CrowdStrike QRadar Integration App
Installation and User Guide

CrowdStrike Falcon EndPoint
Version: 1.0.0

Installation Document

Overview:

This document describes how to integrate the QRadar Platform with CrowdStrike to escalating events.

The integration installs to the QRadar platform a set of custom fields which are designed to support the following use cases:

1. Ingests and displays detection alerts from CS instance
2. Contain systems and Push IOCs
3. Investigate detection alerts from CrowdStrike (Event/alert data) by right clicking into alert and opening CS in new window
4. Detection status management – Ability to change the CrowdStrike status of detections (different detection status available from CrowdStrike)

Prerequisites:

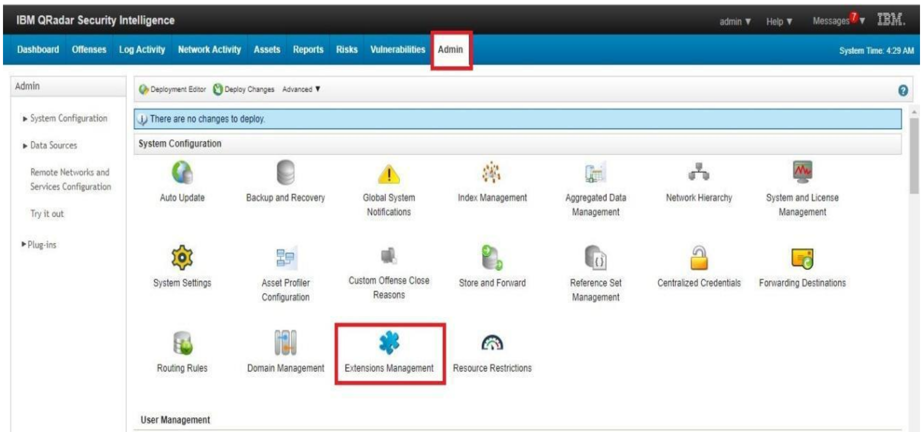
Verify that your environment meets the following requirements:

- QRadar platform version is 7.2.8 Patch 14 or later.
- You designated a Master Administrator account on the QRadar platform.
- You downloaded the CrowdStrike integration file, CrowdStrike-Falcon-EndPoint.zip, from the IBM Security App Exchange

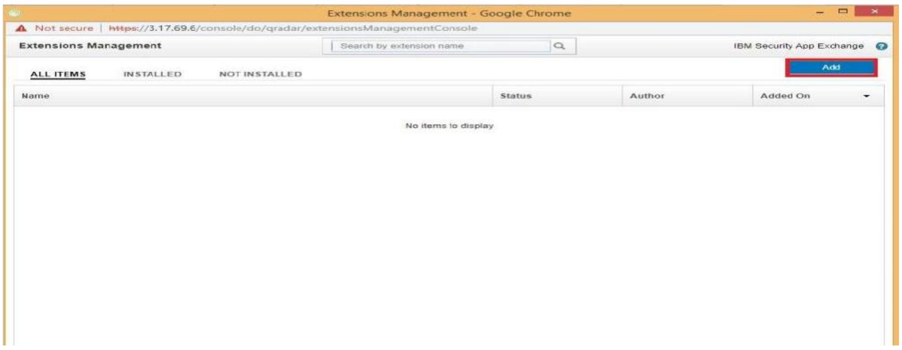
Install the extension:

Perform the following to install the integration on the QRadar:

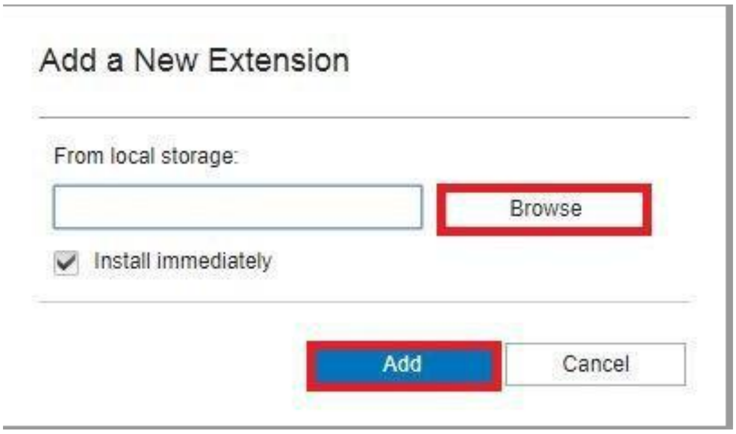
1. Login to QRadar platform
2. Open the *Admin* tab and click *Extension Management* under *System Configuration*



3. Click the *Add* button


Extensions Management - Google Chrome
Not secure | https://3.17.69.6/console/do/qradar/extensionsManagementConsole
Extensions Management
Search by extension name
IBM Security App Exchange
Add
ALL ITEMS
INSTALLED
NOT INSTALLED
Name
Status
Author
Added On
No items to display

4. Browse the downloaded App package which Dev team has sent
5. Click *Install Immediately* and click *Add* then click the Install

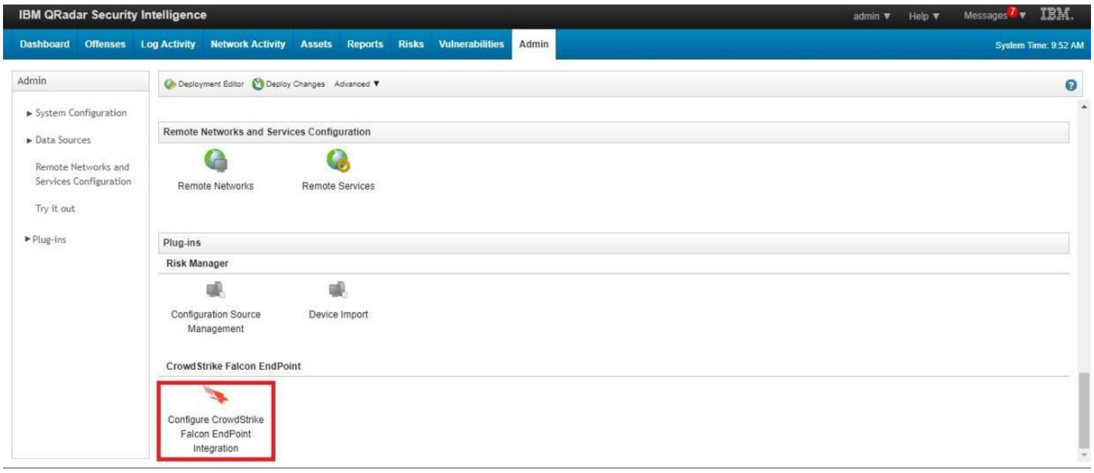


6. Please verify whether there are 26 Custom Event Properties and one Log Source a click the *Install button.*
7. Once the installation is done, click the **Installed** tab and check whether the app is successfully installed

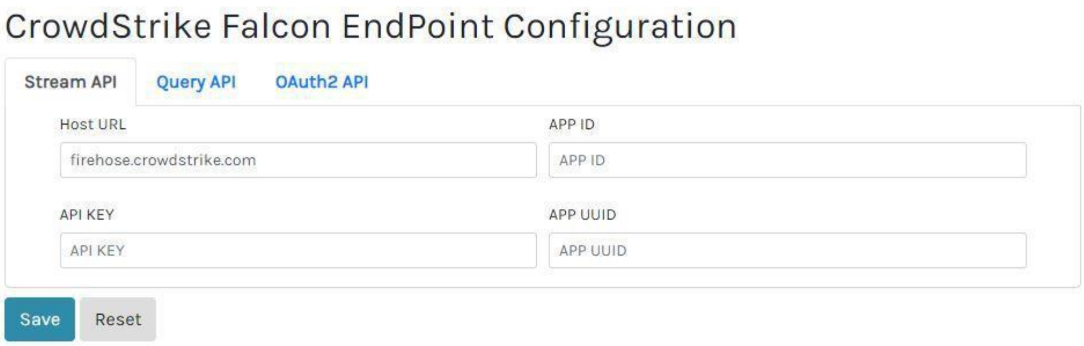
Setup the Configuration:

Once the Installation is done navigate to Admin tab and open the “Configure CrowdStrike Falcon EndPoint Integration” icon and provide the Intel API customer ID and Keys using the below steps,

1. Under the *Plug-ins* click the *Configure CrowdStrike Falcon Intel Integration.*



2. In the popped-up window provide the below,
    a) Stream API tab
        i. Host URL: **firehouse.crowdstrike.com**
        ii. APP ID: As provided by a CS representative
        iii. API Key: As provided by a CS representative
        iv. API UUID: As provided by a CS representative


CrowdStrike Falcon EndPoint Configuration

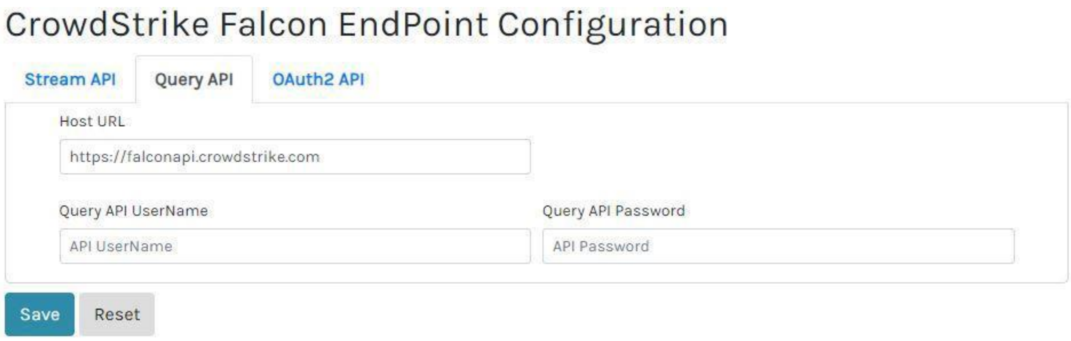
Host URL: firehose.crowdstrike.com

APP ID: APP ID

API KEY: API KEY

APP UUID: APP UUID

    b) Query API tab
        i. Host URL: https://falconapi.crowdstrike.com
        ii. Query API UserName: As provided by a CS representative
        iii. Query API Password: As provided by a CS representative

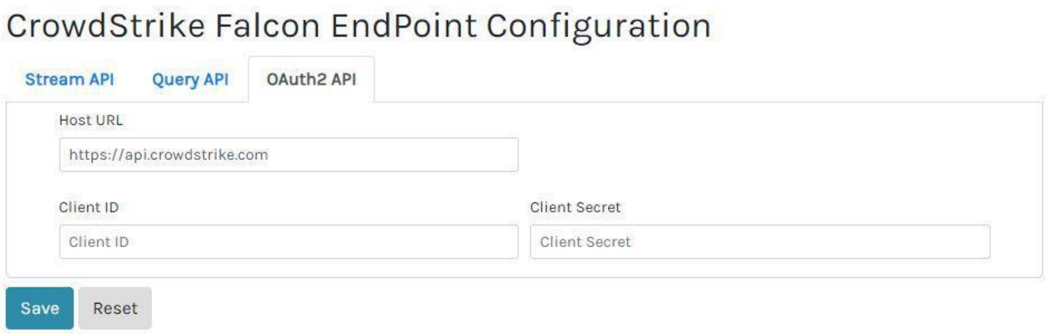

CrowdStrike Falcon EndPoint Configuration

Host URL: https://falconapi.crowdstrike.com

Query API UserName: API UserName

Query API Password: API Password

    c) OAuth2 API tab
        i. Host URL: https://api.crowdstrike.com
        ii. Client ID: As provided by a CS representative
        iii. Client Secret: As provided by a CS representative


CrowdStrike Falcon EndPoint Configuration

Host URL: https://api.crowdstrike.com

Client ID: Client ID

Client Secret: Client Secret

3. Click the Save button

User Document

Overview:

This document describes how to use the CrowdStrike Falcon Endpoint app functionalities in QRadar platform.

The integration enables the below functionalities.

1. QRadar events(in log activity tab) for CrowdStrike Detections.
2. Open the CrowdStrike Falcon host link in new window.
3. Detection status management – Ability to change the CrowdStrike status of the detection.
4. Update Containment status.
5. Upload IOC into CrowdStrike

Prerequisites:

Once app is installed in QRadar Instance, proceed to setup the configuration

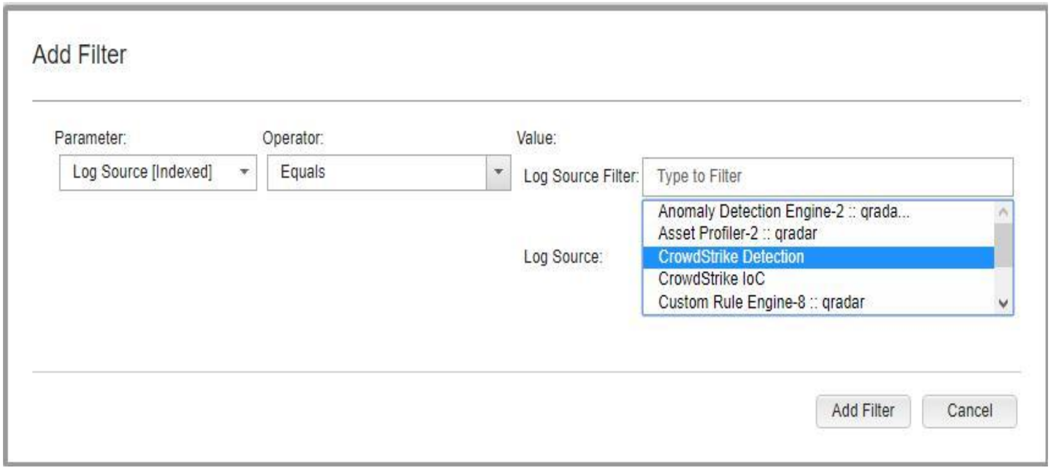
- Navigate to the admin tab and open the ***"Configure CrowdStrike Falcon Endpoint Integration"*** icon and provide the credentials for Stream API, Query API and OAuth2 API.

Functionalities:

QRadar Events for CrowdStrike Detections:

Once the configuration is saved, app will start polling the CrowdStrike detections as events in QRadar.

1. Navigate to the Log Activity tab and add filter to the log source "CrowdStrike Detection" .



Add Filter

Parameter: Log Source [Indexed]

Operator: Equals

Value:

Log Source Filter: Type to Filter

Log Source: CrowdStrike Detection

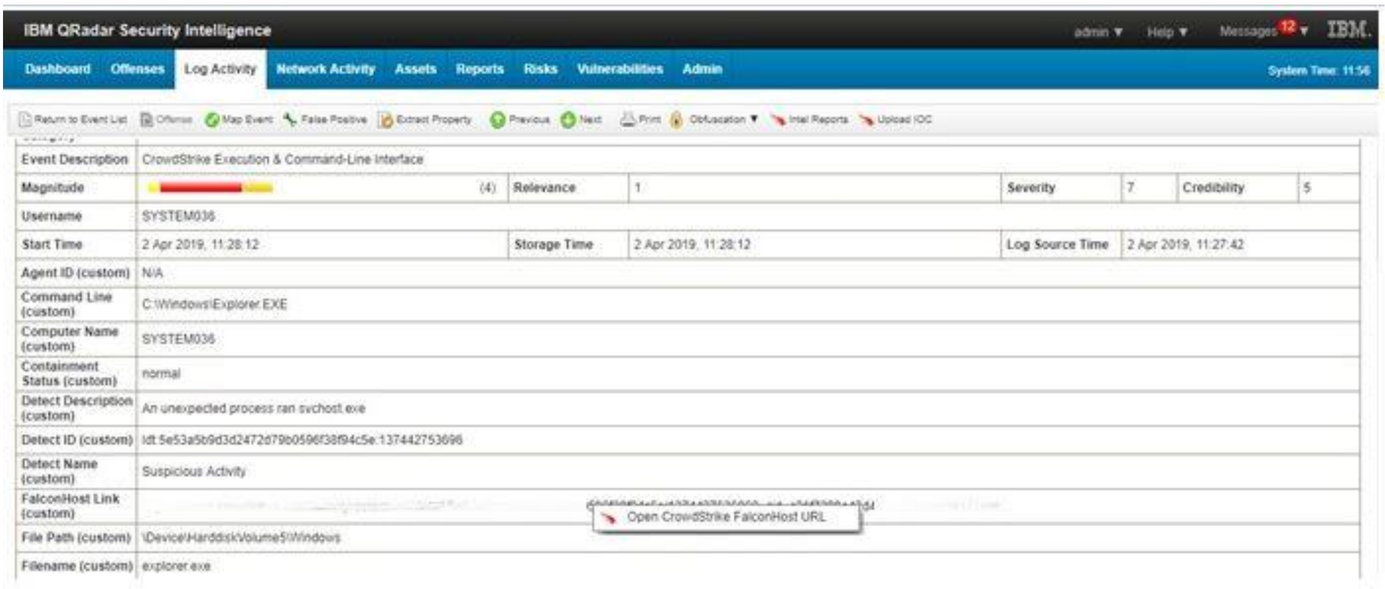
Anomaly Detection Engine-2 :: qrada...
Asset Profiler-2 :: qradar
CrowdStrike Detection
CrowdStrike IoC
Custom Rule Engine-8 :: qradar
Add Filter
Cancel

2. The events will start populating in QRadar.

[Please see next page]

Open the Falcon host link in new window:

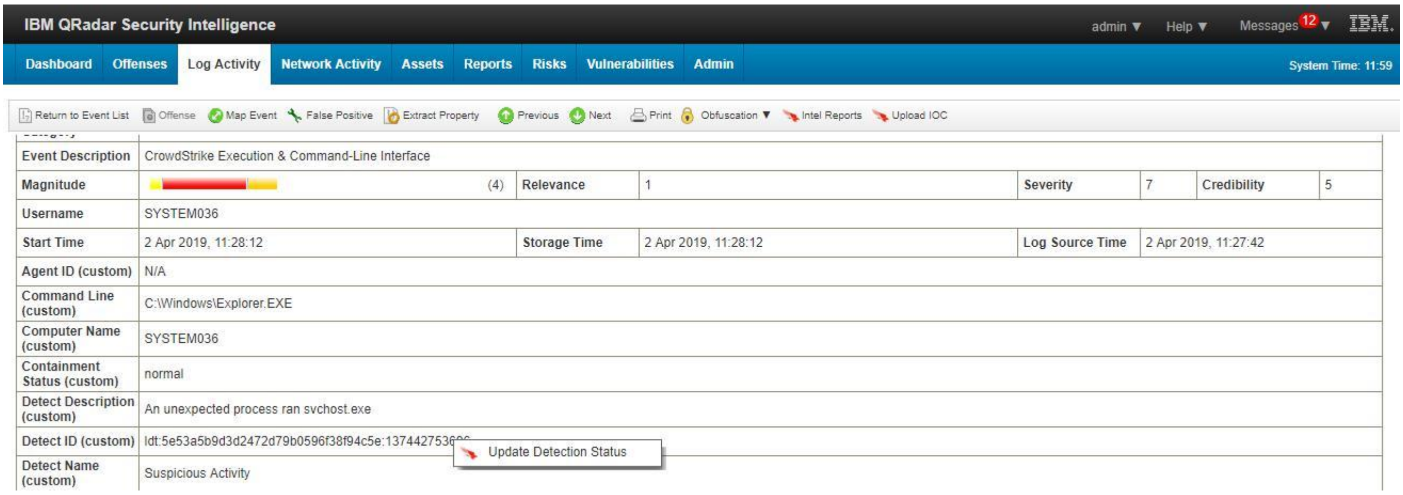
Open the created event for CrowdStrike detection and right click the “FalconHost Link” custom field. It will show “Open CrowdStrike FalconHost URL” menu to open the link in a new window.



Event Description	CrowdStrike Execution & Command-Line Interface						
Magnitude	(4)	Relevance	1	Severity	7	Credibility	5
Username	SYSTEM036						
Start Time	2 Apr 2019, 11:28:12	Storage Time	2 Apr 2019, 11:28:12	Log Source Time	2 Apr 2019, 11:27:42		
Agent ID (custom)	N/A						
Command Line (custom)	C:\Windows\Explorer.EXE						
Computer Name (custom)	SYSTEM036						
Containment Status (custom)	normal						
Detect Description (custom)	An unexpected process ran svchost.exe						
Detect ID (custom)	ldt:5e53a5b9d3d2472d79b0596f38f94c5e:137442753696						
Detect Name (custom)	Suspicious Activity						
FalconHost Link (custom)	[illegible]						
File Path (custom)	\Device\HarddiskVolume5\Windows						
Filename (custom)	explorer.exe						

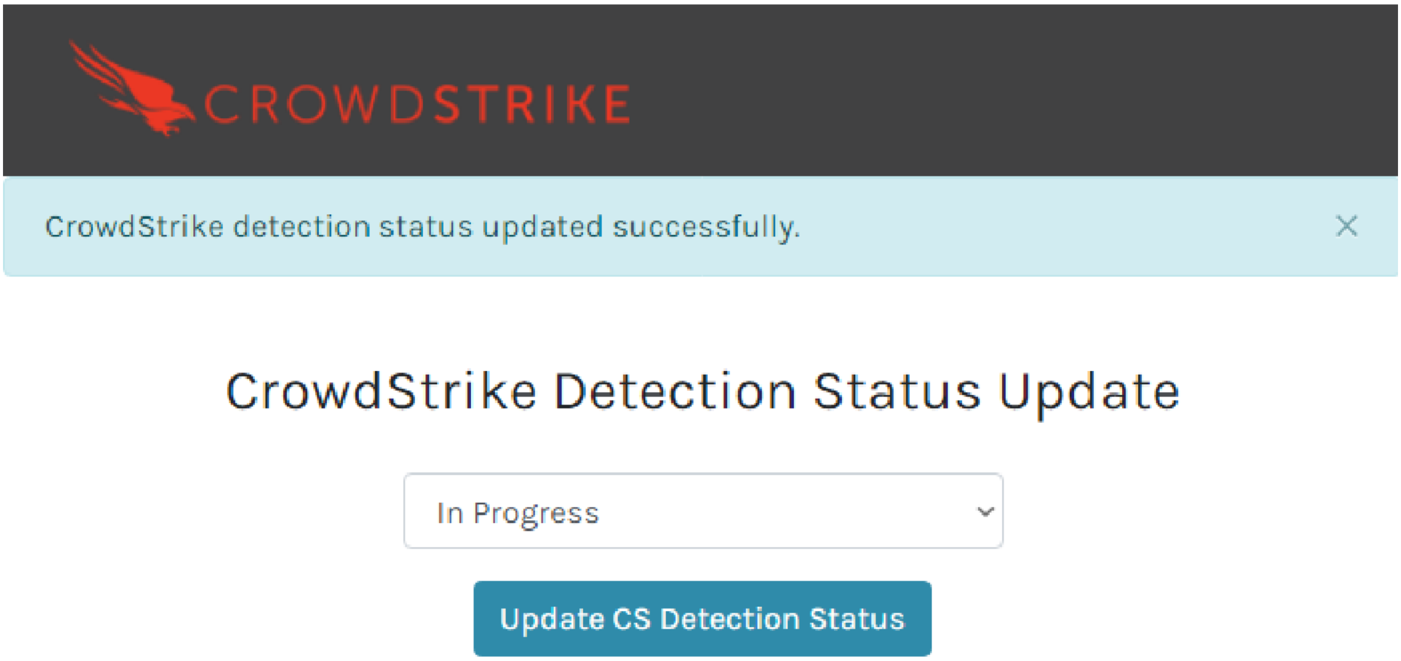
Detection status management:

Open the created event for CrowdStrike detection and right click the “Detect ID” custom field. It will show “Update Detection Status” menu to open the link in a new window.



Event Description	CrowdStrike Execution & Command-Line Interface						
Magnitude	(4)	Relevance	1	Severity	7	Credibility	5
Username	SYSTEM036						
Start Time	2 Apr 2019, 11:28:12	Storage Time	2 Apr 2019, 11:28:12	Log Source Time	2 Apr 2019, 11:27:42		
Agent ID (custom)	N/A						
Command Line (custom)	C:\Windows\Explorer.EXE						
Computer Name (custom)	SYSTEM036						
Containment Status (custom)	normal						
Detect Description (custom)	An unexpected process ran svchost.exe						
Detect ID (custom)	ldt:5e53a5b9d3d2472d79b0596f38f94c5e:1374427536						
Detect Name (custom)	Suspicious Activity						

- Fetch the recent detection status from CrowdStrike and show it in the dropdown.
- To update the detection status, choose any one of the following options in the dropdown (New, In Progress, True Positive, False Positive, Ignored) and click the “Update CS Detection Status” button



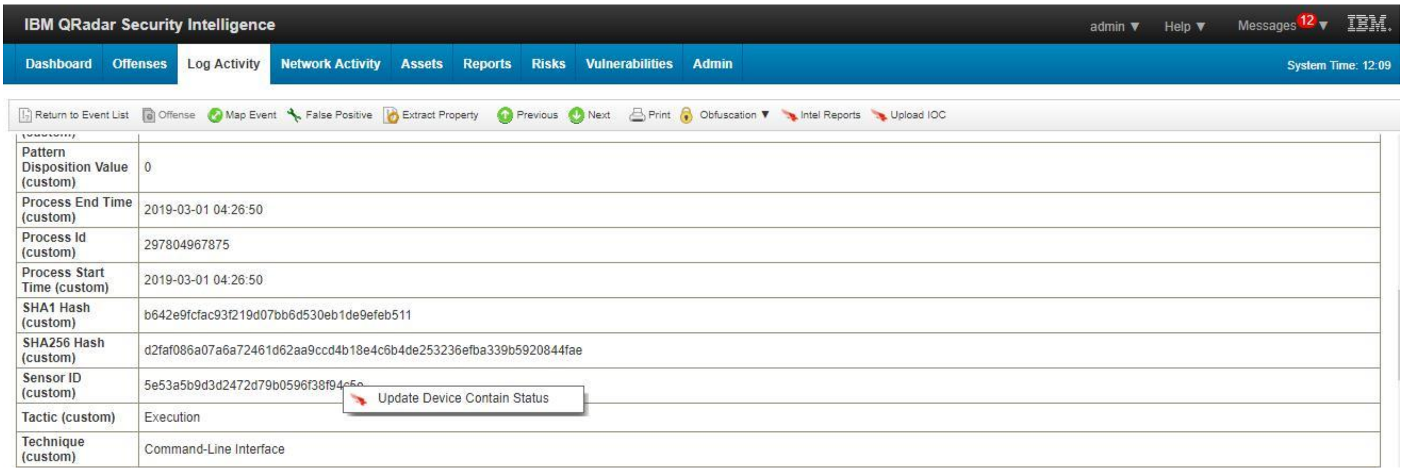
CrowdStrike detection status updated successfully.

CrowdStrike Detection Status Update

In Progress

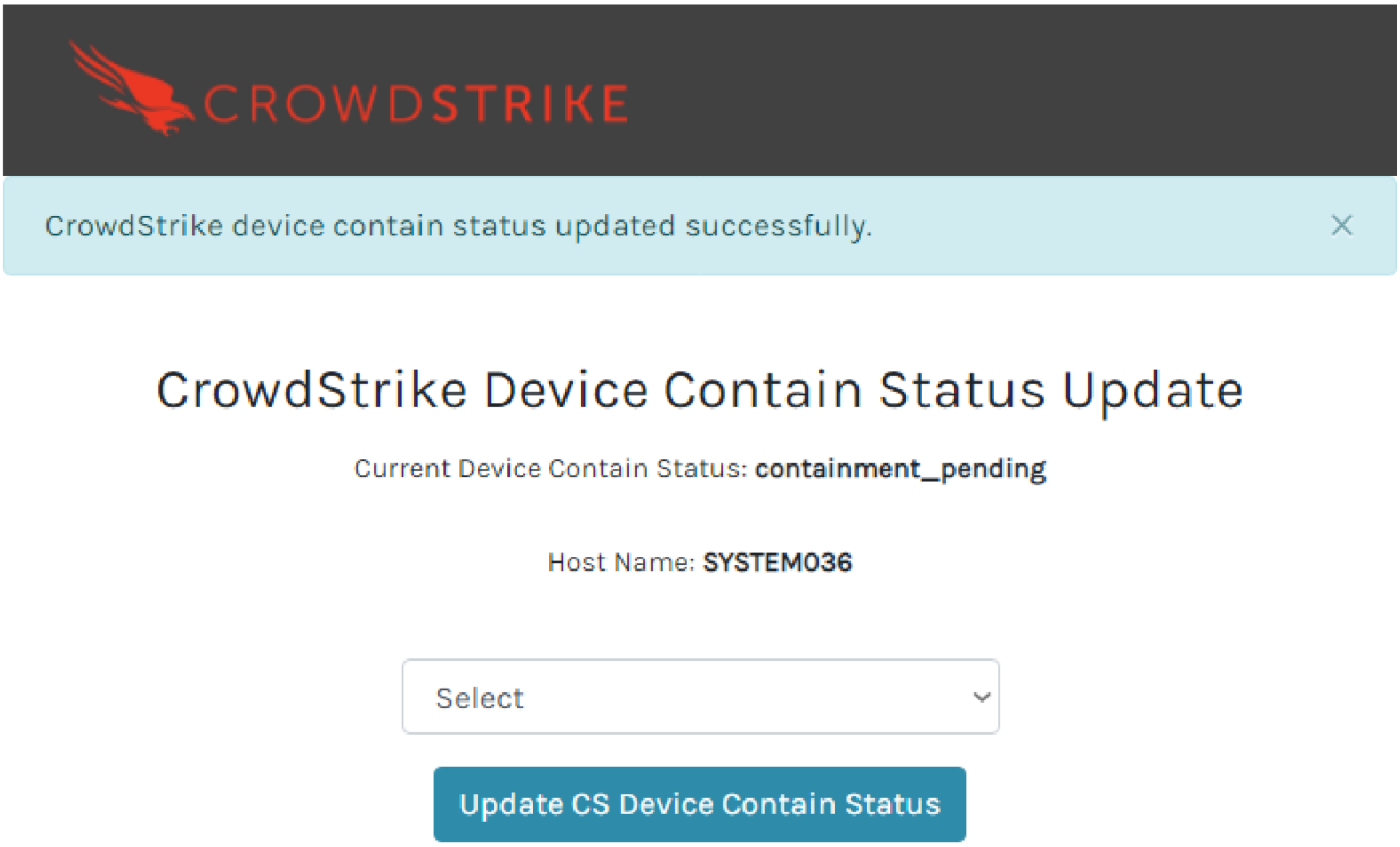
Update Containment Status:

Open the created event for CrowdStrike detection and right click the “Sensor ID” custom field. It will show “Update Device Contain Status” menu to open the link in a new window.



Pattern Disposition Value (custom)	0
Process End Time (custom)	2019-03-01 04:26:50
Process Id (custom)	297804967875
Process Start Time (custom)	2019-03-01 04:26:50
SHA1 Hash (custom)	b642e9fcfac93f219d07bb6d530eb1de9efeb511
SHA256 Hash (custom)	d2faf086a07a6a72461d62aa9ccd4b18e4c6b4de253236efba339b5920844fae
Sensor ID (custom)	5e53a5b9d3d2472d79b0596f38f94c5e
Tactic (custom)	Execution
Technique (custom)	Command-Line Interface

- Fetch the recent device contain status and host name from CrowdStrike, show it in popup window
- To update the device containment status, choose any one of the options (Contain, Lift Contain) and click the “Update CS device Contain Status” button.
- Once updated in CrowdStrike, the recent status will fetch again and show it in the same window



CrowdStrike device contain status updated successfully.

CrowdStrike Device Contain Status Update

Current Device Contain Status: **containment_pending**

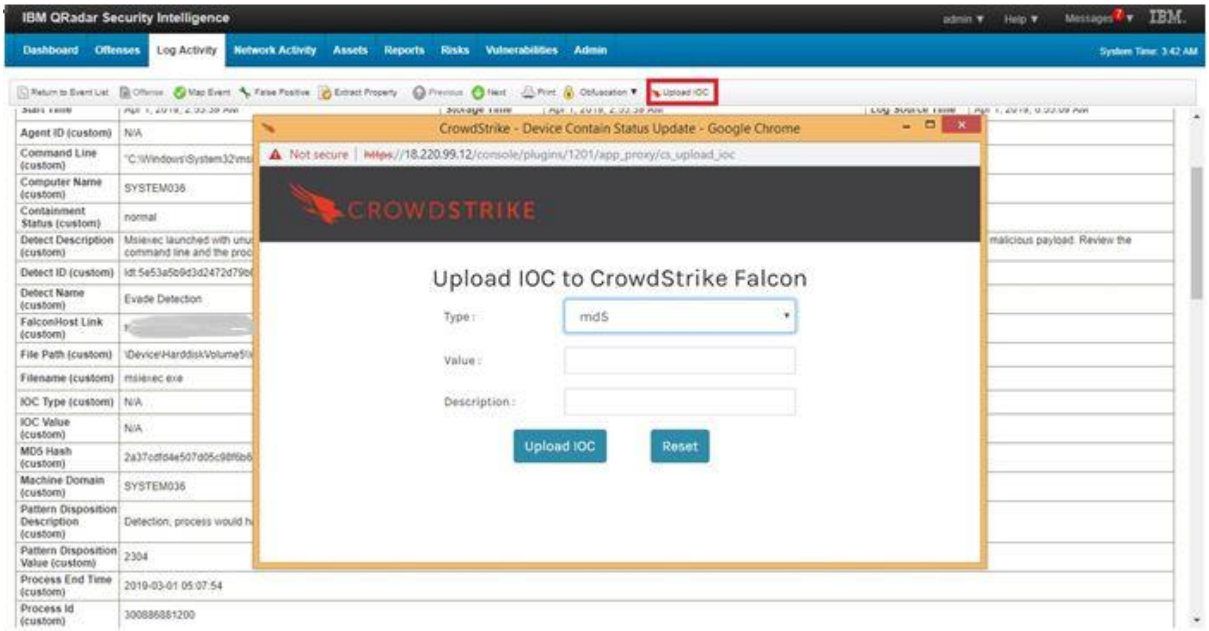
Host Name: **SYSTEM036**

Upload IOC:

Open the event and click the “Upload IOC” button on event details top bar. It will open a new window to upload IOCs into CrowdStrike.

- To upload the IOCs into CrowdStrike, choose any one of the Types (sha256/sha1/md5/domain/ipv4/ipv6) and fill in the Value and Description.
- Click on the “Upload IOC” button to upload IOCs into CrowdStrike.

[Continued in next page]



Start Time	Apr 1, 2019, 2:53:39 AM
Agent ID (custom)	N/A
Command Line (custom)	"C:\Windows\System32\ms
Computer Name (custom)	SYSTEM036
Containment Status (custom)	normal
Detect Description (custom)	Msiexec launched with unu … malicious payload. Review the command line and the proc
Detect ID (custom)	ldt:5e53a5b9d3d2472d79b
Detect Name (custom)	Evade Detection
FalconHost Link (custom)	[redacted]
File Path (custom)	\Device\HarddiskVolume5\
Filename (custom)	msiexec.exe
IOC Type (custom)	N/A
IOC Value (custom)	N/A
MD5 Hash (custom)	2a37cdfd4e507d05c98f6b6
Machine Domain (custom)	SYSTEM036
Pattern Disposition Description (custom)	Detection, process would h
Pattern Disposition Value (custom)	2304
Process End Time (custom)	2019-03-01 05:07:54
Process Id (custom)	300886881200

Storage Time | Apr 1, 2019, 2:53:39 AM

Log Source Time | Apr 1, 2019, 0:53:09 AM

CrowdStrike - Device Contain Status Update - Google Chrome

Not secure | https://18.220.99.12/console/plugins/1201/app_proxy/cs_upload_ioc

CROWDSTRIKE

Upload IOC to CrowdStrike Falcon

Type : md5

Value :

Description :

[End of Document]