaries, suspicious activities, suspicious processes, and vulnerabilities on the Windows platform using Falcon.

Falcon contains a suite of powerful search tools that allow you to analyze, explore, and hunt for suspicious or malicious activity in your environment. These tools include the pre-made search dashboards in the various Falcon apps as well as the ability to run custom queries on the Events Search page in the Investigate App. This guide focuses mainly on using custom queries to hunt, but will also direct you to use Falcon's pre-made dashboards when it makes most sense.

12.2 Hunting with Falcon

Hunting with Falcon is straightforward. By using either the pre-made dashboards and reports or by using custom queries on the Events Search page, you can search for specific events and data points across one, several, or all hosts running the Falcon sensor in your environment. The data returned in an Events Search query is from the last 30 days of sensor activity, though most of the queries you run will need to be narrowed down to a smaller timeframe so that results are usable. You then use your search results to understand and evaluate security events happening in your environment.



All queries in Falcon are powered by the Splunk query language. To learn more about Splunk and Splunk syntax, we recommend that you read the Official Splunk Documentation and the Splunk Enterprise Quick Reference Guide.

Let's start with a simple example.
Show me a list of processes that executed from the Recycle Bin for a specific AID
aid=my-aid ImageFileName=$Recycle.Bin* event_simpleName=ProcessRollup2 | stats values(name) values(MD5HashData) values(ComputerName) values(ImageFileName) count by aid*

In the example above, you should provide an "agent ID" (or "AID" for short), which is a unique ID given to each Falcon sensor. Adding the AID to the query limits the scope of your query to the sensor with that AID and greatly reduces the time and computational cost of your search.

Thus, the above query might end up looking like this:

aid="a9e3b67c7883497f6d18fdd1517b177d" ImageFileName=$Recycle.Bin* event_simpleName=ProcessRollup2 | stats values(name) values(MD5HashData) values(ComputerName) values(ImageFileName) count by aid*

Using the AID in this fashion is just one way to drill down to a specific host. You can also use host name (ComputerName="foo") in the same fashion.

This is just one example but shows how specificity matters greatly when writing Splunk queries. The more specific you can be when writing a query, the fewer results you will have to sort through and the faster the query will run.

Let's see how a simple query can be made more useful for you with a few simple modifications. Below is an example query that returns a large amount of data and takes a long time to run. This query returns a list of *SuspiciousDnsRequest* events, the domains to which the requests were made, the host names from which the requests were made, and the number of times the requests were made:

event_simpleName=SuspiciousDnsRequest | stats values(ComputerName) count by DomainName

The amount of results returned by this query and the time that it takes to run make this query difficult to work with. We can fix both of this by making our query more specific.

Let's start reducing the number of results by limiting the query to a single AID, which would return a list of SuspiciousDnsRequest events that occurred on the host running the Falcon sensor with that particular AID:

aid="a9e3b67c7883497f6d18fdd1517b177d" event_simpleName=SuspiciousDnsRequest | stats values(ComputerName) count by DomainName

Next, we can further reduce our results list by specifying a timeframe. Instead of searching across 30 days of data, let's search for instances of this event in the last 24 hours using the "earliest" and "latest" keywords:

aid="a9e3b67c7883497f6d18fdd1517b177d" event_simpleName=SuspiciousDnsRequest earliest=-24h latest=now | stats values(ComputerName) count by DomainName

We also know that often times requests made only once or twice instead of dozens of times are often more likely to be suspicious. We can limit our results to a specific number of suspicious requests. In this example, we'll say that we only want to see domains to which fewer than three suspicious requests were made. We can do this by adding the event count condition:

aid="a9e3b67c7883497f6d18fdd1517b177d event_simpleName=SuspiciousDnsRequest earliest=-24h latest=now | stats values(ComputerName) count by DomainName | where count <3

Alternatively, we could reduce the number of results further by returning only the top 20 or bottom 20 results based on the number of requests made:

aid="a9e3b67c7883497f6d18fdd1517b177d" event_simpleName=SuspiciousDnsRequest earliest=-24h latest=now | stats values(ComputerName) count by DomainName | head 20

Bottom 20 results:

aid="a9e3b67c7883497f6d18fdd1517b177d" event_simpleName=SuspiciousDnsRequest earliest=-24h latest=now | stats values(ComputerName) count by DomainName | tail 20

It should also be noted that the Events Search and Splunk handle special character escaping differently. For example, if you wanted to enter the path \system32\config\, you would traditionally write it and escape the backslashes like so:

\\system32\\config

However, in the Events Search, this should be written as:

\\\\system32\\\\config\\\\

This is particularly important when your search includes regex syntax.

By adding a timeframe, applying limits and filters, and escaping our searches properly, we can easily reduce the results list of our Splunk query to a useful, manageable amount of information. This decreases the time and complexity of hunting adversaries in your environment.

12.3 Filter out benign data

Hunting with Falcon is all about obtaining meaningful data. Thus, for every query you run, you will most likely want to filter out data that you know is unnecessary. Unnecessary data could be data that is irrelevant to what you are searching for or it could simply be data that you know is benign.

For example, let's say you are hunting suspicious registry changes.

aid=my-aid event_simpleName=ASEP | table timestamp ComputerName RegObjectName | sort - by timestamp*

We can make this more meaningful by filtering out a registry object that we know to be benign using the "does not equal" syntax ("!="). This reduces the amount of results we get and speeds up the time it takes to run the query.

aid=my-aid event_simpleName=ASEP RegObjectName!="Value" | table timestamp ComputerName RegObjectName | sort - by timestamp*

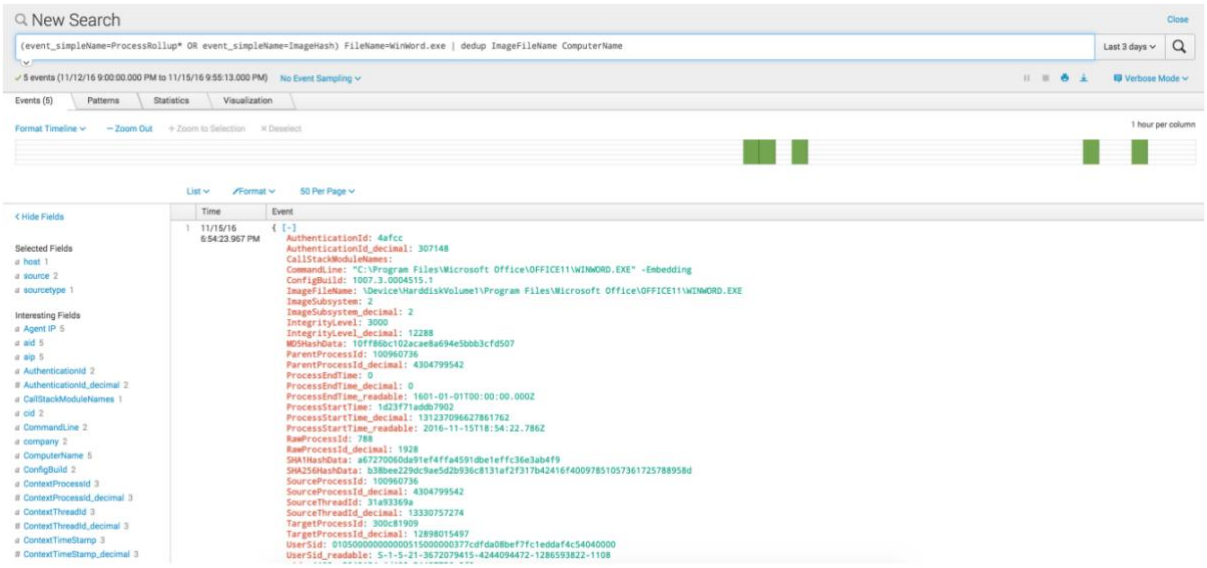
12.4 Use the built-in workflows

The Events Search page has built-in workflows that enable you to quickly and easily run pre-made queries on your search results with the click of a button. This allows you to run powerful queries without writing a single line of Splunk syntax.

To see how this works, we'll run the following example query. This query returns a list of all versions of Microsoft Word that are running on my hosts (removing duplicate entries by *ImageFileName* and *ComputerName*).

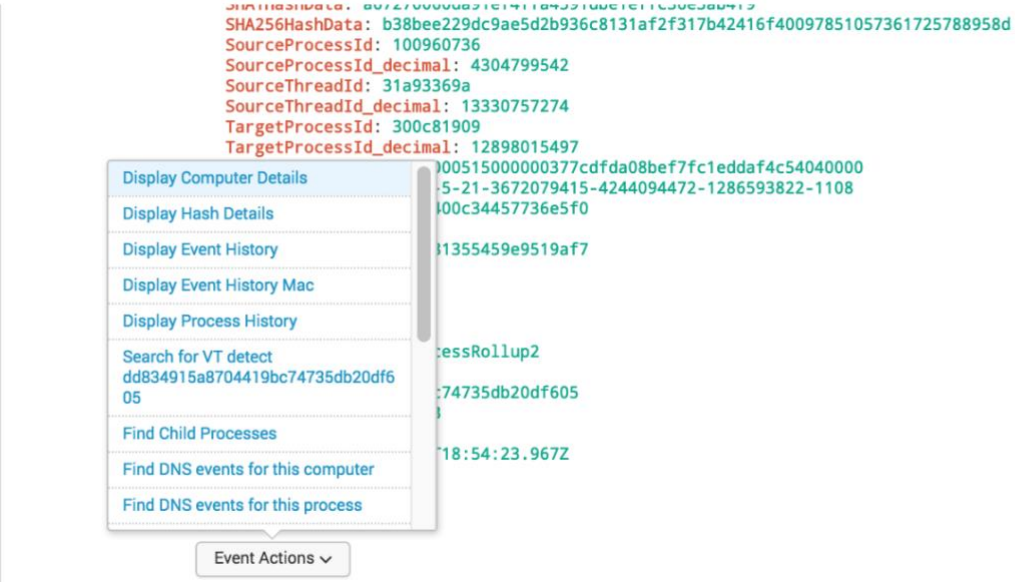
(event_simpleName=ProcessRollup OR event_simpleName=ImageHash) FileName=WinWord.exe | dedup ImageFileName ComputerName*

This query gives us the following results.



In the screenshot above, we see the raw JSON from a ProcessRollup2 event in our search results.

Let's say we now want to see the event associated with the process that spawned this event (the "parent process"). We could write a brand-new query. Or, we could use the built-in workflows. Simply click Event Actions below the raw JSON to access the workflow menu for the event:



Note the number of workflows that are built in. This list will vary depending on the event.

12.5 Hunting queries

Please visit below link to get predefined hunting queries. You can hunt start from suspicious process,
Phishing attacks to finding anomaly, behaviour and exploits.

Hunting queries link.

13 Detection and prevention policy

Use Prevention Policies to manage the activity that will trigger detections and preventions on your hosts, which you'll monitor in the Activity app. Policies are assigned to hosts within Host Groups. The available prevention settings vary by platform.

13.1 Creating a prevention policy

You can have a total of 100 custom policies.

- Go to Configuration > Prevention Policies.
- Click Create new policy.
- Enter a platform, policy name, and description. Accepted characters: a-z, A-Z, 0-9, -, _, :, ;, ., !, and spaces
- Click Create Policy.
- Enable or disable individual prevention settings on the Settings tab.
    - Click a row of policy settings to manage individual preventions within that category.
    - Click Enable All to enable all preventions in that category
- To save your prevention settings, click Save, then click Confirm
- To enable the policy, click Enable. Click Enable Policy to confirm.

13.2 Assigning a prevention policy to a host group

- Go to Configuration > Prevention Policies.
- Find the policy you want to assign to a host group and click Edit Policy on the far right.
- Go to the Assigned Host Groups tab.
- Click Add groups to policy in the upper right.
- Select one or more groups
- Click Add Groups to Policy.

After you assign a host group to a policy, that host group will no longer appear in the list of available groups.

13.3 Disabling a prevention policy

You can temporarily suspend a policy by disabling it. When you disable a policy, the policy stops affecting online hosts. When any offline hosts come back online, the cloud disables the policy on those hosts.

- Go to Configuration > Prevention Policies.
- Near the policy you want to disable, click Edit Policy.
- On the Settings tab, click Disable.
- On the Settings tab, click Disable.

13.4 Deleting a prevention policy

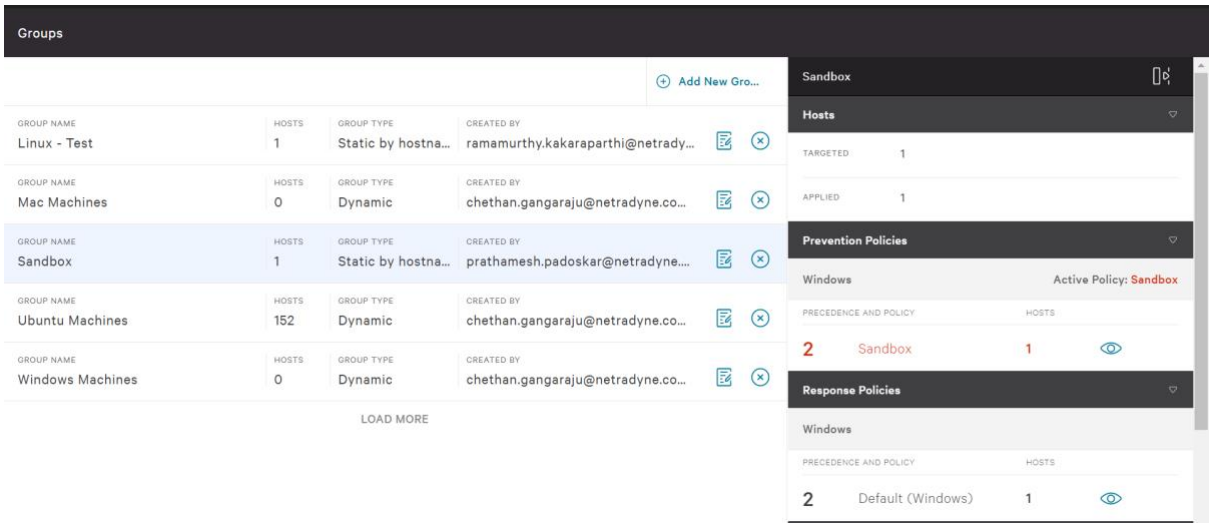
You can permanently remove a policy by deleting it. You must disable the policy before you can delete it.

- On the Settings tab, click Disable.
- Near the policy you want to delete, click Edit Policy.
- On the settings tab, click Delete.
- Click Delete policy

13.5 Verifying active policy

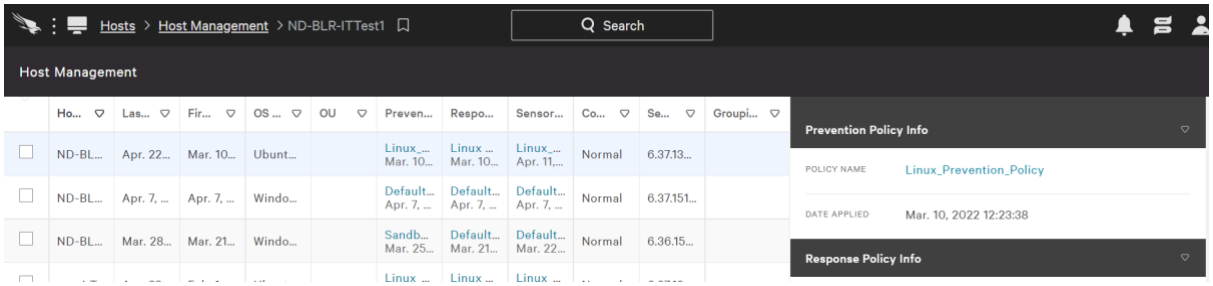
To ensure that the proper settings are applied to your hosts, check a group or host to verify the active policy.

Show a group’s policy precedence by going to Hosts > Groups and selecting the group’s row.



Alternatively, you can view a host’s applied policies by searching for it in Hosts > Host

Management. The active policies are listed in the columns to the right.



13.6 Quarantined files

On Windows and Mac hosts, the Falcon sensor can quarantine suspicious files based on your prevention policies. When the Falcon sensor detects a suspicious file attempting to run, the file is encoded, renamed, and moved into a quarantine directory on its host.

To use quarantining, you first enable it using a prevention policy. You can review and take action on quarantined files when monitoring detections.

- File location: Quarantined files are placed in a compressed file on the host in the quarantine directory:
  - Windows hosts: \Windows\System32\Drivers\CrowdStrike\Quarantine
  - Mac hosts: /Library/Application Support/CrowdStrike/Falcon/Quarantine
- File size: Files larger than 32MB are not quarantined.
- File retention:
  - Quarantined files are deleted from the host after 30 days. You can release files to prevent them from being deleted.
  - Quarantined files are deleted from the CrowdStrike cloud after 90 days.
- Quarantined files are deleted from the CrowdStrike cloud after 90 days.
- Prevention policies: If you disable the quarantining prevention policy on a host, no further files will be quarantined on that host. Any files that were previously quarantined remain quarantined.
- Uninstallation: If you uninstall the sensor, the quarantined files are deleted during uninstallation.
- Do not use quarantining on a host that uses other antivirus software. Unexpected behavior can result if multiple pieces of software attempt to quarantine the same file.
- Quarantining does not apply to the following:
  - Exploit Mitigation
  - Ransomware
  - Exploit Behavior
  - Lateral Movement on Credential access

13.7 Enabling quarantine

Enable or configure quarantining on hosts using prevention policies.

- Find the host's prevention policy in Configuration > Prevention Policies.
- Find the entry with a type of Next-Gen Antivirus and a category of Quarantine. Click Enable All.

14 Custom setting and configuration

14.1 Exclusions

If Falcon is showing detections that you don't want to see, or is preventing activity that you want to allow, you can create exclusions to quiet detections for known file paths and allow trusted processes to run.

Occasionally, Falcon might detect or prevent activity that you expect and allow in your environment. By creating exclusions, you can stop seeing detections that you don't want to see, and allow processes that would otherwise be prevented. The exclusions that you create effectively form an allowlist that explicitly defines your organization's known trusted activity.

You can create these types of exclusions:

Exclusion Type	Description	Events Logged?
Machine learning (ML) exclusion	For trusted file paths, stop all ML-based detections and preventions, or stop files from being uploaded to the CrowdStrike cloud.	Yes
Indicator of attack (IOA) exclusion	Stop all behavioral detections and preventions for an IOA that's based on a CrowdStrike-generated detection.	Yes
Sensor visibility exclusion	For trusted file paths that you want to exclude from sensor monitoring, minimize sensor event collection, and stop all associated detections and preventions. Use sensor visibility exclusions with extreme caution. Potential attacks and malware associated with excluded files will not be recorded, detected, or prevented.	Most events are not logged

14.1.1 Machine learning exclusions

For trusted file paths, reduce false-positive detections by creating machine learning exclusions. Define patterns to exclude files from detections or preventions derived from machine learning techniques:

- Stop static file-based detections and preventions, through ML-based techniques or custom hash blocklists
- Stop file uploads to the CrowdStrike cloud

A machine learning exclusion has three configurable parts:

- An exclusion pattern that defines a file path, name, or extension. Exclusion patterns are written in glob syntax.
- An exclusion type that defines the type of activity that you want to exclude. Choose one or both exclusion types:
    - Detect/Prevent
    - Upload Files to CrowdStrike
- A set of hosts that the exclusion applies to. Choose all hosts or select specific host groups.

14.1.2 Machine learning exclusions

Reduce false-positive detection alerts from IOAs by creating exclusions that stop behavioral IOA detections and preventions. You can create an IOA exclusion directly from a CrowdStrike-generated detection, or by duplicating and then modifying an existing IOA exclusion.

Most types of IOA detections can be excluded through the Falcon console. However, some types of detections (OverWatch detections, custom IOA detections, and some others) cannot be excluded.

Considerations for IOA Exclusions

IOA exclusions are created from within a detection, or by duplicating and then modifying an existing IOA exclusion.

You can exclude most types of IOA detections. However, the following types of detections cannot be excluded:

- OverWatch detections: For assistance with OverWatch detections, contact Support
- Custom IOA detections: To adjust these detections, modify the custom IOA instead
- Forced Address Space Layout Randomization (ASLR) bypass preventions
- Forced Data Execution Protection (DEP) preventions
- Heap Spray Preallocation preventions
- A small set of internal detection types

The Falcon console indicates whether you can exclude a specific IOA detection. If you want to exclude a detection that Falcon indicates cannot be excluded, open a Support case.

14.1.3 Machine learning exclusions

For trusted file paths that you want to exclude from sensor monitoring, sensor visibility exclusions minimize sensor event collection, and stop all associated detections and preventions.

Use sensor visibility exclusions with extreme caution. Potential attacks and malware associated with excluded files will not be recorded, detected, or prevented.

The most common reason to create a sensor visibility exclusion is to improve endpoint performance at the excluded file paths, where sensor event data collection might interfere with highly resource-sensitive tasks. When planning and configuring sensor visibility exclusions, balance performance and security considerations. We recommend using sensor visibility exclusions only on hosts for which the sensor’s performance overhead without exclusions is unacceptable, and we recommend choosing excluded paths with care.

Considerations for sensor visibility exclusions
Use sensor visibility exclusions with extreme caution. If you create a sensor visibility exclusion for a file path, Falcon won’t record all events, won’t report any detections, and won’t perform any prevention actions. This means that you won’t have visibility into potential attacks or malware related to that file path.

When planning and configuring sensor visibility exclusions, balance performance and security considerations. We recommend using sensor visibility exclusions only on hosts for which the sensor’s performance overhead without exclusions is unacceptable, and we recommend choosing excluded paths with care.

Before creating sensor visibility exclusions, consider the potential security risks. If you do create sensor visibility exclusions, we recommend following these best practices:

- Configure exclusions to be as narrow as possible. It's safer to exclude a single executable file than an entire folder or all subfolders.
- Avoid specifying file exclusions for built-in operating system executable files and folders, such as these:
    - bash, /sbin, /bin, /usr/bin
    - java, python, ruby

Additional sensor visibility exclusion considerations.

- The sensor minimizes event reporting for process executions that match file exclusion criteria.
- Processes that match file exclusion criteria will no longer generate the majority of events that would be seen otherwise, including process-related events.
- The sensor will continue to send EndOfProcess events on Windows and macOS.
- Process tree and file name are still captured, but SHA256 digest is not.
- For excluded processes, data will not be available in the following features and contexts:
    - Any app usage dashboard (for example, Falcon Discover)
    - Hash search (Falcon Investigate)
    - FDRv2 app info
- Excluding container-relative paths (and more generally, paths inside a chroot) is not supported.
- Currently, any Linux sensor visibility exclusions apply to both the host and all containers running on the system.

14.2 Planning your exclusions

Consider the potential implications of an exclusion before you put it into effect in your environment.

To maintain a strong security posture, create exclusions to be as specific as possible while meeting your exclusion needs. If your exclusion is too broad, you might inadvertently permit malicious activity that should be detected or blocked.

When you're creating or editing an exclusion, Falcon displays a list of affected detections before you save it. This list shows detections that wouldn't have been generated if the current exclusion were live in your environment. Previewing detections that you would no longer see helps you quickly understand the expected effect of an exclusion before you save it.

For IOA exclusions that are already in effect in your environment, you can view a log of activity that would have triggered a detection if an IOA exclusion hadn't been in place. Reviewing activity that's being excluded helps you understand the actual effects of your IOA exclusions.

CrowdStrike automatically records all changes to your exclusions. Each exclusion type has its own audit log where you can view the revision history for exclusions of that type. We recommend that you include a comment for the audit log whenever you create, edit, or delete an exclusion. In the audit log comment, include any info that would help other people in your organization understand what you changed and why. For example, when creating or editing an exclusion, include info about what activity was excluded and why.

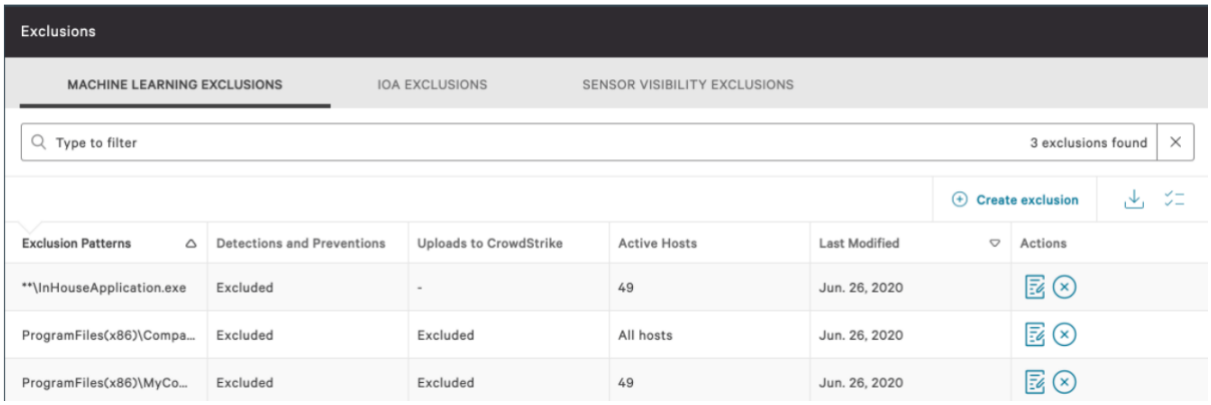
After you create, edit, or delete an exclusion, it can take up to 40 minutes for the changes to go into effect.

14.3. Managing machine learning exclusions

Getting to machine learning exclusions

The Machine Learning Exclusions tab is where you can view, create, edit, and delete ML exclusions, and where you can view the ML exclusion audit log. By default, the list of exclusions is sorted by Last modified.

- Go to Configuration > Detections Management > Exclusions, and then go to the Machine Learning Exclusions tab.

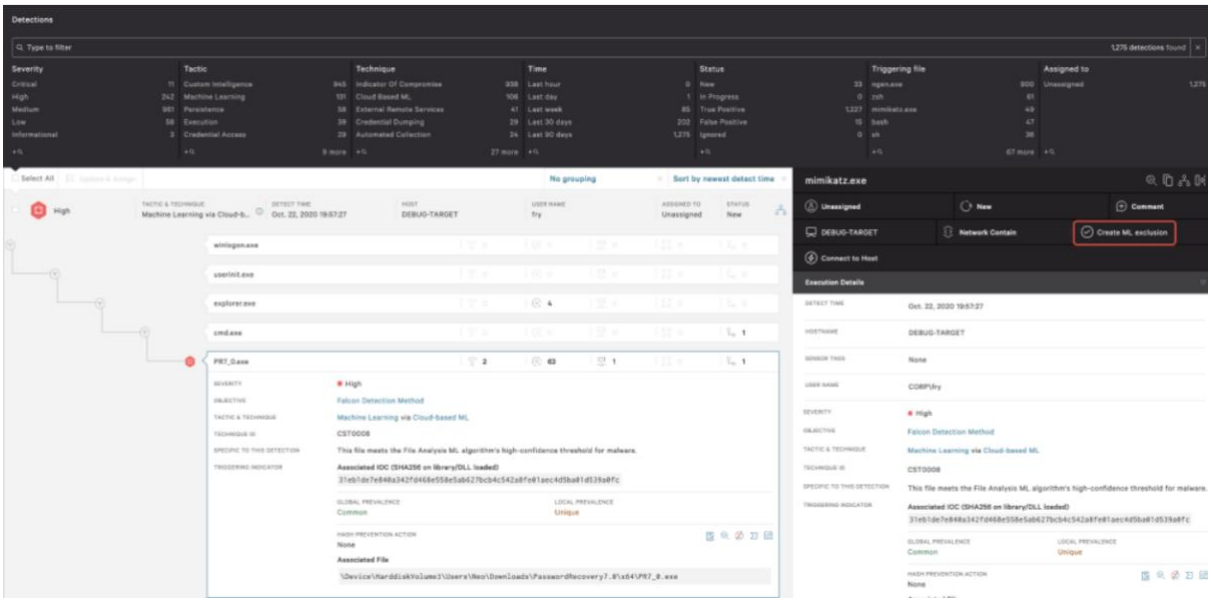


14.3.1 Creating machine learning exclusions

Create a machine learning exclusion from within a detection. The exclusion pattern is prepopulated based on the detection. Verify or change the pattern as needed before saving the exclusion.

Note: Alternatively, you can create a machine learning exclusion on the Machine Learning Exclusions tab on Configuration > Detections Management > Exclusions.

- On Activity > Detections, for the machine learning detection that you want to create an exclusion from, click to expand the detection's Summary.
- Click Create ML exclusion.

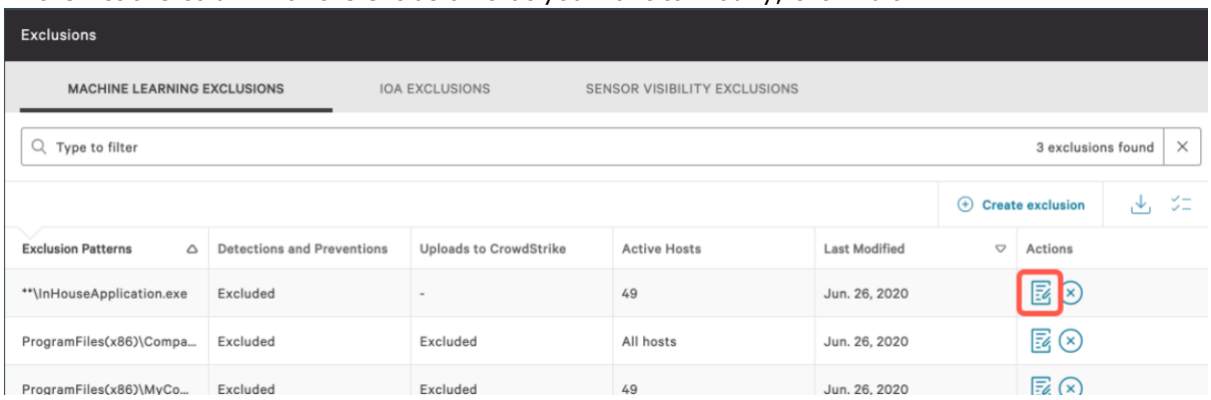


- In Create machine learning exclusion, select the host groups that the exclusion will apply to or select all hosts, and then click Next
- In the Excluded from list, select the actions to apply to the selected host groups:
    - Detections and preventions: Excludes files from ML-based detections and preventions.
    - Uploads to CrowdStrike: Excludes files from being uploaded to the CrowdStrike cloud.
- In the Exclusion pattern field, verify the prepopulated pattern value or enter a new pattern in glob syntax.
- Under Pattern test, test the exclusion pattern:
    - Type a file path, and then click Test pattern
    - Check the confirmation message to see whether your test pattern matches the syntax.
- Enter a comment to include in the audit log.
- If you want to add another exclusion pattern after you save this one, select Create another exclusion with these hosts after saving.
- Click Create.

14.3.2 Editing machine learning exclusions

Modify an existing exclusion to stop ML-based detections and preventions, or to stop file uploads to the CrowdStrike cloud, for a trusted file path.

- Go to Configuration > Detections Management > Exclusions, and then go to the Machine Learning Exclusions tab.
- In the Actions column for the exclusion that you want to modify, click Edit.

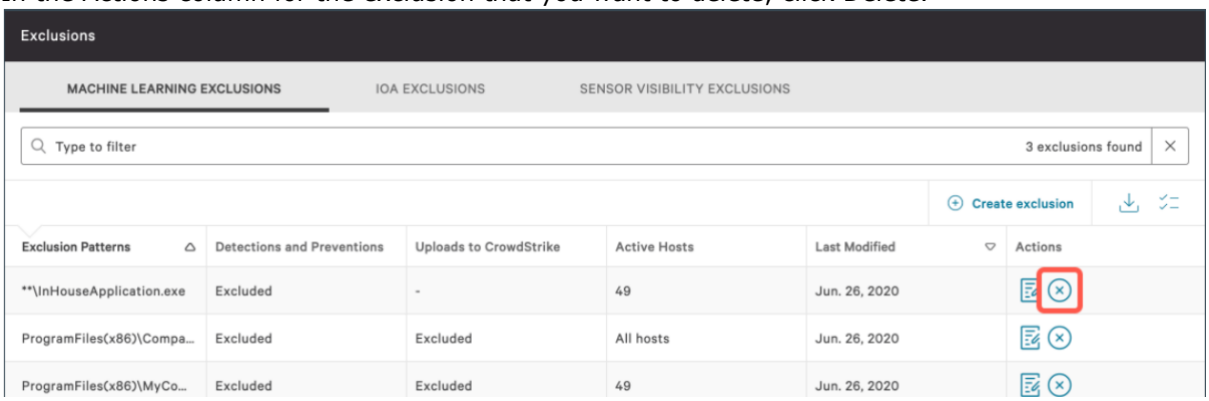


- In Edit machine learning exclusion, select the host groups that the exclusion will apply to, or select all hosts.
- In the Excluded from list, select the actions to apply to the selected host groups:
    - Detections and preventions: Excludes files from ML-based detections and preventions.
    - Uploads to CrowdStrike: Excludes files from being uploaded to the CrowdStrike cloud.
- In the Exclusion pattern field, enter an exclusion pattern in glob syntax.
- Enter a comment to include in the audit log.
- Under Pattern test, test the exclusion pattern:
    - Type a file path, and then click Test pattern.
    - Check the confirmation message to see whether your test pattern matches the syntax.
- If you want to add another exclusion pattern after you save this one, select Create another exclusion with these hosts after saving.
- Click Update.

14.3.3 Deleting machine learning exclusions

Delete exclusions with caution. A deleted exclusion cannot be recovered.

- Go to Configuration > Detections Management > Exclusions, and then go to the Machine Learning Exclusions tab.
- In the Actions column for the exclusion that you want to delete, click Delete.



- In Delete machine learning exclusion, review the list of changes that would apply if the exclusion were deleted.
- Enter a comment to include in the audit log.
- Click Delete exclusion.

14.4 Managing IOA exclusions

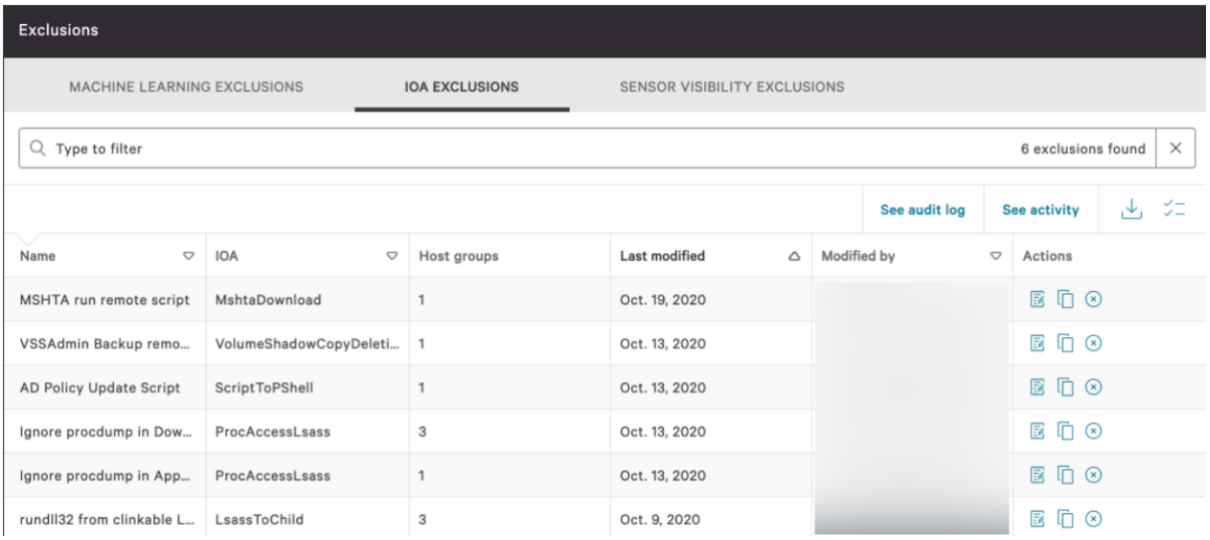
IOA exclusions are created from within a detection, or by duplicating and then modifying an existing IOA exclusion.

Getting to IOA exclusions

The IOA Exclusions tab is where you can view, edit, duplicate, and delete IOA exclusions, and where you can view the IOA exclusion audit log and activity log.

By default, the list of exclusions is sorted by Last modified.

Go to Configuration > Detections Management > Exclusions, and then go to the IOA Exclusions tab.

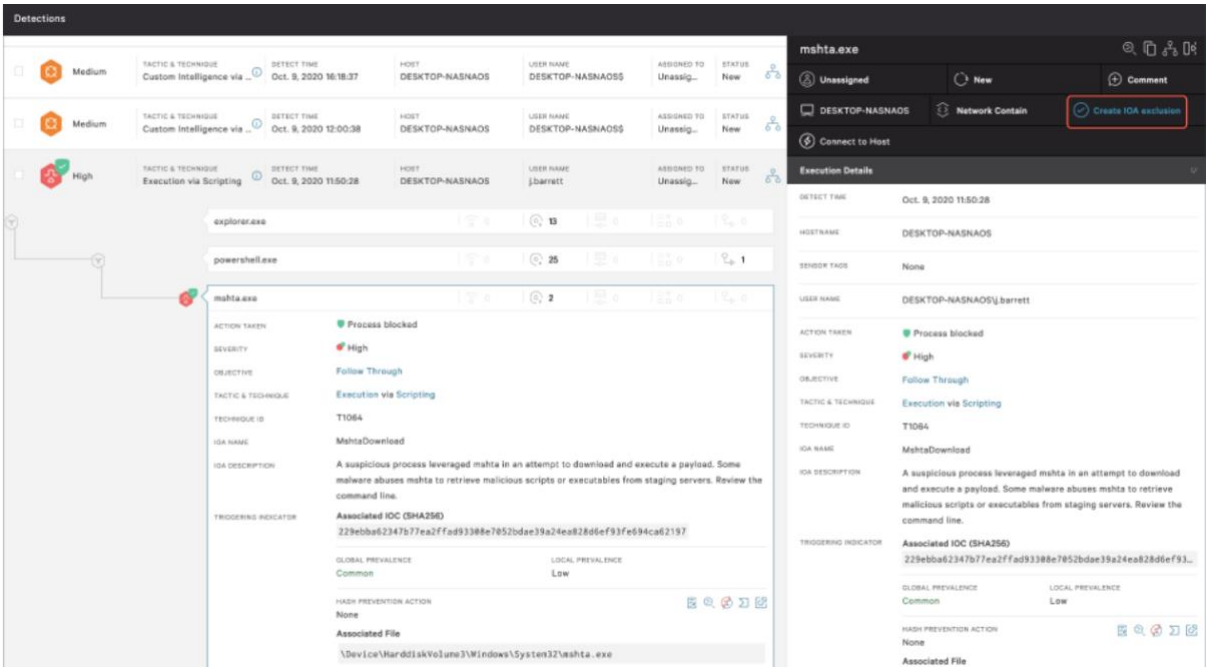


Note: IOA exclusions are created from within a detection, or by duplicating and then modifying an existing IOA exclusion.

14.4.1 Creating IOA exclusions

Add an IOA to your allowlist to reduce behavioral IOA detections and preventions. IOA exclusions are created from within CrowdStrike-generated IOA detections.

- On Activity > Detections, for the CrowdStrike-generated IOA detection that you want to create an exclusion from, click to expand the detection's Summary.
- Click Create IOA exclusion.



- In Create IOA exclusion, select the host groups that the exclusion will apply to, or select all hosts.
- Enter a name and a description for the exclusion.
- In the Image filename field, enter an exclusion pattern in regex format.
- Test the image filename pattern:
  - Type an image filename test string, and then click Test pattern.
  - Check the confirmation message to see whether your test pattern matches the syntax.
- In the Command line field, enter a command line value in regex format.
- Test the command line pattern:
  - Type a command line test string, and then click Test pattern.
  - Check the confirmation message to see whether your test pattern matches the syntax.
- Enter a comment to include in the audit log.
- Click Next.
- Carefully review the list of detections that wouldn't have appeared and associated processes that would have been allowed to run if the exclusion were already in place.
- Click Create exclusion.

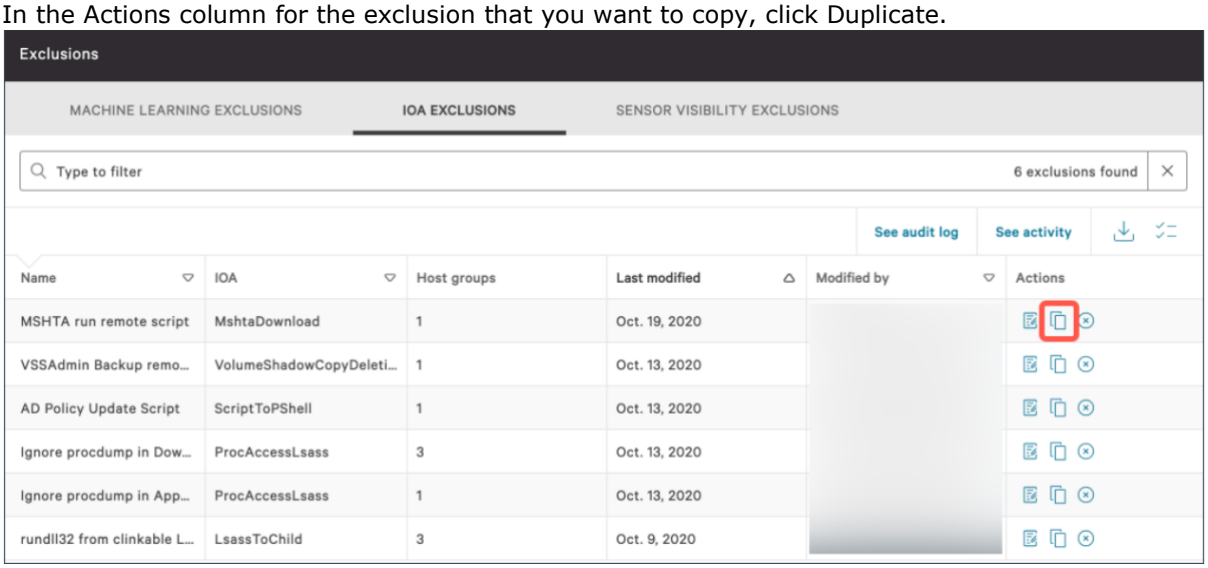
14.4.2 Duplicating IOA Exclusions

Create an IOA exclusion by duplicating an existing IOA exclusion and then modifying the new exclusion's settings. This enables you to create IOA exclusions without needing to start from within an IOA detection.

The fields in the duplicated exclusion are pre-populated with values from the source exclusion. Verify or change these values as needed before saving the new exclusion.

The IOA Name uniquely identifies the IOA pattern and can't be changed.

- Go to Configuration > Detections Management > Exclusions, and then go to the IOA Exclusions tab.
- In the Actions column for the exclusion that you want to copy, click Duplicate.



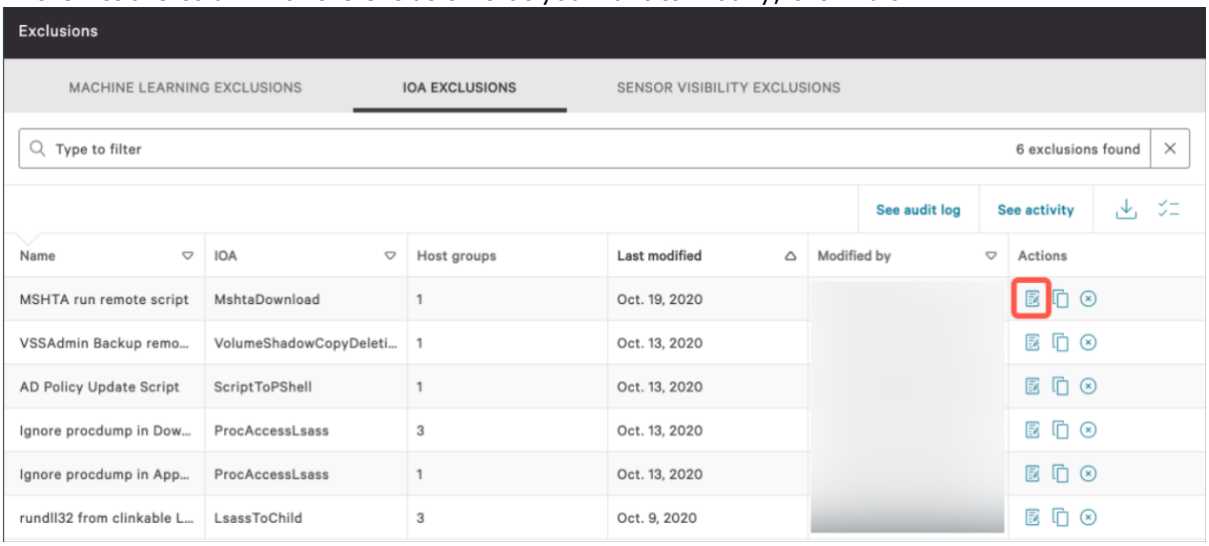
- In Duplicate IOA exclusion, select the host groups that the exclusion will apply to, or select all hosts.
- Enter a name and, optionally, a description for the exclusion.
- In the Image filename field, enter an exclusion pattern in regex format.
- Test the image filename pattern:
  - Type an image filename test string, and then click Test pattern.
  - Check the confirmation message to see whether your test pattern matches the syntax.
- In the Command line field, enter a command line value in regex format.
- Test the command line pattern:
  - Type a command line test string, and then click Test pattern.
  - Check the confirmation message to see whether your test pattern matches the syntax.
- Enter a comment to include in the audit log.
- Click Next.
- Carefully review the list of detections that wouldn't have appeared and associated processes that would have been allowed to run if the exclusion were already in place.
- Click Create exclusion.

14.4.3 Editing IOA Exclusions

Modify an existing IOA exclusion.

- Go to Configuration > Detections Management > Exclusions, and then go to the IOA Exclusions tab.

- In the Actions column for the exclusion that you want to modify, click Edit.



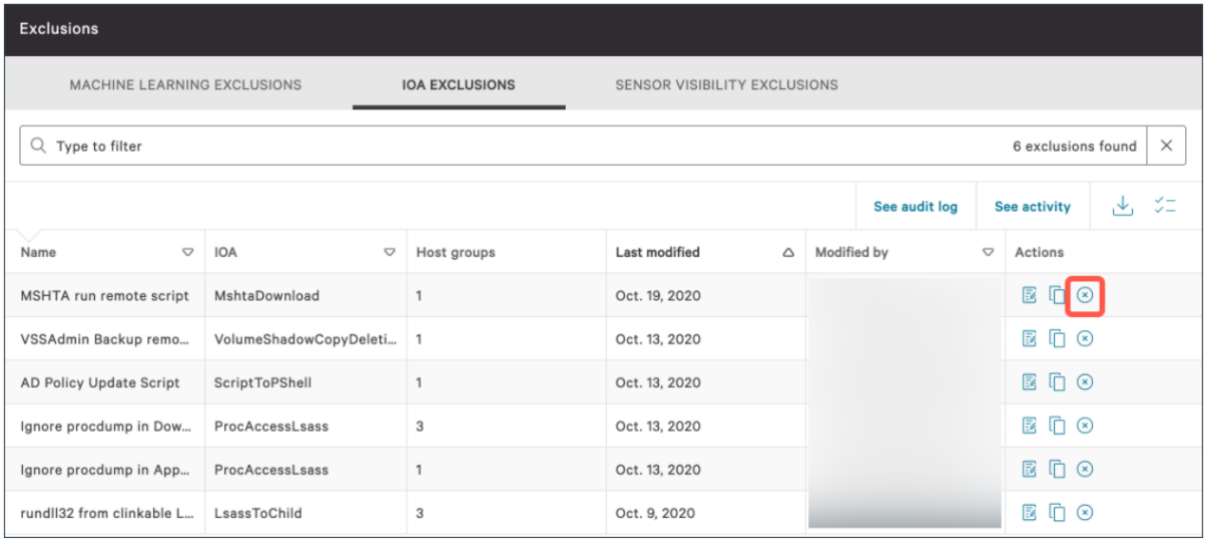
- In Edit IOA exclusion, select the host groups that the exclusion will apply to, or select all hosts.
- Enter a name and a description for the exclusion.
- In the Image filename field, enter an exclusion pattern in regex format.
- Test the image filename pattern:
    - Type an image filename test string, and then click Test pattern.
    - Check the confirmation message to see whether your test pattern matches the syntax.
- In the Command line field, enter a command line value in regex format.
- Test the command line pattern:
    - Type a command line test string, and then click Test pattern.
    - Check the confirmation message to see whether your test pattern matches the syntax.
- Type a command line test string, and then click Test pattern.Check the confirmation message to see whether your test pattern matches the syntax.
- Enter a comment to include in the audit log.
- Click Next.
- Carefully review the list of detections that wouldn't have appeared and associated processes that would have been allowed to run if the updated exclusion were already in place.
- Click Update.

14.4.4 Deleting IOA exclusion

Delete exclusions with caution. A deleted exclusion cannot be recovered.

- Go to Configuration > Detections Management > Exclusions, and then go to the IOA Exclusions tab.

- In the Actions column for the exclusion that you want to delete, click Delete.



- In Delete IOA exclusion, review the list of changes that would apply if the exclusion were deleted.
- Enter a comment to include in the audit log.

- Click Delete exclusion.

14.5 Managing sensor visibility exclusions

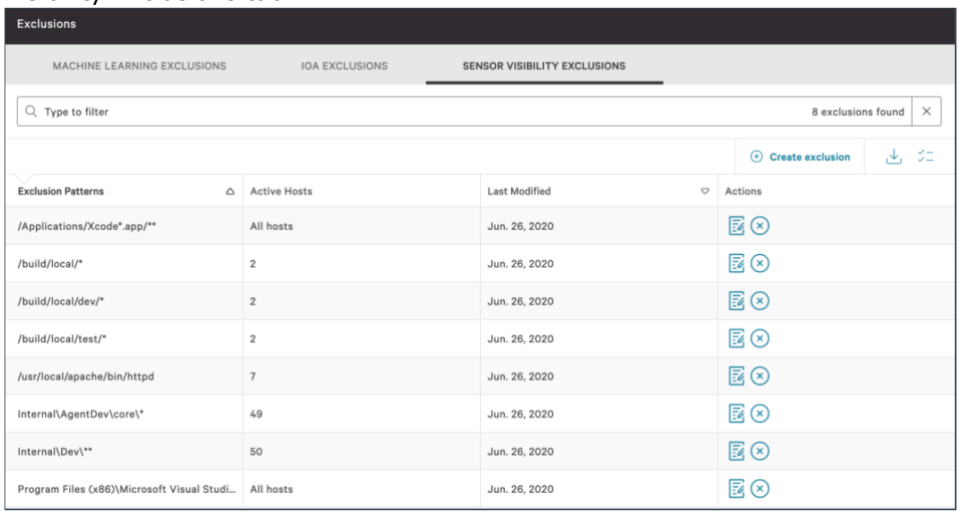
Use extreme caution and consider the potential security risks before creating sensor visibility exclusions.

Getting to sensor visibility exclusions

The Sensor Visibility Exclusions tab is where you can view, create, edit, and delete your sensor visibility exclusions, and where you can view the sensor visibility exclusion audit logs.

By default, the list of exclusions is sorted by Last modified.

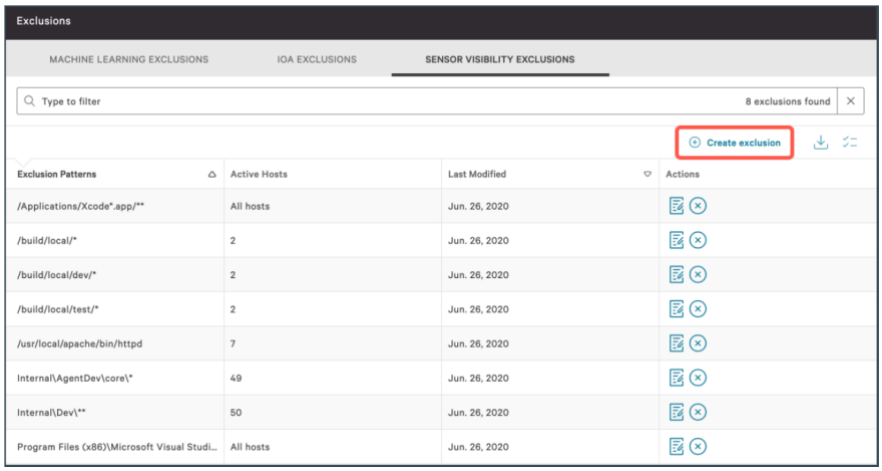
- Go to Configuration > Detections Management > Exclusions, and then go to the Sensor Visibility Exclusions tab.



14.5.1 Creating sensor visibility exclusions

Create an exclusion to stop sensor visibility, detections, and preventions for a trusted file path.

- Go to Configuration > Detections Management > Exclusions, and then go to the Sensor Visibility Exclusions tab.
- Click Create exclusion.



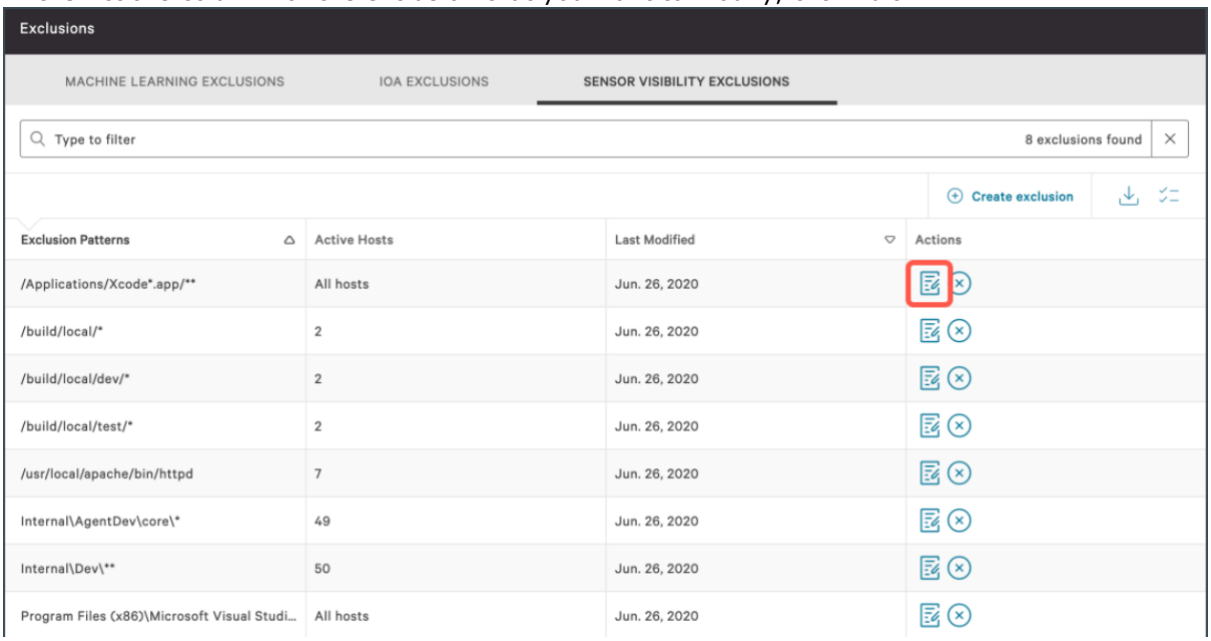
- In Create sensor visibility exclusion, select the host groups that the exclusion will apply to, or select all hosts.
- In the Exclusion pattern field, enter an exclusion pattern in glob syntax.
- Under Pattern test, test the exclusion pattern:
    - Type a file path, and then click Test pattern.
    - Check the confirmation message to see whether your test pattern matches the syntax.
- Enter a comment to include in the audit log.
- If you want to add another exclusion pattern after this one, select Create another exclusion with these hosts after saving
- Click Create exclusion, carefully review the summary of expected changes, and then click Confirm and Create.

14.5.2 Editing sensor visibility exclusions

Modify an existing sensor visibility exclusion.

- Go to Configuration > Detections Management > Exclusions, and then go to the Sensor Visibility Exclusions tab.

- In the Actions column for the exclusion that you want to modify, click Edit.



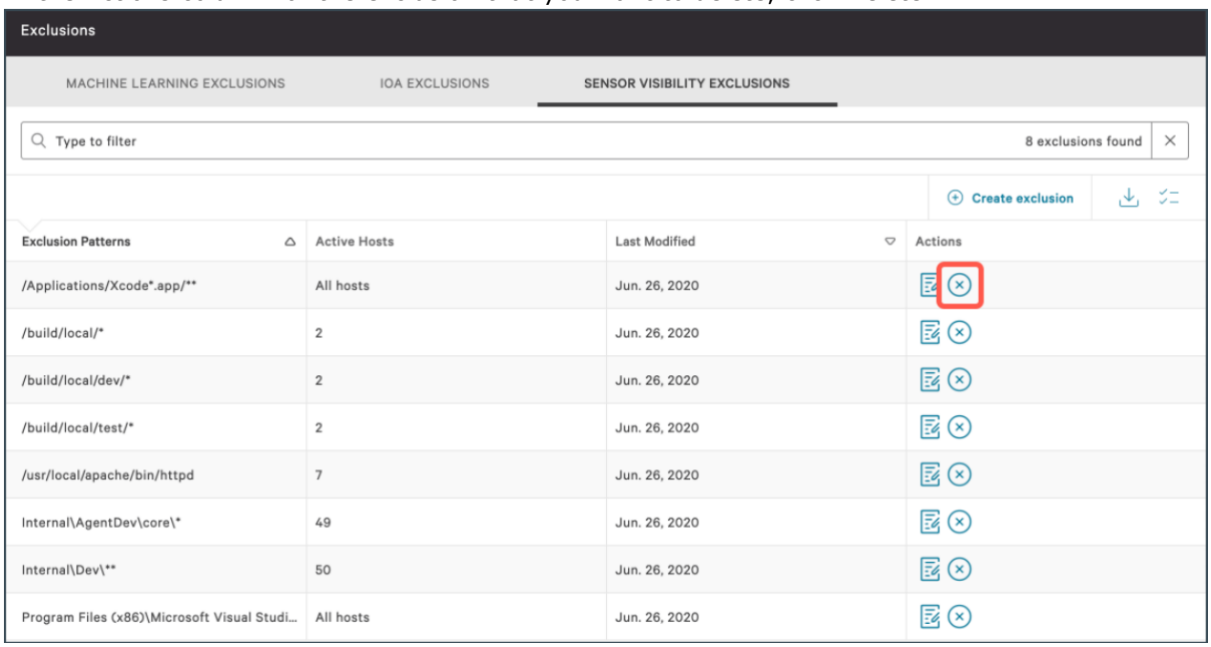
- In Edit sensor visibility exclusion, select the host groups that the exclusion will apply to, or select all hosts.
- In the Exclusion pattern field, enter an exclusion pattern in glob syntax.
- Under Pattern test, test the exclusion pattern:
    - Type a file path, and then click Test pattern
    - Check the confirmation message to see whether your test pattern matches the syntax.
- Enter a comment to include in the audit log.
- If you want to add another exclusion pattern after this one, select Create another exclusion with these hosts after saving.
- Click Update, carefully review the summary of expected changes, and then click Confirm and Update.

14.5.3 Deleting sensor visibility exclusions

Delete exclusions with caution. A deleted exclusion cannot be recovered.

- Go to Configuration > Detections Management > Exclusions, and then go to the Sensor Visibility Exclusions tab.

- In the Actions column for the exclusion that you want to delete, click Delete.

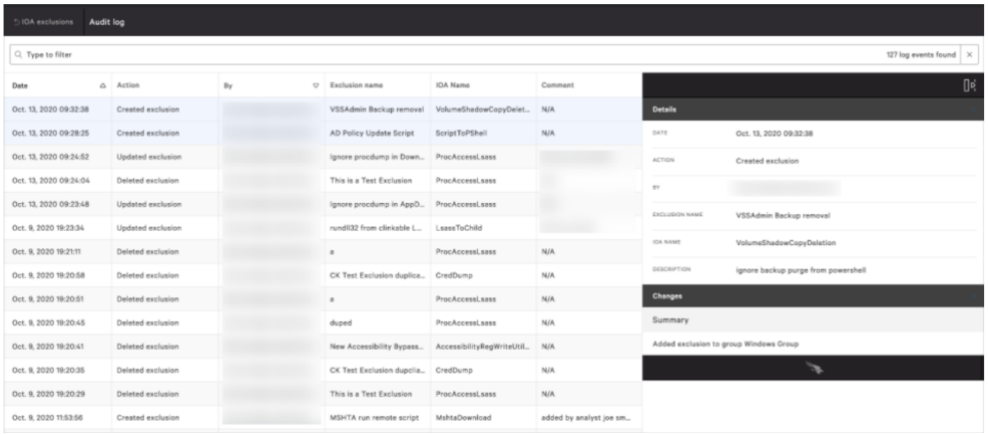


- In Delete sensor visibility exclusion, review the list of changes that would apply if the exclusion were deleted.
- Enter a comment to include in the audit log
- Click Delete exclusion.

14.6 Viewing exclusions audit logs

View the history of changes to your exclusions.

- Go to Configuration > Detections Management > Exclusions.
- On the applicable exclusions tab, click See audit log.
- Sort the columns to adjust your view of the log. In the Action column, logged revisions are defined as Created, Updated, or Deleted.
- Click any revision to see its Details summary.



15 Custom IOC

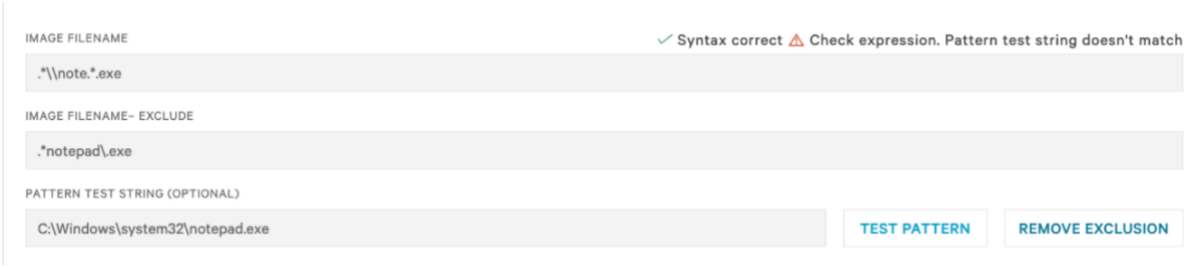
Add your own custom indicators of compromise (IOCs) to gain visibility, while adding false positives to your allowlist and adding executables to your blocklist for a tailored environment.

15.1 Understanding custom IOCs

Configure Falcon to observe custom IOCs in your environment, and specify what action the sensor will take when a matching IOC is observed on a host.

When you successfully add a value for a custom IOA and test it, confirmation appears in the UI.

If you add an exclusion to the rule, an error indicating that the test string no longer matches is shown.



Falcon provides detection capabilities for several types of custom IOCs.
These IOCs are supported for Windows, Mac, and Linux:

- Domain names
- IPv4 addresses
- IPv6 addresses
- SHA-256 hashes
- MD5 hashes

Custom IOCs can be used to add false positive detections to your allowlist, or to add applications to your blocklist to prevent their execution in your environment. It’s not necessary to upload lists of commodity malware or comprehensive lists of all known trusted files because Falcon already maintains comprehensive lists of those IOCs.

15.1 Managing custom IOCs

Getting to custom IOC

The IOC Management page is where you can view, add, edit, export, and delete custom IOCs, and where you can view the custom IOC audit log.

- Go to Configuration > Detections Management > IOC Management.

15.2 Adding custom IOCs

IOCs require certain metadata, and can include additional optional metadata. The Falcon console provides 2 methods for adding IOCs and IOC metadata:

- Manually specify IOC metadata values while adding IOCs.

- Import a file that already contains IOCs and their metadata values. This can be useful for importing previously exported IOCs that contain metadata, or for associating metadata to IOCs offline.

15.3 Adding Custom IOC without Metadata

Use this method to add one or more indicators without metadata.

You must add each type of indicator (hash, domain name, or IP address) separately. However, you can add multiple indicators of the same type in a single operation.

If you bulk-add a batch of indicators, your selected settings apply to all indicators in the batch. You can modify settings for a specific indicator later by editing just that individual indicator.

The specific settings available vary by indicator type.

- Go to Configuration > Detections Management > IOC Management, click the More options icon, and then click one of these options:
  - Add hashes
  - Add domains
  - Add IP addresses
- Click one of these options:
  - Upload: Upload a JSON or CSV file without metadata.
  - Manually add: Add indicators manually. Separate multiple indicators with commas or line breaks.
- Enter a descriptive comment about the indicators.
- Configure indicator settings as described in Custom IOC configuration fields.
- Enter a comment to include in the audit log.
- Click Add.
- Review any errors that were reported.
- If you specified a Block action for hashes, ensure that Custom Blocking is enabled on the Prevention Policies page.

15.4 Importing custom IOCs with metadata

Bulk-import custom IOCs with metadata, and specify the action to take when the sensor observes the indicators on hosts.
You can import any combination of indicator types (hashes, domains, or IP addresses) with metadata in a single CSV or JSON file.

- Go to Configuration > Detections Management > IOC Management, click the More options icon, and then click Import with metadata.
- Select the file that you want to upload.
- Enter a comment to include in the audit log.
- Click Import.
- Review any errors that were reported.
- If you specified a Block action for hashes, ensure that Custom Blocking is enabled on the Prevention Policies page.

15.5 Editing custom IOCs

If you bulk-edit a batch of indicators, your selected settings apply to all indicators in the batch.

Any changes that you make to an individual indicator are applied to only that indicator, and not to any other indicators that were originally added in the same batch.

The specific settings available vary by indicator type.

- Go to Configuration > Detections Management > IOC Management.
- Filter the results as needed, select the checkboxes for the indicators that you want to edit, and then click Edit selected indicators.
- Modify settings as described in Custom IOC configuration fields.
- If you're editing multiple types of indicators, click Next to modify the settings for each additional indicator type.

- Enter a comment to include in the audit log.
- Click Update indicators
- Review any errors that were reported.
- If you specified a Block action for hashes, ensure that Custom Blocking is enabled on the Prevention Policies page.

15.6 Deleting custom IOCs

Delete one or more indicators. After you delete a custom IOC, the Falcon console no longer displays future detections for that indicator in Activity > Detections.

- Go to Configuration > Detections Management > IOC Management.
- Select the checkboxes for the indicators that you want to delete, and then click Delete selected indicators.
- Enter a comment to include in the audit log
- Click Delete indicators.

15.7 Exporting custom IOCs

Export a list of indicators in CSV or JSON format.

- Go to Configuration > Detections Management > IOC Management. A full list of your custom IOCs appears.
- Refine the list of results as needed.
- Click Export, and then click either CSV or JSON. Falcon prepares the file for download.
- Click Download.

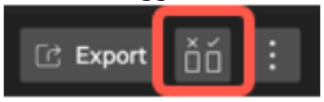
15.8 Viewing custom IOCs

View all your indicators, or refine the results through sorting, filtering, searching by keyword, or specifying which columns are visible.

The Last seen on value indicates when the IOC was last detected executing in your environment.

For IOCs that CrowdStrike migrated on behalf of customers before the deployment of the new IOC Management feature, the username shown is internal@crowdstrike.com.

- Go to Configuration > Detections Management > IOC Management. A full list of your custom IOCs appears.
- Refine the list of results as needed:
    - Apply filters:
        - Click a filter at the top of the list, or click More filters to see additional filtering options.
        - Select or clear the filter-specific metadata options, and then click Apply.
- Search by keyword:
    - Click Search indicators.
    - Type a keyword, and then click Apply.
- Specify which columns are visible:
    - Click the Toggle table columns icon.



    - Select the checkboxes for the columns that you want to see.
- Select the checkboxes for the columns that you want to see.

15.9 Viewing the custom IOC audit log

View the history of changes to your custom IOCs. The audit log lists changes made through both the Falcon console and the CrowdStrike API.

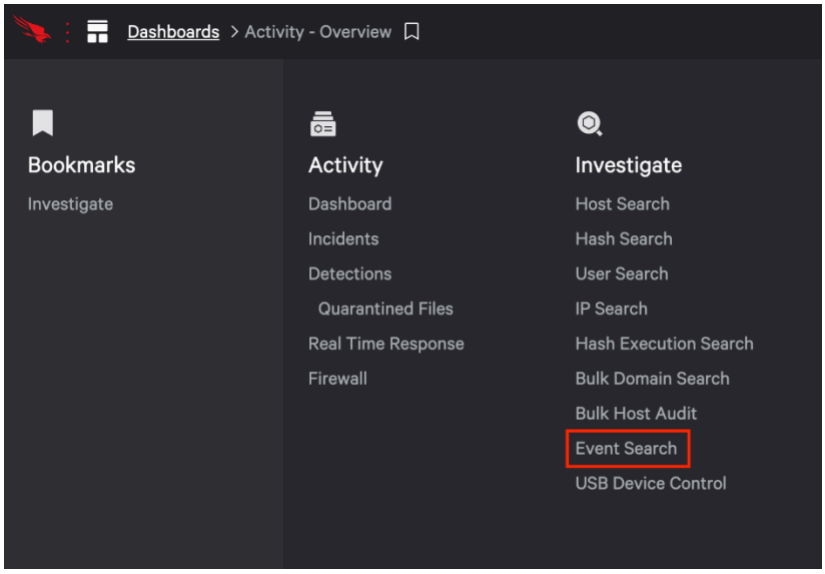
- Go to Configuration > Detections Management > IOC Management, click the More options icon, and then click See audit log
- Adjust your view by filtering or sorting the log entries.
- Click any revision to see additional details.

16 Hunting Scenarios

16.1 Normal Threat Hunt using Crowdstrike falcon

STEP / 01

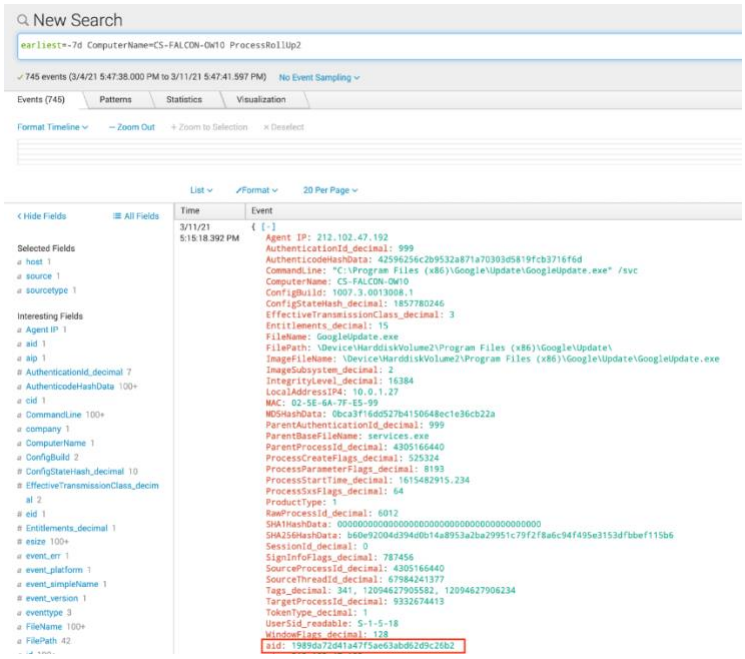
Open the Event Search page in the Investigate module.



STEP / 02

We'll start this search by looking at the events on a single host over the past week. In the search results we see a field in the events called aid this is a unique identifer for this host.

earliest=-7d ComputerName=CS-FALCON-OW10 ProcessRollUp2

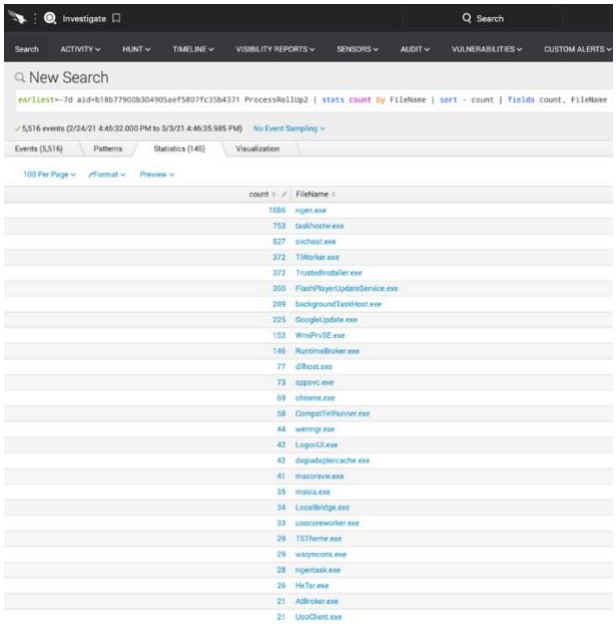


STEP / 03

Our search returned 100's of events, to organize the results we'll "pipe" the output to view the data in a table prioritized by count and filename.

For our next search we'll use the agent id or aid. Since this variable is more reliable than a hostname, we'll change the variable from ComputerName in our next search to use the aid.

earliest=-7d aid=1989da72d41a47f5ae63abd62d9c26b2 ProcessRollUp2 | stats count by FileName | sort - count | fields count, FileName

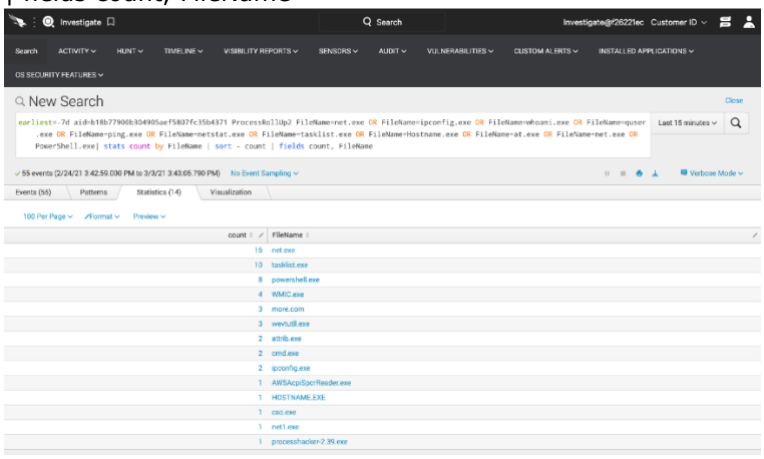


STEP / 04

We now have a list that's easier to read. Let's refine the search one more time to focus on applications often used by administrators but also by adversaries after breaching a system.

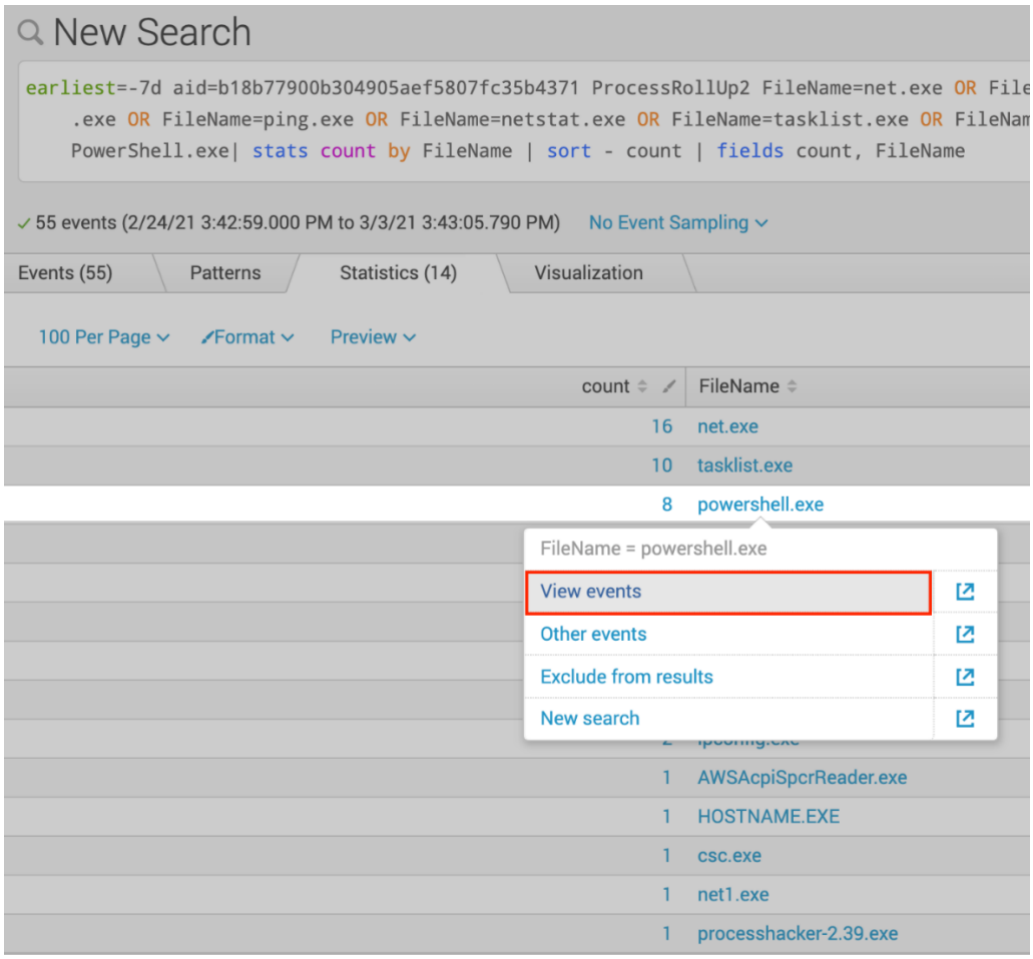
earliest=-7d aid=1989da72d41a47f5ae63abd62d9c26b2 ProcessRollUp2 FileName=net.exe OR FileName=ipconfig.exe OR FileName=whoami.exe OR FileName=quser.exe OR FileName=ping.exe

OR FileName=netstat.exe OR FileName=tasklist.exe OR FileName=Hostname.exe OR FileName=at.exe OR FileName=net.exe OR PowerShell.exe| stats count by FileName | sort - count | fields count, FileName



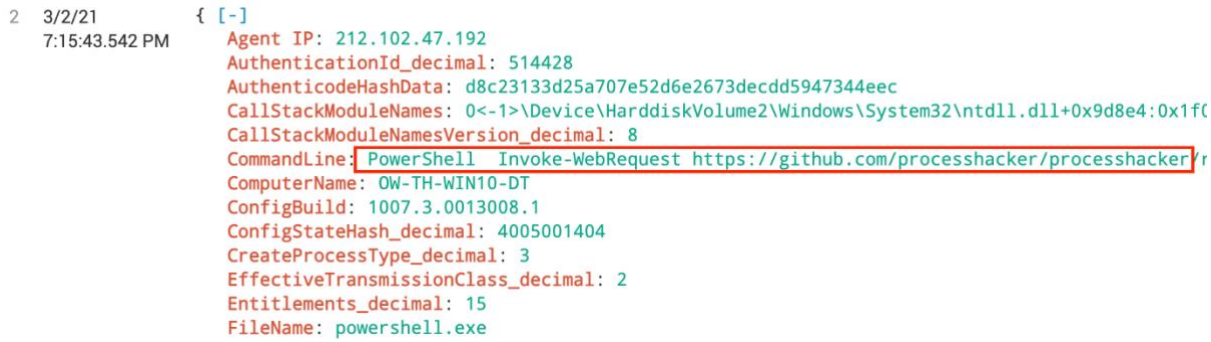
STEP / 05

We now have a list of applications that we can dig a bit more into. Let's investigate PowerShell.exe by clicking on 'powershell.exe' -> view events



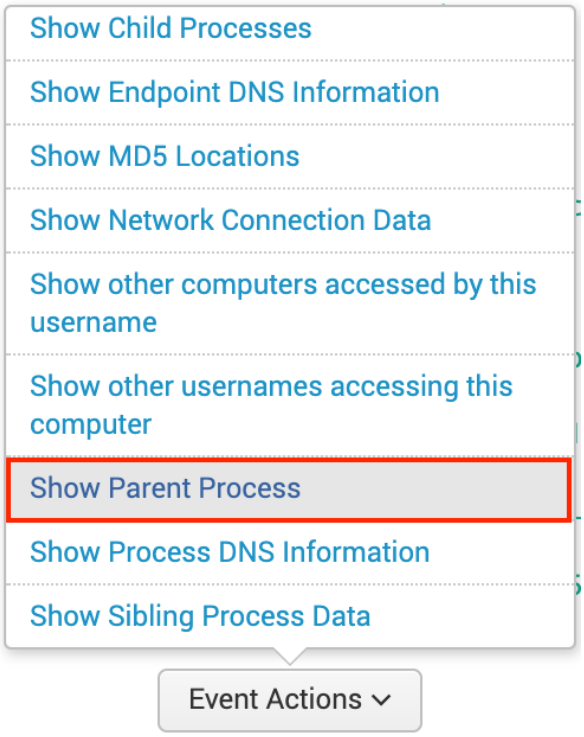
STEP / 06

We now have the events listed with all the individual event data. Scroll through the list until you see a PowerShell command that downloads a file from Github



STEP / 07

This PowerShell command is suspicious. To get a better idea of what's going on here we want to employ a standard threat hunting methodology of building out the process tree. Lucky for us, the Falcon Platform does this for us. To do this, scroll to the bottom of the event and click Event Actions find the Show Parent Process button and click it.



STEP / 08

The Parent Process of this PowerShell command is cmd.exe Let's keep walking up the process tree. Click Event Actions again and click the Show Parent Process option again.

```
Agent IP: 212.102.47.192
AuthenticationId_decimal: 514428
CallStackModuleNames:
0000000000000000000110100000000<-1>\Device\HarddiskVolume2\Windows
EAP:87:RWX-:REFLECTIVE:extension.dll:0xa148000]+0xa14806a|[HEAP:4
CallStackModuleNamesVersion_decimal: 8
CommandLine: C:\Windows\system32\cmd.exe
ComputerName: OW-TH-WIN10-DT
ConfigBuild: 1007.3.0013008.1
ConfigStateHash_decimal: 4005001404
CreateProcessType_decimal: 1
EffectiveTransmissionClass_decimal: 2
Entitlements_decimal: 15
FileName: cmd.exe
FilePath: \Device\HarddiskVolume2\Windows\SysWOW64\
```


STEP / 09

The Parent of CMD.exe is an encoded PowerShell Command. It's becoming obvious that this isn't typical administrator use of command line tools. Click the Show Parent Process option again to see what else we can learn.


```
{ [-]
   Agent IP: 212.102.47.192
   AuthenticationId_decimal: 514428
   CallStackModuleNames: 0<-1>\Device\HarddiskVolume2\Windows\System32\ntdll.dll+0x9d8e4
   CallStackModuleNamesVersion_decimal: 8
   CommandLine: "C:\Windows\syswow64\Windowspowershell\v1.0\powershell.exe" -noexit -e
JABtAG0APQAnAFsARABsAGwASQBtAHAAbwByAHQAKAAoACIAbQBzAHYAYwAiACsAIgByACIAKwAiAHQALgBkAGwA
   ComputerName: OW-TH-WIN10-DT
   ConfigBuild: 1007.3.0013008.1
   ConfigStateHash_decimal: 4005001404
   CreateProcessType_decimal: 1
   EffectiveTransmissionClass_decimal: 2
   Entitlements_decimal: 15
   FileName: powershell.exe
```

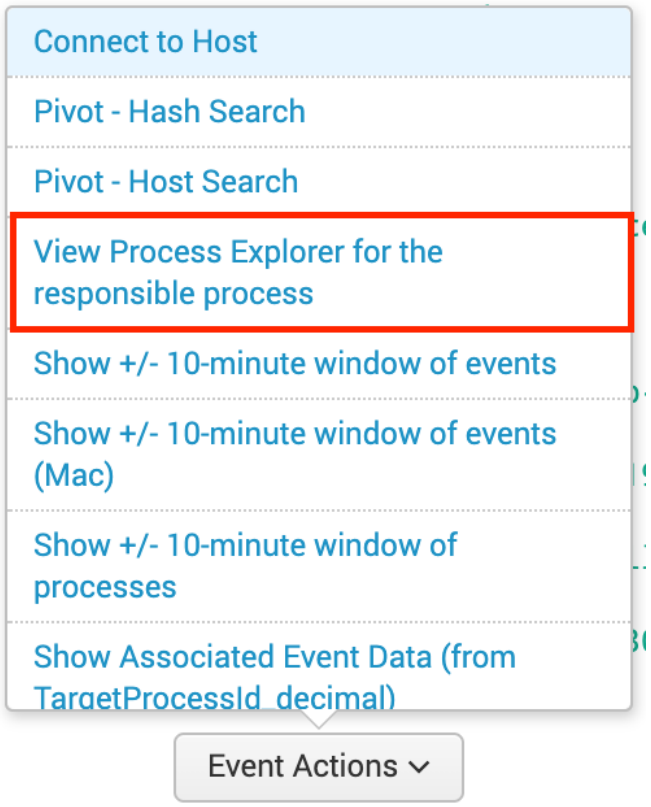

STEP / 10

In the next event we see that the parent process was another PowerShell process but looking closer we see that the GrandParent is WINWORD.exe

```
{ [-]
   Agent IP: 212.102.47.192
   AuthenticationId_decimal: 514428
   AuthenticodeHashData: 0544dd6168f52863ed9b9edde557dcab0aed289b
   CallStackModuleNames: 0<-1>\Device\HarddiskVolume2\Windows\System32\ntdll.dll+0x9d8e4:0x1f0000:(
   CallStackModuleNamesVersion_decimal: 8
   CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ec
JABXAG0APQAnACQAbQBtAD0AJwAnAFsARABsAGwASQBtAHAAbwByAHQAKAAoACIAbQBzAHYAYwAiACsAIgByACIAKwAiAHQALgB
   ComputerName: OW-TH-WIN10-DT
   ConfigBuild: 1007.3.0013008.1
   ConfigStateHash_decimal: 4005001404
   CreateProcessType_decimal: 1
   EffectiveTransmissionClass_decimal: 2
   Entitlements_decimal: 15
   FileName: powershell.exe
   FilePath: \Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\
   GrandParentBaseFileName: WINWORD.EXE
   ImageFileName: \Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
   ImageSubsystem_decimal: 3
   IntegrityLevel_decimal: 12288
   LocalAddressIP4: 10.0.1.27
   MAC: 02-5E-6A-7F-E5-99
   MD5HashData: cda48fc75952ad12d99e526d0b6bf70a
   ParentAuthenticationId_decimal: 514428
   ParentBaseFileName: powershell.exe
   ParentProcessId_decimal: 69188879031
   ProcessCreateFlags_decimal: 0
   ProcessParameterFlags_decimal: 24577
```

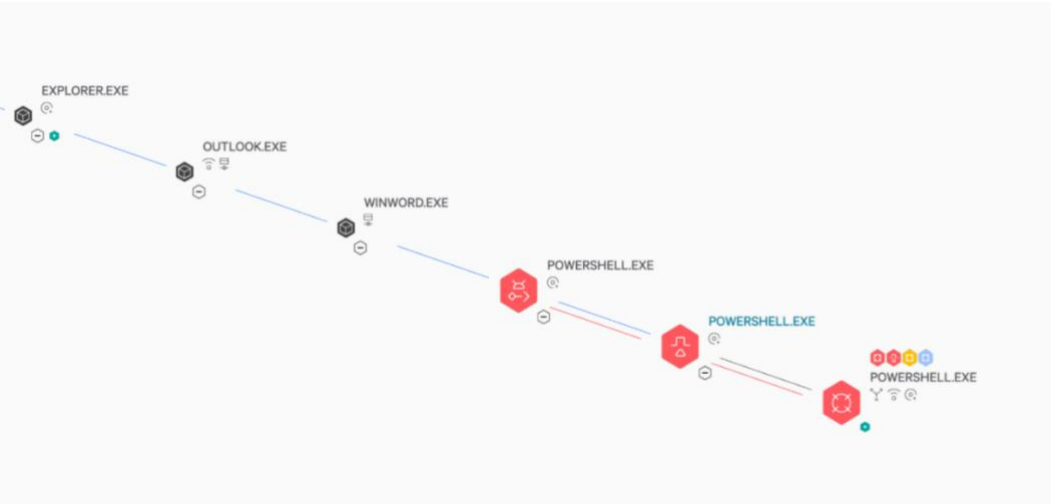

STEP / 11

At this point it would be useful to see the full process tree. Scroll to the bottom of the event and again click on Event Actions. Now this time click on View Process Explorer for the Responsible Process.



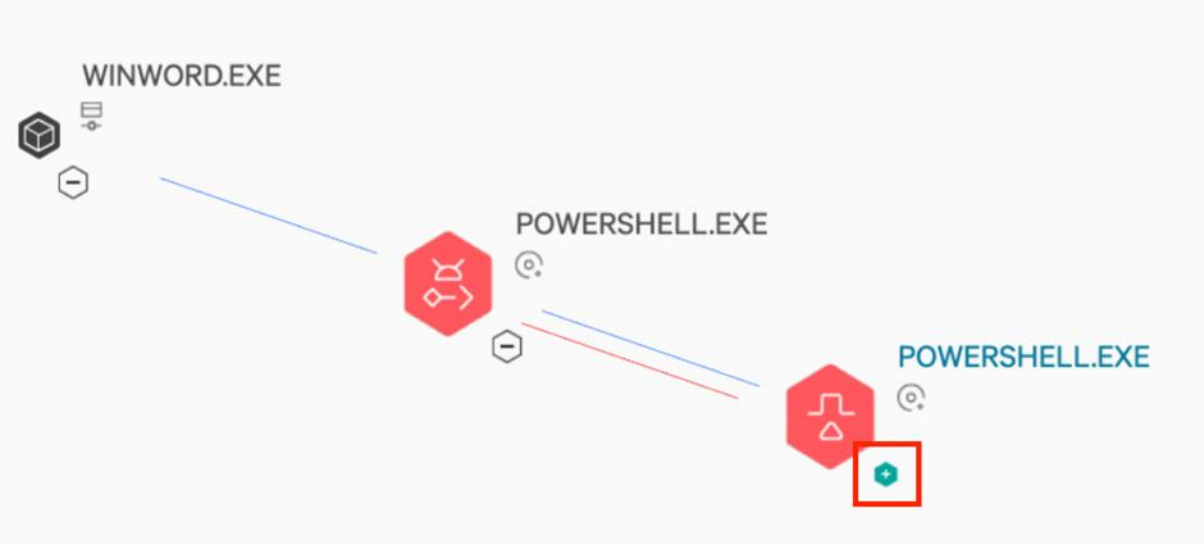
STEP / 12

The Falcon Console will build the process tree associated with these events. This is a powerful tool for analysts and threat hunters to get the visibility they need to really understand what's happening in their organization

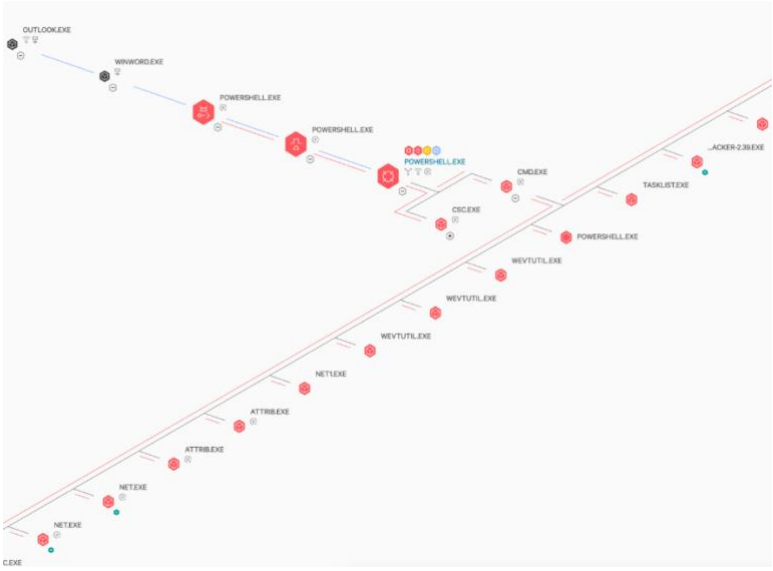


STEP / 13

To see even greater detail click the "+" icon on the last POWERSHELL.exe node in the process tree to see the full extent of this event.



Close inspection of this process tree illustrates what the adversary did. A malcious Word document was used to open PowerShell to launch Dharma ransomware. Falcon blocked the ransomware so the adversary establish persistence through the creation of a new user using the 'net' commands. We then see the use of processhacker and "WMIC" commands in an atttempt to uninstall the security software (which failed).

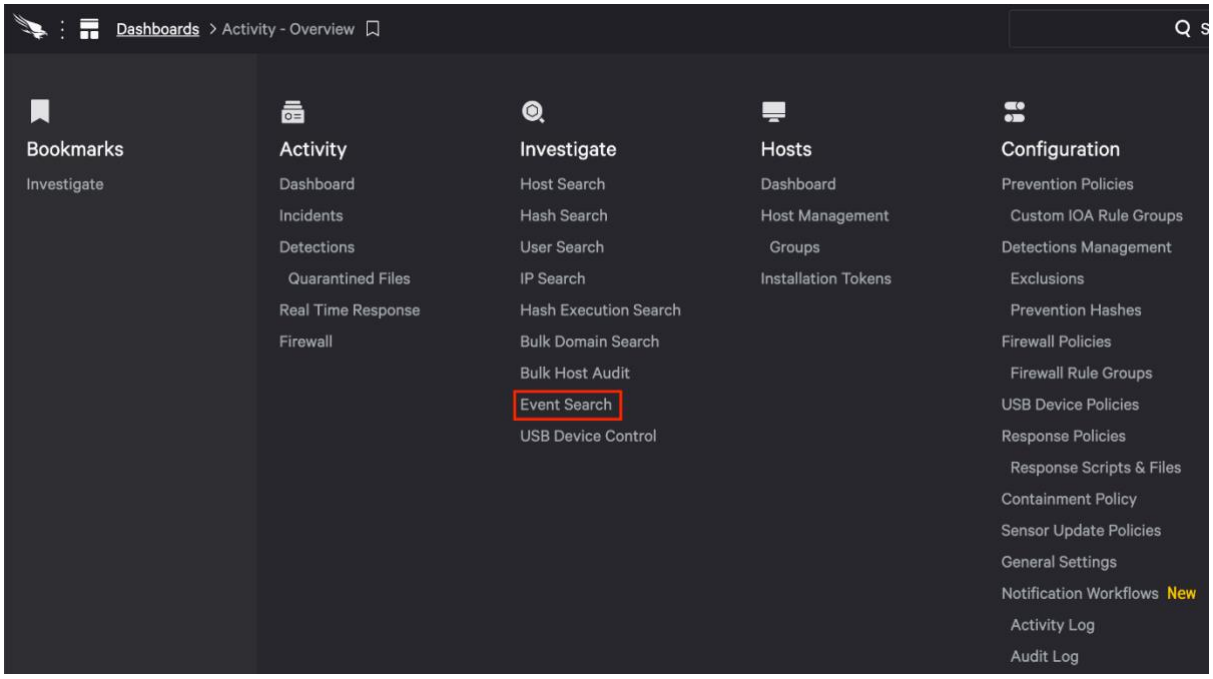


The event search empowers users to search and report on a large volume of data with a flexible, easy to use query language. However, sometimes there is no replacement for visualization and automation to save time when time matters most

16.2 Threat Hunting on Linux

STEP / 01

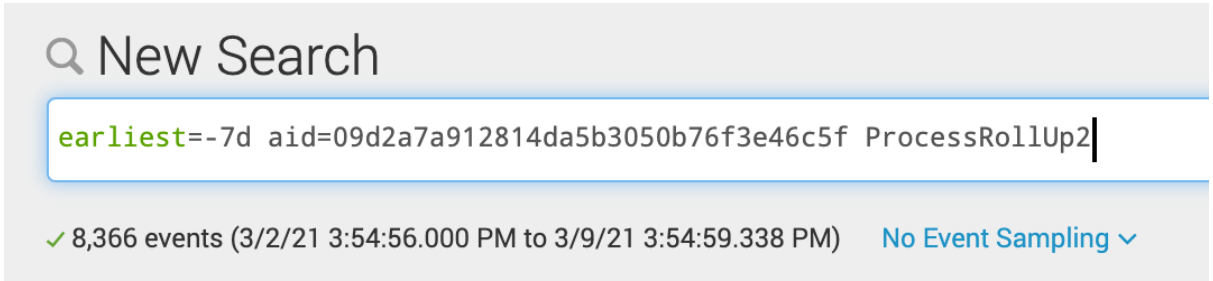
Open the Event Search page in the Investigate module.



STEP / 02

We'll start our search by looking at running processes on the Linux system in this environment. This command could be changed to shorten the time frame or add additional Linux systems, in our case we'll look at a single system over the last week.

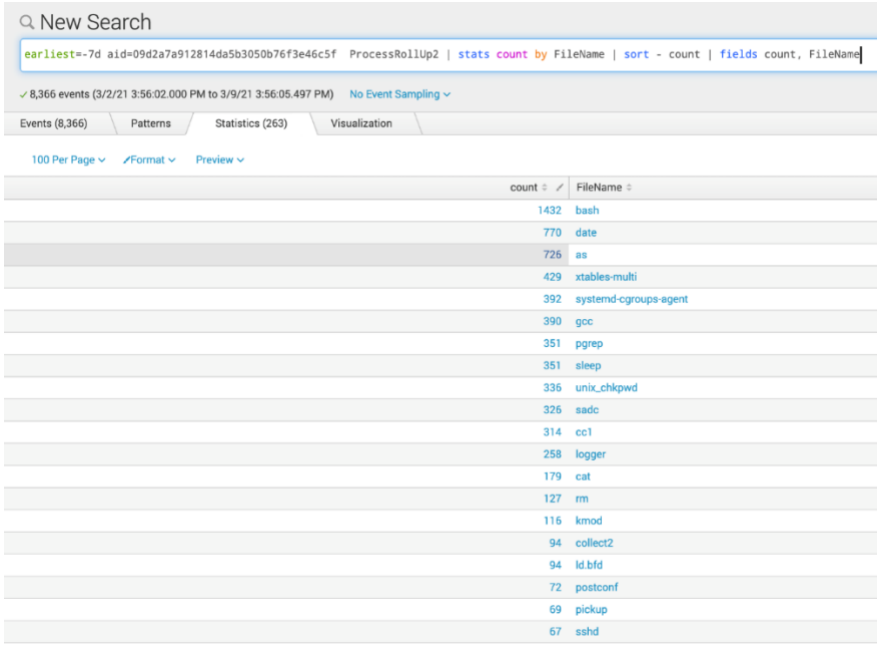
earliest=-7d aid=09d2a7a912814da5b3050b76f3e46c5f



STEP / 03

Our previous search gathers all the events that might be of interest, let's organize the results into a table view.

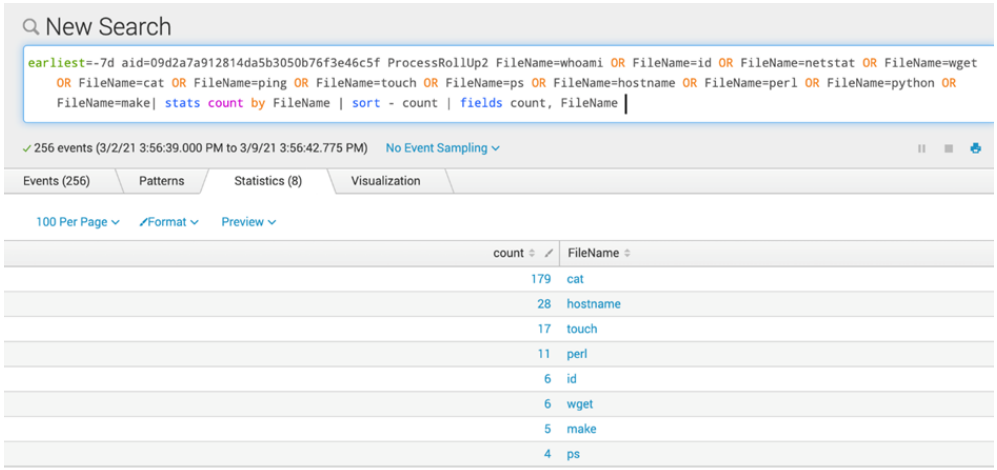
earliest=-7d aid=09d2a7a912814da5b3050b76f3e46c5f ProcessRollUp2 | stats count by FileName | sort - count | fields count, FileName



STEP / 04

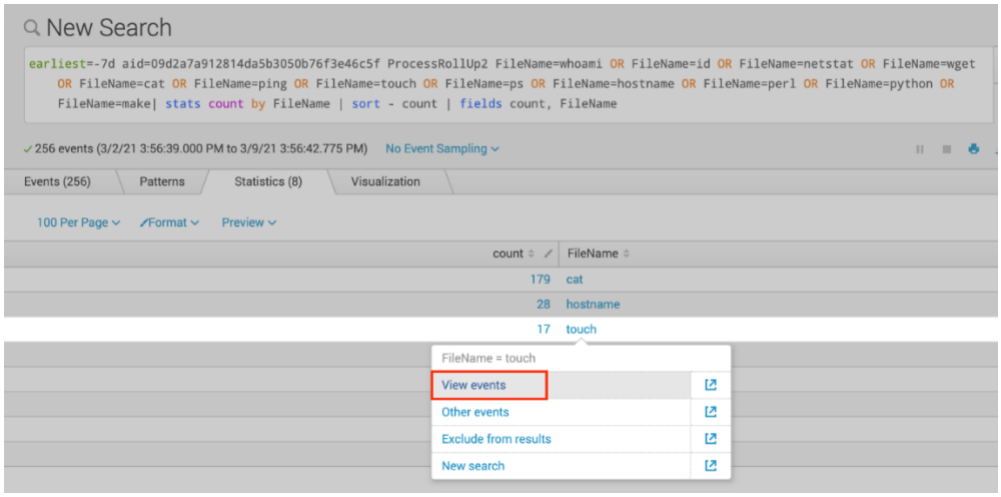
Hunting starts wide and then narrows down the search as we get more and more relevant data. While the table view is helpful to narrow in on applications that could potentially be used in an attack let's focus our search on specific filenames. Copy the new command and paste it into the Event Search field

earliest=-7d aid=09d2a7a912814da5b3050b76f3e46c5f ProcessRollUp2 FileName=whoami OR FileName=id OR FileName=netstat OR FileName=wget OR FileName=cat OR FileName=ping OR FileName=touch OR FileName=ps OR FileName=hostname OR FileName=perl OR FileName=python OR FileName=make| stats count by FileName | sort - count | fields count, FileName



STEP / 05

Once again the results have been narrowed down to a manageable list of potentially interesting commands. Let's investigate the 'touch' command. Click on the word touch then select view event



STEP / 06

The list of events has now been reduced to include only the 'touch' command used on a specific host over the last 7 days. Scroll through the list until you see a touch command that modifies a file related to SSH.

3/8/21
11:35:42.745 PM

{ [-]
Agent IP: 154.3.44.112
CommandLine: touch -r /usr/bin/ssh ./ssh
ComputerName: cs-falcon-th08
ConfigBuild: 1007.8.0011110.1
ConfigStateHash_decimal: 3640934996
EffectiveTransmissionClass_decimal: 2
Entitlements_decimal: 15
FileName: touch
FilePath: /usr/bin/
GID_decimal: 0
ImageFileName: /usr/bin/touch
LocalAddressIP4: 172.17.0.1
MAC: 02-42-8A-4C-E5-97
MD5HashData: bebedf5ac2c220d69fb80c366a7cbbab
ParentBaseFileName: bash
ParentProcessId_decimal: 56851787811
ProcessEndTime_decimal: 1615246542.369
ProcessGroupId_decimal: 56851787811
ProcessStartTime_decimal: 1615246542.367

STEP / 07

This touch command is suspicious. We see that the file ssh was referenced and then the -r switch was used. The -r switch is often used to change the date a file was last accessed or modified. Why would someone want to change or modified the date associated with this file?

To get a better idea of what's going on we want to employ a standard threat hunting methodology of building out the process tree. Lucky for us, the Falcon Platform does this for us. To do this, scroll to the bottom of the event and click Event Actions find the Show Parent Process button and click it

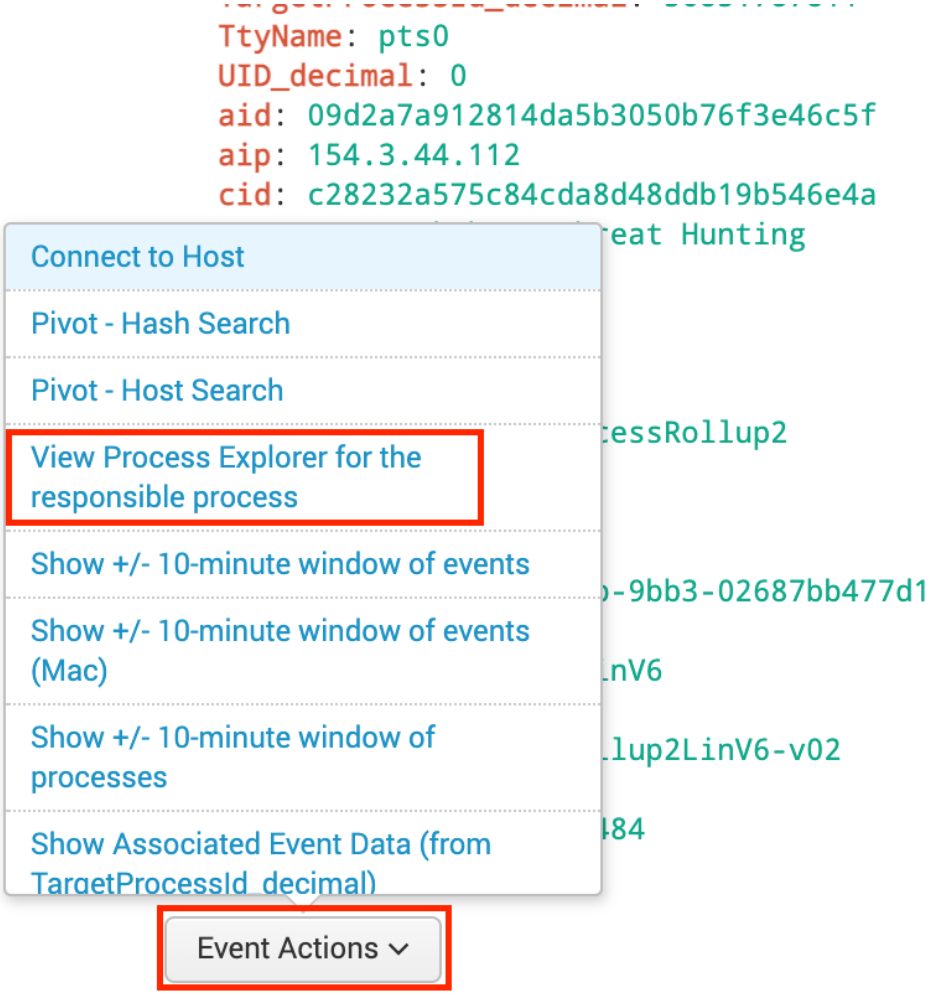
STEP / 08

The Parent Process of the touch command is bash. What else happened inside this bash process tree? What other commands were run in the session

Time	Event
3/8/21 11:18:08.484 PM	{ [-] Agent IP: 154.3.44.112 CommandLine: bash ComputerName: cs-falcon-th08 ConfigBuild: 1007.8.0011110.1 ConfigStateHash_decimal: 2401818837 EffectiveTransmissionClass_decimal: 2 Entitlements_decimal: 15 FileName: bash FilePath: /usr/bin/ GID_decimal: 0 ImageFileName: /usr/bin/bash

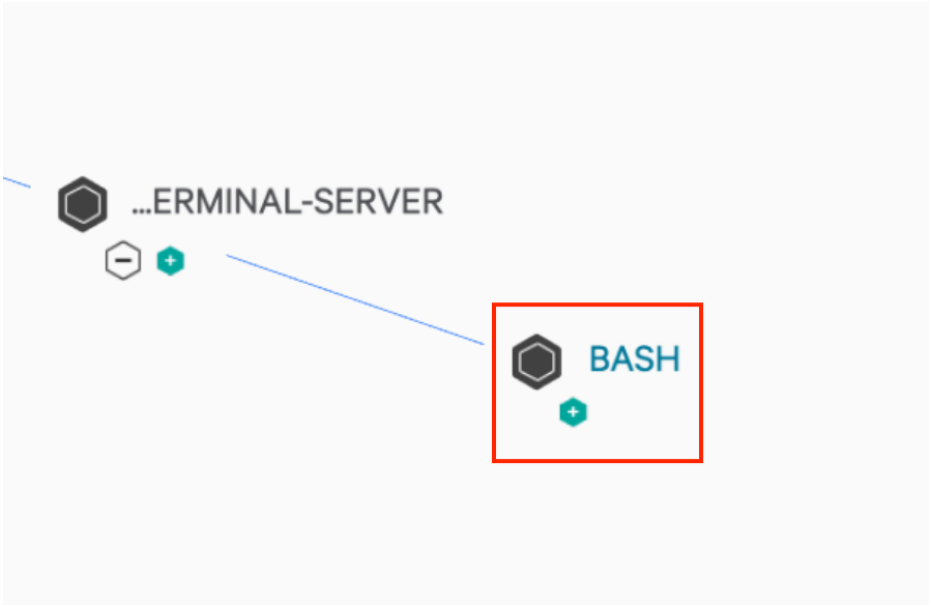
STEP / 09

At this point it would be useful to see the full process tree. Scroll to the bottom of the event and again click on Event Actions. Now this time click on View Process Explorer for the Responsible Process.



STEP / 10

The bash process is now displayed in a process tree but there is so much more here. Click the "+" icon to view the full list of commands used in this attack.



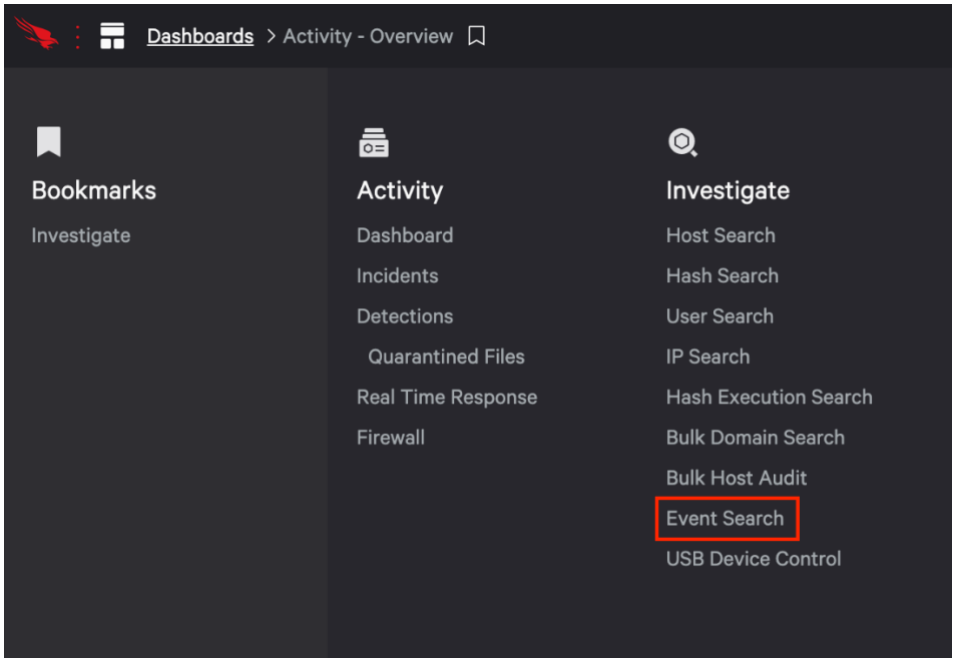
Close inspection of this process tree illustrates what the adversary did. 'wget' was used to download files from the internet and the 'gcc' and 'make' commands show that they compiled a new version of SSH. The initial touch command we saw was then used to modify the new SSH binary and assign it the same time stamp as the original SSH binary on the system. This hides the fact that the new SSH binary was freshly created.

These commands aren't rare or uncommon, admins use them every day in the course of their tasks. Having OverWatch as part of the team to distinguish between legitimate and malicious commands was the differnce between a breach and a prevention.

16.3 Web Shells

STEP / 01

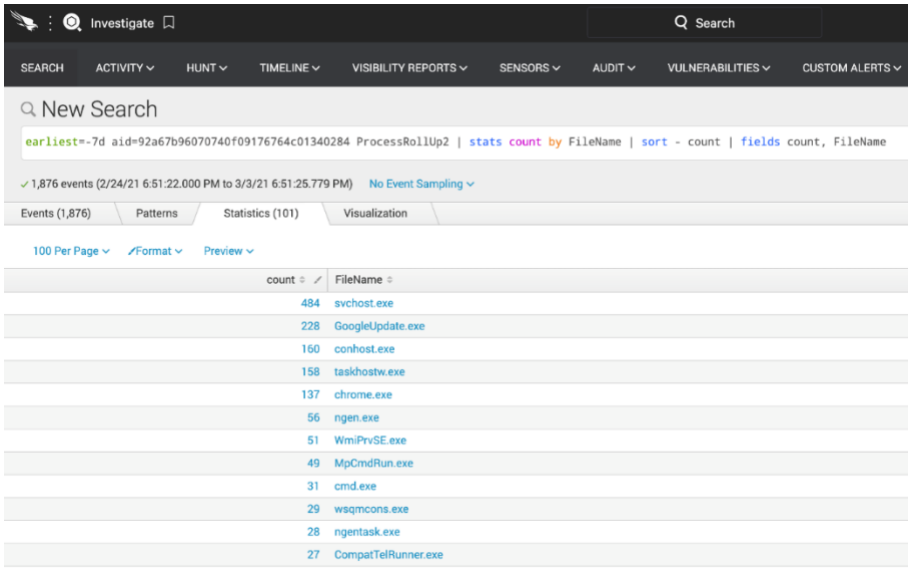
Open the Event Search page in the Investigate module.



STEP / 02

Threat hunting on servers can bring a whole different set of variables. However the methodology is still the same start wide and look for suspicious or anomalous events. We'll start this search by looking at a table view of the events on a server over the past week.

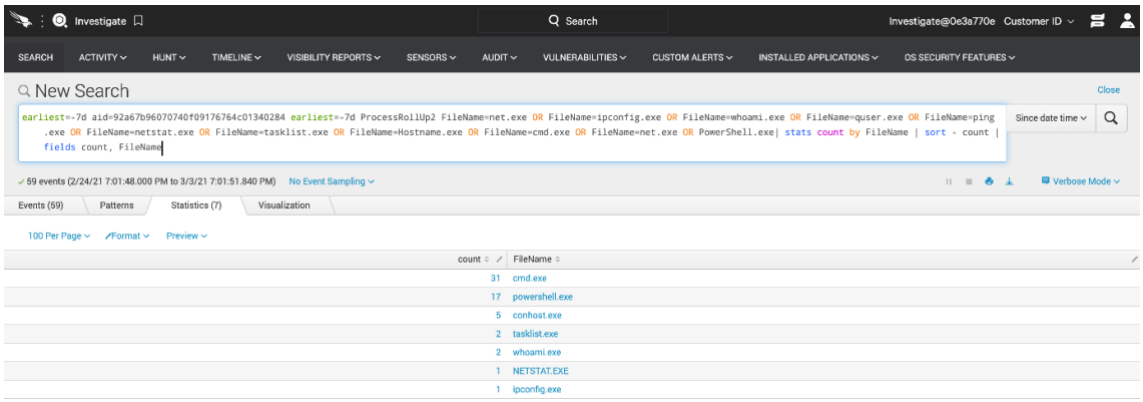
earliest=-7d aid=e119e1b6e95048ce9e5ca50bddee856f ProcessRollUp2 | stats count by FileName | sort - count | fields count, FileName



STEP / 03

Let's reduce the applications to those that are often associated with admin tool usage or suspicious activity. This search could also be really helpful on a desktop search to find anomalous behavior.

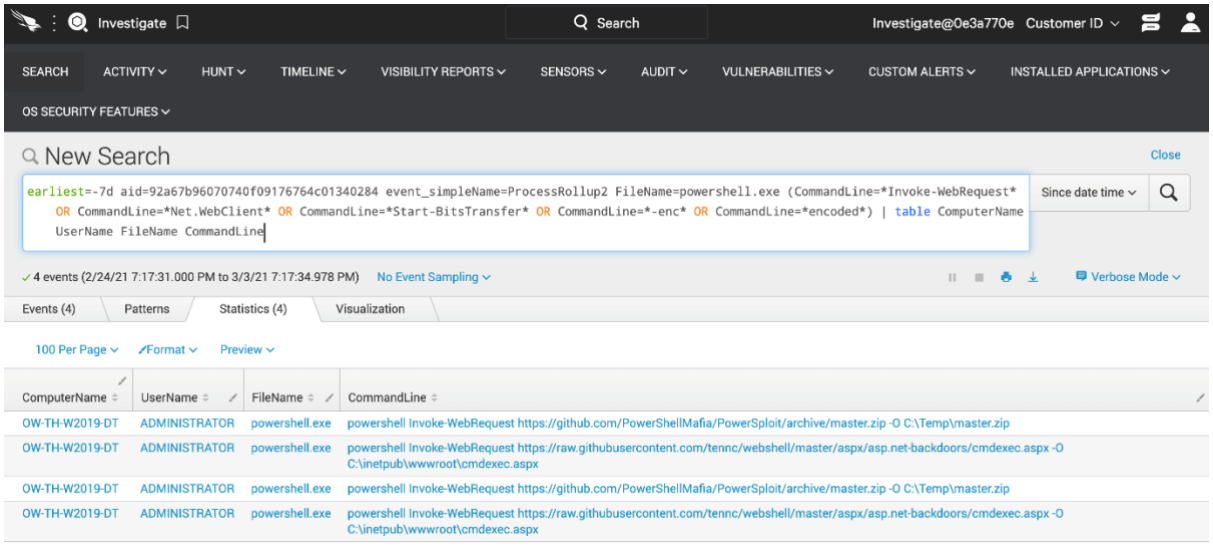
earliest=-7d aid=e119e1b6e95048ce9e5ca50bddee856f earliest=-7d ProcessRollUp2 FileName=net.exe OR FileName=ipconfig.exe OR FileName=whoami.exe OR FileName=quser.exe OR FileName=ping.exe OR FileName=netstat.exe OR FileName=tasklist.exe OR FileName=Hostname.exe OR FileName=cmd.exe OR FileName=net.exe OR PowerShell.exe| stats count by FileName | sort - count | fields count, FileName



STEP / 04

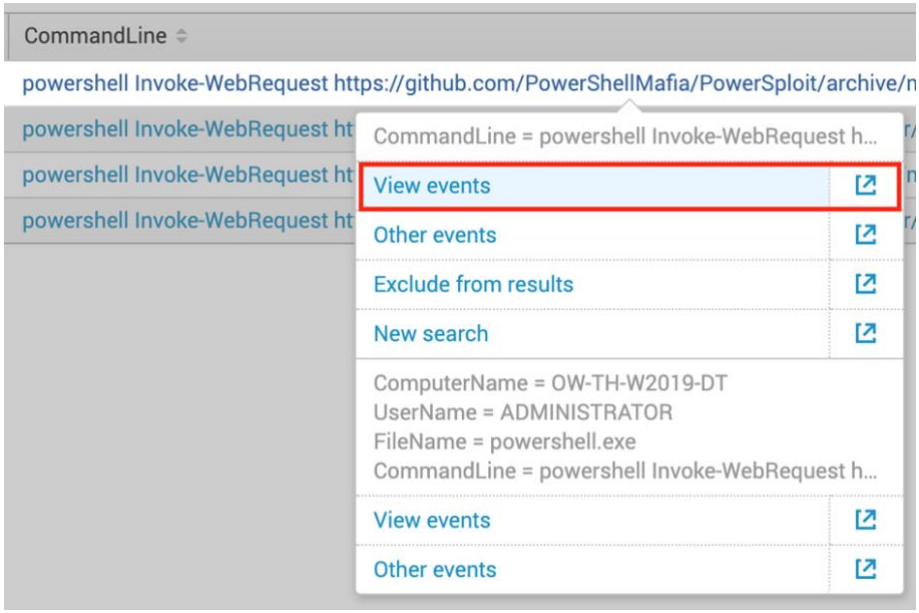
We have a pretty high count of CMD and PowerShell being run. Since this is a server it could be legitimate. Let's explore different ways to change this search so that we can more easily see suspicious use of PowerShell. We'll modify this search to see if PowerShell has been used to download files or run encoded commands

earliest=-7d aid=e119e1b6e95048ce9e5ca50bddee856f event_simpleName=ProcessRollup2 FileName=powershell.exe (CommandLine=*Invoke-WebRequest* OR CommandLine=*Net.WebClient* OR CommandLine=*Start-BitsTransfer* OR CommandLine=*-enc* OR CommandLine=*encoded*) | table ComputerName UserName FileName CommandLine



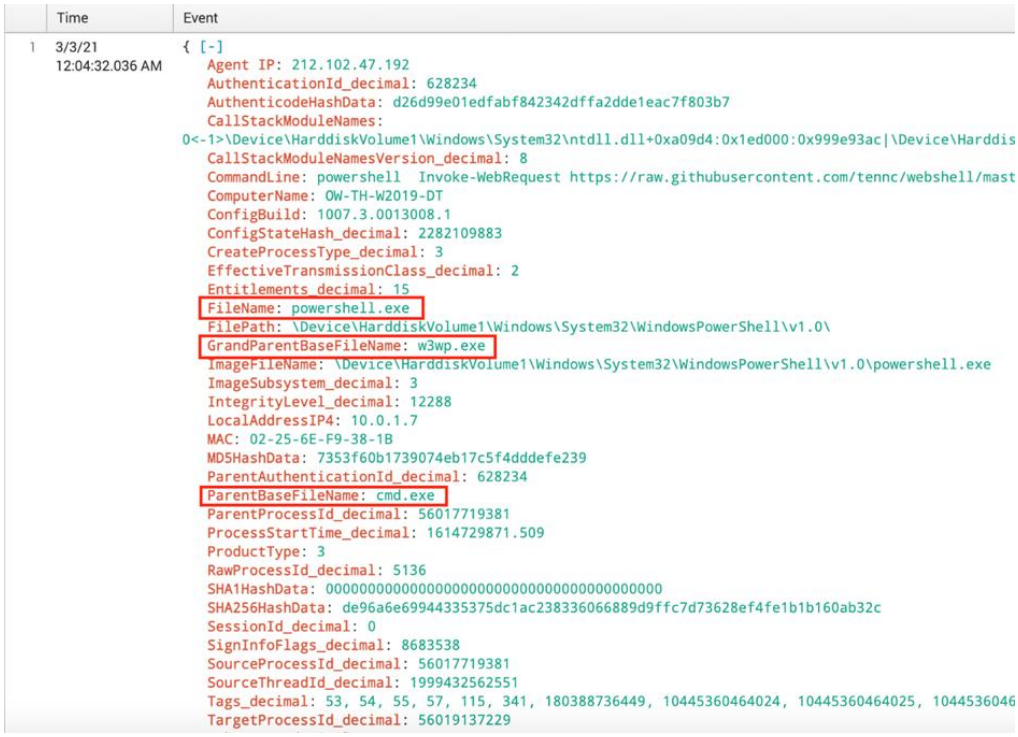
STEP / 05

We have now narrowed down our search to a couple of results that don't look like standard admin usage commands. To dig deeper click on the CommandLinesection of the PowerShell event associated with the download of the .aspx file. In the menu click View events



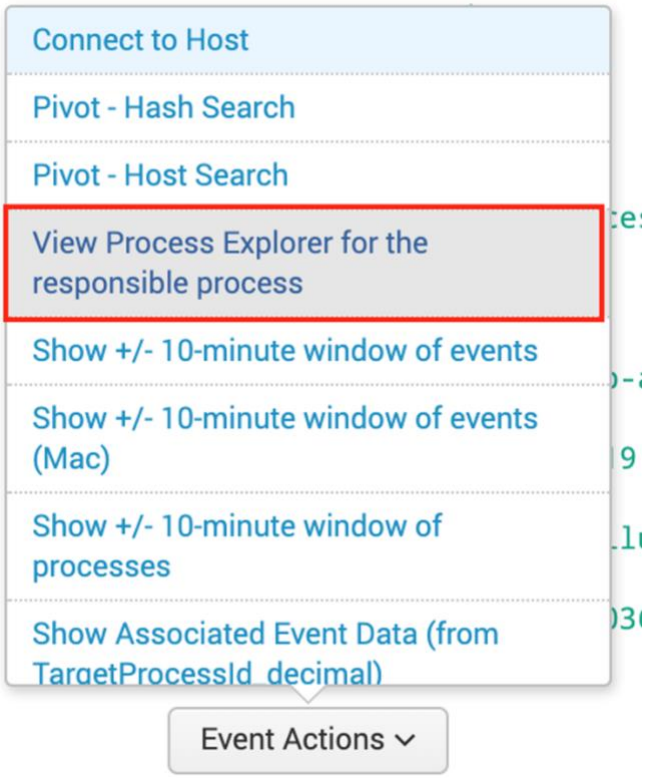
STEP / 06

The event listed tells us a lot. We see that PowerShell downloaded a file, that PowerShell was opened via a command prompt (cmd.exe) and that cmd.exe was opened by a w3wp.exe process. This is concerning as w3wp.exe is associated with an IIS web application and may indicate a vulnerable web server in our organization.



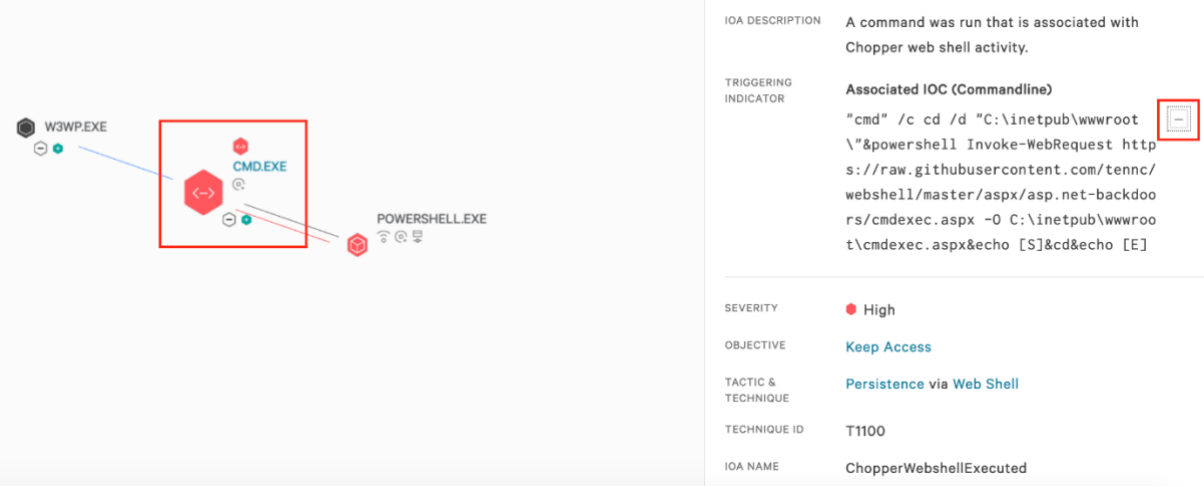
STEP / 07

Let's view these events in context by scrolling to the bottom of the event and clicking the Event Actions menu and then find View Process Explorer for the responsible process button to open a process.



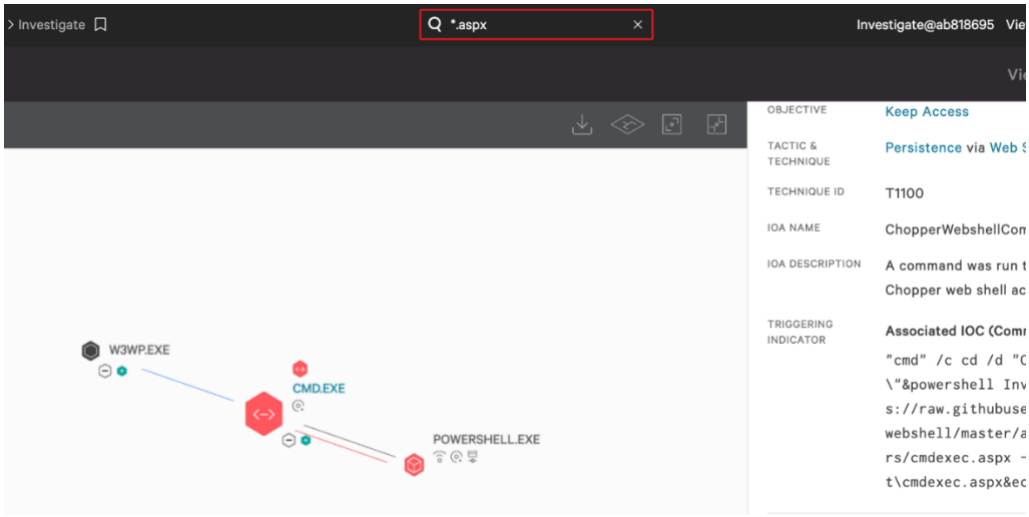
STEP / 08

The full process tree sheds light on what's happening on this system. Not only did a web service launch a command prompt, but after clicking on the CMD.EXE node we get a full picture of what's happening in the Execution Details pane. We see that this system has been compromised using a Chopper webshell. Clicking the "+" button to expand the Triggering Indicator or the Command Line we see that Powershell was used to download a second webshell in an attempt to obfuscate the following commands.



STEP / 09

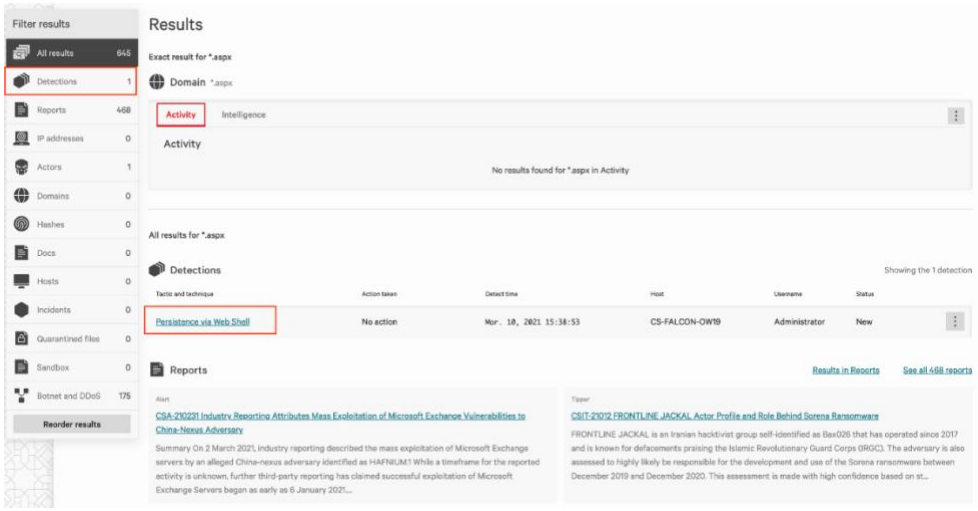
The offending file is cmdexec.aspx, that file extension often being associated with the use of webshells. Let's scan our environment for use of potential webshells. At the top of the screen enter *.aspx in the universal search



STEP / 10

The Universal search is used to scan the Falcon Platform for any mention of the search term. In the case of our file extension we see results in the "Reports", "Actors," and event "Detections". In the instance the detection(s) are associated with the same host and the Mitre Tactic and Technique are all persistence via web shell.

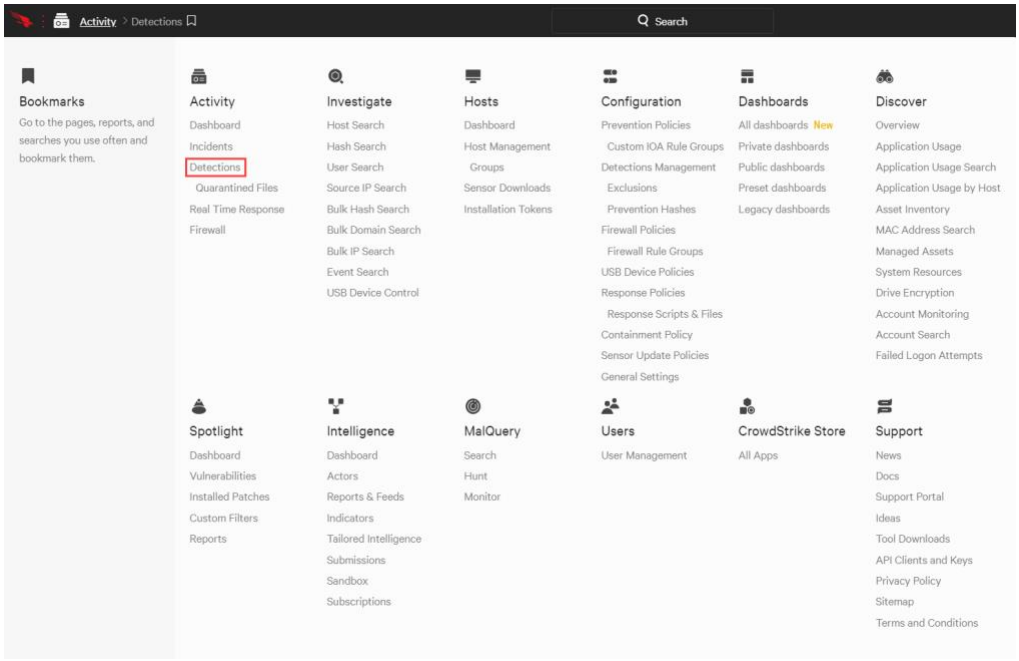
In this scenario we see that a vulnerable IIS webserver permitted an attacker to drop a web shell on the host and gain access. Once that access was in place the attacker downloaded PowerSploit, identified the process ID for the lsass process, and then attempted to download it to steal legitimate credentials.



16.4 Event Searches

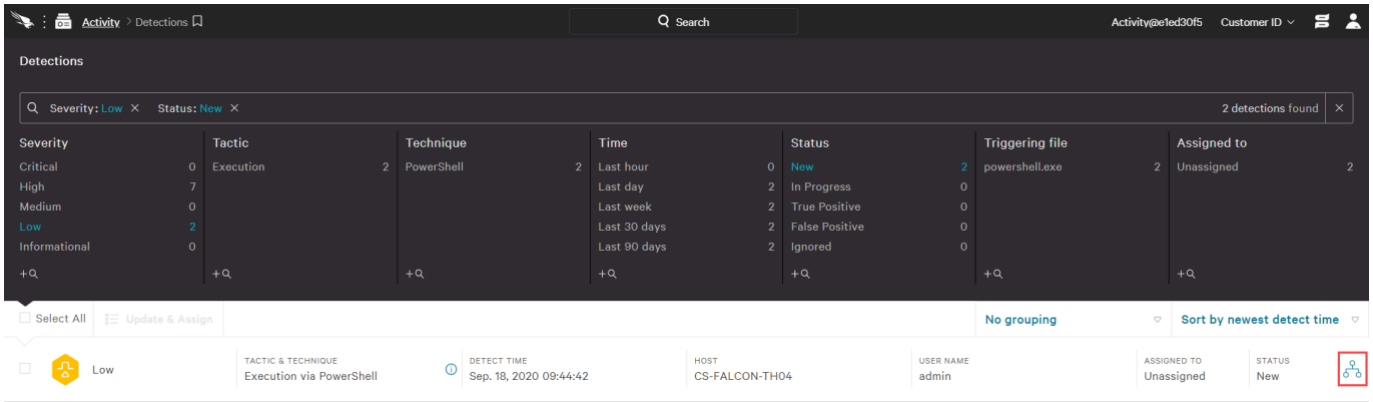
Beginning with a detection scenario, we will review the process tree before shifting to a detailed event view and running different queries against the event data for a specific host.

STEP / 01



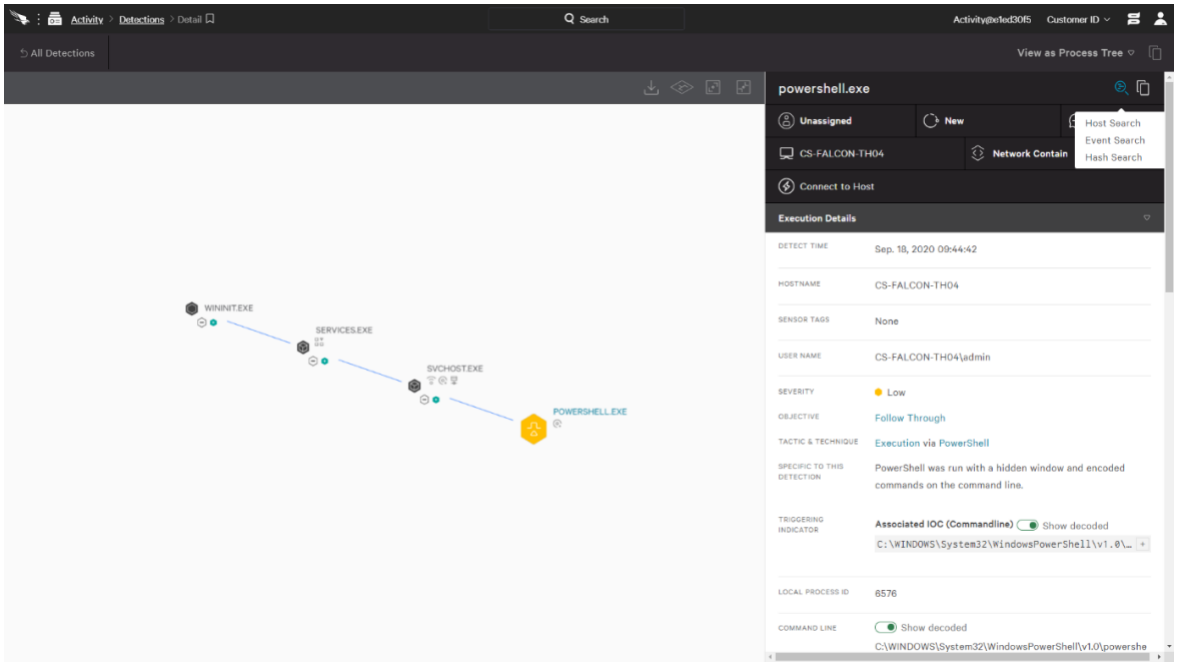
STEP / 02

The Detections page shows a complete list of prevention and detection events in the environment. It can be filtered using the faceted search at the top. To begin this exercise, filter on Low severity detections with the New status and use the graph icon on the right to view the Full detection details for the first detection listed



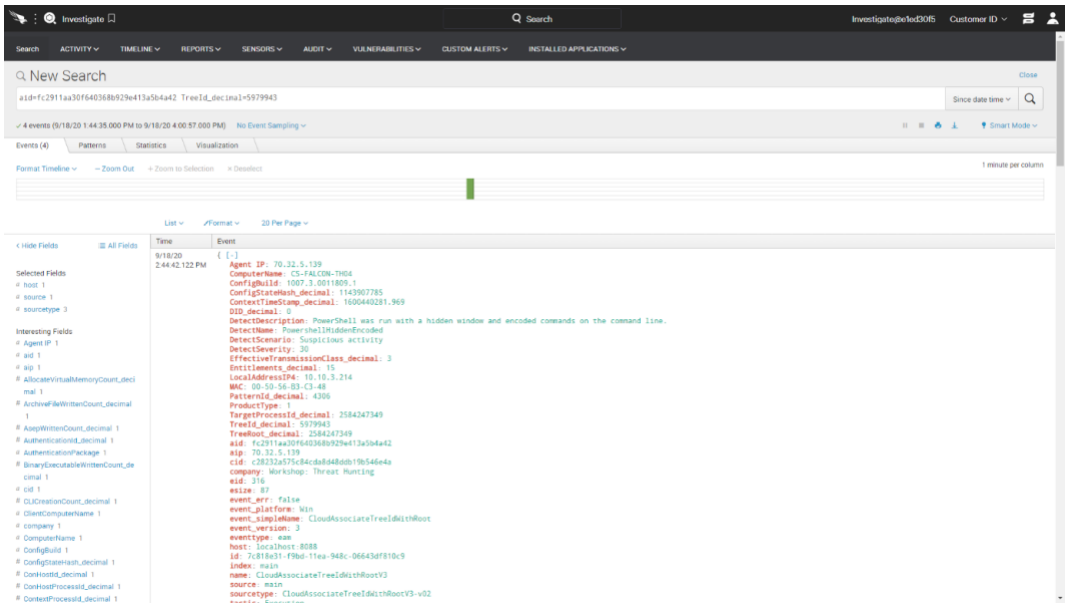
STEP / 03

This view provides a visual illustration of the low-severity PowerShell event along with related execution details. CrowdStrike also provides complete telemetry for all events, which is very useful for threat hunting. To see the details for this event, pivot using the magnifying glass icon to the Event Search.



STEP / 04

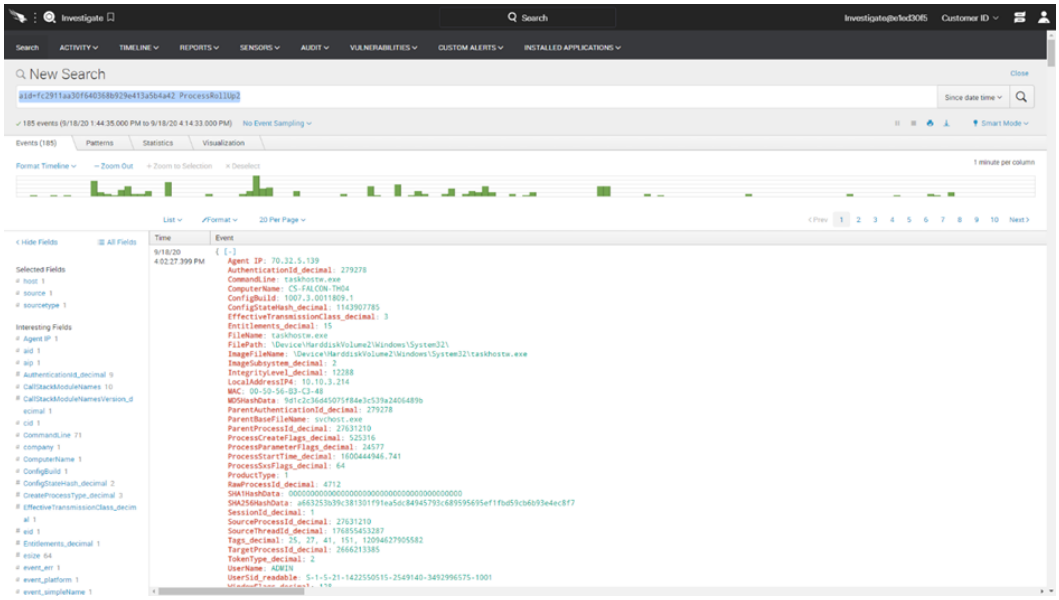
A new tab will open with an event search preconfigured for that host (AID) and specific process tree ID.



STEP / 05

To broaden the search, edit the query to show all process executions for this system AID. This requires replacing the text after the AID to specify an event type

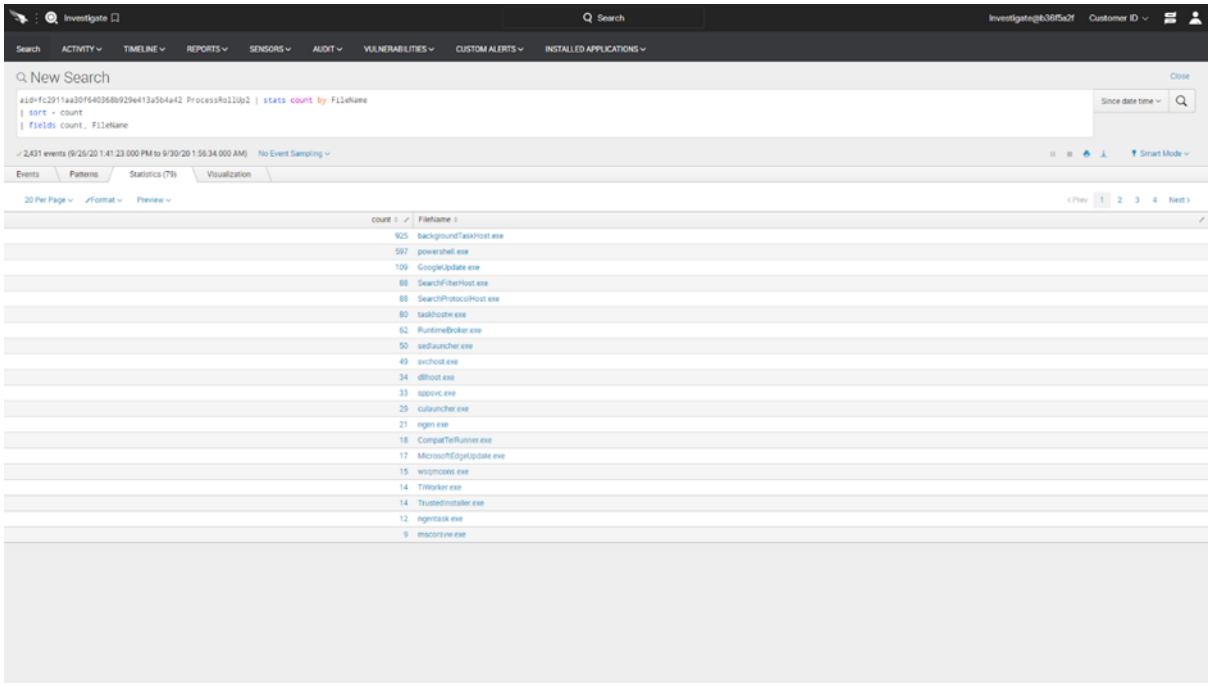
aid=fc2911aa30f640368b929e413a5b4a42 ProcessRollUp2



STEP / 06

Given the number of results, a summary view would make this easier to read. Replace the existing query with the text below to create an easier to read tableview.

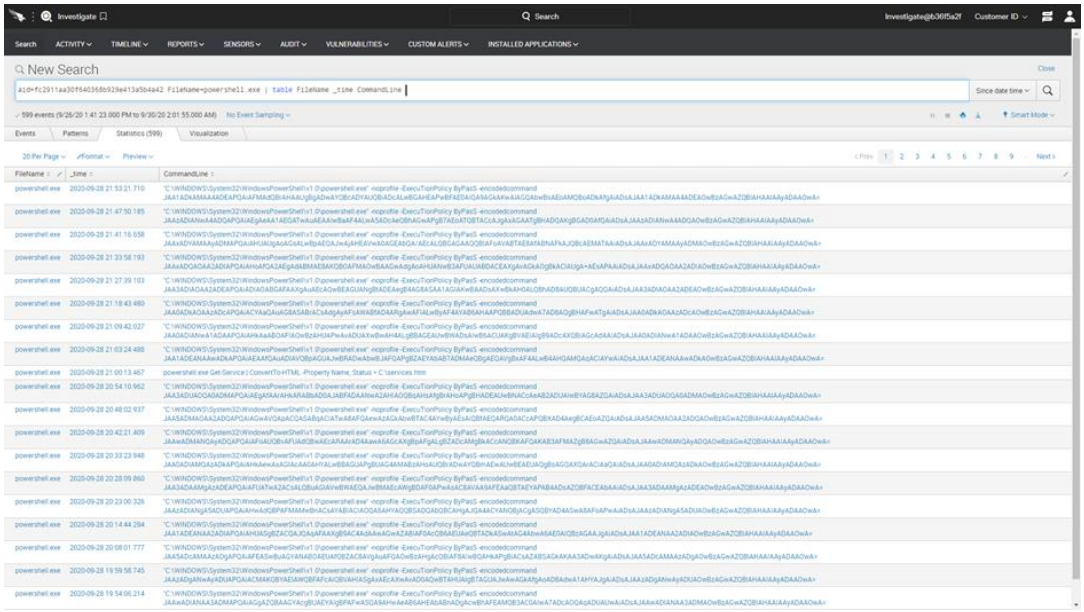
aid=fc2911aa30f640368b929e413a5b4a42 ProcessRollUp2 | stats count by FileName | sort - count | fields count, FileName



STEP / 07

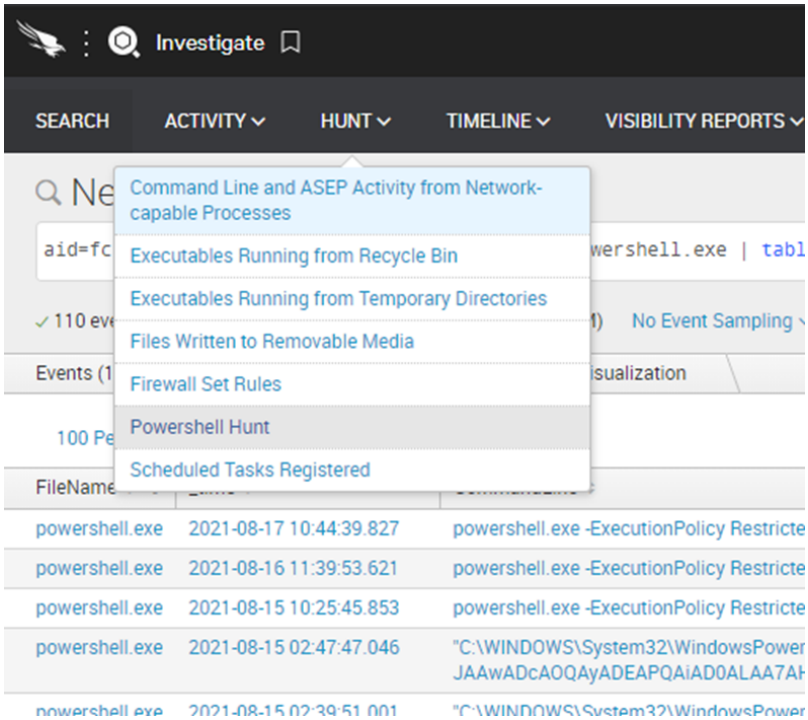
Given the high number of PowerShell executions, the next query will focus on those events. The updated query below will return all PowerShell executions on this host with the time and command line details.

aid=fc2911aa30f640368b929e413a5b4a42 FileName=powershell.exe | table FileName _time CommandLine



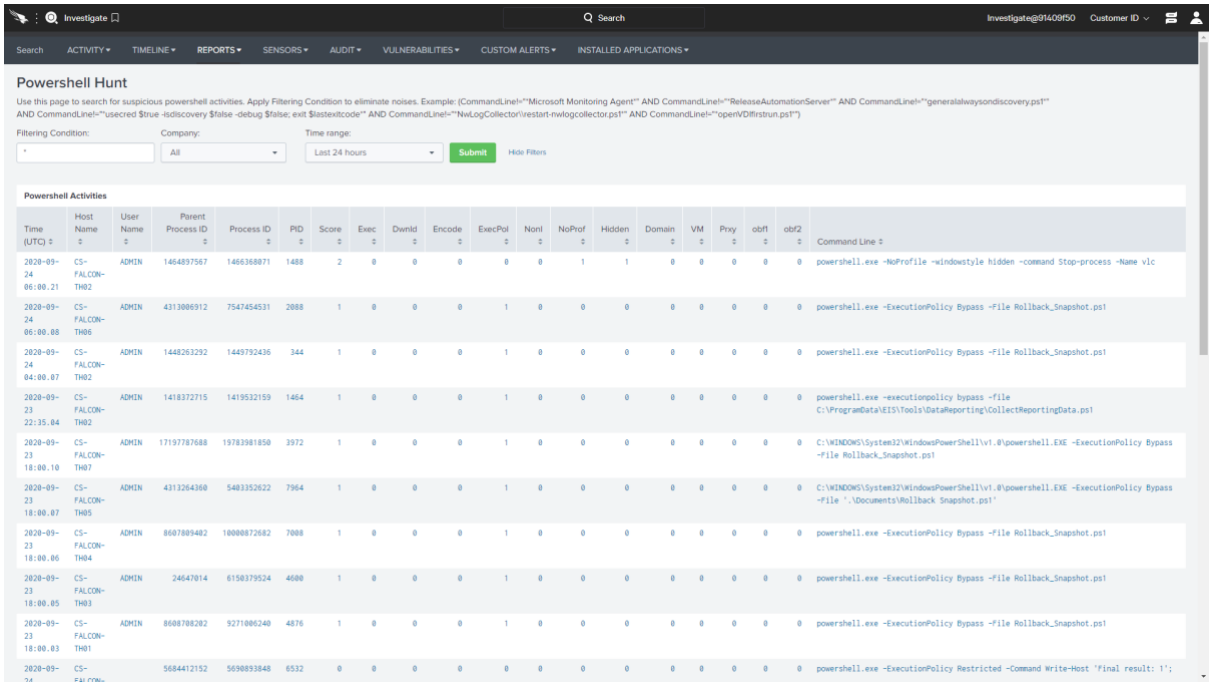
STEP / 08

Because PowerShell is a powerful tool that is commonly leveraged by the adversary, CrowdStrike also provides a dedicated report that reflects all of an organization's PowerShell activity. Navigate to Hunt > Powershell Hunt.



STEP / 09

The report provides a complete list of all PowerShell activity in the environment. Note that this is not just those executions associated with an event or malicious activity. It is every PowerShell execution on managed hosts



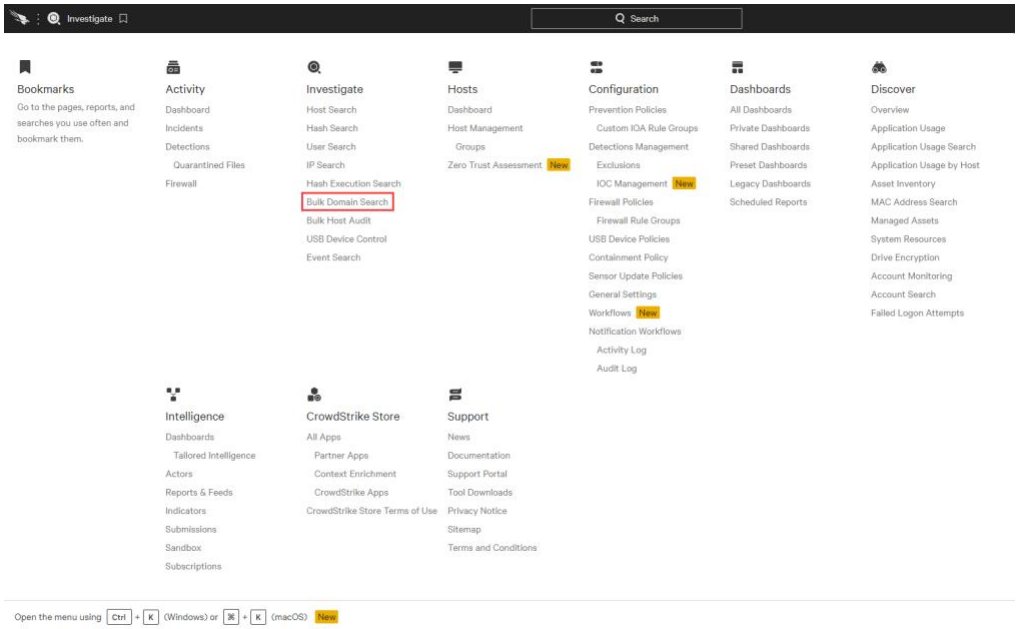
The event search empowers users to search and report on a large volume of data with a flexible, easy to use query language. However, there are times when a simple IOC search is required.

16.5 INDICATOR SEARCHING

Many of us have been in situations where a news article or threat report has drawn attention to a specific attack. Often we are asked to report on any existing impact to the organization based on indicators of compromise. CrowdStrike makes simple search tools available specifically for those types of inquiries.

STEP / 01

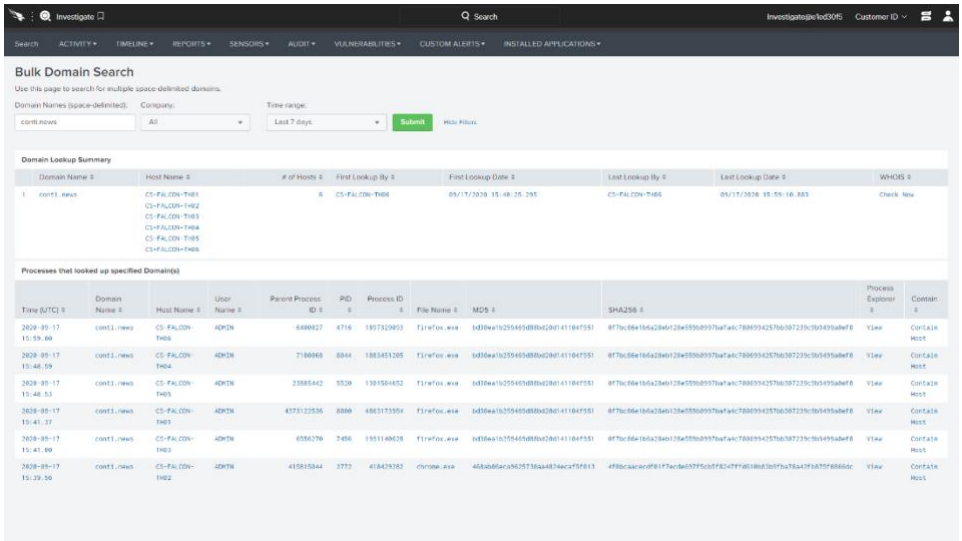
Navigate to Investigate > Bulk Domain Search.



STEP / 02

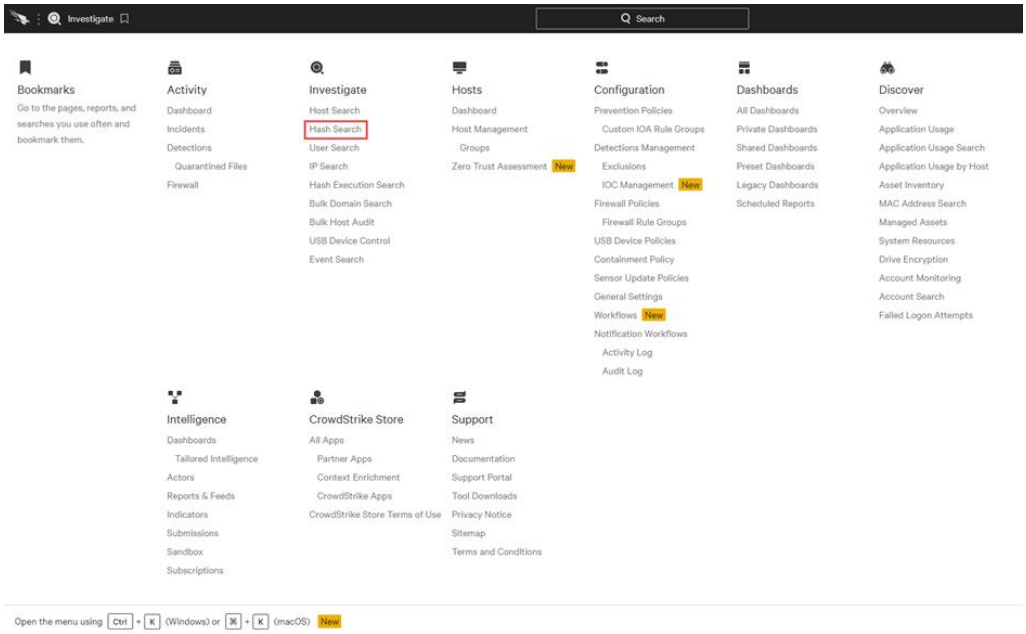
Searching for the domain conti.news will return a report indicating how many hosts in your environment have communicated to that domain

conti.news



STEP / 03

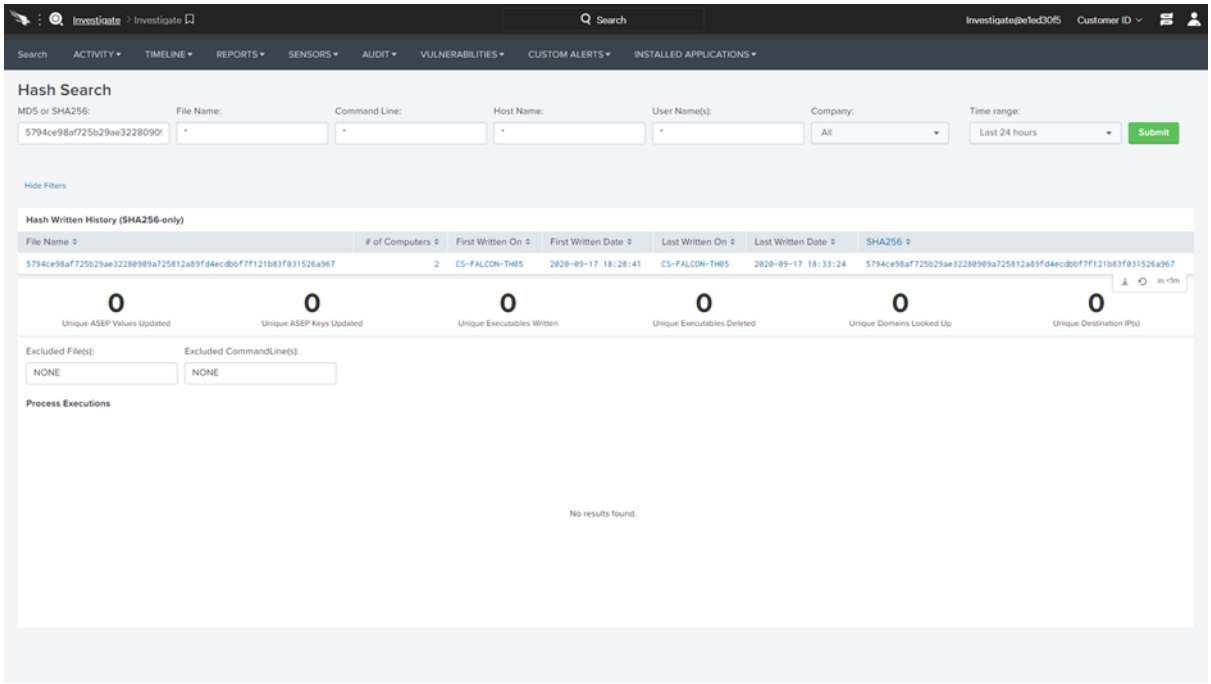
Navigate to Investigate > Hash Search.



STEP / 04

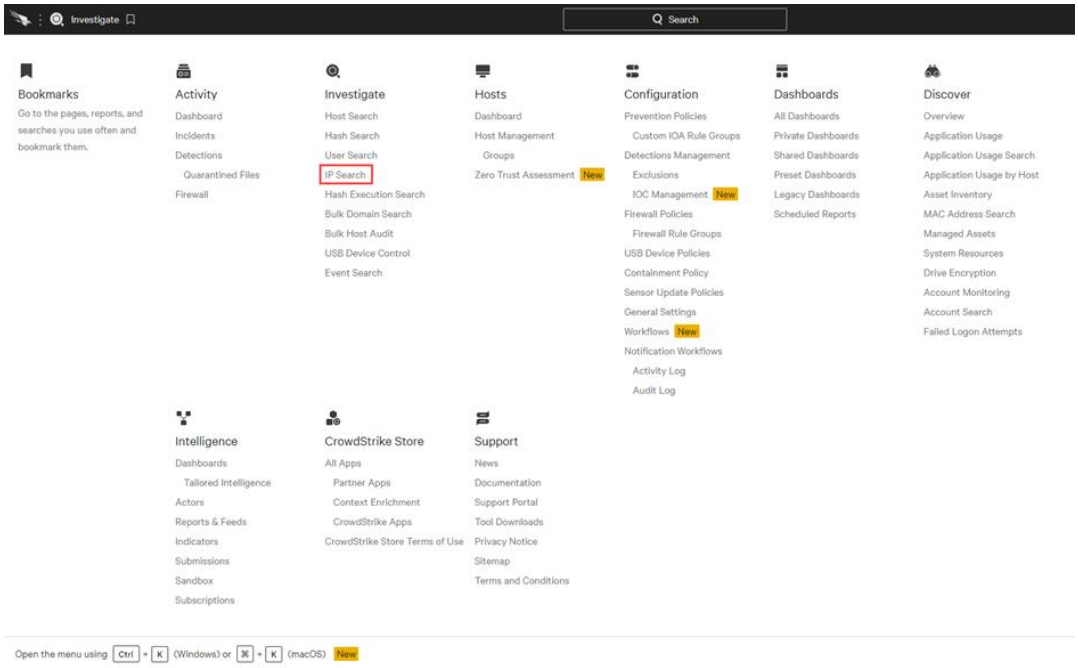
Using the following hash, we can quickly find the number of computers where this file hash is present.

5794ce98af725b29ae32280909a725812a89fd4ecdbbf7f121b83f031526a967



STEP / 05

Navigate to Investigate > Destination IP Search

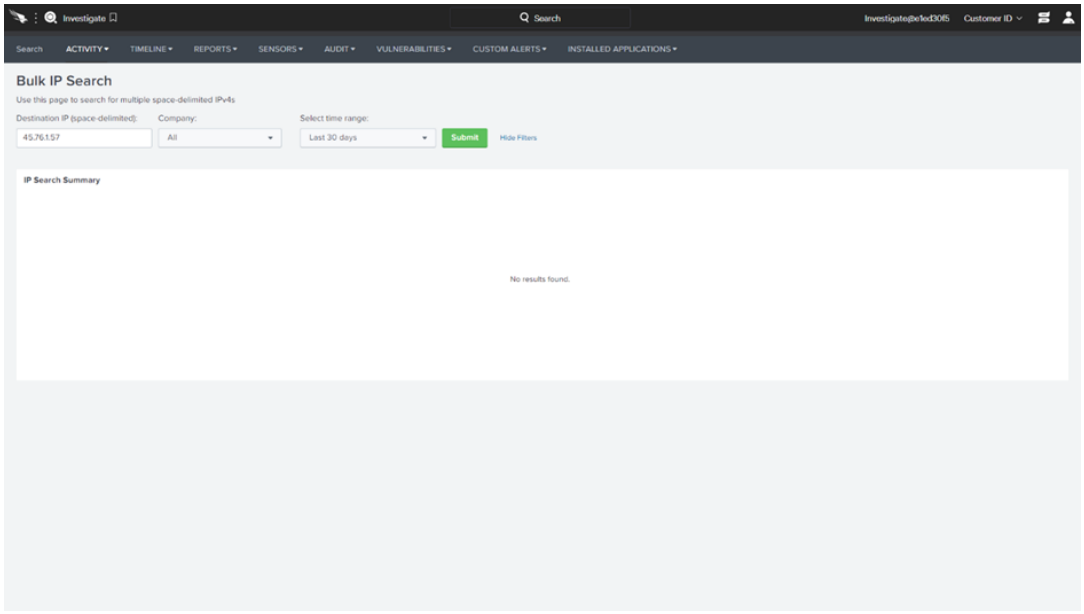


STEP / 06

The IP search report also allows you to find out how many hosts in the environment have communicated with a specific address. It can also help you confirm a lack of traffic to a known bad IP. Enter the following address for Destination IP.

The search should return NO results which means that none of the systems have connected to the known bad IP. That is great news!

45.76.1.57



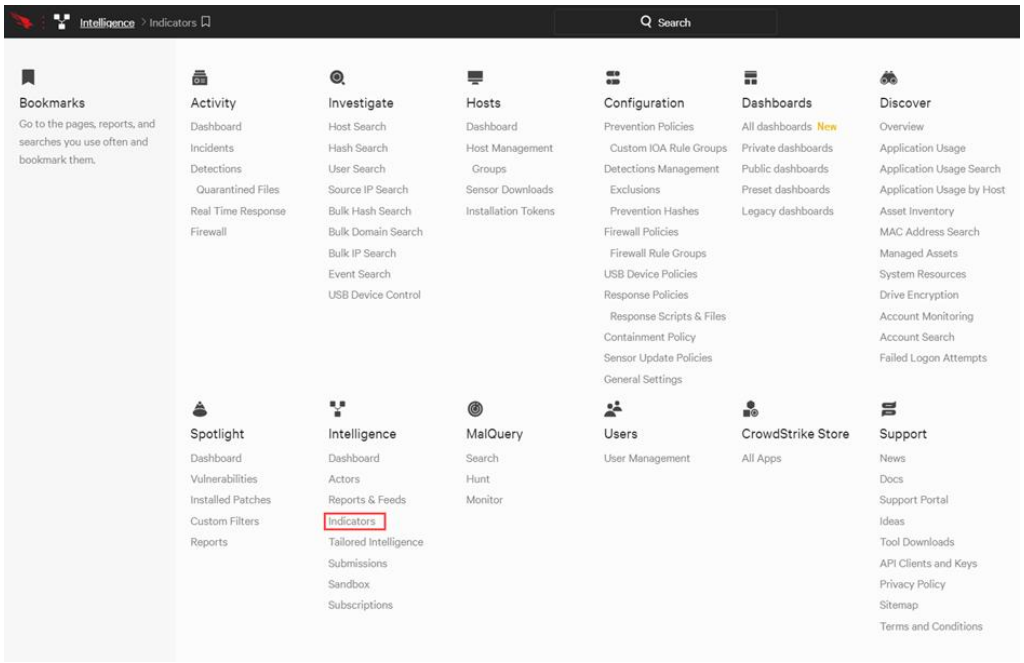
Falcon Insight provides customers with built-in search options to quickly understand the potential presence of different indicators in the environment. But, what if you wanted to understand how those indicators relate to each other?

16.6 THE CROWDSTRIKE INDICATOR GRAPH

While the individual IOC searches give us very useful data points, CrowdStrike also provides a graphical view of that information to help analysts visualize indicators, related intelligence and prevalence. In this scenario, we will use the CrowdStrike Indicator Graph to research the same indicators

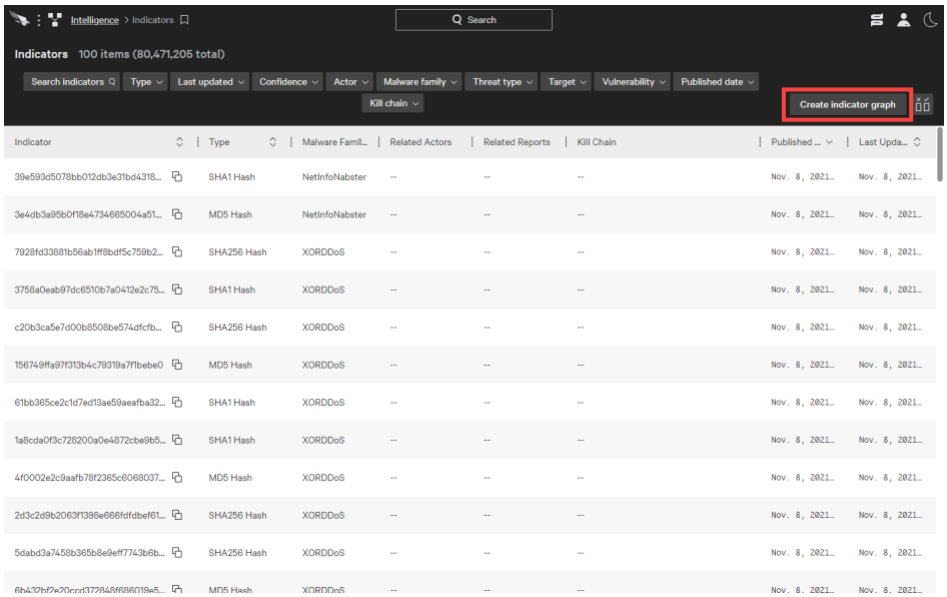
STEP / 01

Navigate to Intelligence > Indicators.



STEP / 02

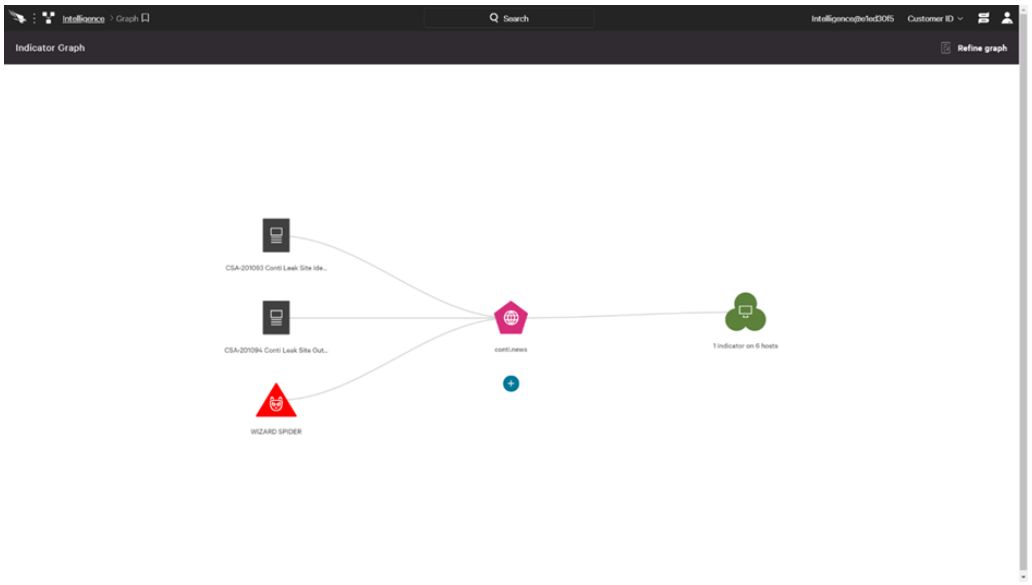
Select Create Indicator graph.



STEP / 03
To build a graph using the same indicators, use + to add the domain.

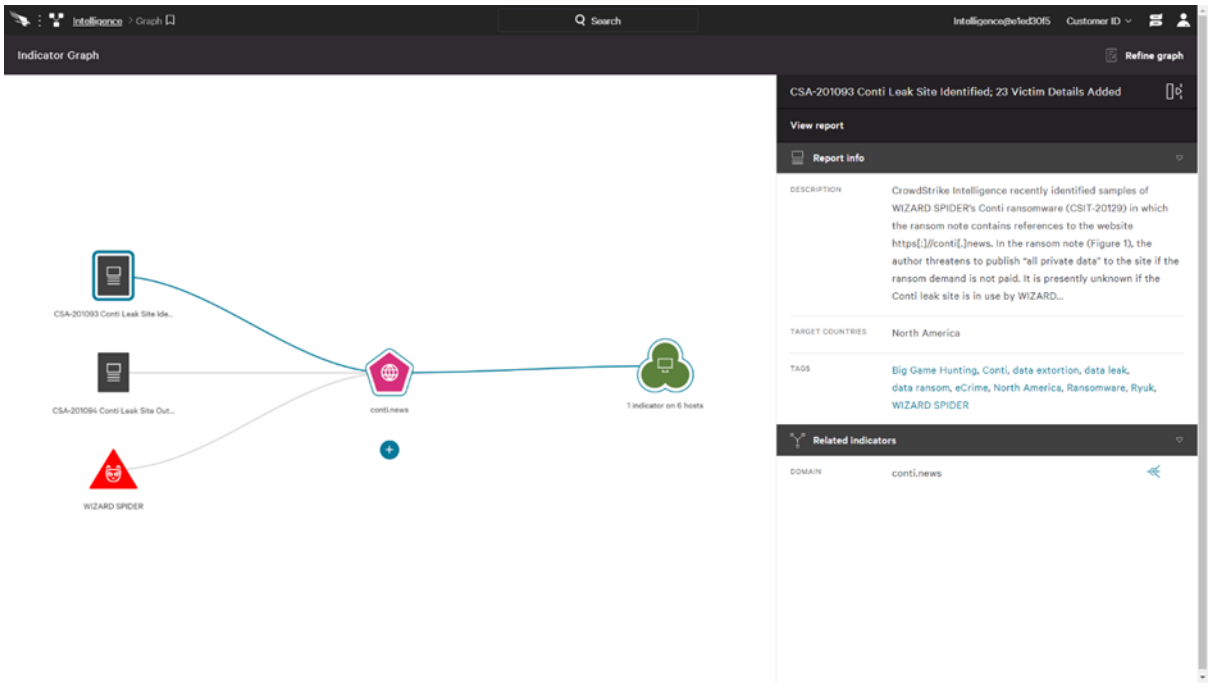
conti.news

STEP / 04
The new indicator appears in the middle with CrowdStrike Intelligence information on the left and a number of related hosts on the right



STEP / 05

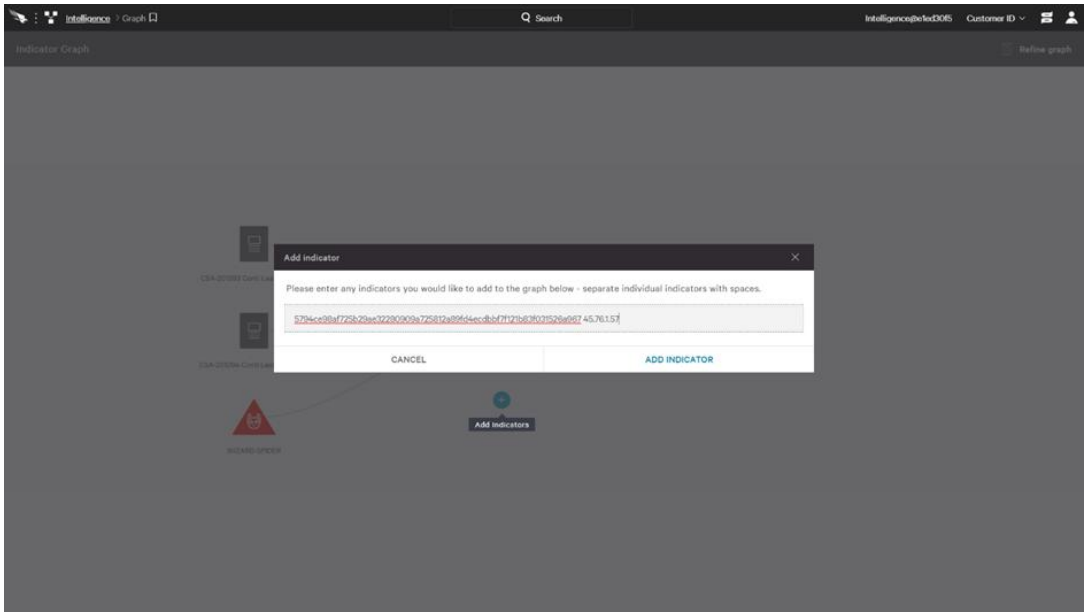
Clicking on a report will show us a summary view as well as the option to view the complete report.



STEP / 06

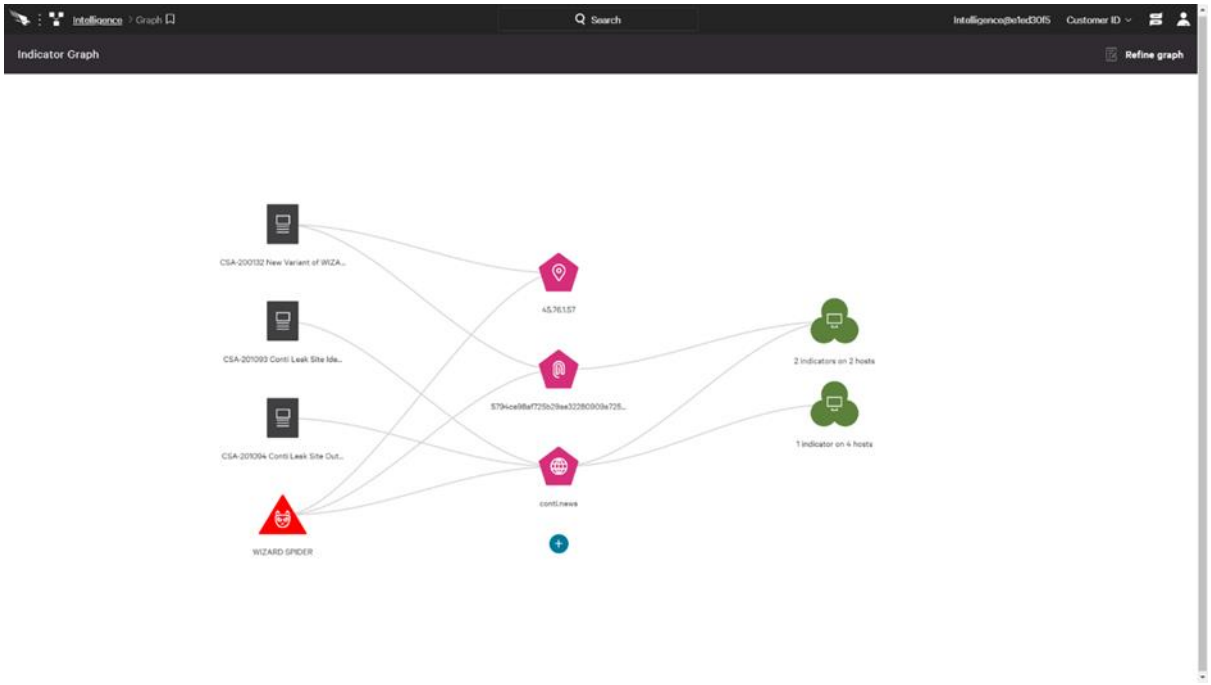
Using +, we can also add multiple additional indicators to this graph simply by leaving a space between each.

5794ce98af725b29ae32280909a725812a89fd4ecdbbf7f121b83f031526a967
45.76.1.57



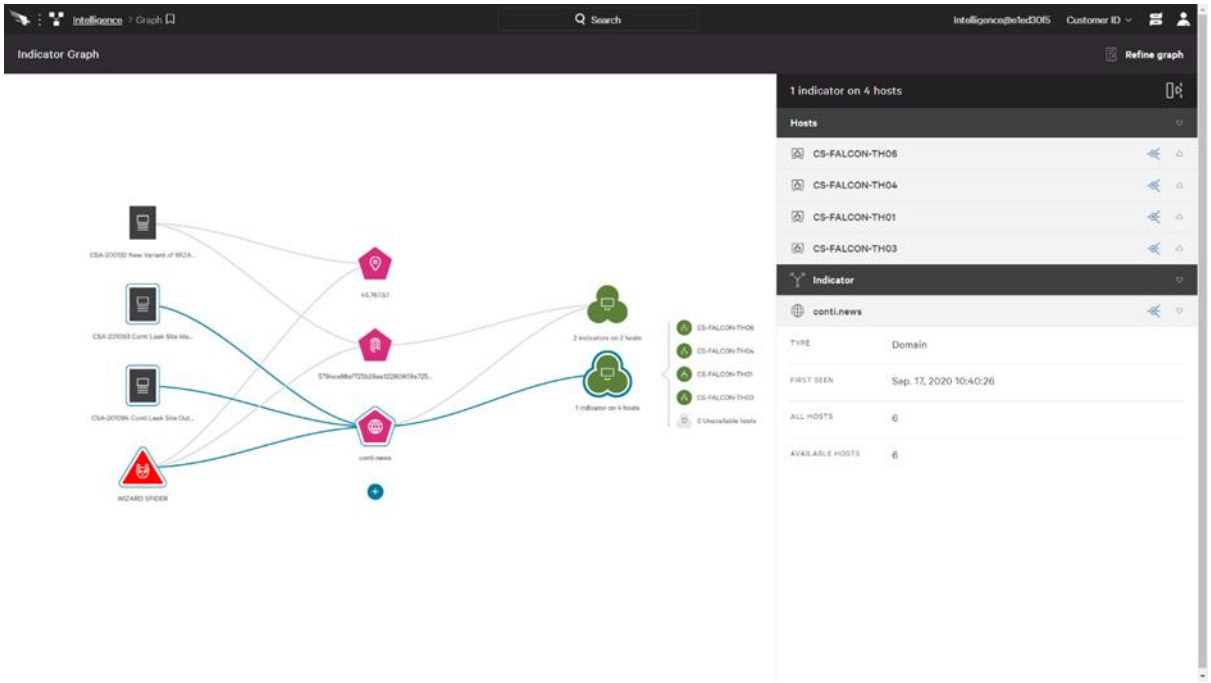
STEP / 07

While the indicator graph shows us the same data available in the event search options, the graphical view provides additional context through CrowdStrike Intelligence information while allowing us to see relational information between multiple indicators.



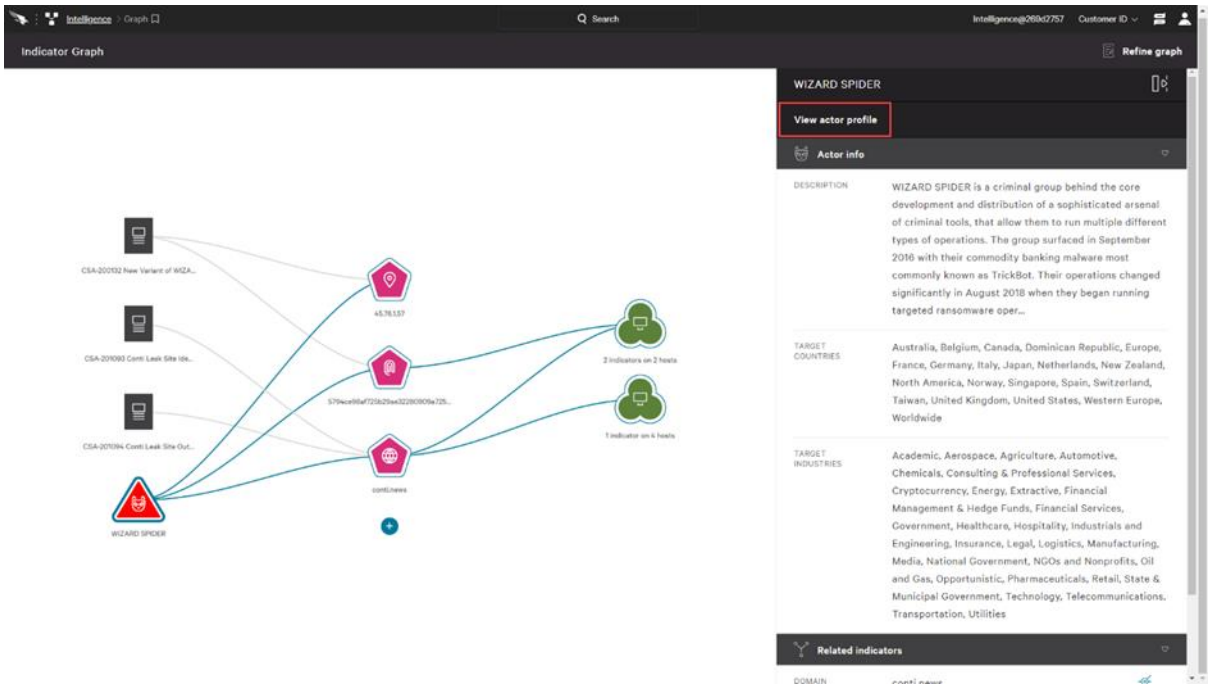
STEP / 08

Drilling into a green host bubble reveals the specific hostnames associated with the indicator.



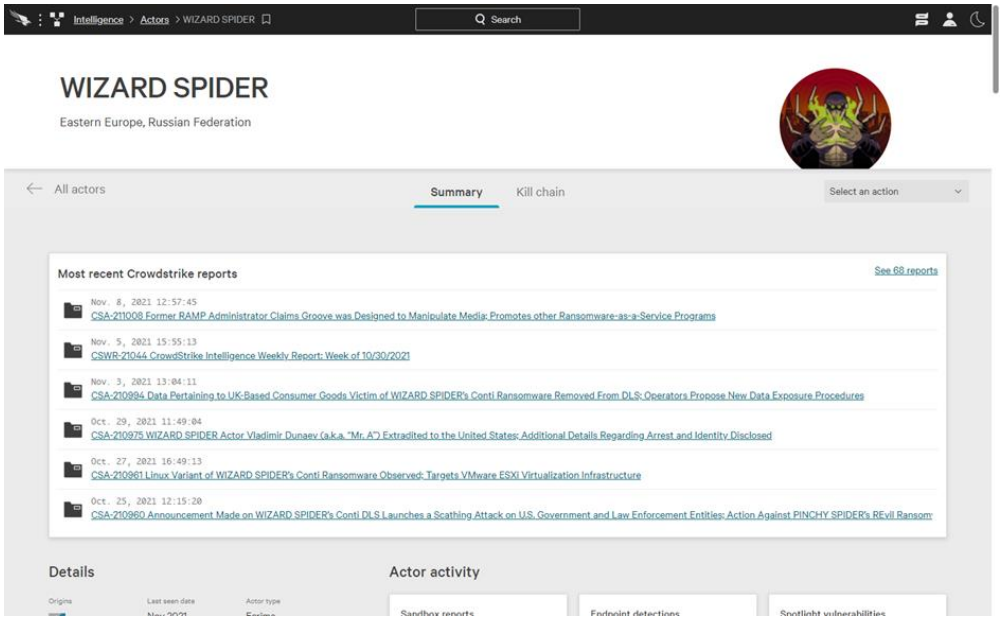
STEP / 09

The graph also illustrates that these indicators have been associated with a known bad actor, WIZARD SPIDER. The summary view is available in the right pane as well as a link to view the complete actor profile

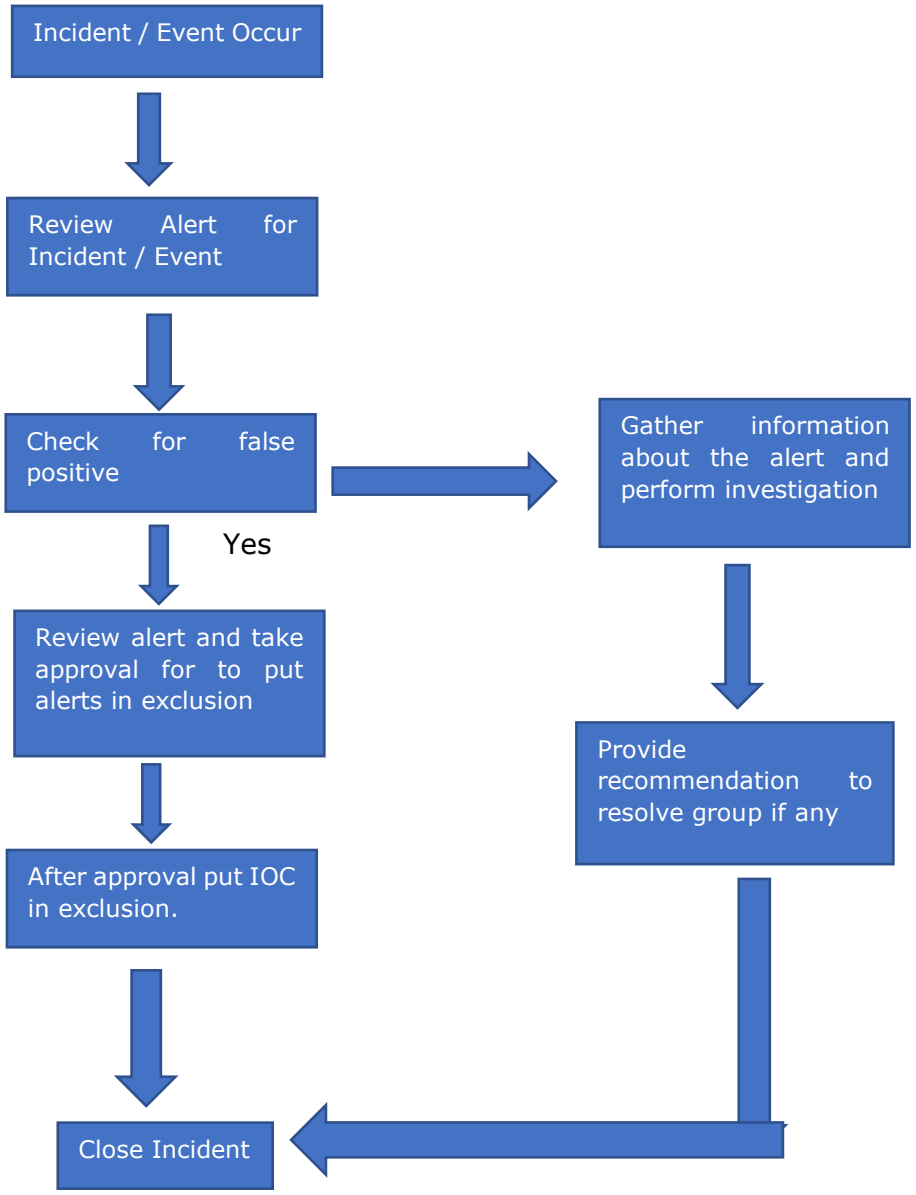


STEP / 10

Open the actor profile to learn more about WIZARD SPIDER.



17 Process Flow



18 Exception

Exception to this procedure above mentioned in all points must be approved through the Netradyne Exception Process.

19 References

change management

Incident Response Plan

20 Appendix A: Document RACI Matrix

Role/Activity	Document Owner/Functional Area Lead	Document Contributor	ND Leadership	Functional Area Team	InfoSec	All ND Member(s)
Ensure document is kept current	**A**	**R**	**I, C**	**R, C**	**C**	**I**
Ensure stakeholders are kept informed	**A**	**R**	**-**	**R**	**C**	**-**
Ensure document contains all relevant information	**A**	**R**	**I, C**	**R, C**	**C**	**I**
Ensure document adheres to document governance policy	**A, R**	**R**	**I**	**R, C**	**R, C**	**I**
Provide SME advice	**I, R**	**A, R**	**I**	**R, C**	**I, C**	**I**
Gathering and adding document contents	**I**	**A, R**	**I, C**	**R, C**	**C**	**I**
Document Approval	**A**	**R**	**I, R**	**I**	**I, R**	**I**

Key

R	Responsible
A	Accountable
C	Consulted
I	Informed