# 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.

Capabilities like

* Custom allowing and blocking.
* Malware blocking
* Exploit blocking
* IOA-based prevention (Indicators of Attack).

The gathered data by the sensors are continuously streamed to advanced threat intelligence cloud. CrowdStrike then links between events across the Falcon sensor community (behavioural patterns). These patterns are detected in real time using CrowdStrike’s **Threat Graph data model**.

## Detection capabilities of Falcon

* **Known Threats –** 
  + cloud-based Antivirus (AV).
  + Indicators of Compromise (IOC).
* **Unknown or zero-day threats –** 
  + Indicators of Attacks (IOA) detections using machine Learning
    - Using CrowdStrike’s Threat Graph model, IOA analysis recognises behavioural patterns to detect new attacks.
* ***Sensor integrating with SIEM*** - Provides the Falcon SIEM Connector which allows you to send detections and audit events to your SIEM. Falcon also provides Streaming API to enable integration with 3rd party SIEMs.
* ***Data Falcon send to cloud*** –
  + gathering the data necessary to identify, understand and respond to attacks.
  + The amount of data transmission to cloud varies depending on each host’s activity.
  + There are some default set of system events that are continually monitored for suspicious activity.
  + When such activity is detected, additional data is collected to better understand the situation.
* ***How Falcon safeguard customer data –***
  + A TLS-encrypted tunnel is used by the CrowdStrike to send between the sensor and the cloud.
  + CrowdStrike uses certificate pinning on sensor side. The sensor only communicates with the endpoints that have a known certificate.
  + You can allow endpoints in firewall that Falcon sensors only communicate with CrowdStrike.
  + CrowdStrike tags the customer data with unique Customer ID, the queries and exchange of data is limited to the scope of specific customer ID, which further secures the data.
  + All data in CrowdStrike cloud, including backups are encrypted with Industry standard AES256 encryption.
  + Direct access to the endpoints is limited to engineers with business need. Access is protected by VPN and multi-factor authentication.

## Before you begin

* Recommended using Falcon AV. Running more than one AV can cause unexpected results.
* Having 2 devices
  + **Test device** with falcon sensor installed in it.
  + **Management device** with Chrome. Used to access Falcon console.
* Setting Falcon account with **Two-factor authentication.**
* When you install Falcon sensor on the devices, those devices are called ***host*.**

## Sensor Installation

**Manual Installation** can be a choice for small number of installs.

* You can download the sensor for OS from ***Host setup and management > Deploy > Sensor downloads***.
* You need to copy customer ID checksum (CCID) as a trial user.

**Automatic Installation** on many devices using a deployment tool such as Windows ***System Center Configuration Manager*** SCCM.

* Download the sensor at ***Host setup and management > Deploy > Sensor downloads***.
* Copy the customer ID checksum (CCID).
* Configure the deployment tool to use this command.
  + <installer\_filename>/install/quite/norestart CID=<CCID>

## Host Group setup

Groups are collections of hosts in the organization. You can use these groups to control the endpoint protection and sensor updates for each group. You might also create groups for general users devices and another group for executive devices.

You can create host groups in ***Host setup and management > Host groups*** .

MHA –

total servers – 190

production servers – 113

Deployment servers – 61

FAX server – 1

Workstation – 353

Identity protection servers – 3

## Prevention policy

Set of rules that control how Falcon responds to potentially malicious activity identified by the sensors.

* When you create your group, Falcon automatically assigned it to use **Default Policy**, which is detection only.

## CrowdStrike Monitoring

### 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.

### Detections in CrowdStrike

These are the CrowdStrike detections that are available in unified view.

* Endpoint detections
* Mobile detections
* Identity-based detections
* Cloud run-time detections

#### 3rd party detections

You can also include 3rd party 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

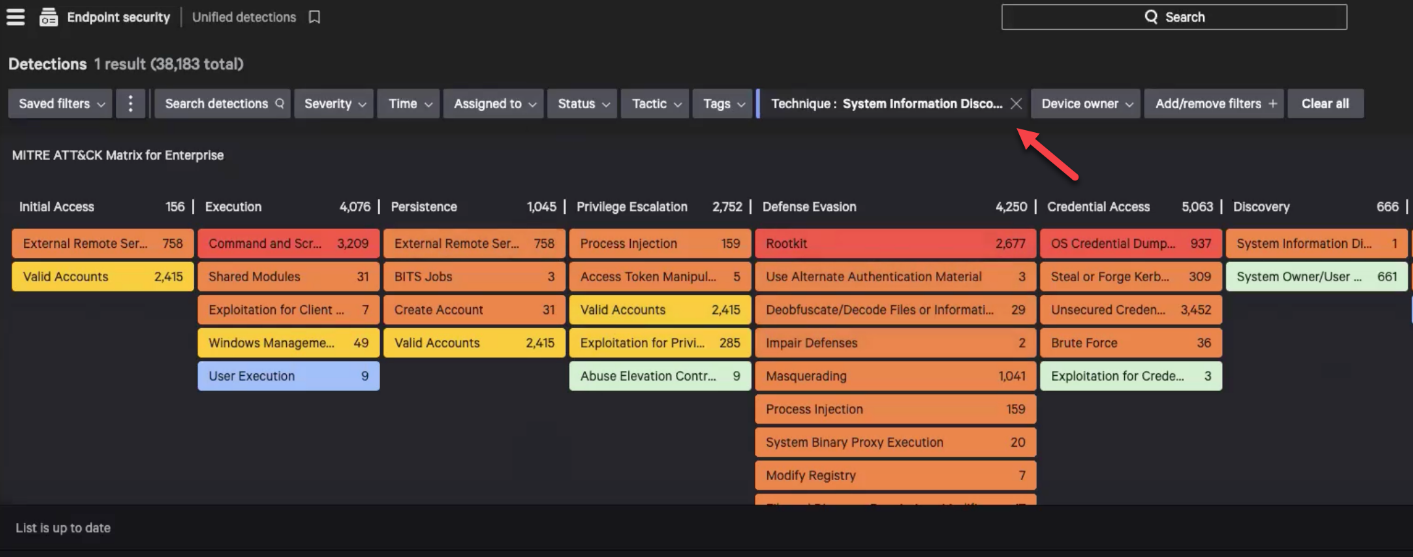
We can include 200 detections in a single incident, where currently a given detection can be added to only one incident. The incidents we create are available in the incident workbench, where we can assign, investigate more deeply.

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**