

The Anatomy of CrowdStrike Threat Hunting

Federated Hermes

BISD Information Security Group

Alexei Hooks

August 3, 2022

Abstract:

CrowdStrike is a cloud-based security tool focused on next-gen antivirus and endpoint detection/response of an organization's system. Throughout my time with Federated Hermes and the Information Security Group, I was able to use CrowdStrike University and third-party resources from the internet to research the most recent update to the CrowdStrike tool: Threat Hunting. The task of outwardly framing security is focused on the prevention of an attack. With a preventative stance, the organization will know where to focus their security efforts and better find indicators of a breach. The knowledge of how threat actors change their attack tactics is a constantly evolving industry. Within this sector of cybersecurity, it is almost impossible to have the upper hand, leading to why working with a preventative stance is so important. Additionally, knowing what threat actors are using to attack organizations can highly decrease the time between response and remediation of an attack.

Using CrowdStrike University, I was able to internalize teachings from the Threat Hunting module that I found relevant to an organization; then included an overhauled version within this document. Working with CrowdStrike was enjoyable, especially the Threat Intelligence dashboard, as it supplies the user a visually streamlined experience that allows for easy consumption of copious amounts of data. Since the tool is complex with multiple dashboards and the ability to customize these dashboards to better suit the organization's needs, I have linked multiple sources within the Supplemental Information section. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Along with this additional information, CrowdStrike University is the best way to gain the more skills within this tool. During my 10 weeks with CrowdStrike, I found enjoyment learning how diverse the toolset can be and I hope that sharing the knowledge I have gained will make the organization's transition into using the tool much simpler. As an additional note, some of the images within this document as not easily visible; considering this I subsequently included kill chains of processes I found useful. I recommend following each lesson using the tool, along with the kill chains, for better understanding of CrowdStrike.

Overview of CrowdStrike Tool:

As CrowdStrike has a large capability, knowing how to navigate and customize the tool is highly necessary as there are many ways to use and engage with the data it provides. The tool is built around a GUI focused on dashboards which each have a certain focus within the security space. These dashboards allow for the user to better search and research ways to improve their security stance in and around the system. The dashboards are as follows:

Endpoint Security:

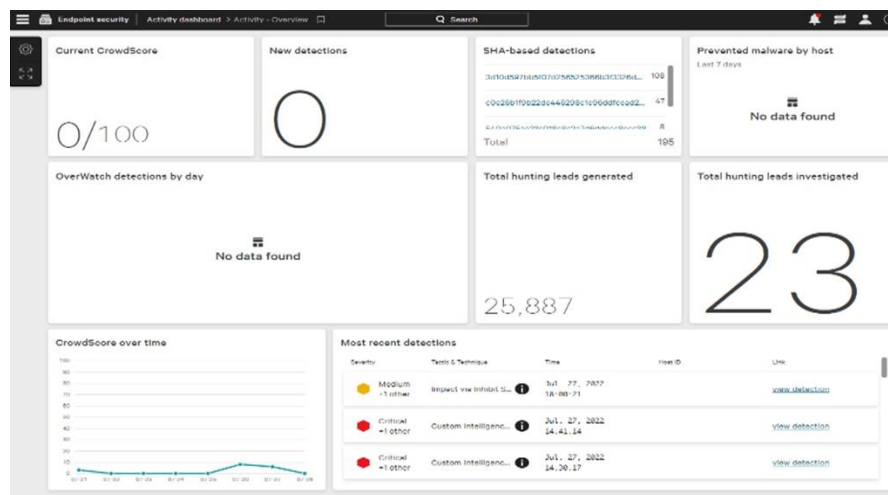


Figure 1: Activity Dashboard

Within the Endpoint Security tab, there are multiple dashboards that deal with monitoring and configuring the user's endpoint security; one of these is the Activity dashboard. It allows users to monitor and locate detections or recent activity on the network. The Activity dashboard is used as a place to quickly update the user of any new occurrences. Within this dashboard, a fantastic way to better update the user quickly is the CrowdScore. This score is a level of threat that is made up of incidents and threats; this score should be maintained at a low percentage. If this number increases by 20 percent, an investigation should be launched in an expedited fashion. To do this, click on the crowd score number and it will take the user to the Endpoint Security | CrowdScore Incidents dashboard, which allows the user access to more information on why the CrowdScore has risen. Individual detections will be shown with a rating of how much of a threat the incident might be to the user's systems on a scale from 0.1 to 10 depending on the severity of threat to the organization. These offer the option to view an incident summary preview, and the ability to drill down further if necessary. Another part of Endpoint Security is the Configuration

section, which allows rules to be set to deal with threats in an ordered fashion. Prevention policies can hold precedence and gives the user the ability to take what they know the system deals with daily, and have it placed in a separate place for inspection, allowing for more serious threats to be visible.

Discover:

The discover tab is a trusty source of finding more information if more than an overview (from the Activity dashboard) of an event is needed. Within this tab, Assets, Accounts, and Applications (AAA) all can be opened and researched to help the user find the underlying cause of the problem. All the dashboards within AAA break down their information into further dashboards, which show information about the entirety of the system. This information will need to be drilled down upon to get the data the user would need to see in a case-by-case basis.

Assets Dashboard:

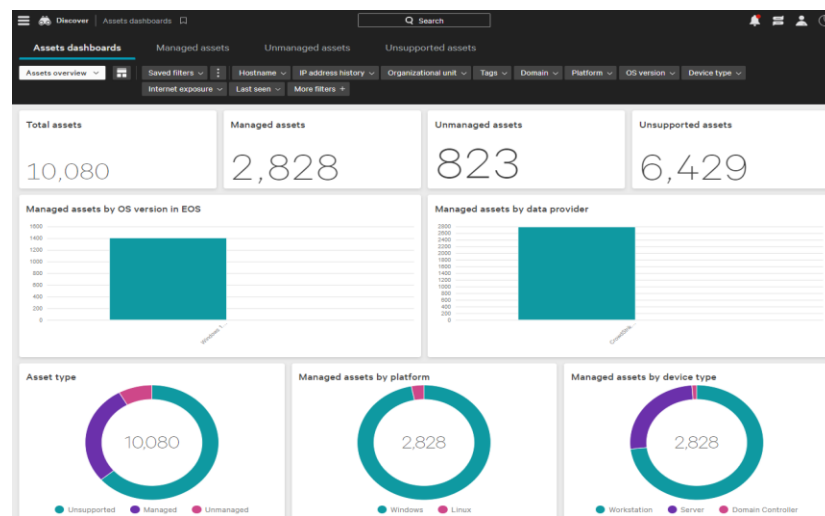


Figure 2: Assets Dashboard

Within the Assets dashboard the user can see breakdowns of how multiple assets are managed, which types of devices are managed assets, and by which platform each asset is managed. This allows the user to become better versed in their system and understand what and how they need to protect.

Accounts Dashboard:

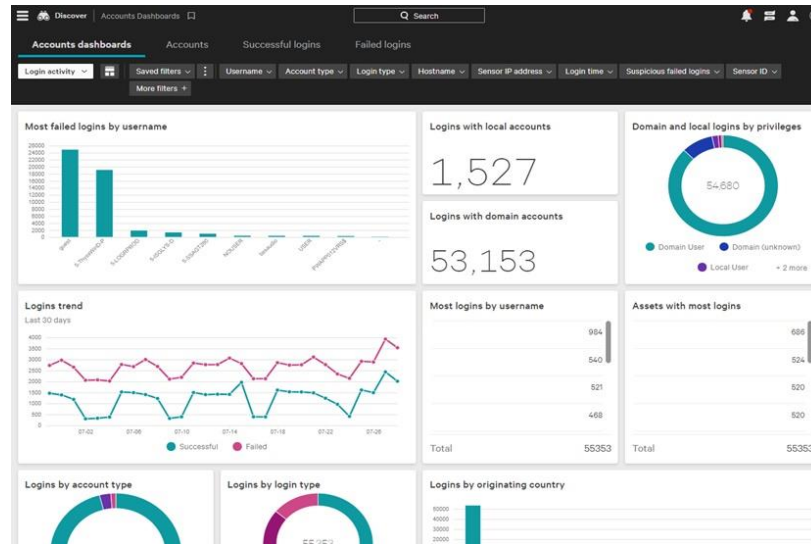


Figure 3: Accounts Dashboard

The accounts dashboard gives the user a scalable view of the system's accounts that are used within an organization. These accounts are servers, tools, and admins within the CrowdStrike interface, and all have detailed stats of how each are behaving within the system. This could be used to see how accounts are logging in/not logging in, or how the tools are privileged within the system.

Application Dashboard:

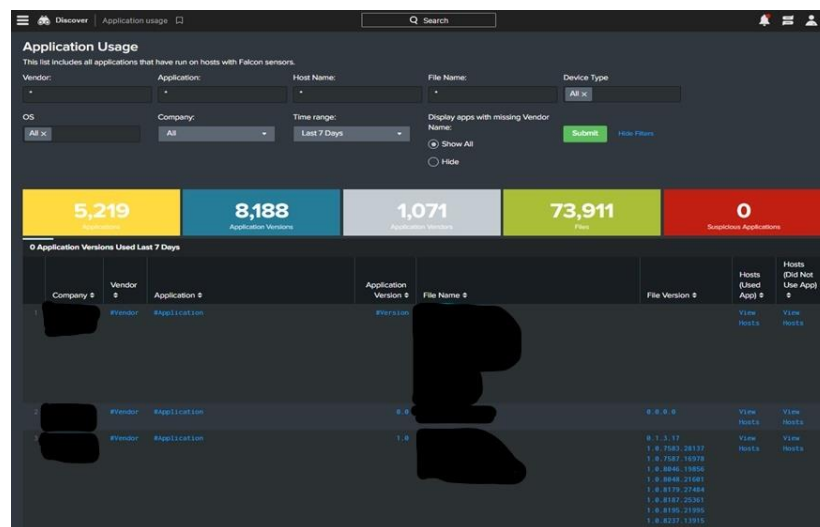


Figure 4: Application Usage Dashboard

Last in the discover tab is the Application dashboard in which CrowdStrike utilizes Splunk to easily search and find a specific application if needed. The application dashboard allows the user to view applications, the current version that application is running, and which host used the application. This process could be used to better analyze a malfunctioning application or see what host may be experiencing issues within the system.

Other Utilities in CrowdStrike:

CrowdStrike is focused on allowing their users to have transparency within their systems, making them as secure as possible. Keeping up with current trends in information security is a terrific way to stay knowledgeable knowledge about the cyber landscape, and gain insight into the latest into cybercriminal trends around the globe. CrowdStrike is a reliable source to clarify data with their reports about malware or other threats through a Request for Information (RFI). RFIs are usually done for questions that need to generate an analytical report suchlike Request Files within OverWatch, which is covered within the Threat Hunting section.

Threat Hunting:



Figure 5: Malware Research Process Timeline

A majority of the threat hunting module on CrowdStrike University is focused on threat intelligence. Not only is threat intelligence new within the dashboard section of the CrowdStrike tool, but it is also a key component to stay ahead of any cyber threats. As cyber threats and security breaches happen often, it is best to have a proactive posture when defending a system. This improves both the preventative measure to limit the threat of an attack, and the number of necessary actions that come with overseeing an incident. With the new update that CrowdStrike rolled out in 2022, the Threat Intelligence tab is full of brand-new toolsets devoted to looking

outward for potential threats. The Threat Intelligence tab allows for companies to see what is going on within the cyber landscape between hackers and the industries they are targeting. By being more aware about the world, one can properly orient the organization to be better equipped to deal with an oncoming attack. This goes along with the thinking that being heavily proactive with security can lead to having less to react to when a threat appears. When moving through the Threat Intelligence dashboard, the user will be able to fully move through the “Malware Research Process,” where users will encounter a piece of malware and be able to analyze/build a rule to protect the user’s organization against it.

OverWatch:

With the acquisition of a new operations package from CrowdStrike, we now have access to OverWatch, a managed threat hunting detection engine and reporting tool dealing with threat intelligence. OverWatch allows a company to let CrowdStrike do the threat hunting for them, along with providing quarterly reports are released with pertinent data about latest trends going on in the cyberspace to the organization. These reports breakdown certain points of data that have had a distinct effect on the industry. The ability to search OverWatch for specific keywords allows the user to find quarterly reports that will apply to them, streamlining the research process.

Also, within OverWatch, there is a tool called the Hunting Snapshot tab, which allows the user to see how numerous hunting leads generated, investigated, and total triggered detections within the user’s system. This allows the user to see what CrowdStrike can do with data and how many hunting leads may be within the organization’s system.

The last tab within OverWatch is the Submissions tab. This tab allows the user to submit malware files to CrowdStrike for analysis. There are two options: requested and unrequested files. Requested files, just like an RFI, will be analyzed and the user will receive recommended actions on how to alleviate any issues that this malware could be posing to the user’s organization. Unrequested files will only be used to better the malware database that exists with CrowdStrike for OverWatch, and the user will not have any form of contact after submission. To do this, all the users must do is include a Submission Name and link the malware file; the maximum size this file can be is 256 Mb.

Threat Actors Tab:

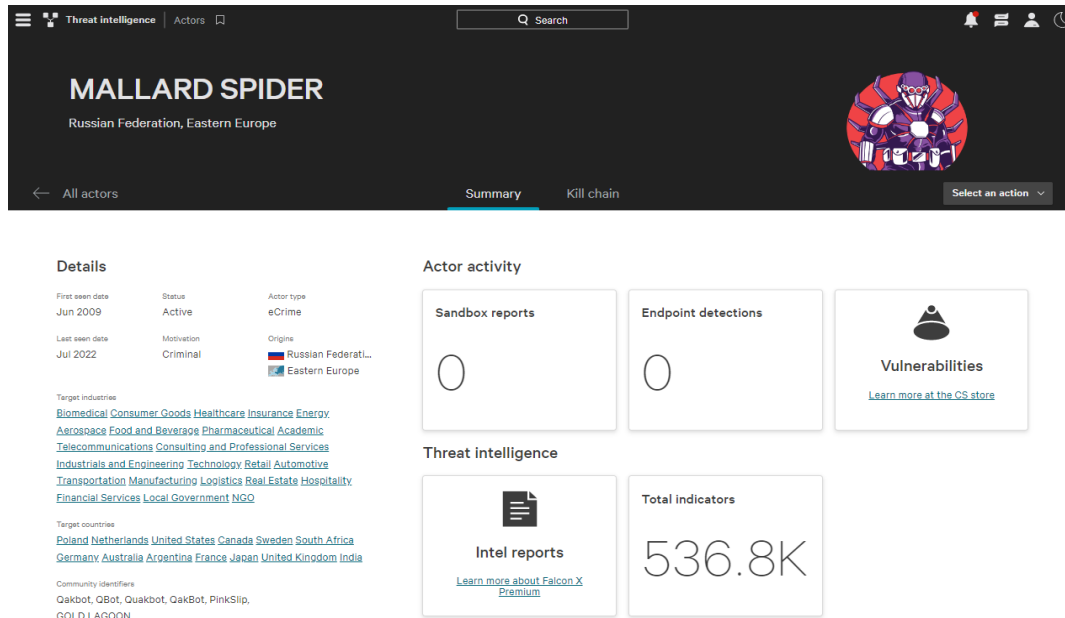


Figure 6: Example of a Threat Actor

Within the Threat Intelligence tab, there is a section dedicated to Threat Actors who are active and prominent in the cyber threat space. This area of CrowdStrike lets the user know if any detections within the system are associated with any of these actors. Each actor is named between different animals depending on their motivation and can be separated accordingly. Below is a breakdown of the three distinct types of Threat Actors by motivation. It is then further broken down in the State-Sponsored section by place of origin.

Different Types of Threat Actors:

Criminal: Spider

Hacktivist: Jackal

State-Sponsored (SS):

China = Panda

Vietnam = Buffalo

Iran = Kitten

Russian Federation = Bear

East Asia/North Korea = Chollima East Asia/South Korea = Crane

South Asia/India = Tiger

South Asia/Pakistan = Leopard

South America/Columbia = Ocelot

Turkey = Wolf

Syrian Arab Republic = Hawk

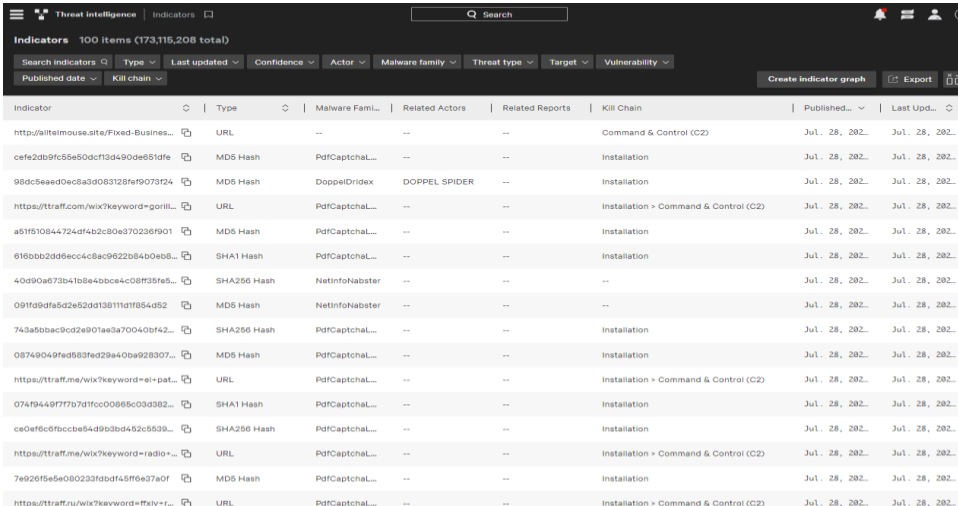
Georgia = Lynx

(For each animal in (SS), a respective Country/Territory where they originate from is assigned)

Other filters allow the user to modify what they will be able to see, to customize visuals about which actors might be targeting companies (like the user's organization). Each info card on an actor can be expanded for more information on them. This included extra details about the threat actor, a description of their history, and what malware they are linked to, allowing the user to better search out actors that could be a threat to the user's organization. Having a description on the type of malware a Threat Actors uses (who targets the user's industry) allows the organization to better defend themselves from further threat, as they can utilize rules against these specific attacks. Below is the kill chain that the user can utilize to better filter Threat Actors:

Threat Intelligence > Actors > Search Actors or Filter Actors by Motivation/Origin

Indicators Tab:



Indicator	Type	Malware Family	Related Actors	Related Reports	Kill Chain	Published	Last Updated
http://ailemouse.aile/Fixed-Busines...	URL	--	--	--	Command & Control (C2)	Jul. 28, 202...	Jul. 28, 202...
cefe2b9fc55e50dcf13d490de651de	MD5 Hash	Pd/CaptchaL...	--	--	Installation	Jul. 28, 202...	Jul. 28, 202...
98dc5eae90ec8a3d0831228f9079724	MD5 Hash	DoppelDrindex	DOPPEL SPIDER	--	Installation	Jul. 28, 202...	Jul. 28, 202...
https://traff.com/wix?keyword=goril...	URL	Pd/CaptchaL...	--	--	Installation > Command & Control (C2)	Jul. 28, 202...	Jul. 28, 202...
a51f510844724df4b2c80e370236f901	MD5 Hash	Pd/CaptchaL...	--	--	Installation	Jul. 28, 202...	Jul. 28, 202...
161b5bb29d9e6cc4c8ac9622d64b0e08...	SHA1 Hash	Pd/CaptchaL...	--	--	Installation	Jul. 28, 202...	Jul. 28, 202...
40d90a673b41b8e4b0e4c08f35fe5...	SHA256 Hash	NetInfoNabster	--	--	--	Jul. 28, 202...	Jul. 28, 202...
091f09dfa5d2e52d13811d1f854052	MD5 Hash	NetInfoNabster	--	--	--	Jul. 28, 202...	Jul. 28, 202...
743a5bbac9cd2901a83a70040bf42...	SHA256 Hash	Pd/CaptchaL...	--	--	Installation	Jul. 28, 202...	Jul. 28, 202...
06749049fed583fed29a40b92307...	MD5 Hash	Pd/CaptchaL...	--	--	Installation	Jul. 28, 202...	Jul. 28, 202...
https://traff.me/wix?keyword=el-pat...	URL	Pd/CaptchaL...	--	--	Installation > Command & Control (C2)	Jul. 28, 202...	Jul. 28, 202...
074f9449f77b791fcc0086c03d382...	SHA1 Hash	Pd/CaptchaL...	--	--	Installation	Jul. 28, 202...	Jul. 28, 202...
ce0ef6cfbcbcb84d9b3bd9452c5539...	SHA256 Hash	Pd/CaptchaL...	--	--	Installation	Jul. 28, 202...	Jul. 28, 202...
https://traff.me/wix?keyword=radio+...	URL	Pd/CaptchaL...	--	--	Installation > Command & Control (C2)	Jul. 28, 202...	Jul. 28, 202...
7e920f5e6e080230bd45f9e37a0f	MD5 Hash	Pd/CaptchaL...	--	--	Installation	Jul. 28, 202...	Jul. 28, 202...
https://traff.ru/wix?keyword=fxlv+r...	URL	Pd/CaptchaL...	--	--	Installation > Command & Control (C2)	Jul. 28, 202...	Jul. 28, 202...

Figure 7: Example of Indicator Search Page

Another tab within Threat Intelligence is the Indicators tab, which allows users to search through hashes and create indicator graphs. To understand how to properly get important data, the definitions of indicators that CrowdStrike supplies should be clear. There are two distinct types of indicators, IOCs (Indicators of Compromise) and IOAs (Indicators of Attack). Indicators themselves come from evidence (taken from the user's system or outside sources) or behaviors which can be more easily tracked and monitored. The difference between IOCs and IOAs is:

- IOCs are evidence based and are reactive in their security stance

- IOCs come from data that has already happened (Investigating a crime scene)
- IOAs are behavior or action based which are proactive in their security stance
 - IOAs come from analyzing the threat landscape (Preparing for impending attack)

Intelligence > Indicators > Search Bar(type) > Click Item > Related Actors and Other Analysis

Within the Indicator tab, the IGE (Indicator Graph Explorer) allows the user to visualize how certain IOCs line up with objects in the user's environment without Splunk queries. Visualizing how malware could live in a system can better protect over a wider variety of threats.

Intelligence > Indicators > Click Icon on Item > Info > Graph related Indicator

By clicking on a specific indicator, which are labeled depending on the malware family, the user will be able to see the labels that are attached to the indicator, threat type (what industry it may affect), and if there is a threat actor associated with the indicator. This entire tab can really help the user understand a specific piece of malware or how it may be used against their organization.

Malquery Search:

The next tab within the Threat Intelligence section is the Malquery search; this tab is like a google search bar for malware. When using the search engine, users can look for specific pieces of malware to know more about the threat. This could be a unique ASCII, Hex, or Wide tag to search out anything to do with that identifier such as a ransom message from a ransomware attack or a unique Bitcoin address. After entering a search, the user will find different files and associated information with any threat actors of malicious processes that might be in CrowdStrike's database. This process could help in searching and analyzing related malware to find if there is anything associated with the query. After obtaining a new piece of malware, the ability to use the Malquery Search can help the user better understand how the malware acts or see if anyone has ever seen this before. This can be useful to understand what the next steps should be in the organization's Malware Research Process.

Threat Intelligence > Malquery Search > Enter a Search

Sandbox:

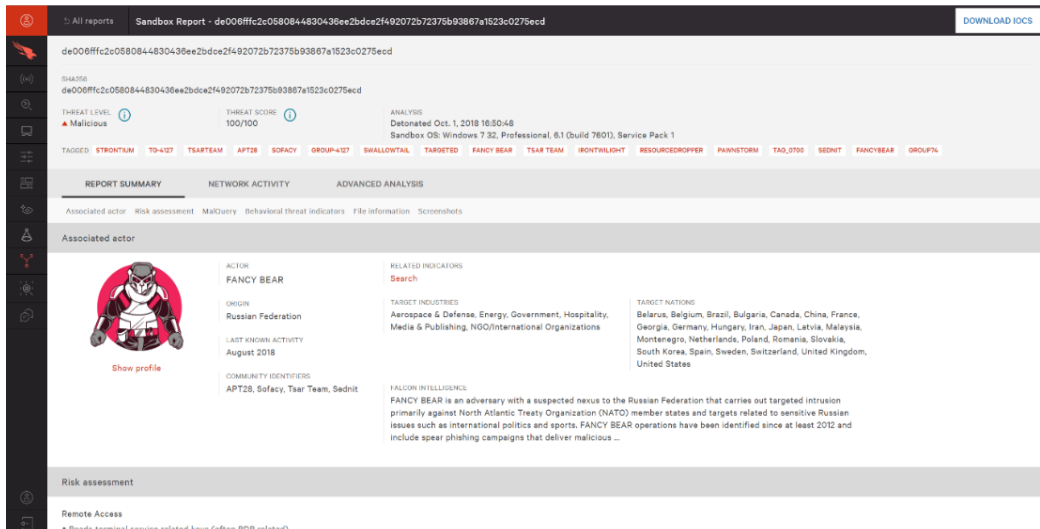


Figure 8: Example of Sandbox Report

The Sandbox is a place for malware that has not been found within CrowdStrike's database to be synthetically run to see what processes the file uses, then allow the user to know how to protect against it. With Sandbox, the user is allowed to detect unknown threats through hybrid analysis which uses data from both runtime analysis and database reference to see how the execution of steps will play out within a piece of malware. The Sandbox uses the kernel to conquer the malware file of the user's choice to uncover the behavior of the file along with how it interacts with the user's system. As the user will be able to see all execution pathways both before and after execution, this allows users to identify more IOCs within the user's system. The Sandbox is also a safe way to analyze malware because even if the system gets infected, the Sandbox will automatically be reset to its original state, making the process purely for the user's education, without fear of harm to the user's own machines. Included below is an image of a Sandbox Report, which is the final product after running malware within Sandbox. It allows users to see the actor associated to the malware, how it will step through the user's system, and what processes will be affected. Below is a kill chain of how to view the logs that the user wants to review after submitting malware to report on:

Intelligence > Sandbox > Submit Sample > Generate Report > View Logs

Conclusion:

CrowdStrike has a multitude of different uses and operations to be explored which can leave an organization more secure from potential threats. Using the overview that was provided in this document should allow the user to hop into CrowdStrike and run processes that can improve the overall security posture of the user's organization. Having this basic knowledge can allow a user to start with CrowdStrike, but there is much more room for growth as queries and other processes can be utilized with more efficiency. These processes can be found within CrowdStrike University and third-party website hyperlinks that can be found below, or in other online forums. CrowdStrike as a company is very transparent in their quest to help others secure systems and can often be found releasing the latest information about tips and tricks for their tools. As the focus of this document was on Threat Hunting, I implore anyone reading this to be mindful of their security stance, as having a reactive stance can lead to more issues down the line. Staying up to date and exploring the world of threat intelligence can lead to a preventative stance, safeguarding the technology and data the user's organization cares for most.

Supplemental Information:



Overall CrowdStrike Links:

Malware Research Process Timeline

[*Introduction to Falcon Malquery \(Malware Search Engine\) \(crowdstrike.com\)*](#)

A Quick Look Through CrowdStrike from Cybrary

[*Crowdstrike Tips & Tricks / Cybrary*](#)

How to Create Exclusions

[*How to Create Exclusions in CrowdStrike – Red Canary help*](#)

Information on how to use and Customize Dashboards within CrowdStrike

[*How to Use CrowdStrike Dashboards*](#)

Cool Shortcut Queries and Ideas for CrowdStrike's Splunk Queries

[*2021-09-10 - Cool Query Friday - The Cheat Sheet : crowdstrike \(reddit.com\)*](#)

Threat Hunting Specific Links:

Additional Information for CrowdStrike Malquery

[*Introduction to Falcon Malquery \(Malware Search Engine\) \(crowdstrike.com\)*](#)

Additional Information for CrowdStrike Sandbox

[*Falcon Sandbox / Data Sheet / CrowdStrike*](#)

Video and Information about Automating Threat Intel

[*How to Automate Threat Intelligence with Falcon X \(crowdstrike.com\)*](#)

Information on how to use CrowdStrike for Detection

[*How to Generate Your First Detection in CrowdStrike Falcon - YouTube*](#)

How to Better Visualize and Detect IOCs within your Organization

[*How to Hunt for Indicators of Compromise in CrowdStrike Falcon - YouTube*](#)

Example of Sandbox Report

[*https://www.crowdstrike.com/blog/tech-center/automate-intel-falcon-x/*](https://www.crowdstrike.com/blog/tech-center/automate-intel-falcon-x/)