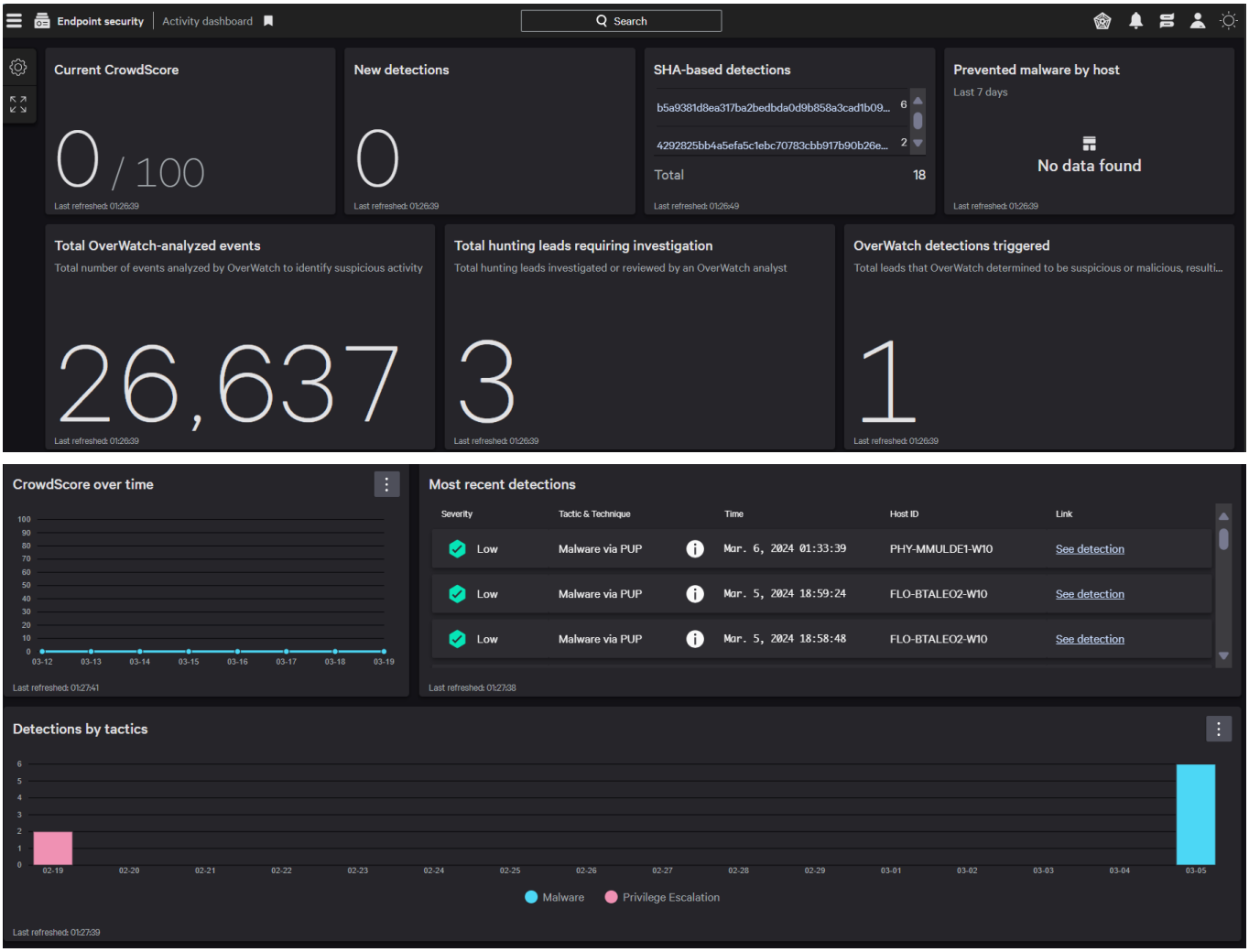
A dashboard is used to get a holistic view over a cloud environment that monitors the features that you would want a generic overview of. In the Endpoint Security Activity dashboard you can see:



- **Current CrowdScore:**
  This is an overall score of the entire environment showing how safe it is out of a 100. CrowdScore leverages the power of Cloud native platform to help clients address common challenges and be more effective in investigating and remediating incidents. It is sort of like the rating of the security of your cloud environment, and crowdscore provides an immediate indication of the current threat level to help organizations prioritize time and resources.

  Along with the score there is a historical trend line as well covering the crowdscore for the past 7 days, by establishing this baseline and monitoring, teams can be more informed and prepared about the threat level state.

With CrowdScore the related detections are compiled into incidents. This summary view gives us an active, real time list of incidents that are impacting the organization.

CrowdScore aggregates all of the relevant data for a threat into a new interface element we refer to as an incident. Incidents are ranked by CrowdScore with much higher granularity than the confidence values assigned to individual alerts. And the incident ranking is based on an analysis of all of the contextual data compromising an incident. That context is very data-rich compared to the limited amount of information available based on individual alert definitions themselves.

Incidents have a time span associated with them, as opposed to being simple, instantaneous events without accompanying contextual information. Incidents can be replayed, visually depicting the unfolding of the incident activity, providing the analyst with an intuitive understanding of the time component of an incident. CrowdScore also identifies likely occurrences of lateral movement.

CrowdScore actually *improves* with the development and the addition of new indicators of attack(IOAs). And CrowdScore can incorporate custom, user-developed IOAs just as easily as IOAs that come with the CrowdStrike Falcon platform.

- ## Malware Infection Protections

Falcon uses multiple methods to prevent and detect malware. These methods include Machine Learning, exploit blocking, custom blacklisting and behavioral analysis with what we call indicators of Attack(IOAs). This unified combination of methods protects you against known, unknown and file-less malware.

1: Go the prevention settings of the Falcon User Interface

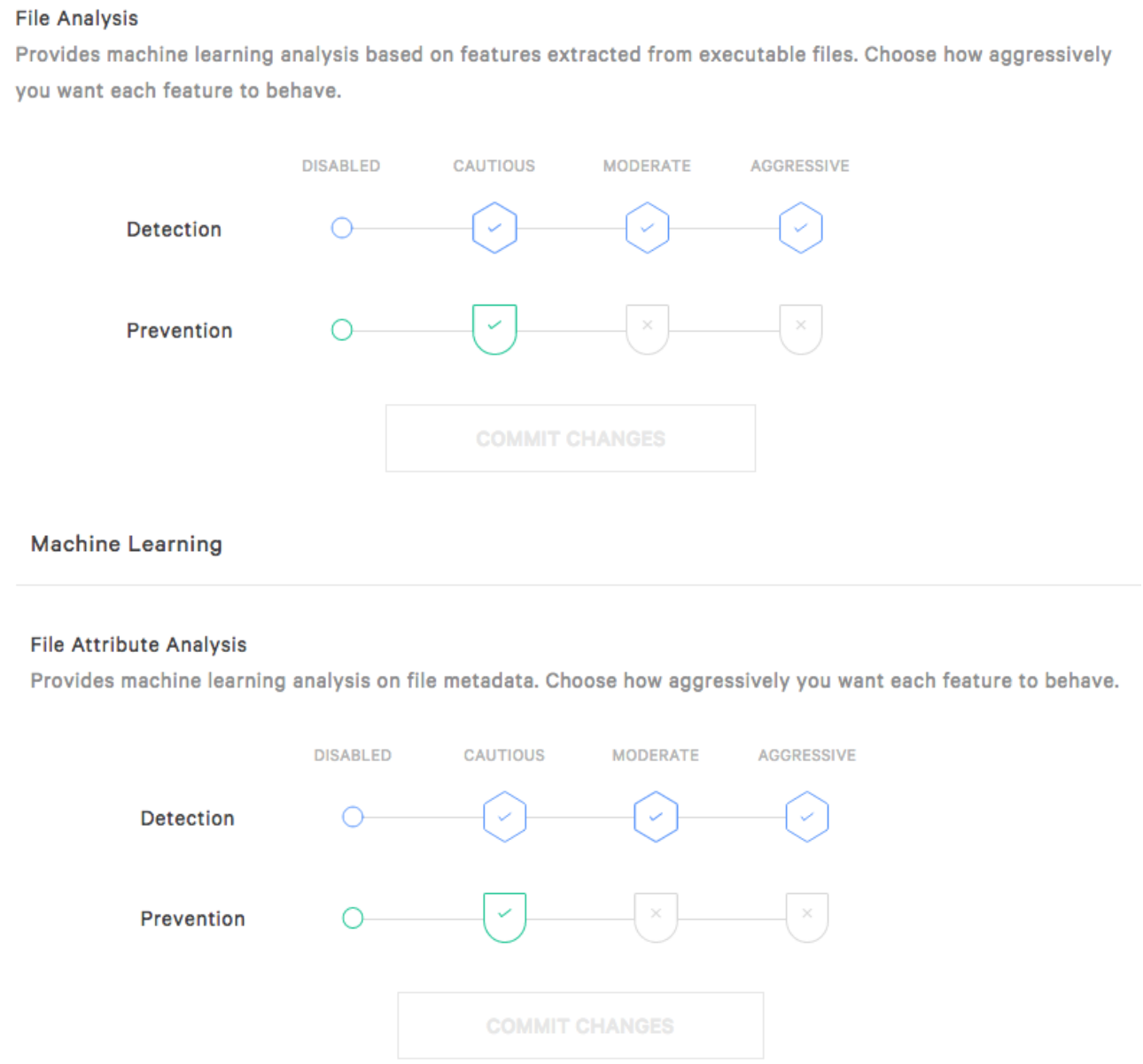
You can configure prevention features in the configuration app. Once in the app, make sure you are in prevention policy. Please note that you need **Admin** credentials to configure prevention features on the Prevention app settings page. Also, the configuration changes are almost immediate and only take a couple of seconds to be updates on the endpoints.

2: Configure Machine Learning:

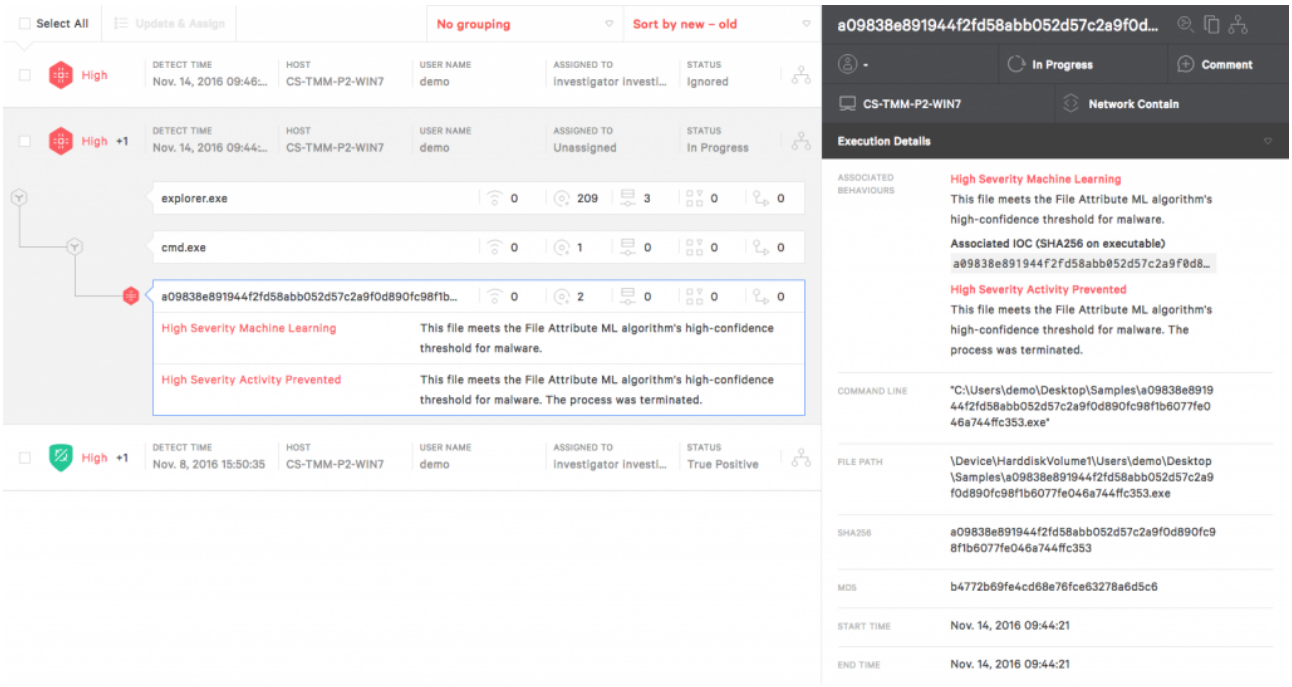
- Let’s start by configuring Machine Learning. Machine Learning allows Falcon to block malware without using signatures. Instead, it relies on mathematical algorithms to analyze files.
- The File Attribute Analysis provides machine learning analysis on file metadata, while Static file Analysis provides analysis on features extracted from executable files.
- Notice that you can set up independent thresholds for detection and for prevention. So, you could for example choose to receive detection alerts for any suspicious files, even if it’s a just a little bit suspicious by selecting Aggressive, but you can choose to

automatically prevent only if the machine learning is very sure that it's malicious, by selecting Cautious.

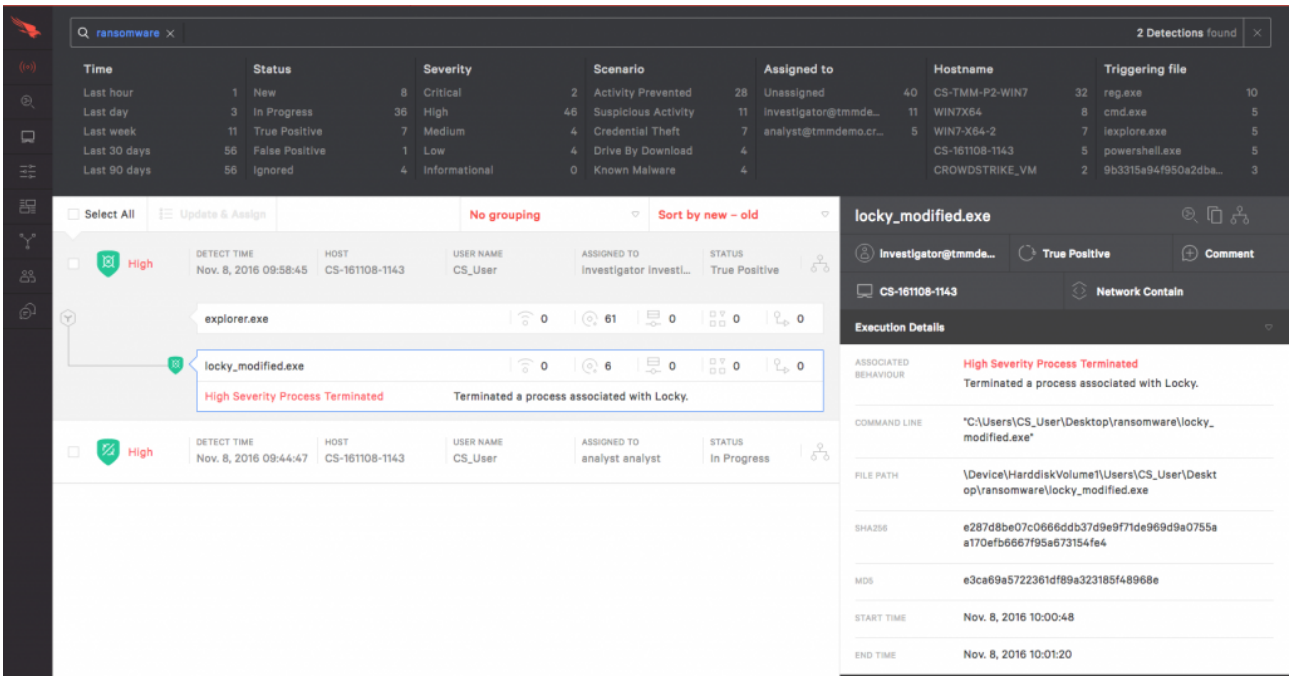
- To edit those settings, click Edit and then chose the setting you want. You can set prevention and detection separately to either Disabled, Cautious, Moderate, or Aggressive, but logically, the Detection settings always have to be stronger or equal to the Prevention setting.
- Click Save when you are done



This is what a Machine Learning Block will display in the Falcon User Interface.



Below is an example of ransomware being caught by machine learning.



3: Preventing file-less malware with exploit blocking

The Falcon machine learning engine is great to block known and unknown malware but, malware does not always come in the form of a file that can be analyzed by machine learning. Malware can be deployed directly into memory using exploit kits. This is why Falcon also includes an exploit blocking function.

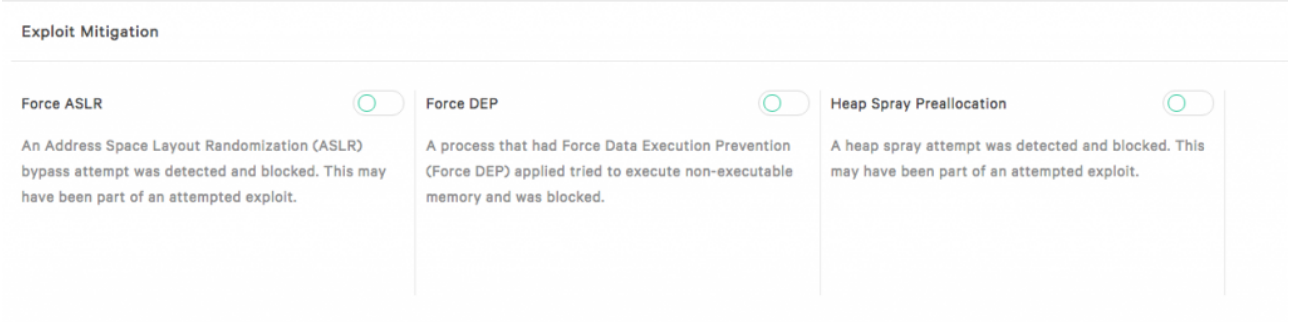
Note:
File-less malware is malware that is not written to disk but is run straight into memory. This is different from malware-free attacks where the adversary do not use malware. Instead

they might, for example, use social engineering, exploits or credentials thefts. Falcon also prevents malware-free attacks with exploit blocking and Indicators of Attacks.

Each of the exploit protection can be turned on or off in the same window as the machine learning configuration.

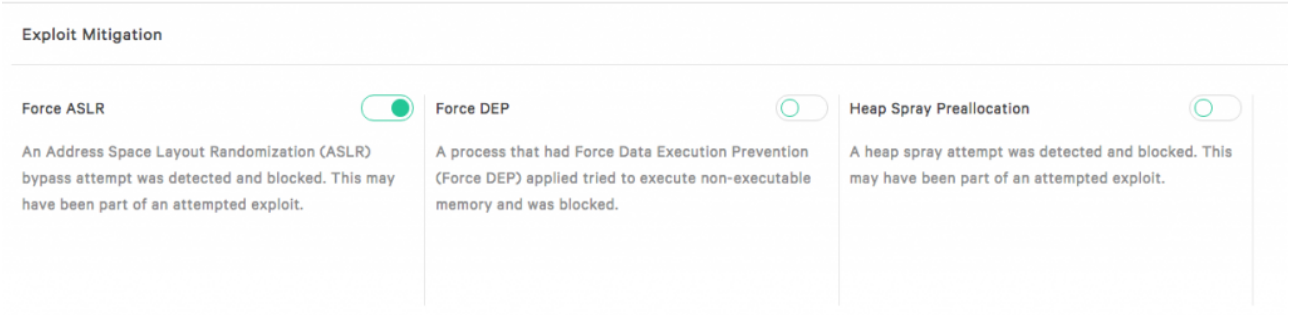
To turn an exploit mitigation on or off, just slide the toggle for the exploit mitigation you want to change.

In our example we are going to turn on Force ASLR mitigation.



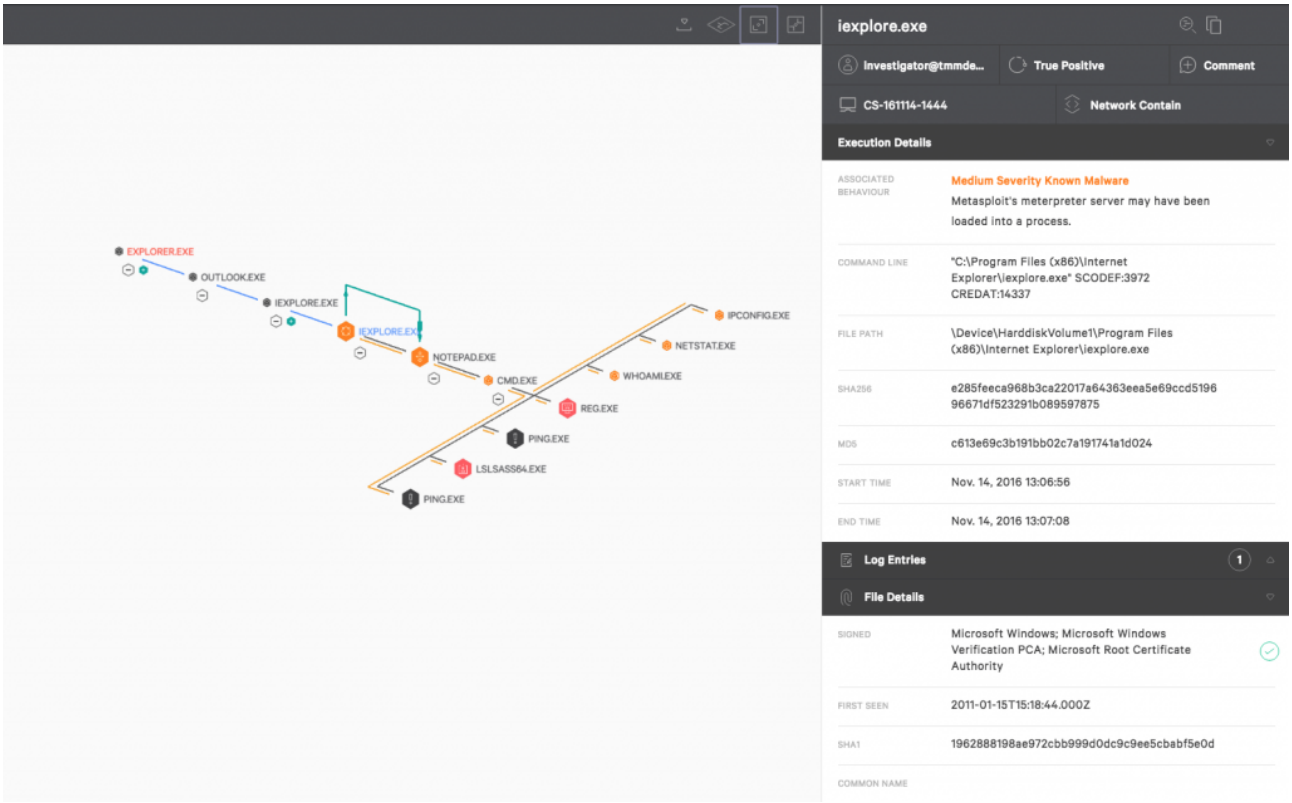
Let's slide the toggle to the right and confirm the changes.

The toggle is changed to green and enabled.



If you want to disable the prevention for that exploit, slide to toggle to the left and confirm that you want to disabled.

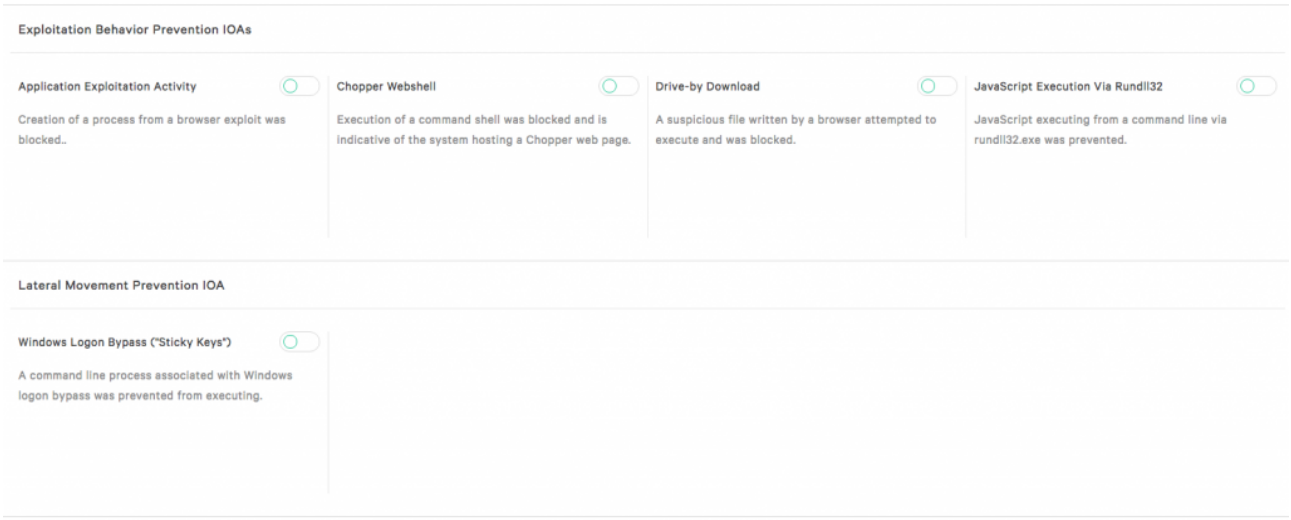
Here is an example of exploit blocking detection in the Falcon User Interface.



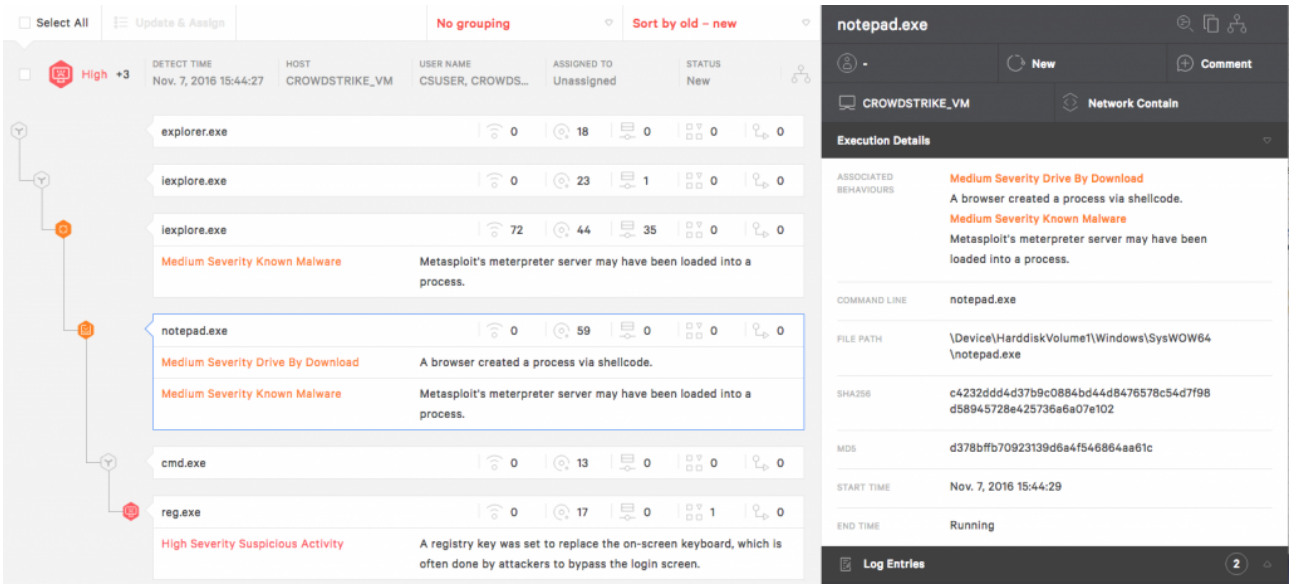
4: Preventing malware with Indicators of Attacks

Exploit blocking provides another layer of protection but may not be sufficient at times because some file-less malware do not use exploit kits. Ransomware, for example, has some infamous examples of file-less ransomware that does not use exploits. This is why Falcon also uses Indicators of Attacks, or IOAs, to protect the systems. IOAs look across both legitimate activity and suspicious activities and detect stealthy chains of event that indicate malware infection attempts. Because most IOAs also prevent attacks that do not use malware, they are enabled by default. But some, such as adware and ransomware specific IOAs can be configured.

You can enable or disable them in the current window by sliding the toggles just like we did for exploit blocking.

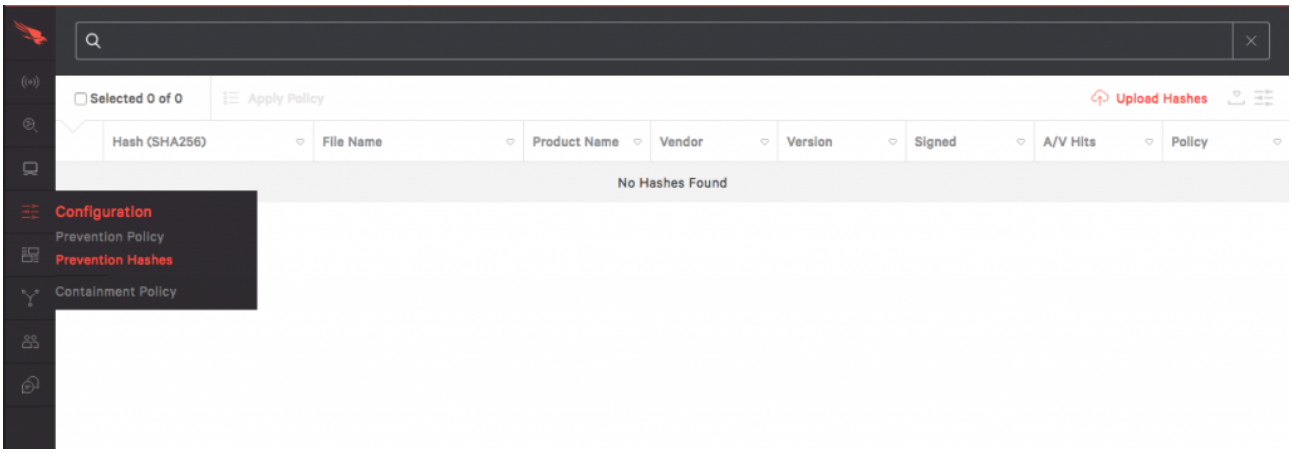


Remember, earlier we saw an example of ransomware blocked by machine learning. Now we can see another ransomware, blocked, but this time, it was prevented by an Indicator of Attack.

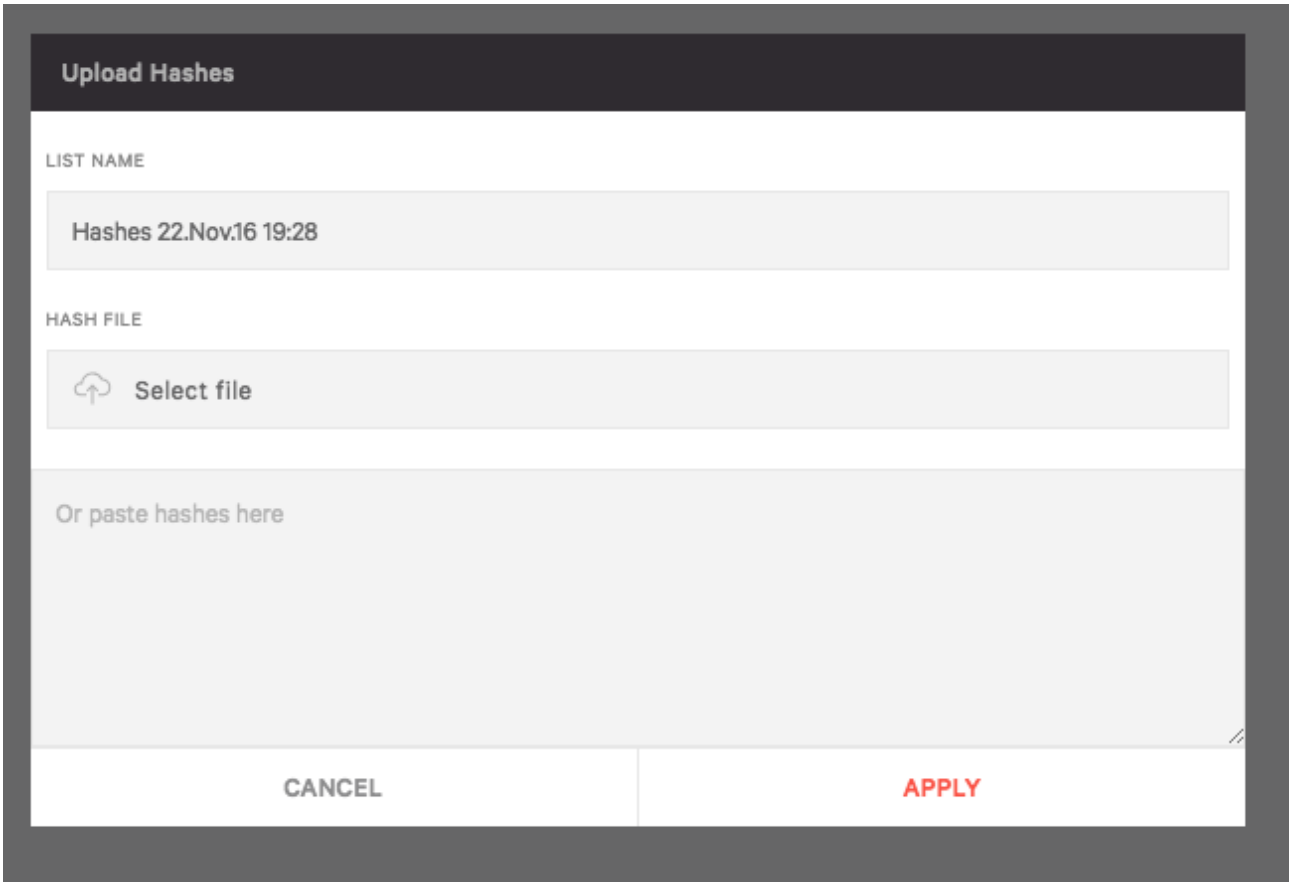


5: Preventing malware with custom Blacklisting

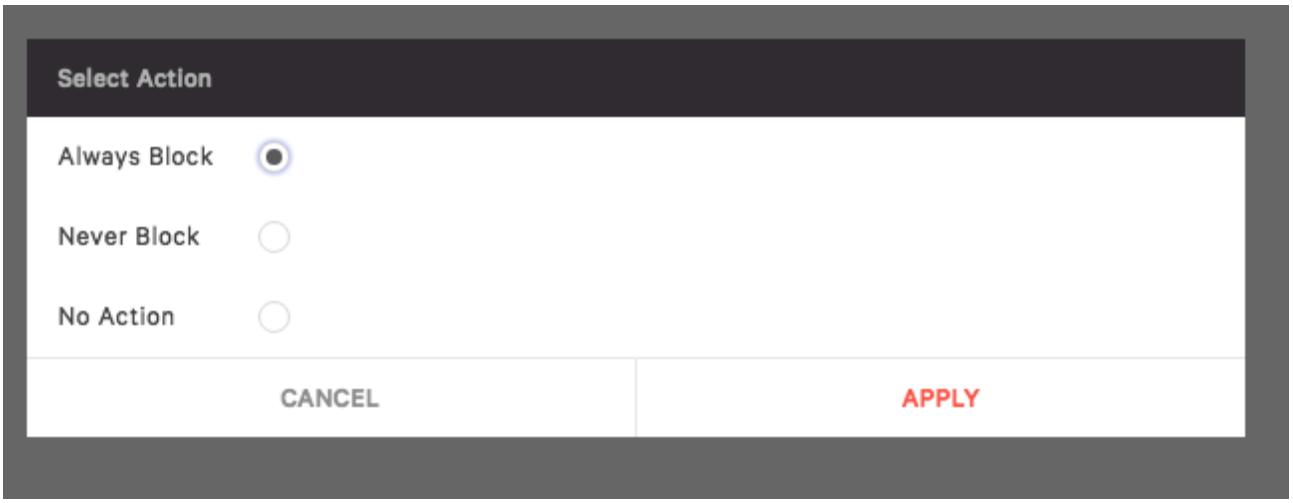
There are cases when you might want to blacklist some applications because you are certain that you never want them to run in your environment.
Falcon allows you to upload hashes from your own blacklists or whitelists. For that, we have to be in the Configuration App, Prevention Hashes window. To add hashes to our blacklist select the “Upload Hashes” in the upper right hand corner. Note, you’ll need admin privileges.



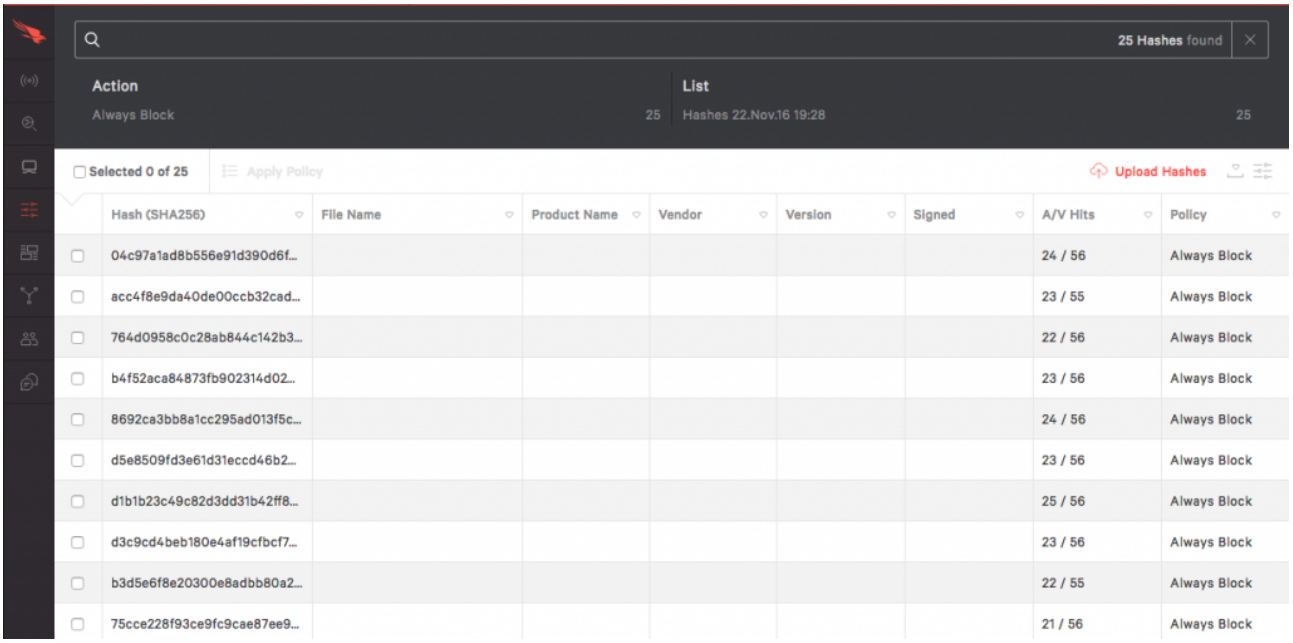
Then we'll drag and drop the list. The list can be a text file with one MD5 or SHA1 hash per line. All valid MD5 and SHA256 hashes will be uploaded. Rows with non-MD5/SHA256 hash format will be ignored.



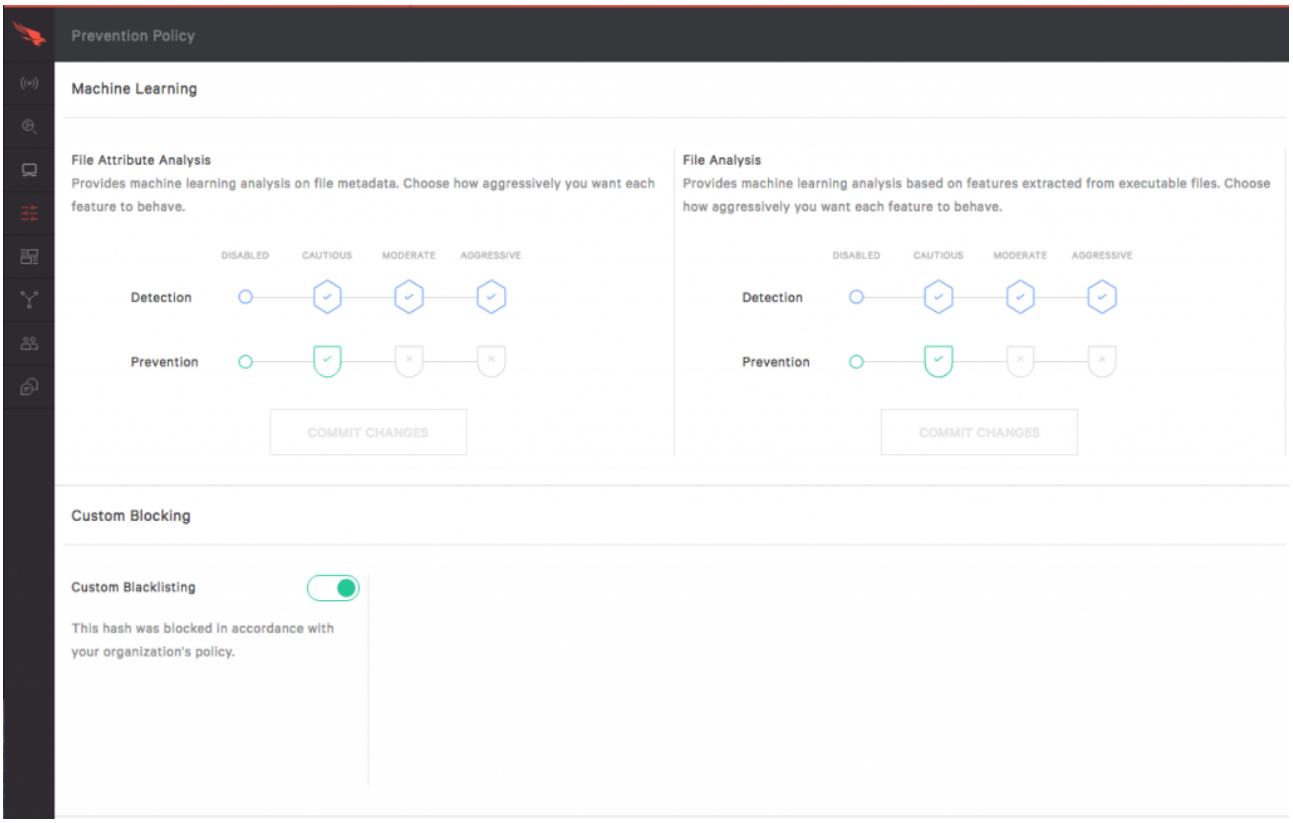
After clicking "Apply" an action to take when hashes are encountered in the environment needs to be selected. If creating a whitelist select "Never Block". In this case I'll select "Always Block" and then "Apply"



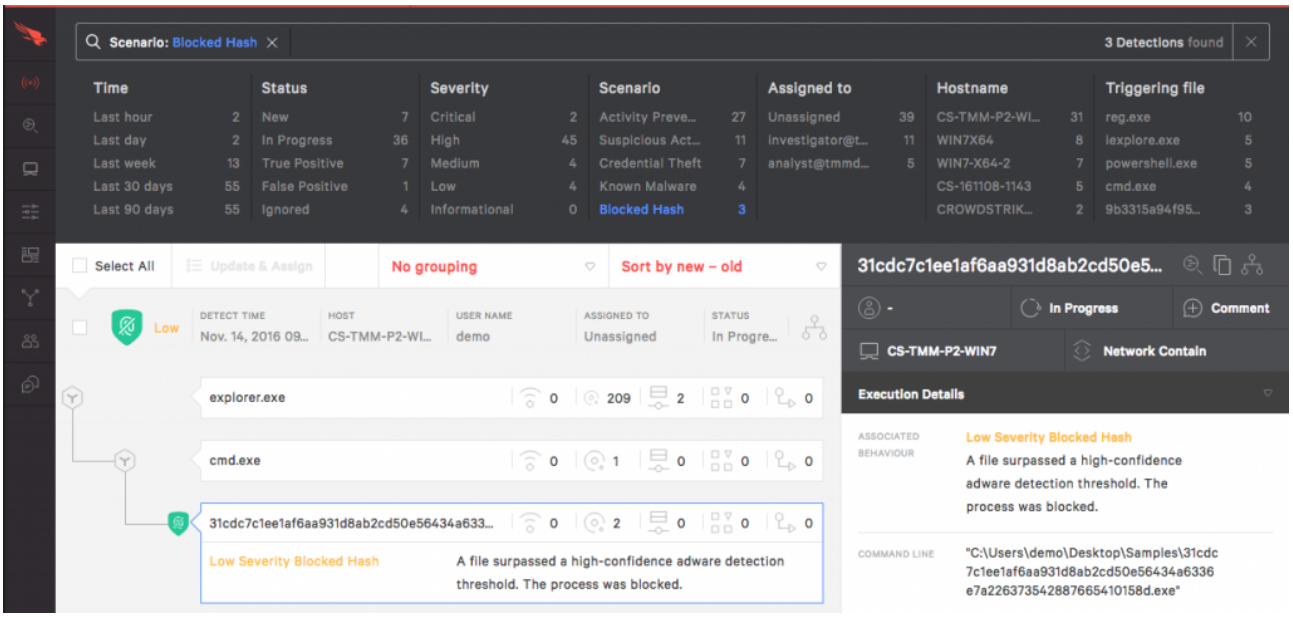
You can see that the hash has been uploaded. If you want to upload more hashes later, click on the upload icon on the top right corner of the window.



Now we also need to make sure that custom blacklisting prevention is enabled.
For that, let’s go back to the settings page and check. If it’s not enabled, you can use to toggle to enable it.



This is how this prevention shows up in the Falcon User Interface. It will show as being blocked according to your organization policy.



Cloud Security Overview

CrowdStrike Cloud Security secures your entire cloud-native stack, on any cloud, across all workloads, containers, and Kubernetes applications.

These product are part of the Cloud Security solution:

- **Cloud Security Posture Management (CSPM)** gives visibility into your entire cloud infrastructure. CSPM continuously monitors your cloud services for critical security issues, common configuration errors, and patterns of suspicious behavior. Guided remediation and policy and compliance enforcement help keep your cloud environment secure. To learn more, see CSPM Overview.

CSPM terminology:

- **Assessment**: An individual instance when CSPM compares your cloud settings to the CSPM policies.
- **Indicator of misconfiguration (IOM)**: A configuration setting that doesn't follow recommended security guidelines and might become a security vulnerability in a cloud environment. In CSPM, IOMs are labeled as findings.
- **Indicator of attack (IOA)**: A pattern of suspicious behavior that suggests an attack might be underway. In CSPM, IOAs are labeled as findings.
- **Findings**: IOMs and IOA detected by assessments and posted on CSPM dashboards and assessment pages.
- **Severity**: A qualitative ranking of security risk as defined by CSPM. from least severe to most severe,: Informational, Medium, and High.
- **Confidence**: A High, Medium, or Low score based on IOA events and correlated events.
- **Score**: An overall IOA risk score based on Severity and Confidence.
- **Correlated event**: Events indicating actor behavior before or after the IOA-triggered event. Correlated events increase the Confidence score.
- **Service subtype**: Components of cloud services that are inspected to identify security risks, such as security group or encryption.

Policies

CSPM policies are a set of rules defined to detect misconfigurations of the cloud resources (IOMs) or to detect suspicious behavior patterns (IOAs). You can enable or disable default policies that are defined by CrowdStrike, and you can also define your own custom policies.

Compliance benchmarks

Your cloud configuration is compared against industry benchmarks for compliance. You can enable or disable alerts for individual benchmarks, and you can also create your own custom compliance frameworks.

Assessment schedules

You can select how frequently your cloud environment is assessed for misconfigurations. You can also exclude AWS services and regions from assessment.

You can monitor all the CSPM findings here in Cloud Security> Monitor> Activity


Saved filters
Company
Cloud group
Clear all
Registered and unregistered cloud accounts
AWS
Azure
GCP
Registered
Unregistered
Last refreshed: 14:30:34
Coverage
Containers
Images
Servers
Managed
Unmanaged
Last refreshed: 14:30:36
Unmanaged asset trend
11-21
11-22
11-23
11-24
11-25
11-26
11-27
Unmanaged containers
Unmanaged servers
Unassessed images
Unregistered cloud accounts
Last refreshed: 14:30:35
IOA findings
High
Critical
High
Medium
Informational
Last refreshed: 14:30:34
Misconfigurations
High
Critical
High
Medium
Informational
Last refreshed: 14:30:34
Detection trends
Critical
Misconfigurations
IOA events
Last refreshed: 14:30:34
Server protection risk by severity
Servers with cloud containers
Linux on-prem servers
Linux cloud servers
+ 3 more
Last refreshed: 14:30:34
Server detections by tactic
All
Critical
High
Medium
Low
Informational
Last refreshed: 14:30:34
Server detection trends
Critical
Detections
Last refreshed: 14:30:34
Container detection by severity
Critical
High
Medium
Low
Informational
Last refreshed: 14:30:34
Container findings by seve...
Unidentified conta...
Critical
High
Medium
Low
Informational
Last refreshed: 14:30:34
Container detection trends
Critical
Detections
Kubernetes IOM
Unidentified containers
Last refreshed: 14:30:35
Servers & containers vulnera...
Servers
Vulnerable images in use
ExPRT.AI
Image assessment trends

Explanation of managed threat hunting

Threat hunting is a proactive, ongoing search through data, environments, and endpoints to discover activities that evade detection from existing security tools. Threat hunters make observations that identify, prioritize, and notify of potential threats before an attack.

OverWatch hunting methodology is focused on adversary behavior. The methodology doesn't focus only on vulnerabilities that an adversary might exploit. Instead, it identifies the adversary's goal and what they try to accomplish—regardless of CVE. Even so, the team stays up-to-date with the overall threat landscape and routinely identifies various classes of attack and targeted post-exploitation attempts. OverWatch also works closely with CrowdStrike's Intelligence team who identify emerging threats and vulnerabilities across the world.

Here are two basic examples of managed threat hunting:

- OverWatch observes that a user remotely connected to a server using Remote Desktop Protocol (RDP) and executes suspicious commands. Within minutes of the event, OverWatch investigates all logins to that system, compares interactive and RDP logins, and investigates this user's usage of RDP across your environment.
- OverWatch identifies a suspicious process on a host. OverWatch investigates where that suspicious file executed in your environment and how many times. Using the CrowdStrike Threat Graph, OverWatch determines how prevalent this file is across other customers and if the file demonstrates similar behavior elsewhere.

The examples show that OverWatch is proactive, unlike a Security Operations Center (SOC) which is reactive. Many SOCs wait for rule-based security tools to send notifications before taking action. In contrast, threat hunting seeks to uncover and prevent the adversary's next action before it occurs. Threat hunting also recognizes that adversaries are able to evade automated and rule-based systems that SOCs often rely on.

Because of these differences, a threat hunting team and a SOC team are complementary. The SOC helps provide responses to notifications of known malicious activity identified by automated tooling. However, due to time constraints, expertise, and the tools needed to effectively hunt, SOC teams cannot perform the functions of a professionally managed threat hunting service.

FALSE POSITIVES:

In an EDR solution there is always a 50% chance of encountering false positives, this is also what analysts report as 'alert fatigue'. FP's get repetitive and are an unnecessary overhead on the EDR's part to always encounter the same kind or multiple FP's repeatedly.

The EDR classifying an action or object as a threat even when it is not is the true definition of False positives and a False negative is the reverse where it seems that there is no error or alert from the object/action but there should have been. The difference between the two is the reason False positives are also considered as part of the alert base initially.

The way to deal with them are fortunately optimizing the solution to build better efficiency and SO's can take the following steps to address them:

1. Review and classify alerts
   If you see an alert due to any behavior that is detected as suspicious or malicious and it shouldn't be either you can suppress them as well as alerts that are not false positives but unimportant. This helps to train your threat protection solution and can reduce the number of false positives or false negatives over time and reduces alert fatigue or alert queues redundancies.
2. Review remediation actions that were taken
   Actions such as quarantining or stopping files/processes are regarded as remediation steps that can be reviewed or undoed if not required. MDE is extremely malleable in this option as it allows undoing multiple actions at one time.
3. Review and define exclusions
   Exclusions are to be done very mindfully as it is defined or detected by the EDR but there are no remediations are set to it. You can set different kinds of indicators from MDE or Intune for different kinds of exclusions.
4. Submit an entity for analysis
   You can submit entities, such as files and fileless detections, to Microsoft for analysis.

Microsoft security researchers analyze all submissions, and their results help inform Defender for Endpoint threat protection capabilities. When you sign in at the submission site, you can track your submissions.Your submission is immediately scanned by our systems to give you the latest determination even before an analyst starts handling your case. It's possible that a file might have already been submitted and processed by an analyst.

5. Review and adjust your threat protection settings

   Defender for Endpoint offers a wide variety of options, including the ability to fine-tune settings for various features and capabilities. If you're getting numerous false positives, make sure to review your organization's threat protection settings. You might need to make some adjustments to:

   - Cloud-delivered protection
   - Remediation for potentially unwanted applications
   - Automated investigation and remediation

MITRE ATT&CK FRAMEWORKc: