Crowdstrike Malware Investigation and Response with Mission Control

By: Jit Arora
Senior Security Solution Architect
Splunk

Purpose

This document is intended for customers using Crowdstrike Falcon and ingesting data in Splunk Cloud with Enterprise Security. Crowdstrike Falcon Detect provides advance capabilities in detecting malicious indicators across the endpoint fleet, and the “Crowdstrike Falcon” app in Splunk presents the information about detections and incidents in the dashboards. Users can analyse the crowdstrike data and alerts in these dashboards and perform the investigation and containment manually. Since the tasks and activities involved in the investigation process are repeatable, it makes this use case a good candidate for automation.

Utilizing the power of Mission Control incident management and automation via Splunk SOAR, the Crowdstrike Falcon detections and incidents can be managed in the Incident Review section of Mission Control, along with the incidents from all other security domains. These incidents can be responded to, at machine speed, and with the inclusion of human element for decision making process to remediate and contain the incident with Crowdstrike, the whole incident workflow can be managed within Splunk.

This document describes the content specifically built for implementation of this use case.

Assumptions

1. This solution requires a Splunk Cloud deployment with Enterprise Security and Mission Control.

2. Crowdstrike Falcon should be implemented across the servers and endpoints and the Crowdstrike Falcon detect data should be ingested in Splunk.

3. Crowdstrike OAuth API connector configured with correct set of permissions in Mission Control SOAR

Solution

Although the Crowdstrike Falcon alerts for detections and incidents are available in the Splunk app for Crowdstrike Falcon, managing them in the Crowdstrike Falcon app creates isolation and doesn’t provide comprehensive visibility and centralised control for incident management.
Creating a simple correlation search in Enterprise Security for these detections and incidents, can help bring together these Crowdstrike alerts in the Incident Review queue of Splunk Analyst, so they can manage these incidents together with the other incidents.

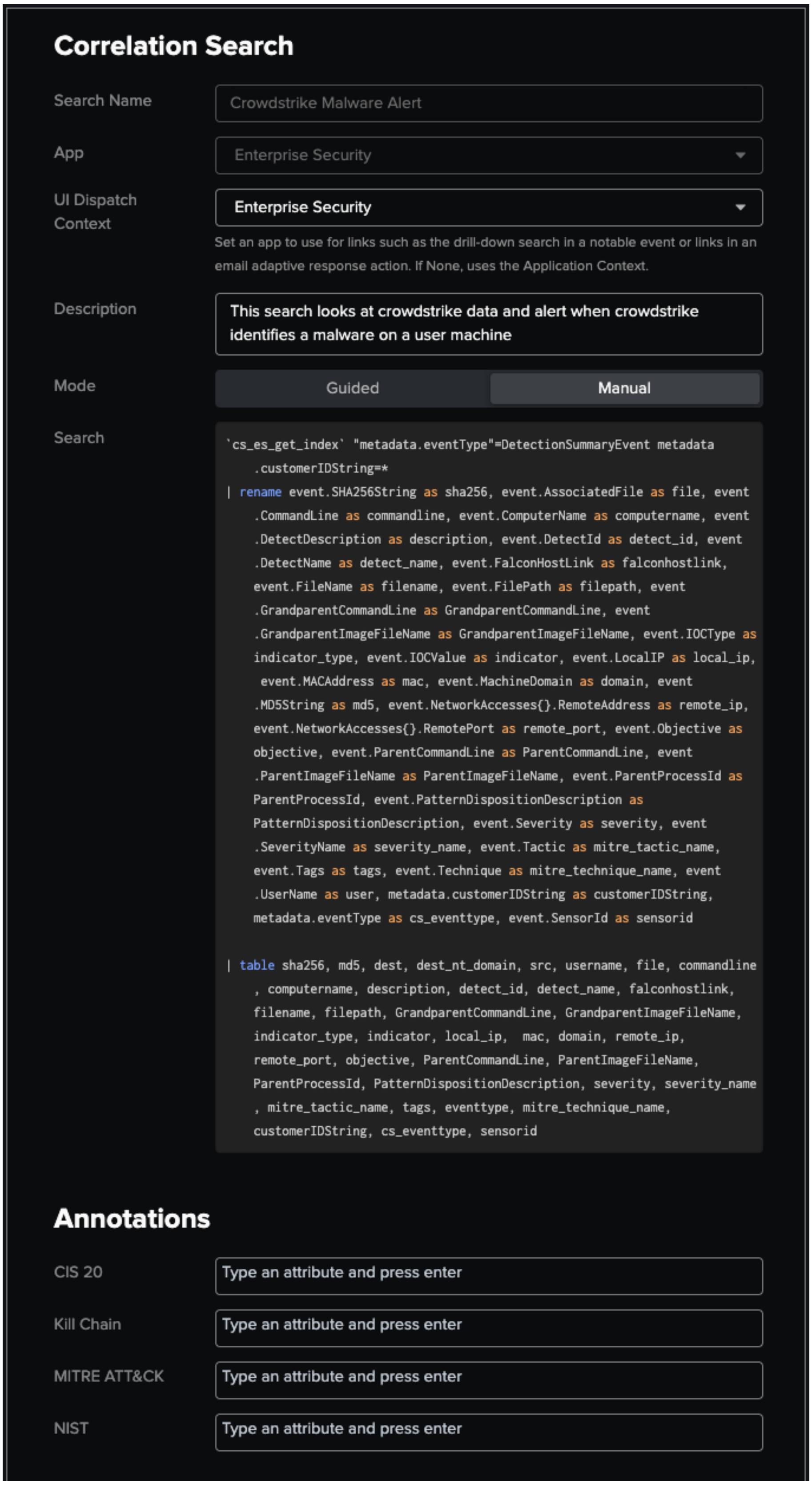
First, to create notables or incidents for Crowdstrike Falcon Detections in Splunk Mission Control, create a correlation search in Enterprise Security, using the below SPL (this is sourced from the Crowdstrike Falcon app with a little tweak)

```
 `cs_es_get_index` "metadata.eventType"=DetectionSummaryEvent metadata.customerIDString=*
 event.SHA256String as sha256, event.AssociatedFile as file, event.CommandLine as commandline,
 event.ComputerName as computername, event.DetectDescription as description, event.DetectId as detect
 event.DetectName as detect_name, event.FalconHostLink as falconhostlink, event.FileName as filename,
 event.FilePath as filepath, event.GrandparentCommandLine as GrandparentCommandLine,
 event.GrandparentImageFileName as GrandparentImageFileName, event.IOCType as indicator_type, event.I
 as indicator, event.LocalIP as local_ip,  event.MACAddress as mac, event.MachineDomain as domain,
 event.MD5String as md5, event.NetworkAccesses{}.RemoteAddress as remote_ip,
 event.NetworkAccesses{}.RemotePort as remote_port, event.Objective as objective, event.ParentCommand
 ParentCommandLine, event.ParentImageFileName as ParentImageFileName, event.ParentProcessId as
 ParentProcessId, event.PatternDispositionDescription as PatternDispositionDescription, event.Severit
 severity, event.SeverityName as severity_name, event.Tactic as mitre_tactic_name, event.Tags as tags
 event.Technique as mitre_technique_name, event.UserName as user, metadata.customerIDString as
 customerIDString, metadata.eventType as cs_eventtype, event.SensorId as sensorid

sha256, md5, dest, dest_nt_domain, src, username, file, commandline, computername, description, detec
 detect_name, falconhostlink, filename, filepath, GrandparentCommandLine, GrandparentImageFileName,
 indicator_type, indicator, local_ip,  mac, domain, remote_ip, remote_port, objective, ParentCommandL
 ParentImageFileName, ParentProcessId, PatternDispositionDescription, severity, severity_name,
 mitre_tactic_name, tags, eventtype, mitre_technique_name, customerIDString, cs_eventtype, sensorid
```

The values mentioned above with the ‘rename’ and ‘table’ commands are utilised in the downstream Mission Control Incidents and SOAR playbook. Should you require to change the names of any of these fields, please note that you will have to change them in the Incident Review settings and in SOAR playbooks as well. The Mission Control configuration and SOAR playbooks I have prepared are based on the above search.

Correlation Search configuration (screenshots)



Correlation Search

Search Name: Crowdstrike Malware Alert

App: Enterprise Security

UI Dispatch Context: Enterprise Security

Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.

Description: This search looks at crowdstrike data and alert when crowdstrike identifies a malware on a user machine

Mode: Guided | Manual

Search

```
`cs_es_get_index` "metadata.eventType"=DetectionSummaryEvent metadata
    .customerIDString=*
| rename event.SHA256String as sha256, event.AssociatedFile as file, event
    .CommandLine as commandline, event.ComputerName as computername, event
    .DetectDescription as description, event.DetectId as detect_id, event
    .DetectName as detect_name, event.FalconHostLink as falconhostlink,
    event.FileName as filename, event.FilePath as filepath, event
    .GrandparentCommandLine as GrandparentCommandLine, event
    .GrandparentImageFileName as GrandparentImageFileName, event.IOCType as
    indicator_type, event.IOCValue as indicator, event.LocalIP as local_ip,
     event.MACAddress as mac, event.MachineDomain as domain, event
    .MD5String as md5, event.NetworkAccesses{}.RemoteAddress as remote_ip,
    event.NetworkAccesses{}.RemotePort as remote_port, event.Objective as
    objective, event.ParentCommandLine as ParentCommandLine, event
    .ParentImageFileName as ParentImageFileName, event.ParentProcessId as
    ParentProcessId, event.PatternDispositionDescription as
    PatternDispositionDescription, event.Severity as severity, event
    .SeverityName as severity_name, event.Tactic as mitre_tactic_name,
    event.Tags as tags, event.Technique as mitre_technique_name, event
    .UserName as user, metadata.customerIDString as customerIDString,
    metadata.eventType as cs_eventtype, event.SensorId as sensorid

| table sha256, md5, dest, dest_nt_domain, src, username, file, commandline
    , computername, description, detect_id, detect_name, falconhostlink,
    filename, filepath, GrandparentCommandLine, GrandparentImageFileName,
    indicator_type, indicator, local_ip,  mac, domain, remote_ip,
    remote_port, objective, ParentCommandLine, ParentImageFileName,
    ParentProcessId, PatternDispositionDescription, severity, severity_name
    , mitre_tactic_name, tags, eventtype, mitre_technique_name,
    customerIDString, cs_eventtype, sensorid
```

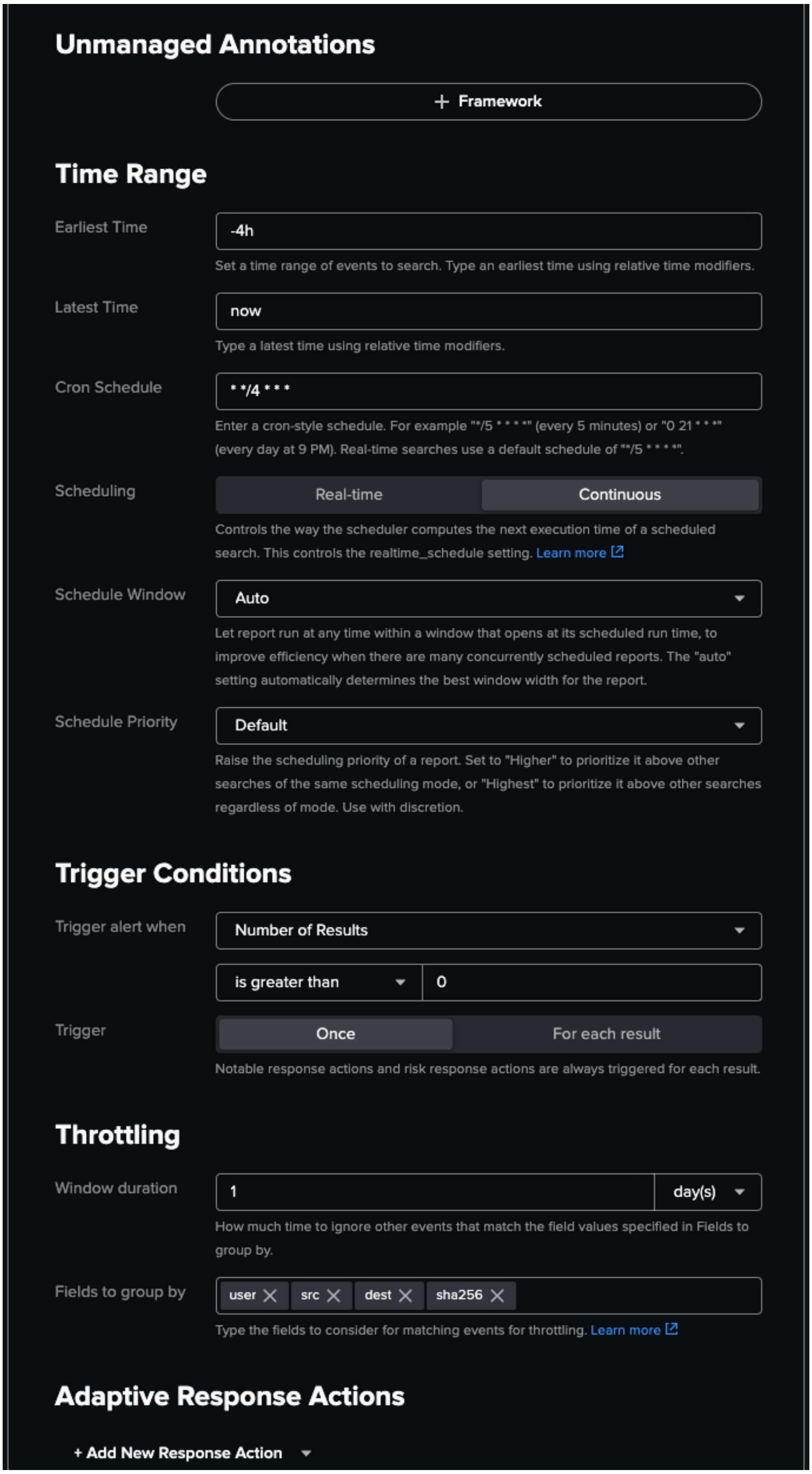
Annotations

CIS 20: Type an attribute and press enter

Kill Chain: Type an attribute and press enter

MITRE ATT&CK: Type an attribute and press enter

NIST: Type an attribute and press enter



Unmanaged Annotations

Time Range

Earliest Time: -4h

Set a time range of events to search. Type an earliest time using relative time modifiers.

Latest Time: now

Type a latest time using relative time modifiers.

Cron Schedule: * */4 * * *

Enter a cron-style schedule. For example "*/5 * * * *" (every 5 minutes) or "0 21 * * *" (every day at 9 PM). Real-time searches use a default schedule of "*/5 * * * *".

Scheduling: Real-time [✓ Continuous]

Controls the way the scheduler computes the next execution time of a scheduled search. This controls the realtime_schedule setting. Learn more

Schedule Window: Auto

Let report run at any time within a window that opens at its scheduled run time, to improve efficiency when there are many concurrently scheduled reports. The "auto" setting automatically determines the best window width for the report.

Schedule Priority: Default

Raise the scheduling priority of a report. Set to "Higher" to prioritize it above other searches of the same scheduling mode, or "Highest" to prioritize it above other searches regardless of mode. Use with discretion.

Trigger Conditions

Trigger alert when: Number of Results

is greater than 0

Trigger: [✓ Once] For each result

Notable response actions and risk response actions are always triggered for each result.

Throttling

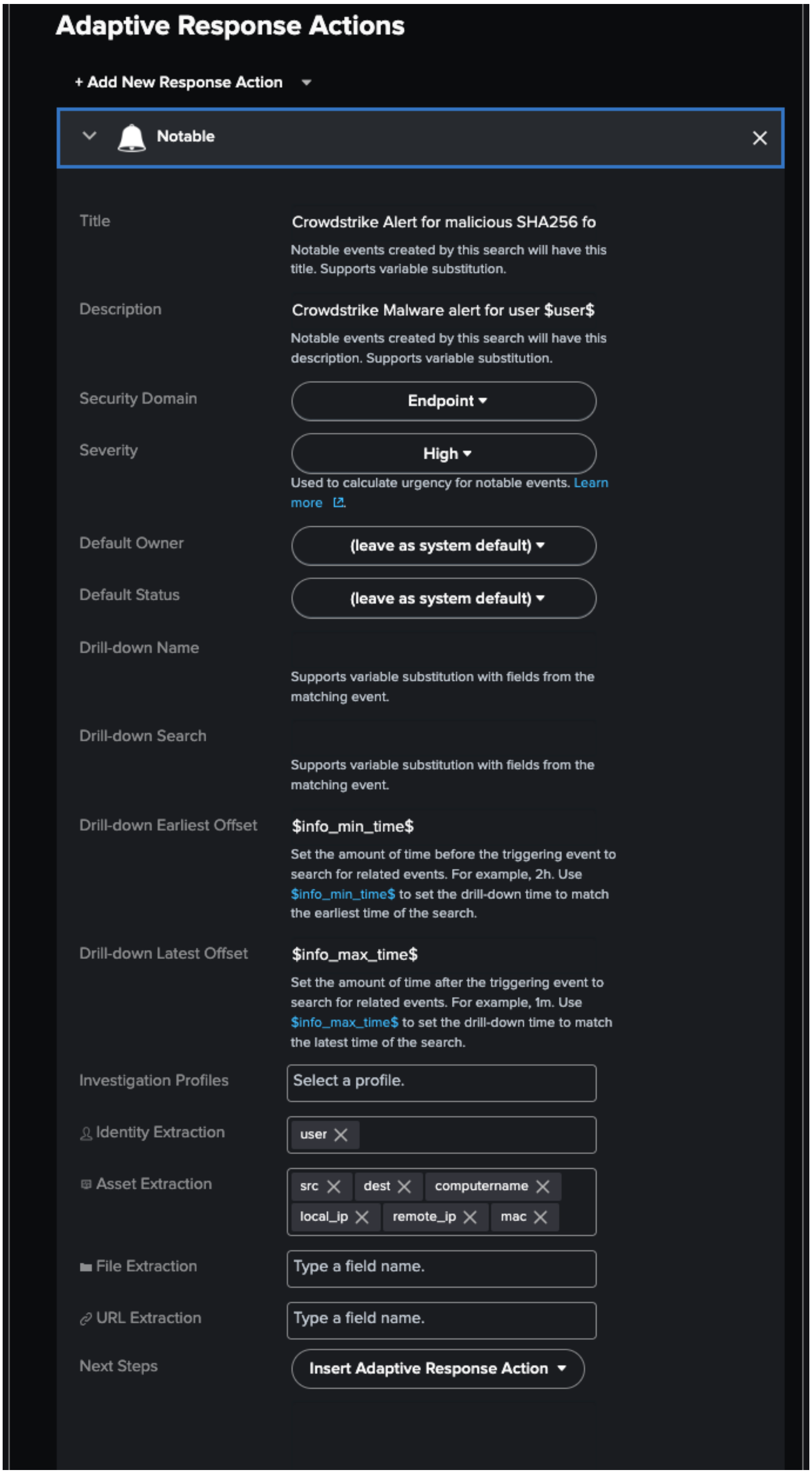
Window duration: 1 day(s)

How much time to ignore other events that match the field values specified in Fields to group by.

Fields to group by: user ✕ src ✕ dest ✕ sha256 ✕

Type the fields to consider for matching events for throttling. Learn more

Adaptive Response Actions



Adaptive Response Actions

Title: Crowdstrike Alert for malicious SHA256 fo

Notable events created by this search will have this title. Supports variable substitution.

Description: Crowdstrike Malware alert for user $user$

Notable events created by this search will have this description. Supports variable substitution.

Security Domain: Endpoint

Severity: High

Used to calculate urgency for notable events. Learn more

Default Owner: (leave as system default)

Default Status: (leave as system default)

Drill-down Name:

Supports variable substitution with fields from the matching event.

Drill-down Search:

Supports variable substitution with fields from the matching event.

Drill-down Earliest Offset: $info_min_time$

Set the amount of time before the triggering event to search for related events. For example, 2h. Use $info_min_time$ to set the drill-down time to match the earliest time of the search.

Drill-down Latest Offset: $info_max_time$

Set the amount of time after the triggering event to search for related events. For example, 1m. Use $info_max_time$ to set the drill-down time to match the latest time of the search.

Investigation Profiles: Select a profile.

Identity Extraction: user

Asset Extraction: src, dest, computername, local_ip, remote_ip, mac

File Extraction: Type a field name.

URL Extraction: Type a field name.

Next Steps: Insert Adaptive Response Action

The description, title, time range, mitre annotations and other settings can be modified as per customer’s requirement.

Mission Control configuration

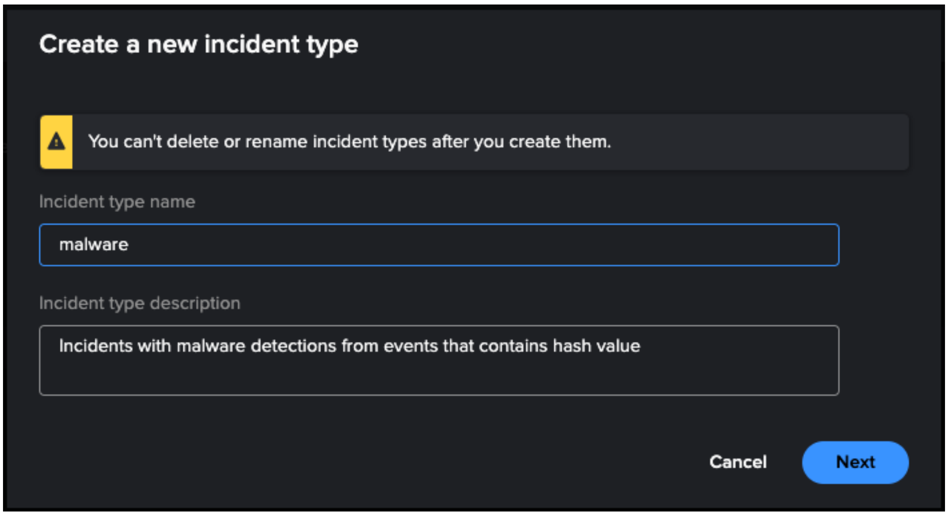
Incident types

Create a new incident type, in my case I created a new one with value: “malware”

Navigation: Mission Control -> Settings -> Incident Settings –> Incident type

Click on “Incident type” button on the far right

Add the new incident type – malware with a description



Create a new incident type

You can't delete or rename incident types after you create them.

Incident type name: malware

Incident type description: Incidents with malware detections from events that contains hash value

Incident type macro

Now, you need to assign the incoming notables from the “Crowdstrike Malware Alert” correlation search you created earlier with this new incident type, using the Incident type macro feature of Mission Control

Navigation: Mission Control -> Settings -> Incident Settings –> Incident type macro

e.g.

```
ident_type=case(threat_collection="email_intel","threat_email",
ollection="ip_intel","threat_ip",
ame="Endpoint - Crowdstrike Malware Alert - Rule","malware",
ault")
```

In the above macro configuration, I have added a new case statement condition for

`search_name="Endpoint - Crowdstrike Malware Alert – Rule”`

assign the

`incident_type = "malware"`

Response template

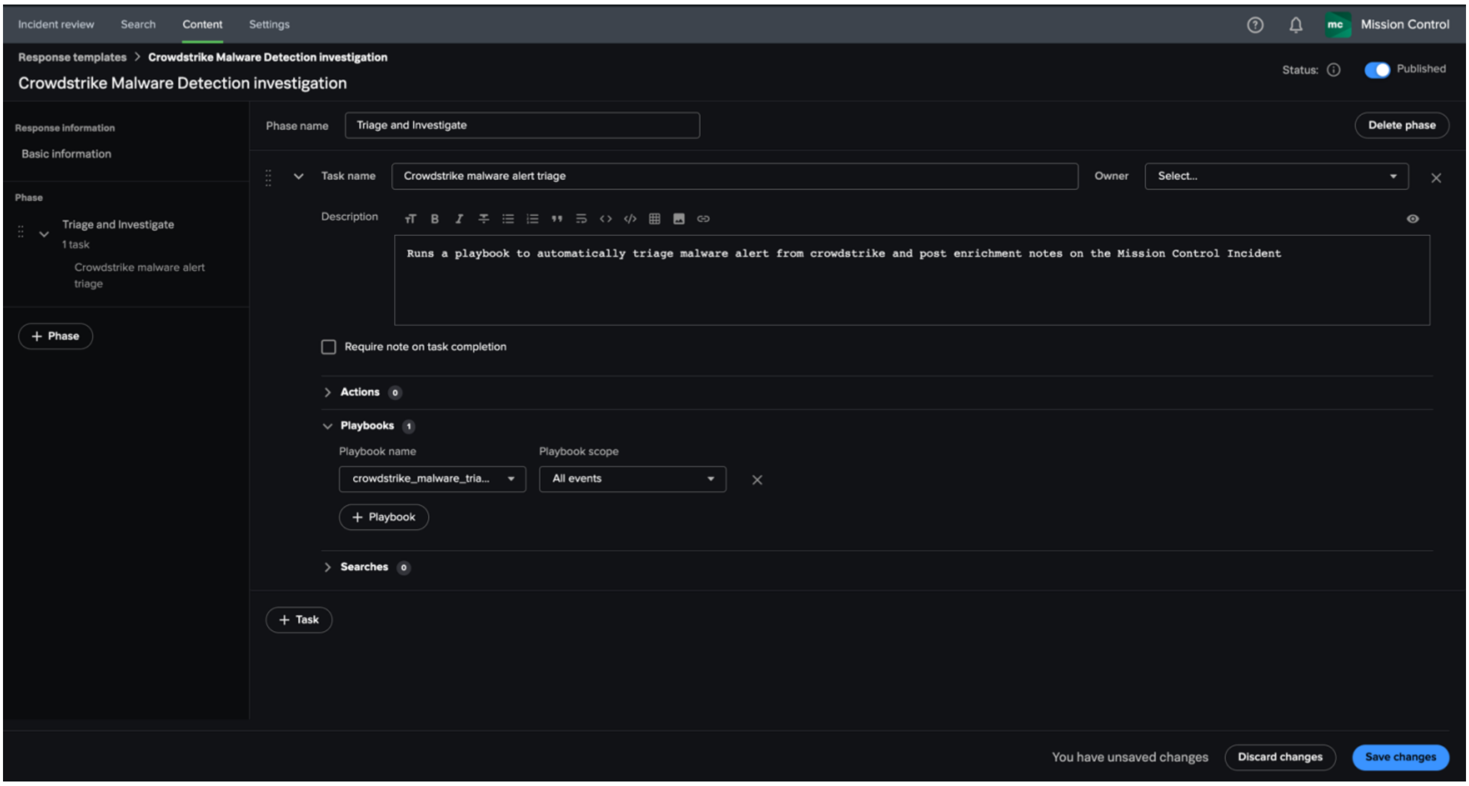
Next, we will create a Response template in Mission Control, which will be automatically assigned to all the incidents for “Crowdstrike Malware Alert”

Navigation: Mission Control -> Content -> Response templates –> Response templates

Click on “Response Template” button on the far right

Create a new response template like below screenshot:

Please note: at this stage, you can leave the “Playbooks” assignment blank, as you will create a playbook in Mission Control SOAR in the next steps.



Response templates > Crowdstrike Malware Detection investigation

Crowdstrike Malware Detection investigation

Status: Published

Triage and Investigate
1 task
Crowdstrike malware alert triage

Phase name: Triage and Investigate

Task name: Crowdstrike malware alert triage

Owner: Select...

Description:

```
Runs a playbook to automatically triage malware alert from crowdstrike and post enrichment notes on the Mission Control Incident
```

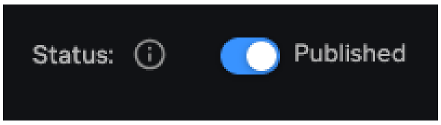
□ Require note on task completion

Playbooks 1

Playbook name	Playbook scope
crowdstrike_malware_tria...	All events

You have unsaved changes

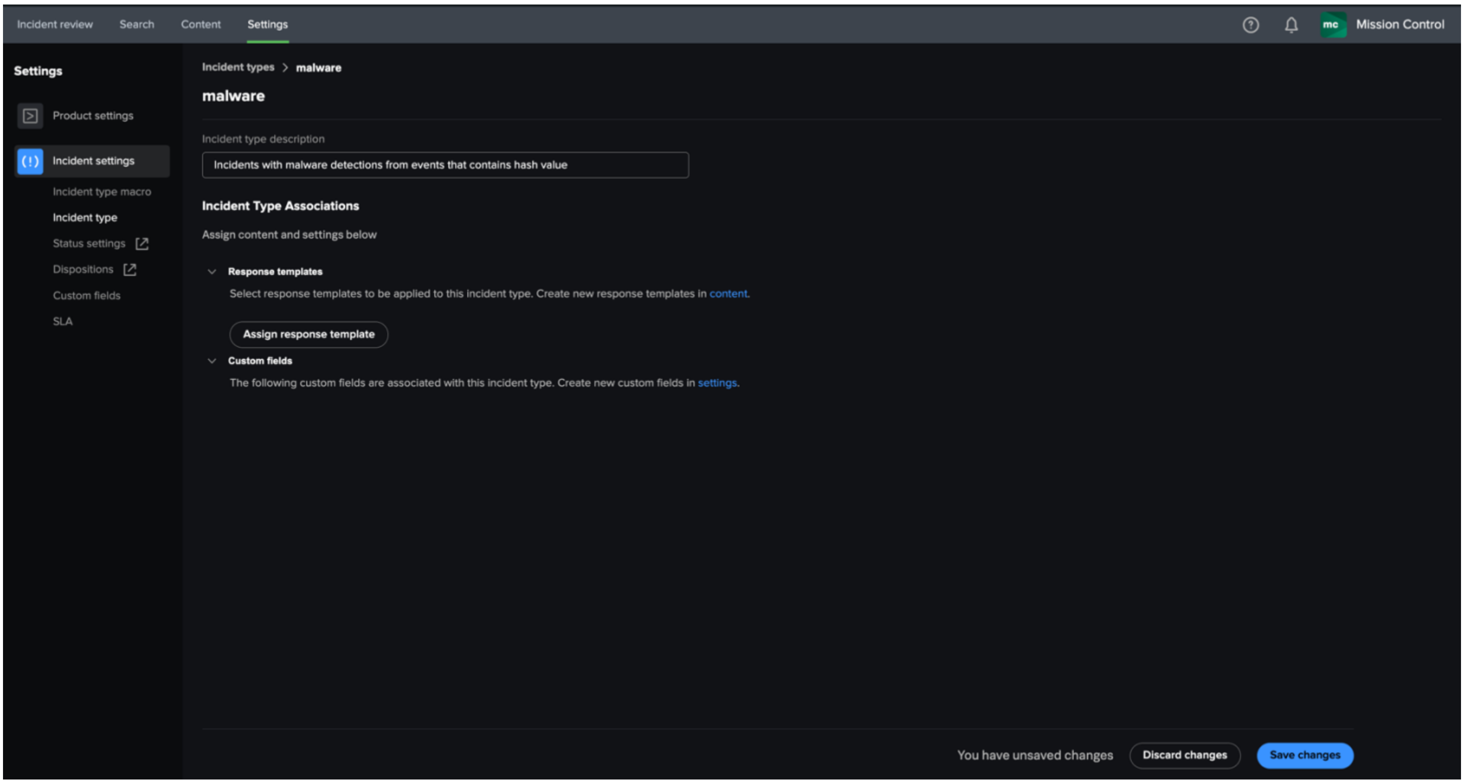
Save the Response template and publish it, by moving the enable button on the far right



Attach the Response template to the Incident type

Navigation: Mission Control -> Settings -> Incident Settings –> Incident type

Click on the “malware” incident type



malware

Incident type description: Incidents with malware detections from events that contains hash value

Incident Type Associations

Assign content and settings below

Response templates

Select response templates to be applied to this incident type. Create new response templates in content.

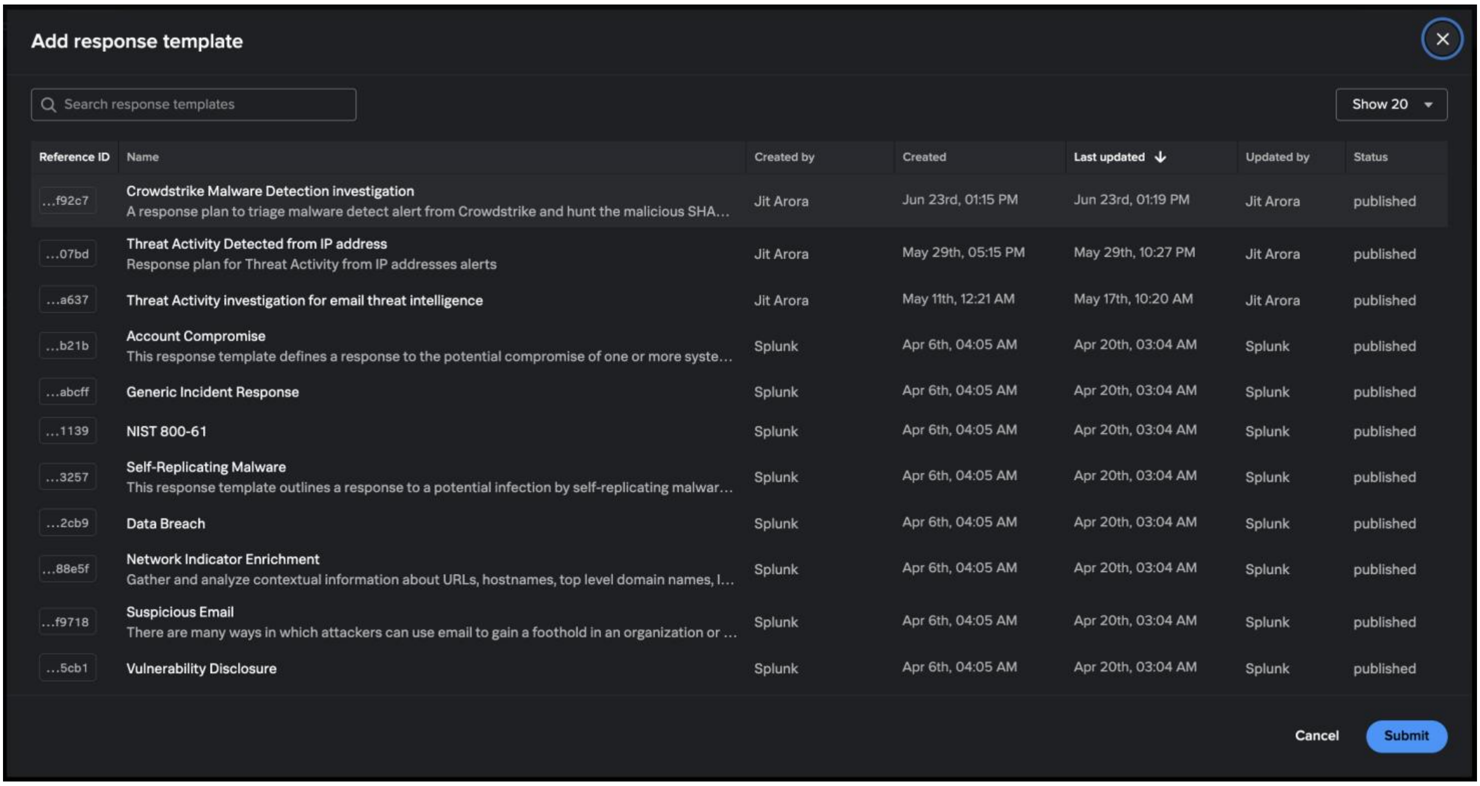
Custom fields

The following custom fields are associated with this incident type. Create new custom fields in settings.

You have unsaved changes

Click on the “Assign response template” button

Select the “Crwordstrike Malware Detection Investigation” response template and click on Submit



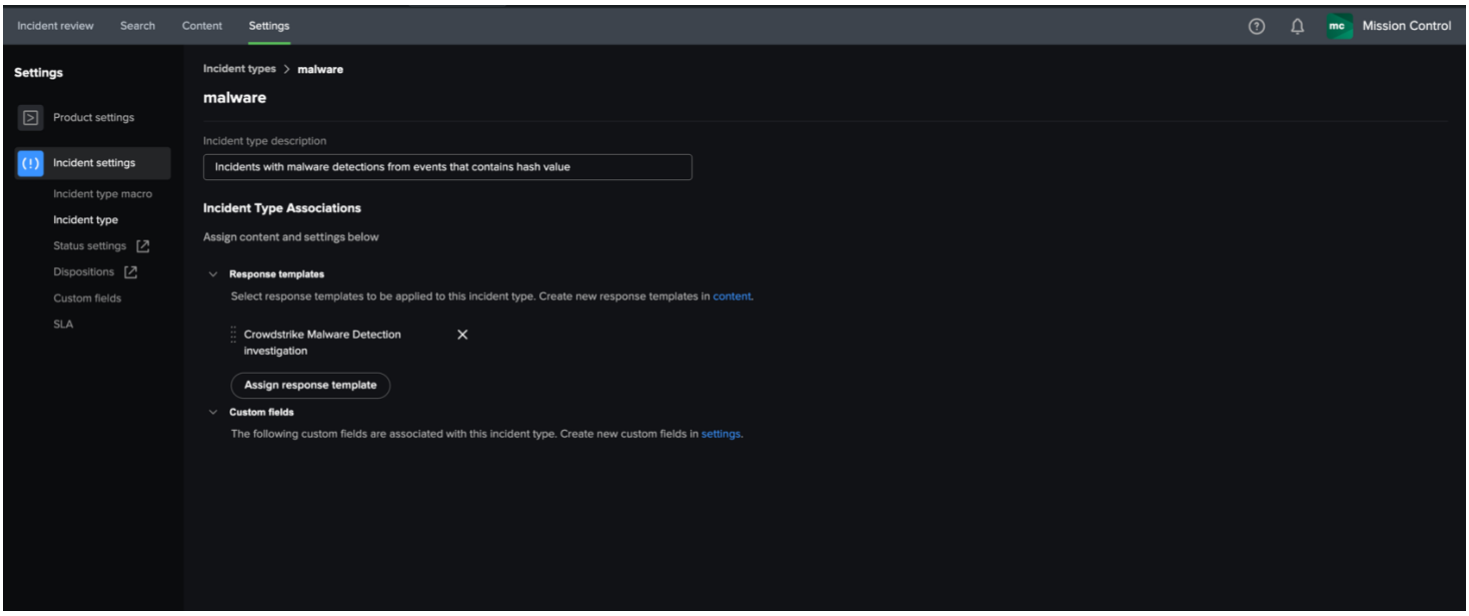
Add response template

Search response templates

Show 20

Reference ID	Name	Created by	Created	Last updated	Updated by	Status
…f92c7	Crowdstrike Malware Detection investigation A response plan to triage malware detect alert from Crowdstrike and hunt the malicious SHA…	Jit Arora	Jun 23rd, 01:15 PM	Jun 23rd, 01:19 PM	Jit Arora	published
…07bd	Threat Activity Detected from IP address Response plan for Threat Activity from IP addresses alerts	Jit Arora	May 29th, 05:15 PM	May 29th, 10:27 PM	Jit Arora	published
…a637	Threat Activity investigation for email threat intelligence	Jit Arora	May 11th, 12:21 AM	May 17th, 10:20 AM	Jit Arora	published
…b21b	Account Compromise This response template defines a response to the potential compromise of one or more syste…	Splunk	Apr 6th, 04:05 AM	Apr 20th, 03:04 AM	Splunk	published
…abcff	Generic Incident Response	Splunk	Apr 6th, 04:05 AM	Apr 20th, 03:04 AM	Splunk	published
…1139	NIST 800-61	Splunk	Apr 6th, 04:05 AM	Apr 20th, 03:04 AM	Splunk	published
…3257	Self-Replicating Malware This response template outlines a response to a potential infection by self-replicating malwar…	Splunk	Apr 6th, 04:05 AM	Apr 20th, 03:04 AM	Splunk	published
…2cb9	Data Breach	Splunk	Apr 6th, 04:05 AM	Apr 20th, 03:04 AM	Splunk	published
…88e5f	Network Indicator Enrichment Gather and analyze contextual information about URLs, hostnames, top level domain names, l…	Splunk	Apr 6th, 04:05 AM	Apr 20th, 03:04 AM	Splunk	published
…f9718	Suspicious Email There are many ways in which attackers can use email to gain a foothold in an organization or …	Splunk	Apr 6th, 04:05 AM	Apr 20th, 03:04 AM	Splunk	published
…5cb1	Vulnerability Disclosure	Splunk	Apr 6th, 04:05 AM	Apr 20th, 03:04 AM	Splunk	published

The Incident settings for malware should like like below:



malware

Incident type description

Incidents with malware detections from events that contains hash value

Incident Type Associations

Assign content and settings below

Response templates

Select response templates to be applied to this incident type. Create new response templates in content.

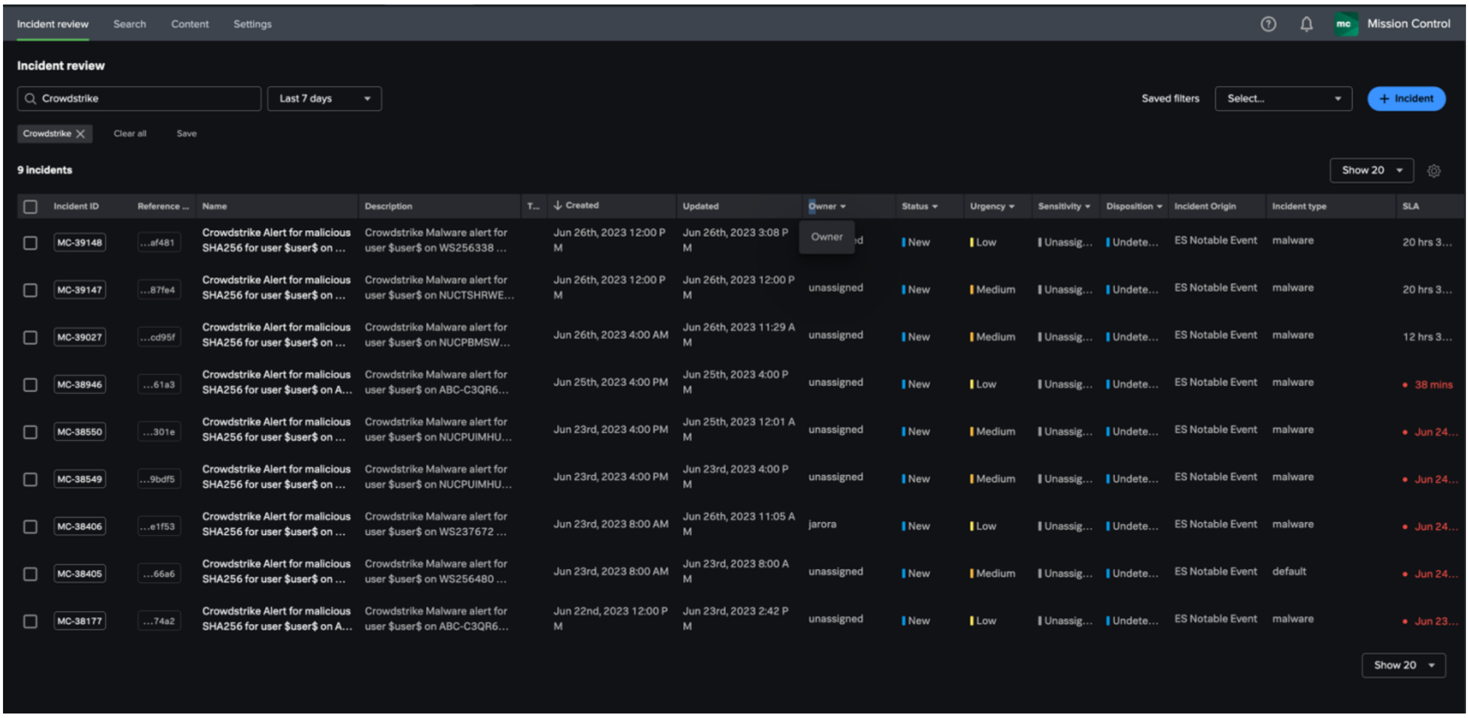
Crowdstrike Malware Detection investigation ✕

Custom fields

The following custom fields are associated with this incident type. Create new custom fields in settings.

Test the Incident creation and attachment of Response template

Based on the schedule for correlation search configured earlier, available detections in Crowdstrike data and the tasks completed for Incident type and Response Template configuration, the Mission Control Incident review queue should have some incidents with incident type “malware” and Response plan showing in the Response tab of the incident.



Incident review

Crowdstrike | Last 7 days

Crowdstrike ✕ Clear all Save

Saved filters Select... + Incident

9 incidents

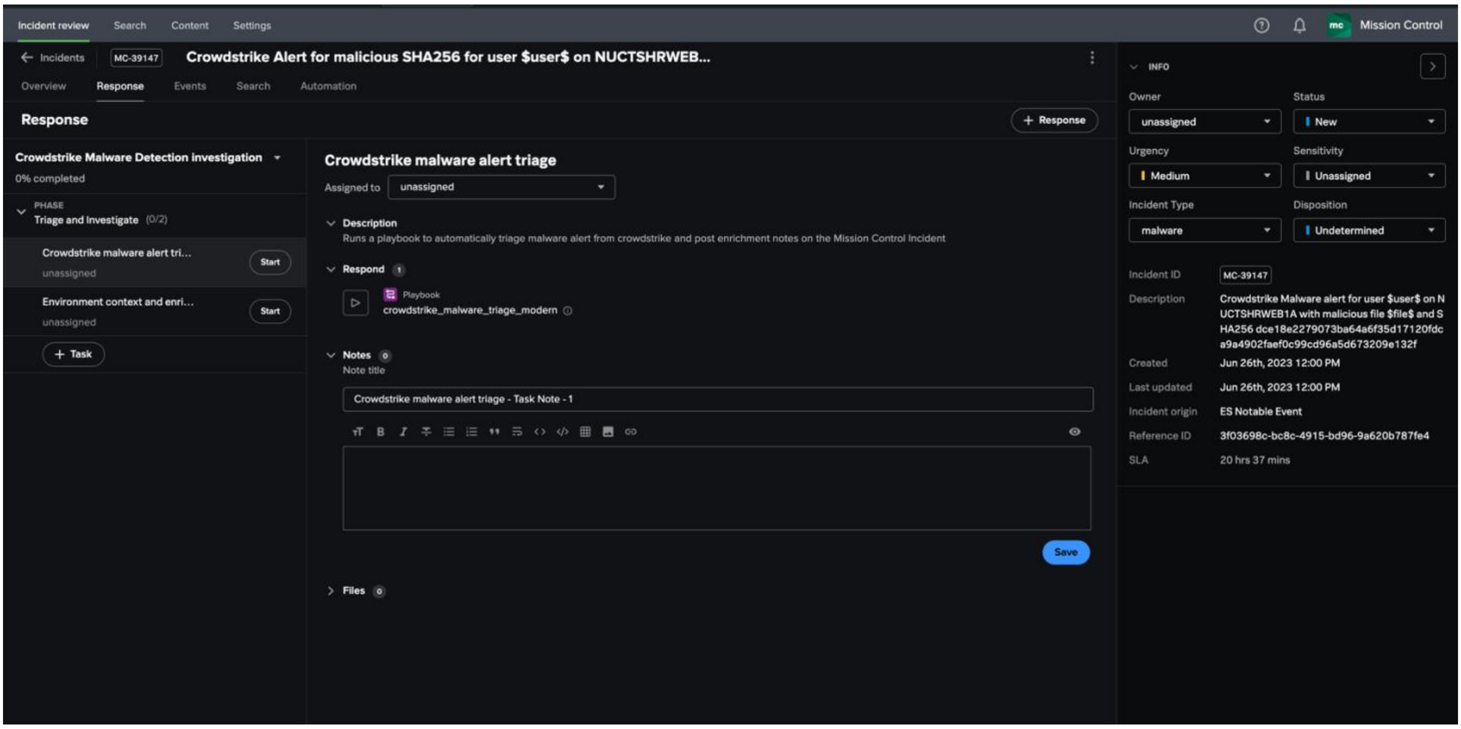
Show 20

□	Incident ID	Reference ...	Name	Description	T...	↓ Created	Updated	Owner	Status	Urgency	Sensitivity	Disposition	Incident Origin	Incident type	SLA
□	MC-39148	...af481	Crowdstrike Alert for malicious SHA256 for user $user$ on ...	Crowdstrike Malware alert for user $user$ on WS256338 ...		Jun 26th, 2023 12:00 PM	Jun 26th, 2023 3:08 PM	Owner d	New	Low	Unassig...	Undete...	ES Notable Event	malware	20 hrs 3...
□	MC-39147	...87fe4	Crowdstrike Alert for malicious SHA256 for user $user$ on ...	Crowdstrike Malware alert for user $user$ on NUCTSHRWE...		Jun 26th, 2023 12:00 PM	Jun 26th, 2023 12:00 PM	unassigned	New	Medium	Unassig...	Undete...	ES Notable Event	malware	20 hrs 3...
□	MC-39027	...cd95f	Crowdstrike Alert for malicious SHA256 for user $user$ on ...	Crowdstrike Malware alert for user $user$ on NUCPBMSW...		Jun 26th, 2023 4:00 AM	Jun 26th, 2023 11:29 AM	unassigned	New	Medium	Unassig...	Undete...	ES Notable Event	malware	12 hrs 3...
□	MC-38946	...61a3	Crowdstrike Alert for malicious SHA256 for user $user$ on A...	Crowdstrike Malware alert for user $user$ on ABC-C3QR6...		Jun 25th, 2023 4:00 PM	Jun 25th, 2023 4:00 PM	unassigned	New	Low	Unassig...	Undete...	ES Notable Event	malware	● 38 mins
□	MC-38550	...301e	Crowdstrike Alert for malicious SHA256 for user $user$ on ...	Crowdstrike Malware alert for user $user$ on NUCPUIMHU...		Jun 23rd, 2023 4:00 PM	Jun 25th, 2023 12:01 AM	unassigned	New	Medium	Unassig...	Undete...	ES Notable Event	malware	● Jun 24...
□	MC-38549	...9bdf5	Crowdstrike Alert for malicious SHA256 for user $user$ on ...	Crowdstrike Malware alert for user $user$ on NUCPUIMHU...		Jun 23rd, 2023 4:00 PM	Jun 23rd, 2023 4:00 PM	unassigned	New	Medium	Unassig...	Undete...	ES Notable Event	malware	● Jun 24...
□	MC-38406	...e1f53	Crowdstrike Alert for malicious SHA256 for user $user$ on ...	Crowdstrike Malware alert for user $user$ on WS237672 ...		Jun 23rd, 2023 8:00 AM	Jun 26th, 2023 11:05 AM	jarora	New	Low	Unassig...	Undete...	ES Notable Event	malware	● Jun 24...
□	MC-38405	...66a6	Crowdstrike Alert for malicious SHA256 for user $user$ on ...	Crowdstrike Malware alert for user $user$ on WS256480 ...		Jun 23rd, 2023 8:00 AM	Jun 23rd, 2023 8:00 AM	unassigned	New	Medium	Unassig...	Undete...	ES Notable Event	default	● Jun 24...
□	MC-38177	...74a2	Crowdstrike Alert for malicious SHA256 for user $user$ on A...	Crowdstrike Malware alert for user $user$ on ABC-C3QR6...		Jun 22nd, 2023 12:00 PM	Jun 23rd, 2023 2:42 PM	unassigned	New	Low	Unassig...	Undete...	ES Notable Event	malware	● Jun 23...

Show 20

Note the Incident type field above

Click on one of the incident and go into details and then click on the Response tab



MC-39147 Crowdstrike Alert for malicious SHA256 for user $user$ on NUCTSHRWEB...

Response

Crowdstrike Malware Detection investigation
0% completed

PHASE
Triage and Investigate (0/2)

Crowdstrike malware alert tri...
unassigned

Environment context and enri...
unassigned

Crowdstrike malware alert triage

Assigned to: unassigned

Description
Runs a playbook to automatically triage malware alert from crowdstrike and post enrichment notes on the Mission Control Incident

Respond 1
Playbook
crowdstrike_malware_triage_modern

Notes 0
Note title: Crowdstrike malware alert triage - Task Note - 1

Files 0

INFO

Owner: unassigned
Status: New
Urgency: Medium
Sensitivity: Unassigned
Incident Type: malware
Disposition: Undetermined

Incident ID	MC-39147
Description	Crowdstrike Malware alert for user $user$ on NUCTSHRWEB1A with malicious file $file$ and SHA256 dce18e2279073ba64a6f35d17120fdca9a4902faef0c99cd96a5d673209e132f
Created	Jun 26th, 2023 12:00 PM
Last updated	Jun 26th, 2023 12:00 PM
Incident origin	ES Notable Event
Reference ID	3f03698c-bc8c-4915-bd96-9a620b787fe4
SLA	20 hrs 37 mins

The response plan is attached successfully to the incident

SOAR Playbook

The playbook is configured to capture the malicious SHA256 identified in Crowdstrike alert and operate on it with various actions provided by the SOAR Connector for Crowdstrike - "Crowdstrike OAuth API"
The flow of the playbook is described as:

1. Playbook is launched from the response plan assigned to the incident in Mission Control

2. It fetches the incident and response plan data using get_incident, get_phase and get_task API in the Mission Control block of SOAR

3. From the incident data, it uses the SHA256 value to look for existing indicators in Crowdstrike using the get_indicator action

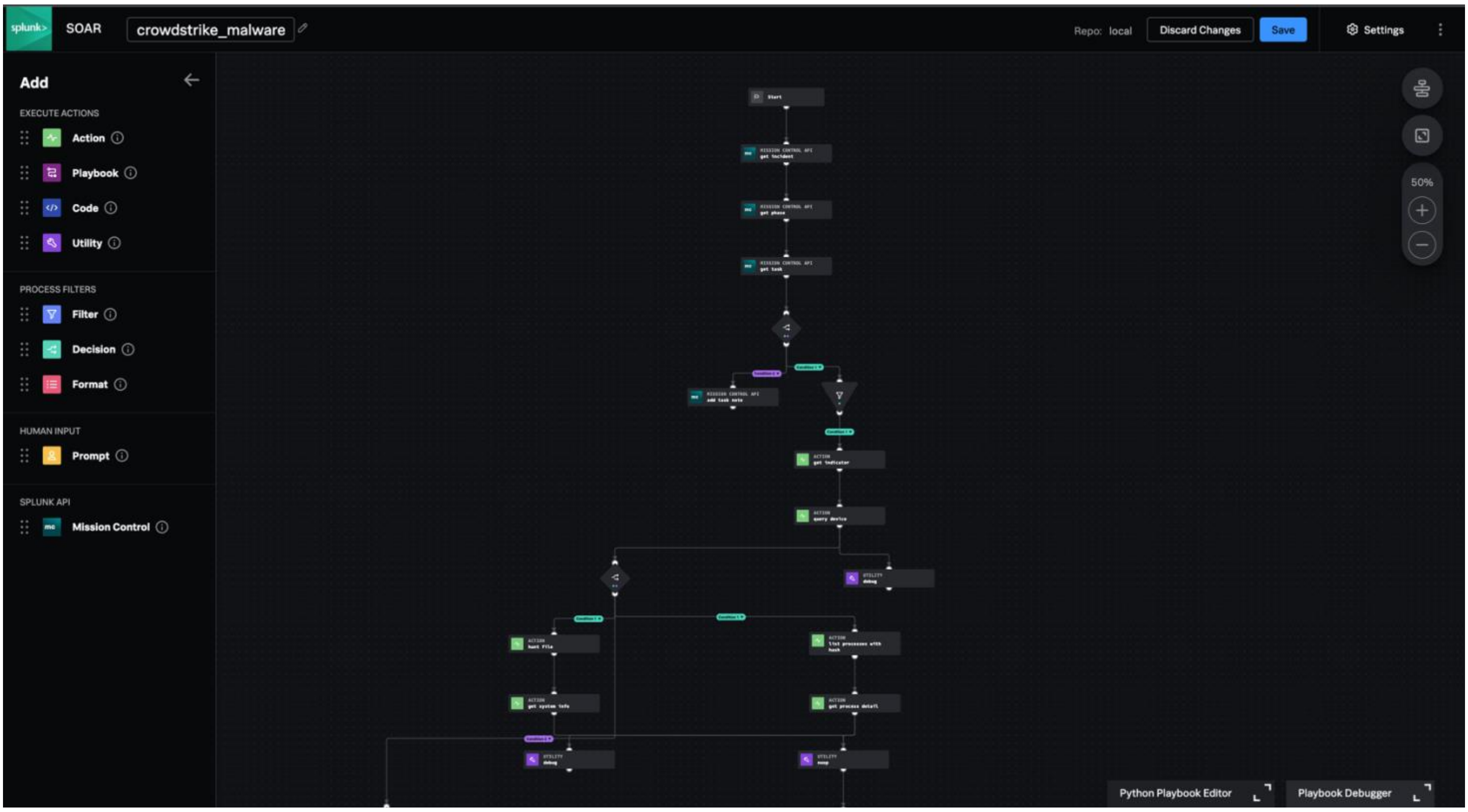
4. From the incident data, it uses the hostname value to query the device details from Crowdstrike, using the query_device action

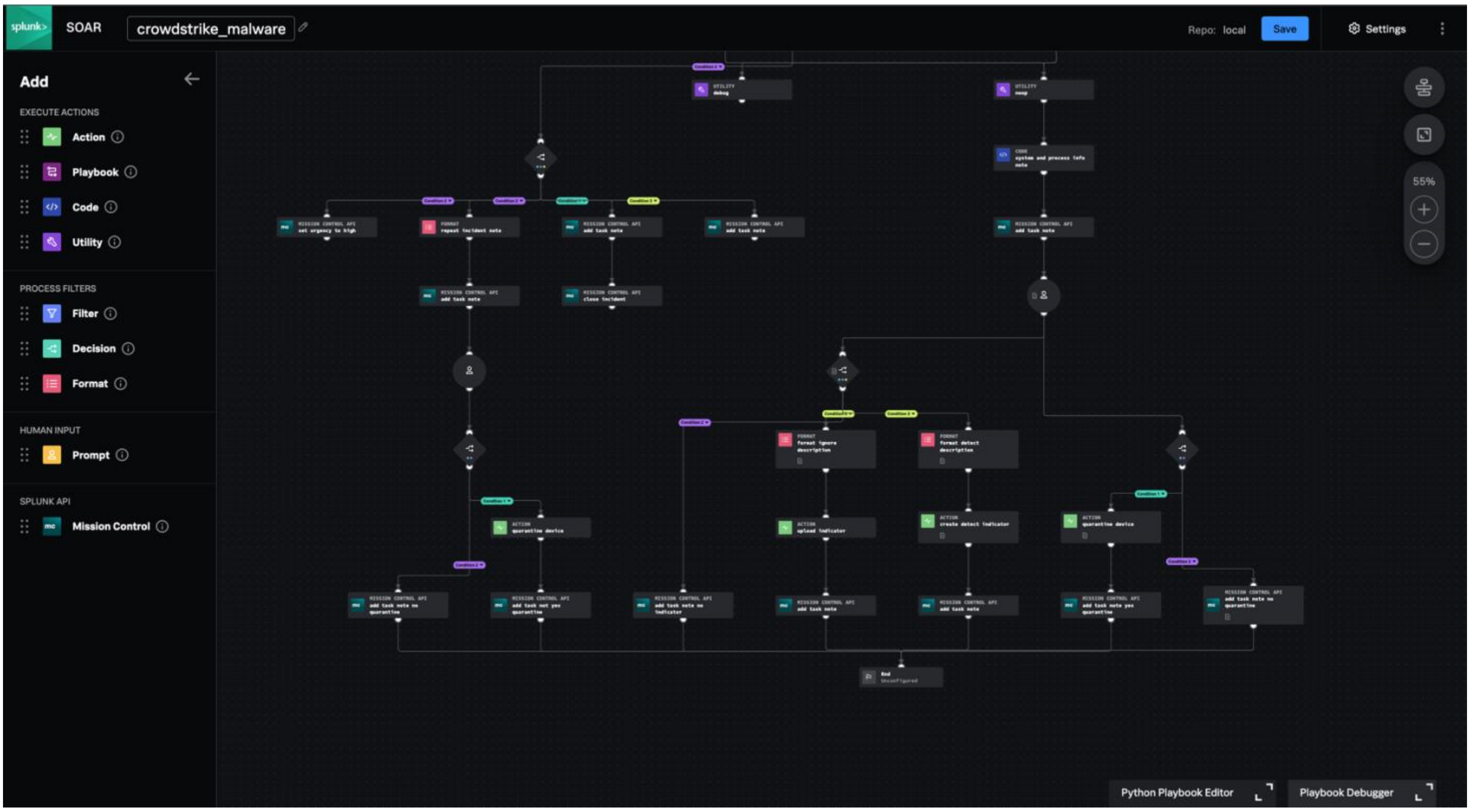
5. If the indicator is not found in crowdstrike, it performs the following actions and write the summary as a task note in the Mission Control response plan
   a. List processes with hash
   b. Get process details
   c. Hunt file in crowdstrike and identify number of affected hosts
   d. Get system information of all affected hosts

6. Based on the output of above action and summary written in the task note, it prompts the incident owner to make a decision on below:
   a. Should SOAR create the indicator in Crowdstrike for future detections
   b. Should the endpoint be quarantined by Crowdstrike as containment

7. If the indicator is found in crowdstrike, it performs the following actions and write the summary as a task note in Mission Control response plan
   a. If the value of "policy" in crowdstrike for the indicator is "none", it adds a task note to the incident as indicator is not malicious and close the incident
   b. If the value of "policy" in crowdstrike for the indicator is "detect", it raise the incident urgency to "High" and creates a task note about the indicator being a repeat offender and prompts the incident owner to decide further actions as below:
      i. Should the endpoint be quarantined in crowdstrike
   c. If the value of policy is neither "detect" nor "none", it raises an exception in the task note as "The playbook received an unexpected indicator policy and needs to be extended to handle this situation." – this can be further developed for this use case

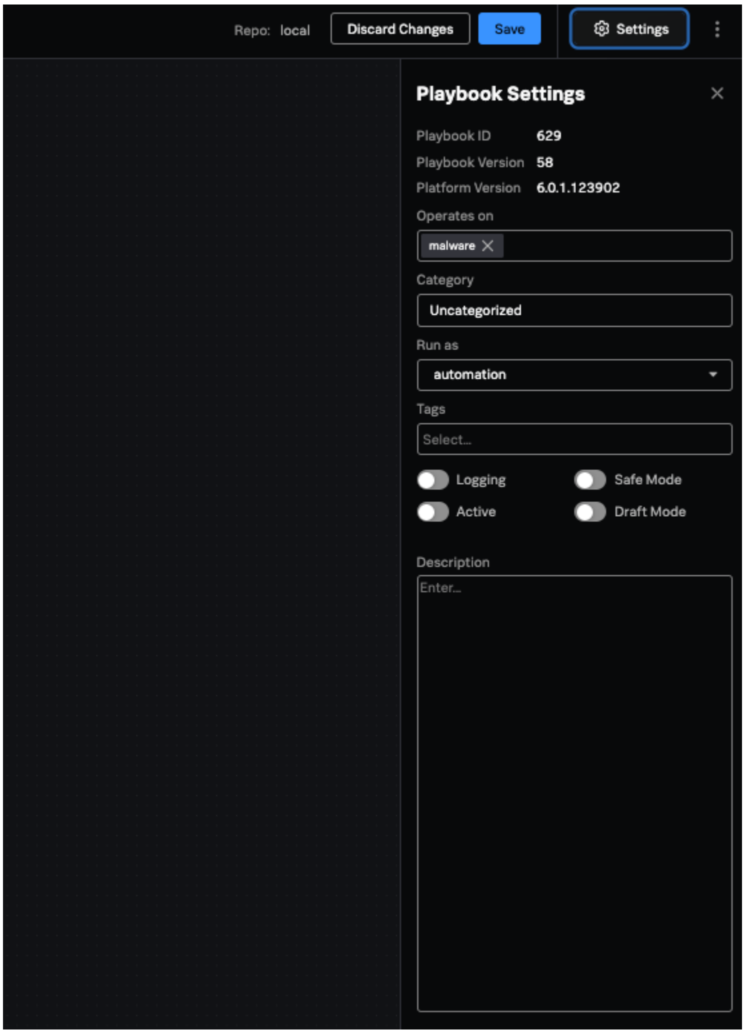
Below is the screenshot of the playbook:





***The inspiration of this playbook comes from the original "crowdstrike_malware_triage" community playbook which was created a long time ago and was built in the Classic Visual Playbook Editor of Splunk Phantom.*
*I have used same the response workflow as was in the original playbook and used all the latest and greatest features of Mission Control to create this in Modern VPE.***

Import the playbook in your Splunk SOAR environment and configure the playbook to use Crowdstrike OAuth API asset
Configure the playbook to run on incident_type "malware" in Settings:



Playbook Settings

Playbook ID 629

Playbook Version 58

Platform Version 6.0.1.123902

Operates on: malware

Category: Uncategorized

Run as: automation

Tags: Select...

Logging

Safe Mode

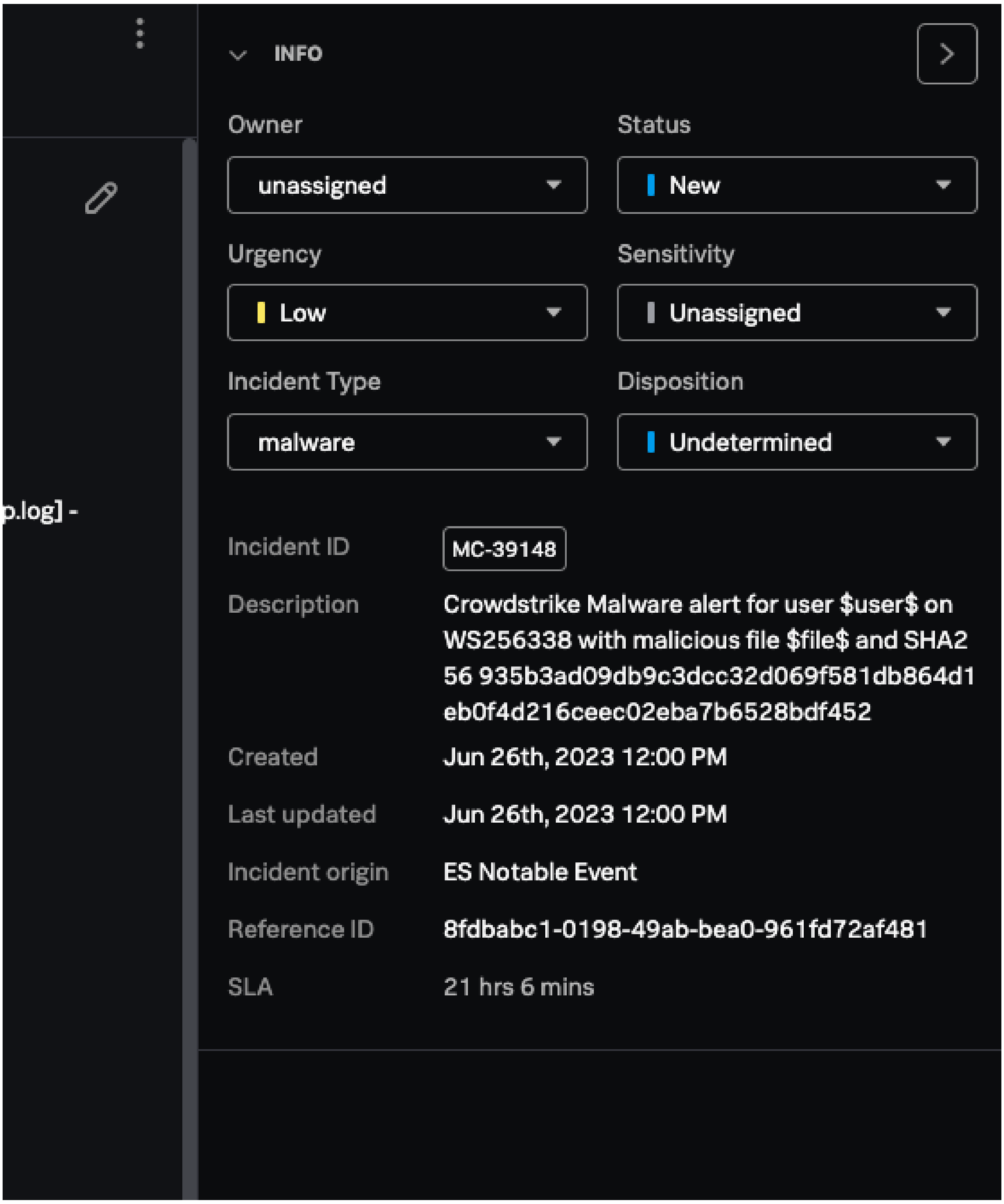
Active

Draft Mode

Description: Enter...

Perform testing of the playbook

Browse to the details of a Crowdstrike incident in Mission Control and copy the incident ID (shown as “Reference ID” in the below screenshot)



Owner: unassigned

Status: New

Urgency: Low

Sensitivity: Unassigned

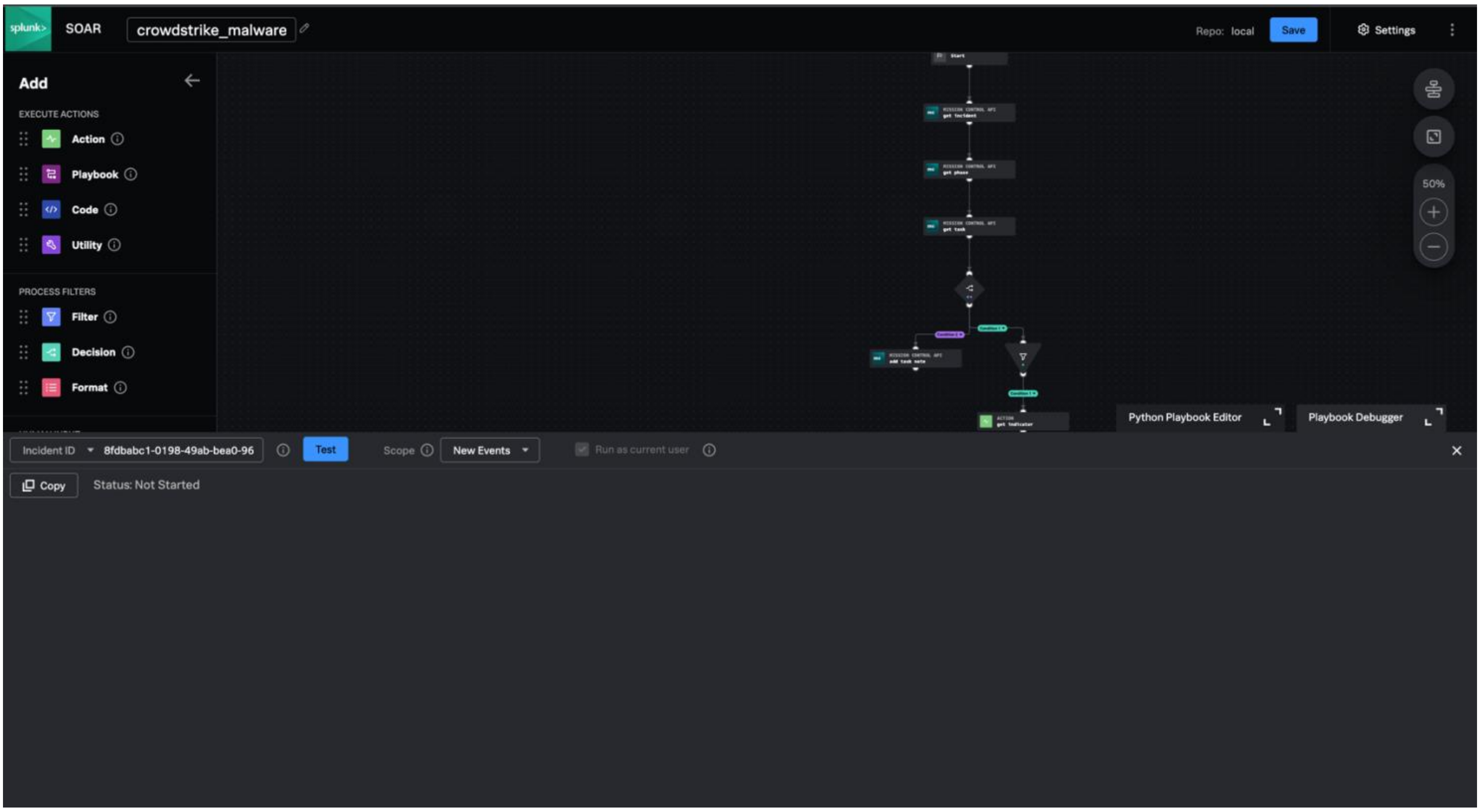
Incident Type: malware

Disposition: Undetermined

Incident ID	MC-39148
Description	Crowdstrike Malware alert for user $user$ on WS256338 with malicious file $file$ and SHA256 935b3ad09db9c3dcc32d069f581db864d1eb0f4d216ceec02eba7b6528bdf452
Created	Jun 26th, 2023 12:00 PM
Last updated	Jun 26th, 2023 12:00 PM
Incident origin	ES Notable Event
Reference ID	8fdbabc1-0198-49ab-bea0-961fd72af481
SLA	21 hrs 6 mins

Open the playbook in VPE, and click on the Playbook Debugger window at the bottom.

Paste the incident id value copied earlier in the Playbook Debugger and click on Test



Incident ID 8fdbabc1-0198-49ab-bea0-96

Scope New Events

☑ Run as current user

Status: Not Started

Troubleshoot and resolve all the errors and ensure successful functionality of the playbook by:

1. Going through the playbook debug log
2. Ensuring all the notes are being created in the incident
3. Ensuring the correct user prompts are appearing in the Mission Control prompt section

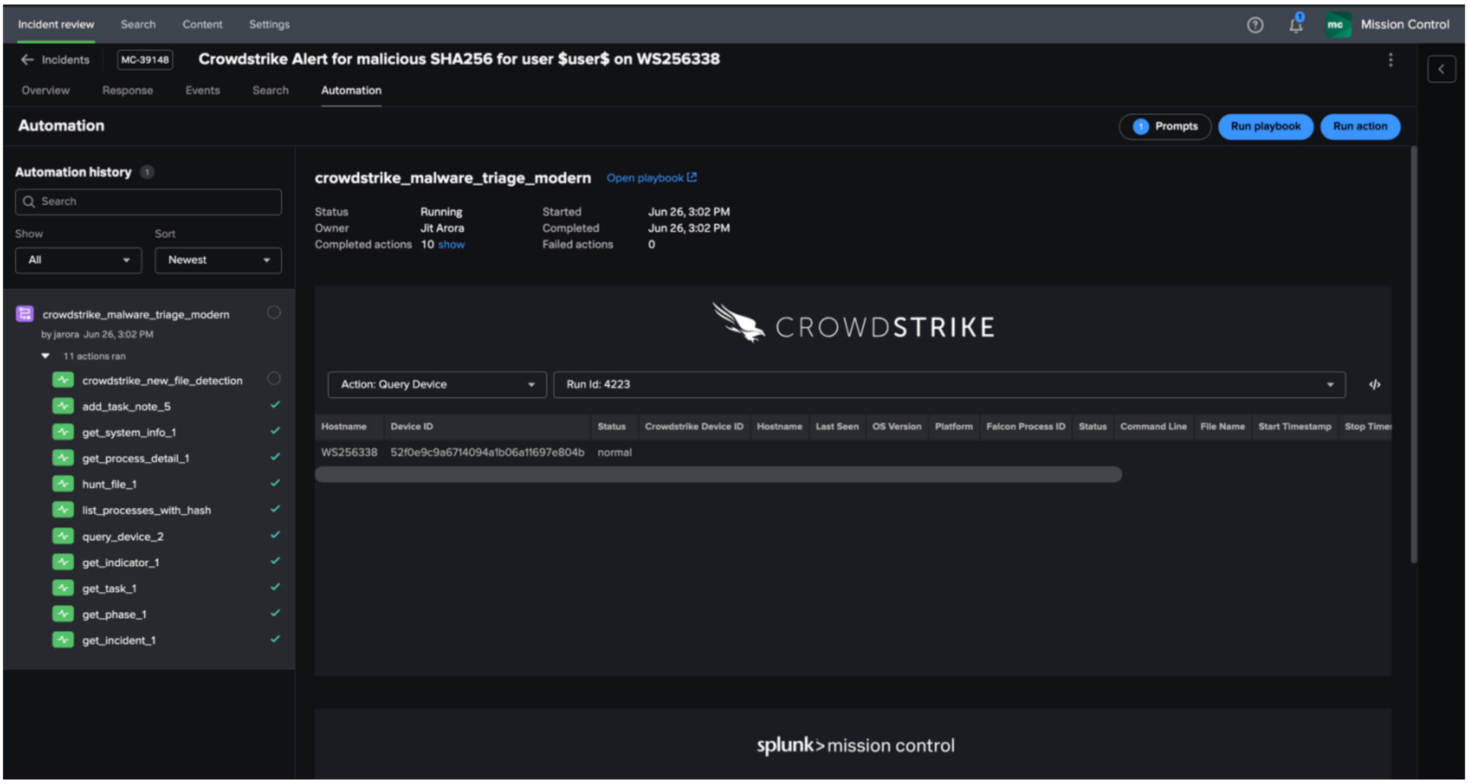
After the successful testing of playbook and sufficient confidence in the response workflow, the playbook can be made "Active" in the playbook settings, which will enable it to run automatically as soon as the incident is created in Mission Control.

This will enable analyst to receive the information and user prompts when they arrive at the incident, rather than waiting for the playbook to complete lengthy information gathering tasks, if they choose to fire the playbook manually for each incident.

Optionally, the user prompts can also be coupled with simple email notifications, so that analyst can be notified via email when there is a response task waiting for them in Mission Control.

Example screenshots:

Playbook execution paused at the user prompt (showing as 1 prompt for MC Analyst)



Crowdstrike Alert for malicious SHA256 for user $user$ on WS256338

Automation

Automation history 1

Show: All | Sort: Newest

crowdstrike_malware_triage_modern
by jarora Jun 26, 3:02 PM
11 actions ran

- crowdstrike_new_file_detection
- add_task_note_5 ✓
- get_system_info_1 ✓
- get_process_detail_1 ✓
- hunt_file_1 ✓
- list_processes_with_hash ✓
- query_device_2 ✓
- get_indicator_1 ✓
- get_task_1 ✓
- get_phase_1 ✓
- get_incident_1 ✓

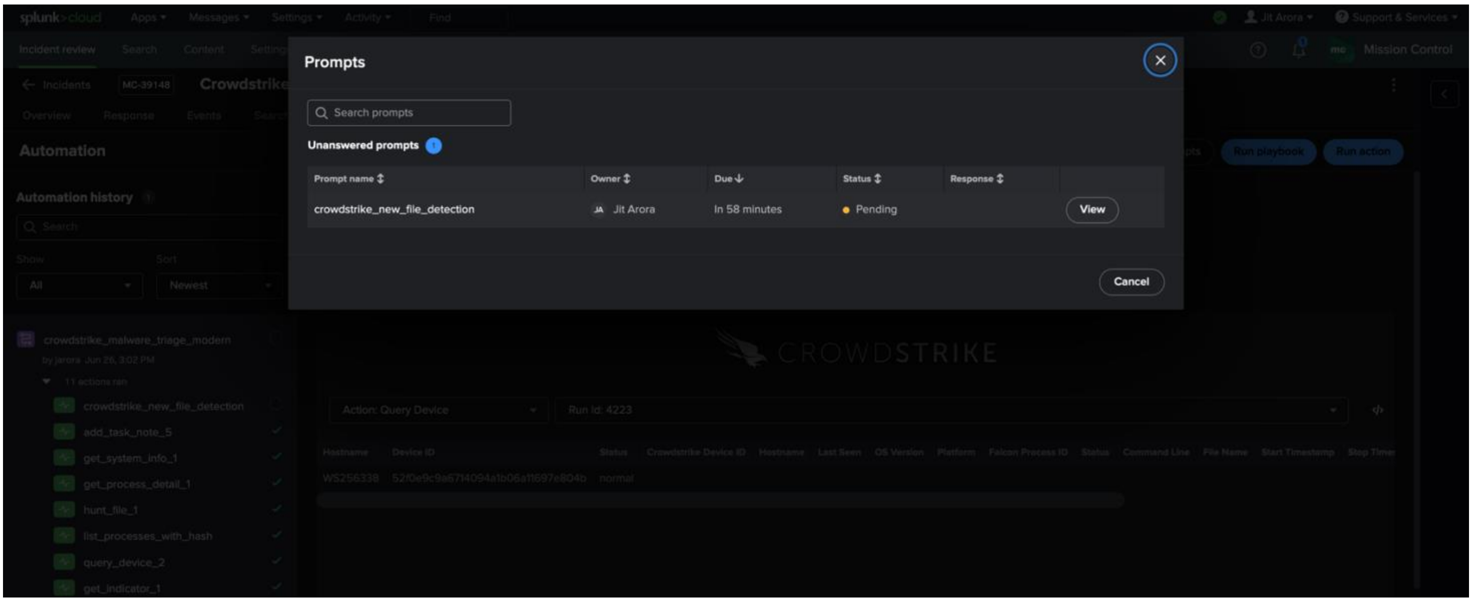
crowdstrike_malware_triage_modern

Status	Running	Started	Jun 26, 3:02 PM
Owner	Jit Arora	Completed	Jun 26, 3:02 PM
Completed actions	10 show	Failed actions	0

Action: Query Device | Run Id: 4223

Hostname	Device ID	Status	Crowdstrike Device ID	Hostname	Last Seen	OS Version	Platform	Falcon Process ID	Status	Command Line	File Name	Start Timestamp	Stop Time
WS256338	52f0e9c9a6714094a1b06a11697e804b	normal											

After clicking on the Prompt

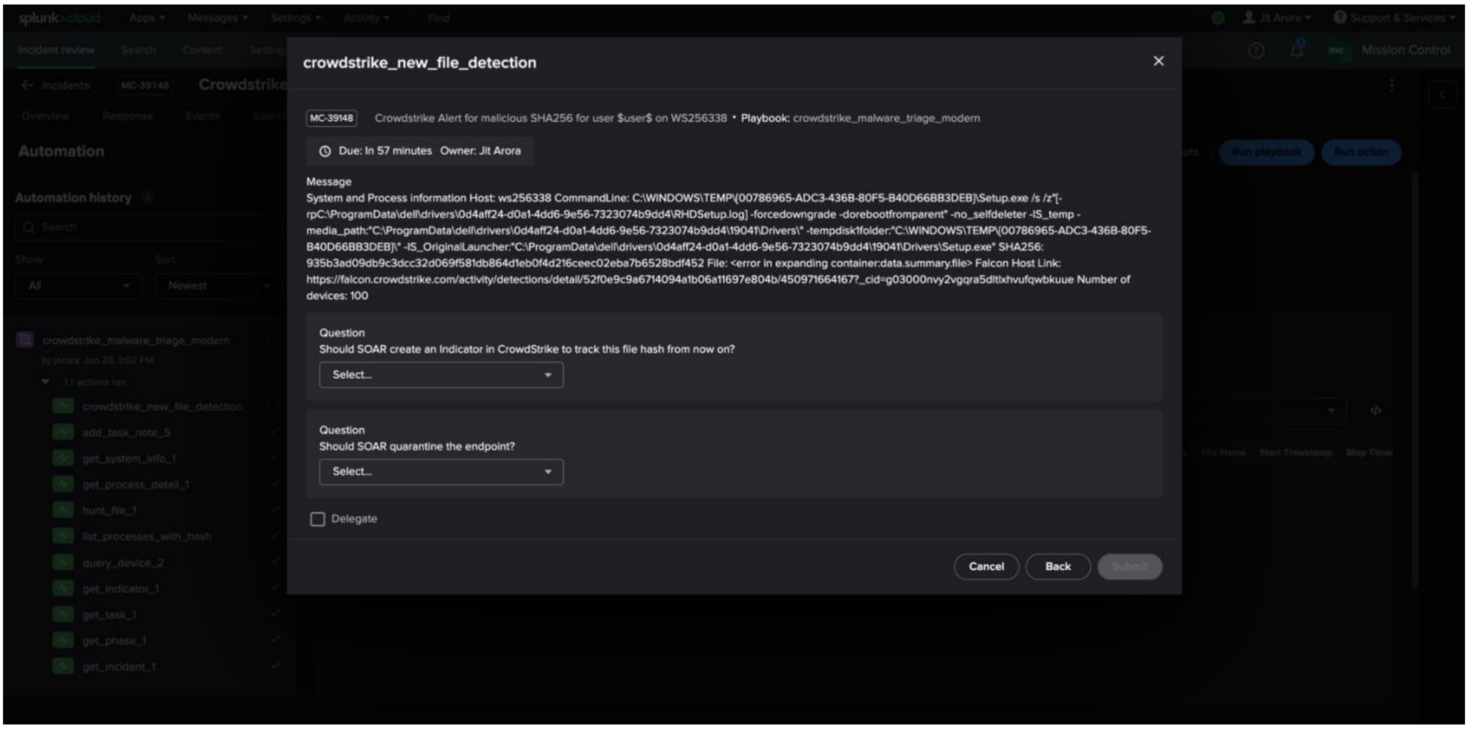


Prompts

Unanswered prompts 1

Prompt name	Owner	Due	Status	Response
crowdstrike_new_file_detection	JA Jit Arora	In 58 minutes	● Pending	

Details of the message and available action in the prompt



crowdstrike_new_file_detection

MC-39148 Crowdstrike Alert for malicious SHA256 for user $user$ on WS256338 • **Playbook:** crowdstrike_malware_triage_modern

Due: In 57 minutes Owner: Jit Arora

Message

System and Process Information Host: ws256338 CommandLine: C:\WINDOWS\TEMP\{00786965-ADC3-436B-80F5-B40D66BB3DEB}\Setup.exe /s /z"[-rpC:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\RHDSetup.log] -forcedowngrade -dorebootfromparent" -no_selfdeleter -IS_temp -media_path:"C:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers\" -tempdisk1folder:"C:\WINDOWS\TEMP\{00786965-ADC3-436B-80F5-B40D66BB3DEB}\" -IS_OriginalLauncher:"C:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers\Setup.exe" SHA256: 935b3ad09db9c3dcc32d069f581db864d1eb0f4d216ceec02eba7b6528bdf452 File: <error in expanding container:data.summary.file> Falcon Host Link: https://falcon.crowdstrike.com/activity/detections/detail/52f0e9c9a6714094a1b06a11697e804b/450971664167?_cid=g03000nvy2vgqra5dltlxhvufqwbkuue Number of devices: 100

Question

Should SOAR create an Indicator in CrowdStrike to track this file hash from now on?

Select...

Question

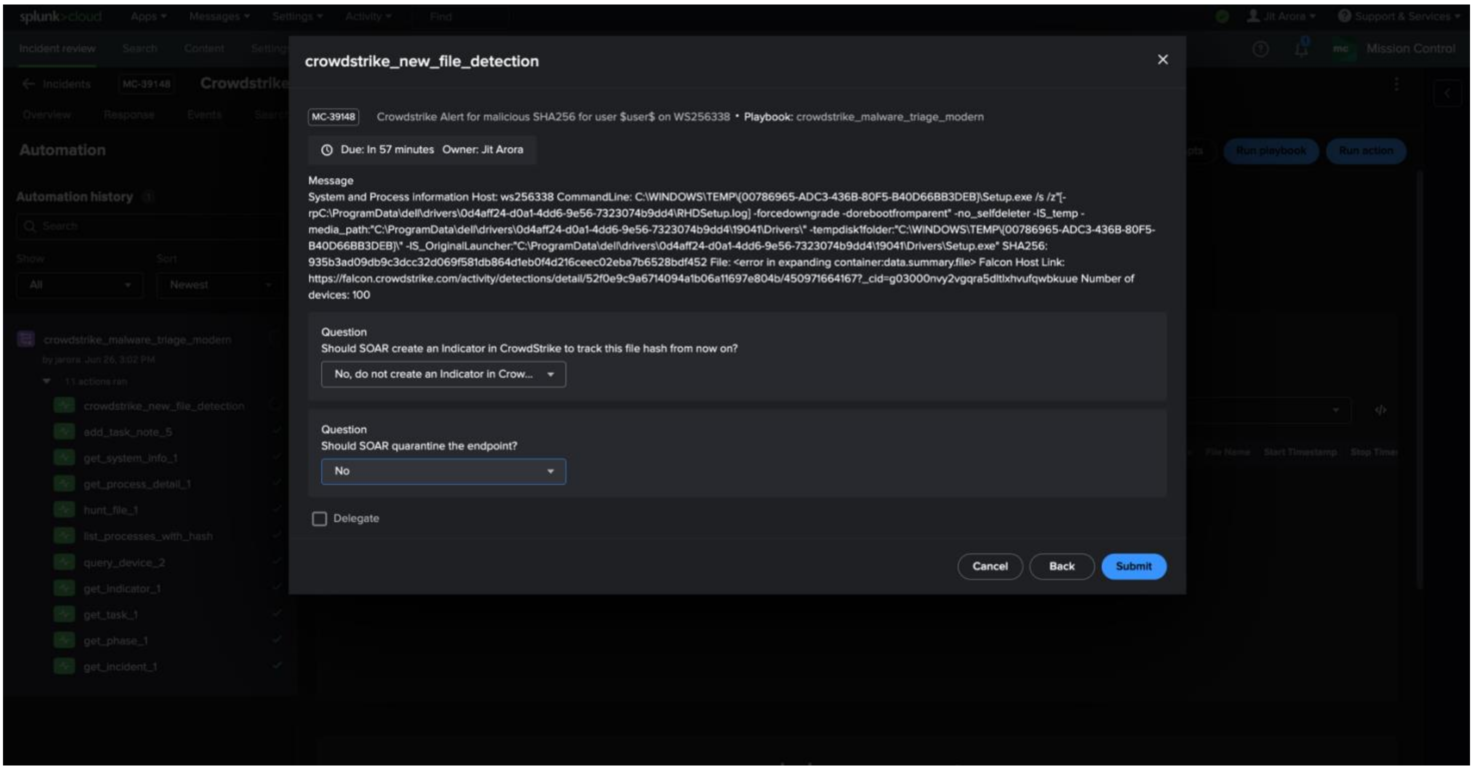
Should SOAR quarantine the endpoint?

Select...

□ Delegate

Cancel Back Submit

After submitting the appropriate response



crowdstrike_new_file_detection

MC-39148 Crowdstrike Alert for malicious SHA256 for user $user$ on WS256338 • **Playbook:** crowdstrike_malware_triage_modern

Due: In 57 minutes Owner: Jit Arora

Message

System and Process Information Host: ws256338 CommandLine: C:\WINDOWS\TEMP\{00786965-ADC3-436B-80F5-B40D66BB3DEB}\Setup.exe /s /z"[-rpC:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\RHDSetup.log] -forcedowngrade -dorebootfromparent" -no_selfdeleter -IS_temp -media_path:"C:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers\" -tempdisk1folder:"C:\WINDOWS\TEMP\{00786965-ADC3-436B-80F5-B40D66BB3DEB}\" -IS_OriginalLauncher:"C:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers\Setup.exe" SHA256: 935b3ad09db9c3dcc32d069f581db864d1eb0f4d216ceec02eba7b6528bdf452 File: <error in expanding container:data.summary.file> Falcon Host Link: https://falcon.crowdstrike.com/activity/detections/detail/52f0e9c9a6714094a1b06a11697e804b/450971664167?_cid=g03000nvy2vgqra5dltlxhvufqwbkuue Number of devices: 100

Question

Should SOAR create an Indicator in CrowdStrike to track this file hash from now on?

No, do not create an Indicator in Crow...

Question

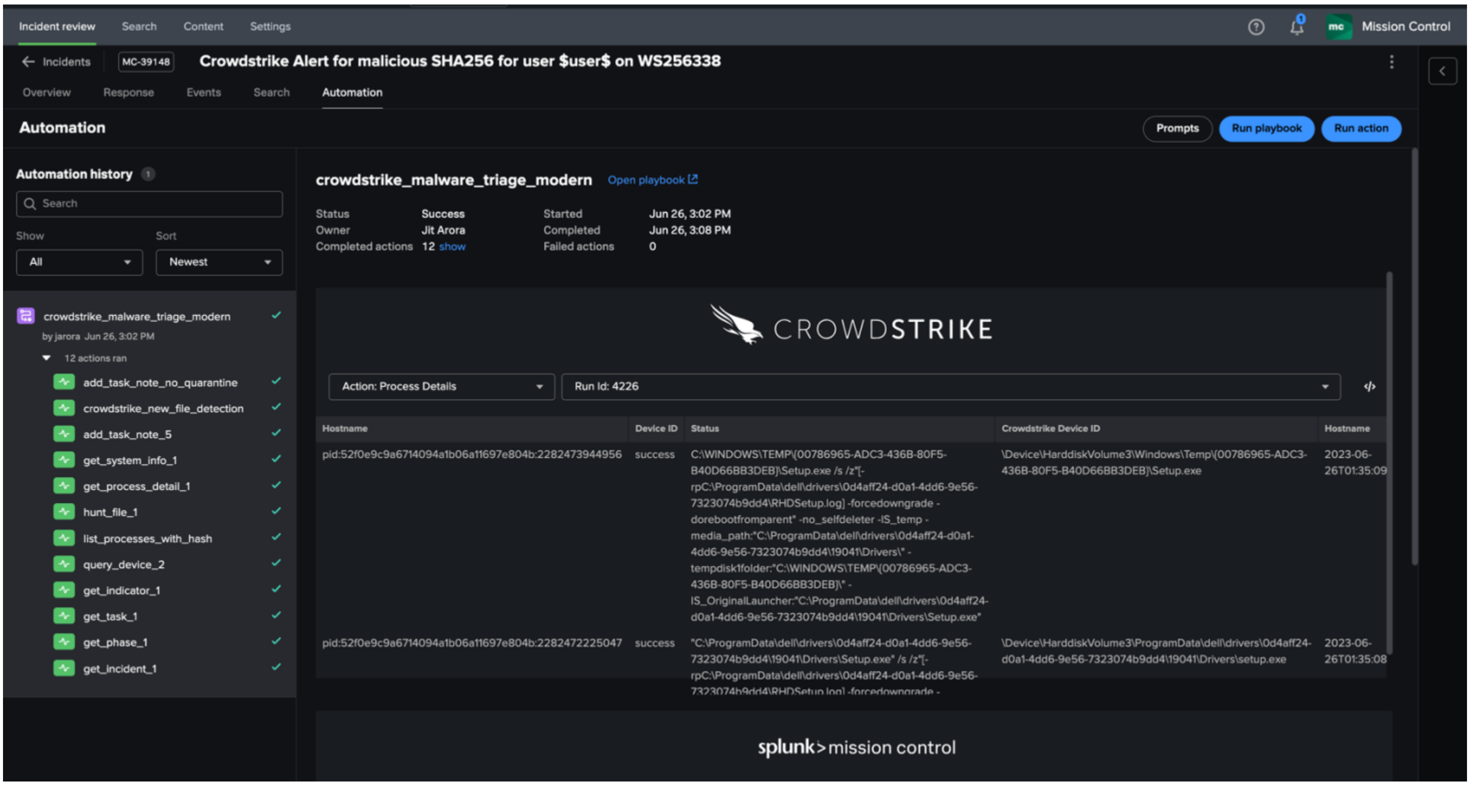
Should SOAR quarantine the endpoint?

No

□ Delegate

Cancel Back Submit

All playbook actions completed successfully



Crowdstrike Alert for malicious SHA256 for user $user$ on WS256338

Automation

Automation history 1

Show: All — Sort: Newest

crowdstrike_malware_triage_modern ✓
by jarora Jun 26, 3:02 PM
12 actions ran

- add_task_note_no_quarantine ✓
- crowdstrike_new_file_detection ✓
- add_task_note_5 ✓
- get_system_info_1 ✓
- get_process_detail_1 ✓
- hunt_file_1 ✓
- list_processes_with_hash ✓
- query_device_2 ✓
- get_indicator_1 ✓
- get_task_1 ✓
- get_phase_1 ✓
- get_incident_1 ✓

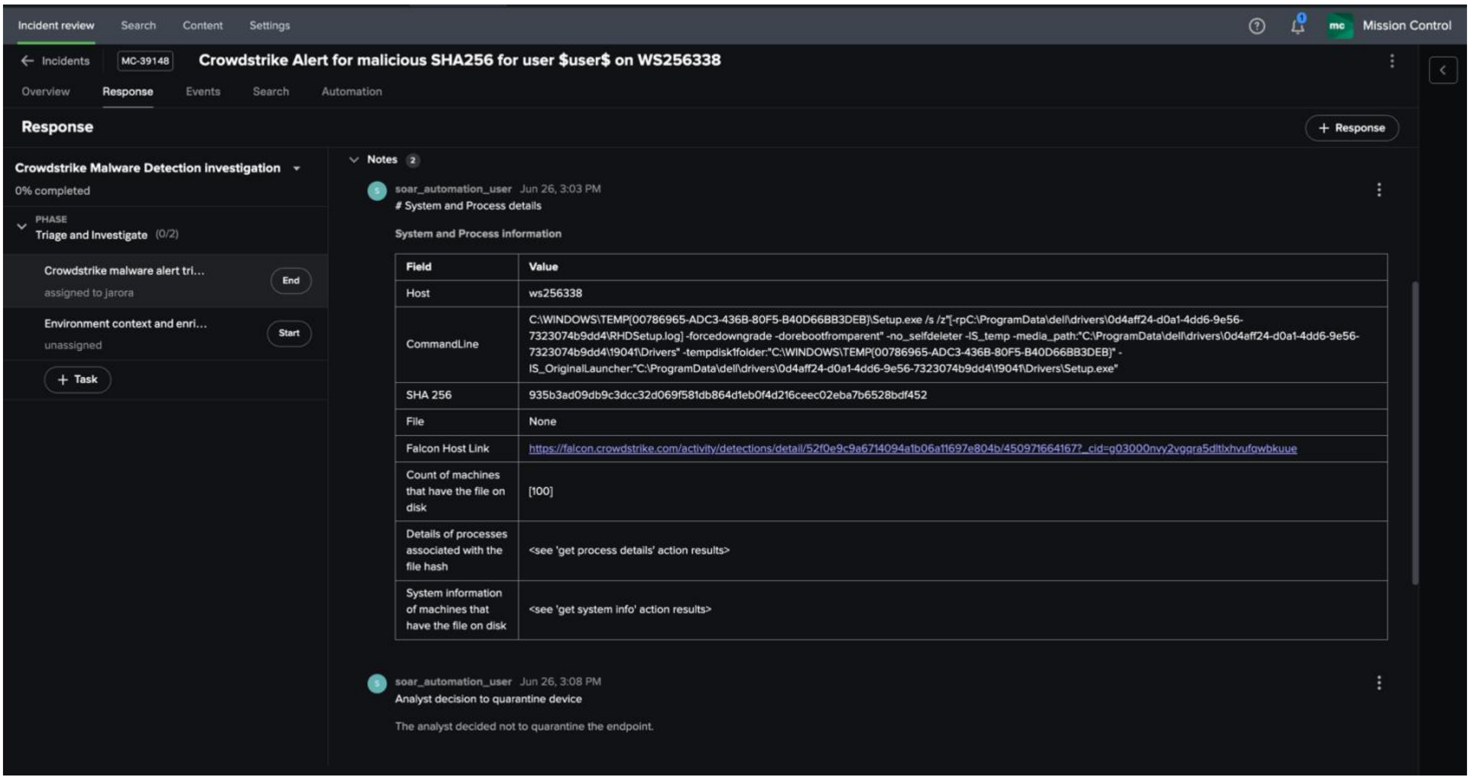
crowdstrike_malware_triage_modern

Status	Success	Started	Jun 26, 3:02 PM
Owner	Jit Arora	Completed	Jun 26, 3:08 PM
Completed actions	12 show	Failed actions	0

Action: Process Details — Run Id: 4226

Hostname	Device ID	Status	Crowdstrike Device ID	Hostname
pid:52f0e9c9a6714094a1b06a11697e804b:2282473944956	success	C:\WINDOWS\TEMP\{00786965-ADC3-436B-80F5-B40D66BB3DEB}\Setup.exe /s /z"[-rpC:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\RHDSetup.log] -forcedowngrade -dorebootfromparent" -no_selfdeleter -IS_temp -media_path:"C:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers\" -tempdisk1folder:"C:\WINDOWS\TEMP\{00786965-ADC3-436B-80F5-B40D66BB3DEB}\" -IS_OriginalLauncher:"C:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers\Setup.exe"	\Device\HarddiskVolume3\Windows\Temp\{00786965-ADC3-436B-80F5-B40D66BB3DEB}\Setup.exe	2023-06-26T01:35:09
pid:52f0e9c9a6714094a1b06a11697e804b:2282472225047	success	"C:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers\Setup.exe" /s /z"[-rpC:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\RHDSetup.log] -forcedowngrade -	\Device\HarddiskVolume3\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers\setup.exe	2023-06-26T01:35:08

Task notes added to the incident



Crowdstrike Alert for malicious SHA256 for user $user$ on WS256338

Response

Crowdstrike Malware Detection investigation
0% completed

PHASE
Triage and Investigate (0/2)

Crowdstrike malware alert tri...
assigned to jarora

Environment context and enri...
unassigned

Notes 2

soar_automation_user Jun 26, 3:03 PM
System and Process details

System and Process information

Field	Value
Host	ws256338
CommandLine	C:\WINDOWS\TEMP\{00786965-ADC3-436B-80F5-B40D66BB3DEB}\Setup.exe /s /z"[-rpC:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\RHDSetup.log] -forcedowngrade -dorebootfromparent" -no_selfdeleter -IS_temp -media_path:"C:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers" -tempdisk1folder:"C:\WINDOWS\TEMP\{00786965-ADC3-436B-80F5-B40D66BB3DEB}" -IS_OriginalLauncher:"C:\ProgramData\dell\drivers\0d4aff24-d0a1-4dd6-9e56-7323074b9dd4\19041\Drivers\Setup.exe"
SHA 256	935b3ad09db9c3dcc32d069f581db864d1eb0f4d216ceec02eba7b6528bdf452
File	None
Falcon Host Link	https://falcon.crowdstrike.com/activity/detections/detail/52f0e9c9a6714094a1b06a11697e804b/450971664167?_cid=g03000nvy2vggra5dltlxhvufqwbkuue
Count of machines that have the file on disk	[100]
Details of processes associated with the file hash	<see 'get process details' action results>
System information of machines that have the file on disk	<see 'get system info' action results>

soar_automation_user Jun 26, 3:08 PM
Analyst decision to quarantine device

The analyst decided not to quarantine the endpoint.

Summary

This process can bring the advance capabilities of Crowdstrike Falcon to the centre of incident triage, investigation and response in Splunk Mission Control. Many decisions and logics involved in this response workflow are kept at a basic level, so it is recommended to take into consideration the nature and behaviour of customer's organisation and modify those thresholds and logics accordingly to achieve a comprehensive investigation and analysis.

This content and the playbook prepared for this use case is open to public on my GitHub and can be customised and extended to achieve the desired outcome.

Any feedback is welcome that I can incorporate into this documentation and content.

Happy Splunking with Mission Control ☺