# Monitoring in Falcon CrowdStrike

## What is Falcon.

* Falcon is an Endpoint protection solution that provides advanced.
  + Detection
  + Prevention
  + Monitoring
  + Search capabilities
* Provides the visibility across endpoints throughout an environment.

***Components***

* Sensor
* Cloud

Taking proactive detections and prevention actions by installing a lightweight sensor on every endpoint which also gathers appropriate system events.

The gathered data by the sensors are continuously streamed to CrowdStrike. CrowdStrike then corelate the events (behavioural patterns). These patterns are detected in real time using CrowdStrike’s **Threat Graph data model**.

## Known and unknown threat Detection capabilities of Falcon

**For known threats**, CrowdStrike provides Cloud-based Antivirus and Indicators of compromise (IOC).

**For Unknown threats or zero-day threats**, Using CrowdStrike’s Threat Graph model, IOA analysis using Machine Learning, recognises behavioural patterns to detect new attacks.

### Unified Detection Monitoring

Unified view is a central interface where you view and monitor detections. You see the same data that are available in separate, module specific views.

### CrowdStrike XDR

To leverage CrowdStrike capabilities, these are the supported CrowdStrike subscriptions.

* Endpoint detections
* Mobile detections
* Identity-based detections

#### Third party XDR integrations to send detections to CrowdStrike.

You can also include 3rd party XDR detections and work on them in CrowdStrike. These are some of the XDR 3rd party data-sources supported in CrowdStrike.

* Core light zeek.
* ExtraHopReveal(x).
* Microsoft Graph API for Microsoft Defender for Office 365 and Azure Active Directory.
* Mimecast Email security.
* Netskope SSE
* Okta Identity management
* PaloAlto Next Gen Firewall
* Skyhigh Security Secure web Gateway

## Incident creation

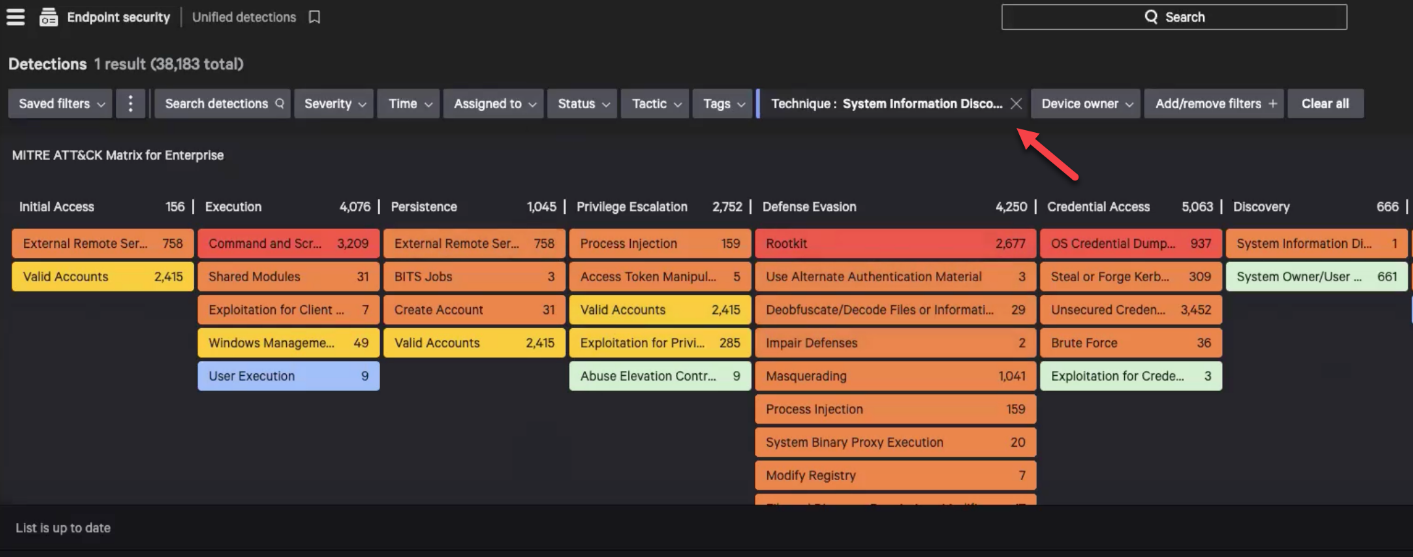
We can include 200 detections in a single incident, where currently a given detection can be added to only one incident. The incidents we create are available in the incident workbench, where we can assign, investigate more deeply.

After we create an incident, a link to that incident is included to the related detections.

## Filter with Mitre Attack Matrix

We can filter the detections based on the Mitre Attack Matrix. You need to enable Mitre Attack Matrix and select the type of Matrix to filter by based on the environment.

* ATT&CK Matrix for Enterprise
* ATT&CK Matrix for Mobile
* ATT&CK Matrix for ICS
* Falcon Detection Methods for Enterprise
* Falcon Detection Methods for Mobile



## File Integrity Monitoring

With the help of ***FileVantage***, we can see when potentially unauthorized changes happening in your environment. FileVantage monitors the sensitive directories, files and registries for changes and reports them in real time on a dashboard.

* To create and edit file integrity rules, assign them to file integrity policies and assign file integrity policies to host groups.
* FileVantage stores file integrity data for 30 days. To storage data locally beyond this retention period, we can use **Falcon data replicator**