



# Building Playbooks in Google SecOps

Using Playbooks in Security Operations



January 2024

Using [goo.gle/secops-workshop](https://goo.gle/secops-workshop)

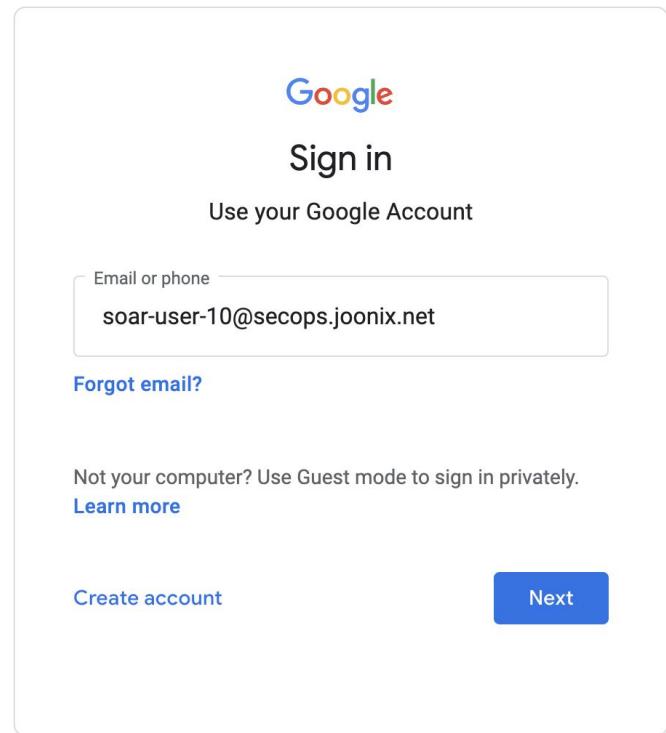


# Agenda

- SecOps Overview
- The Basics
- Playbook Walk Through
- Alert Views
- Playbook Simulator
- Build Your Own Playbook

# Login Instructions (1)

- 1) Open a new Incognito Window in your Chrome Browser
- 2) Navigate to the Google SecOps instance URL:  
**<https://goo.gle/secops-workshop>**
- 3) Use the account assigned to you by your instructor that uses Google Workspace as Identity Provider



The image shows a screenshot of the Google Sign-in page. At the top right, it says "Sign in" and "Use your Google Account". Below that is a text input field labeled "Email or phone" containing "soar-user-10@secops.joonix.net". To the left of the input field is a "Forgot email?" link. At the bottom left, there's a "Create account" link, and at the bottom right, a blue "Next" button.



# Login Instructions (2)

4) If you get “Verify It’s you” screen, click on “Confirm your recovery email” option

Google

### Verify it's you

To help keep your account safe, Google wants to make sure it's really you trying to sign in

[Learn more](#)

[soar-user-10@secops.joonix.net](#) ▾

Choose how you want to sign in:

- Get a verification code at [soa\\*\\*\\*\\*\\*@se\\*\\*\\*\\*\\*.net](#)
- Use another phone or computer to finish signing in
- Confirm your recovery email
- Get help

5) Type “[soarworkshop-instructor@secops.joonix.net](#)” as the recovery email and click Next

Google

### Verify it's you

To help keep your account safe, Google wants to make sure it's really you trying to sign in

[Learn more](#)

[soar-user-10@secops.joonix.net](#) ▾

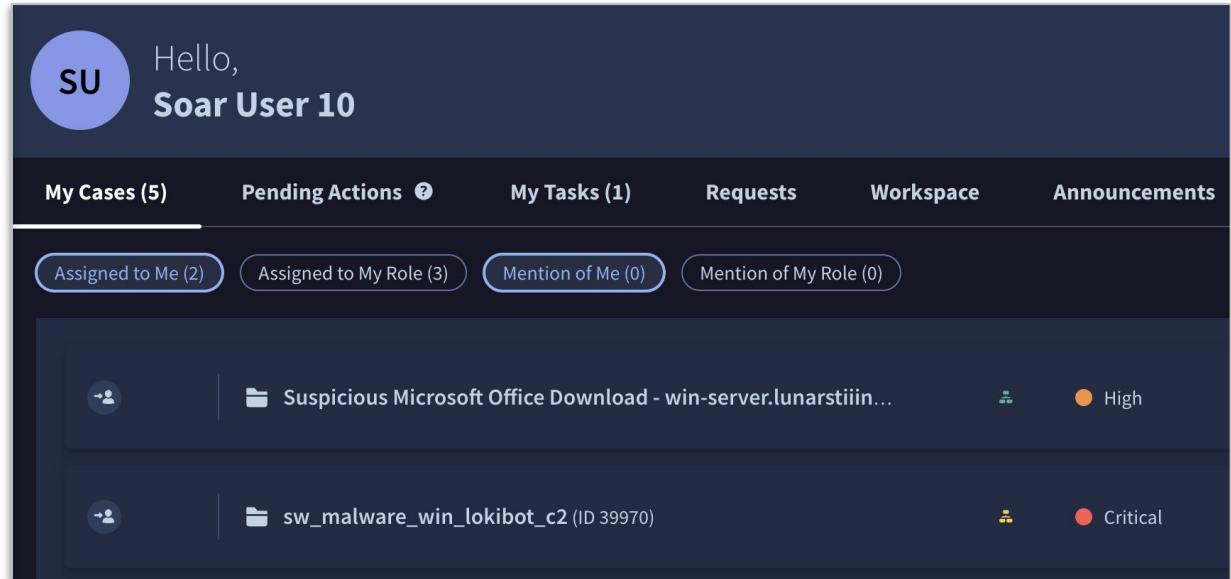
Confirm the recovery email address you added to your account: [soa\\*\\*\\*\\*\\*@se\\*\\*\\*\\*\\*.net](#)

Enter recovery email address

[Try another way](#) [Next](#)

# Login Instructions (3)

- 6) We are now logged into Google SecOps with a view similar to this



Hello,  
**Soar User 10**

My Cases (5) Pending Actions (3) My Tasks (1) Requests Workspace Announcements

Assigned to Me (2) Assigned to My Role (3) Mention of Me (0) Mention of My Role (0)

Suspicious Microsoft Office Download - win-server.lunarstiin... (High)  
sw\_malware\_win\_lokibot\_c2 (ID 39970) (Critical)

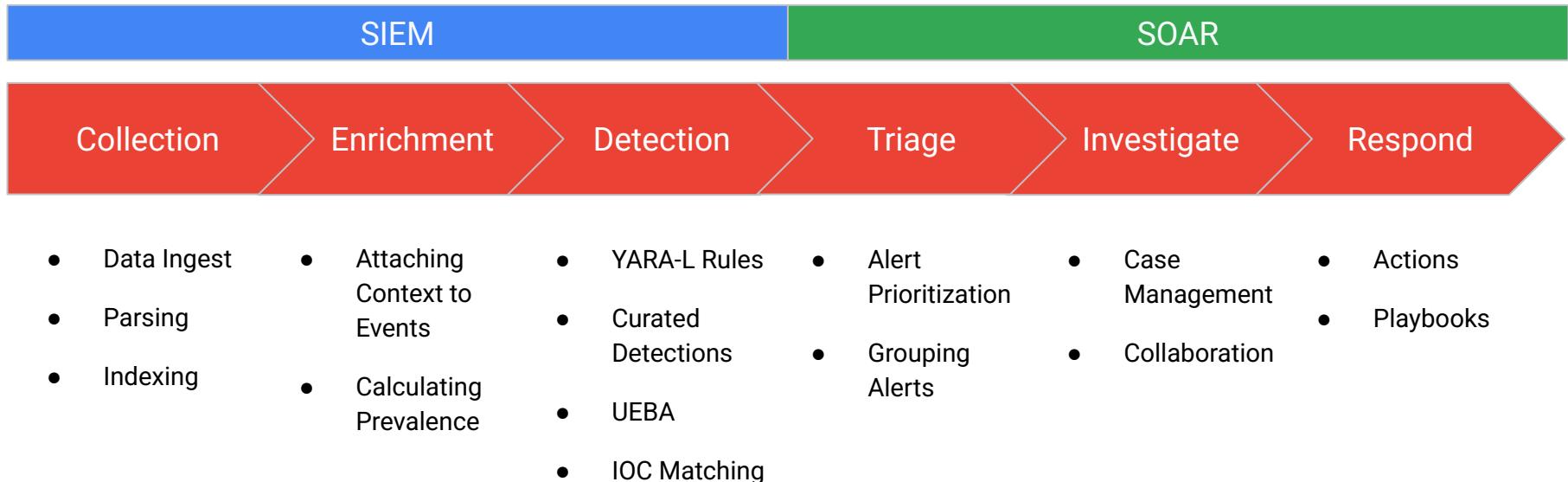


Google SecOps

# SecOps Overview



# Google's Security Operations Platform





# Terminology

- **Alerts** : Detections generated by rules and made up of events
- **Case** : A collection of one or more alerts grouped by common values and time
- **Entity** : Objects of interest in an alert
  - Examples include hostname, username, filehash, domain, ip address, process name and more
- **Integration** : Third party solutions that Google SecOps can send or receive API calls from
- **Action** : Part of integrations. Used for specific API calls with third parties
- **Connector** : Responsible for alert ingestion
- **Job** : Acts as a scheduler and allows for a health check sync
- **Playbook** : Workflow of action blocks executed following a trigger
  - **Trigger** : Mandatory block that starts a playbook

# Playbooks

Provide a method to automate actions that an analyst might otherwise have to manually perform when an alert is created

Allows analysts to respond to specific alerts in a prescribed, repeatable manner

Inject specific analyst inputs into the process and then allow the system to go down other paths based on the input provided

It is expected that users have gone through the Case Management in Google SecOps workshop or have comparable experience as this builds on concepts covered in that workshop



Google SecOps

# The Basics

# Playbook Editor



# Google SecOps

The screenshot shows the Google SecOps Playbooks interface. On the left, there's a sidebar with navigation icons and sections for 'Default' and 'Imported Playbooks'. A red box highlights the 'SOAR Workshop' section, which contains four entries: 'Case Management W...', 'Case Management W...', 'Initial Severity Block', and 'Playbook Workshop ...'. The main area displays the 'Case Management W...' playbook, which is currently 'View only'. It shows the creation details: 'SOAR Workshop' (Workshop 10), 'September 11, 2024 17:43:22', and 26 steps. A note states: 'This playbook is used in the Case Management Workshop and is triggered by an alert from the'. Below this is a toolbar with 'Playbook' and 'Alert View' tabs, and various icons for step selection and management. To the right, a large grid-based diagram visualizes the playbook's logic flow, with nodes representing steps like 'Initial Severity Block' and 'Case Management W...'. A purple button labeled 'Edit with Gemini' is also visible.

# Playbook Editor



# Google SecOps

The screenshot shows the Google SecOps Playbooks interface. The left sidebar displays a navigation tree under 'Default' with sections for 'Imported Playbooks' and 'SOAR Workshop'. Under 'SOAR Workshop', two items are listed: 'Case Management W...' and 'Initial Severity Block'. The main workspace is titled 'Case Management W...' and is marked as 'View only'. It shows a timeline of steps starting with a yellow 'Initial Severity Block' step followed by several blue 'Analyze' steps. A complex branching logic diagram is visible on the right, with nodes labeled 'Initial Severity Block', 'Analyze', 'Assign', and 'Close Case'. A purple callout bubble suggests editing with Gemini. The top right features a 'Simulator' toggle, a temperature gauge, and a 'Save' button.

Google



# Playbook Tool Grouping

Conditions to start  
the execution of a  
Playbook

Conditions (if), and  
multiple choices  
questions



## Triggers

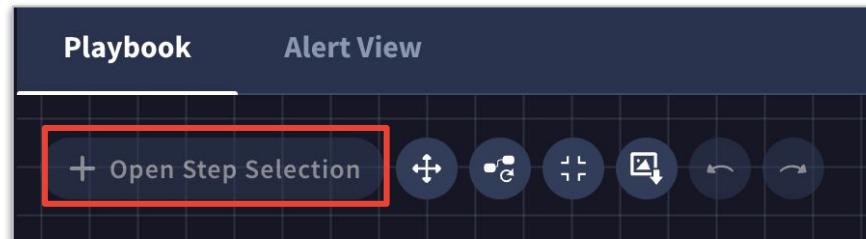
## Actions ?

## Flow

## Blocks

Enrichments, Data  
collection, Allow/Block  
and much more...  
(Installed from Marketplace,  
Configured in Response -  
Integrations Setup)

Sub-playbooks;  
actions and flow





# Triggers

Triggers Actions ? Flow Blocks

Search... Alert Trigger Value Alert Type All Custom List Custom Trigger Network Name Product Name Tag Name

## Custom trigger

This will trigger the playbook on each alert containing conditions based on data in the case.

### Parameters

[Alert.Name] [ ] Or [ ]

sw\_malware\_win\_lokiot\_c2 [ ]

Alert.Name Equal sw\_malware\_win\_lokiot\_c2

+ = Equal  
() Contains  
!= Not Equal  
!() Not Contains  
\*\_ Starts With  
> Greater Than  
< Less Than  
[] Empty  
![ ] Not Empty

# Actions

Triggers Actions ? Flow Blocks

- EmailV2
- Flow
- GoogleChronicle
- Mandiant ^
- Enrich Entities
- Enrich IOCs
- Get Malware Details
- Get Related Entities
- Ping
- MitreAttck
- Siemplify

### Priority change

Automatically change case priority to the given input

Parameters Settings Sample Output

Choose Instance \* ⓘ Shared\_Siemplify\_1

Entities ⓘ All entities

Priority \* ⓘ

Critical

Informative

Low

Medium

High

Critical

### Mandiant - Get Malware Details

M Mandiant - Get Malware Details\_1

Get information about malware from Mandiant.

Parameters Settings Sample Output

Choose Instance \* ⓘ Shared\_Mandiant

Entities ⓘ All entities

Malware Names \* ⓘ [Mandiant\_Enrich Entities\_1.JsonResult| "EntityResult.attributed\_associations.name"]

Create Insight ⓘ

Fetch Related IOCs ⓘ

Max Related IOCs To Return ⓘ 100



Google SecOps

# Flow

Triggers Actions ⓘ Flow Blocks

Search...

- Condition
- MultiChoiceQuestion
- Previous Actions Conditions

Condition

**Id external domain suspicious ?**

This condition determines the progress of the playbook. Conditions are built based on cases data (cases, alerts, vents, entities and environment properties) as-well as data that comes back from previous playbook steps.

**Parameters** **Settings**

Entities \* (i)  
All entities

**Parameters** + Add Branch

1 Branch  
This branch was selected 5 out of 5 runs

Logical Operator And ▼

[Build context - Domain Details.is\_success] [ ] = True [ ]  
+  
E Branch "Else"

# Blocks

Chronicle | Playbooks

## Initial Severity Block

SOAR Workshop All Environments

Playbook

+ Open Step Selection

The screenshot shows the Chronicle Playbooks interface. At the top, there are tabs for Triggers, Actions, Flow, and Blocks, with 'Blocks' being the active tab. Below the tabs is a search bar. The main area is titled 'Initial Severity Block'. The playbooks editor shows a flow starting from an 'Inputs' step, leading to a 'Set by alert severity' condition step. This condition splits the flow into four parallel paths, each leading to a 'Set initial Priority' step and then an 'Output' step. The outputs are labeled Output\_1, Output\_2, Output\_3, and Output\_4.



### Condition

#### Set by alert severity

This condition determines the progress of the playbook. Conditions are built based on cases data (cases, alerts, vents, entities and environment properties) as-well as data that comes back from previous playbook steps.

Parameters Settings

Entities \* All entities

Parameters + Add Branch

1 Critical [Event.detection\_1\_severity] 0 CRITICAL

Logical Operator Or

2 High [Event.detection\_1\_severity] 0 HIGH

Logical Operator Or

3 Medium [Event.detection\_1\_severity] 0 MEDIUM

Logical Operator Or

Cancel Save

Google SecOps

The screenshot shows the 'Condition' configuration dialog for the 'Set by alert severity' step. It includes sections for 'Parameters' and 'Settings', and lists three conditions: 'Critical', 'High', and 'Medium'. Each condition is defined by a logical operator ('Or') and a specific event detection severity value (0). The 'Save' button is at the bottom right.

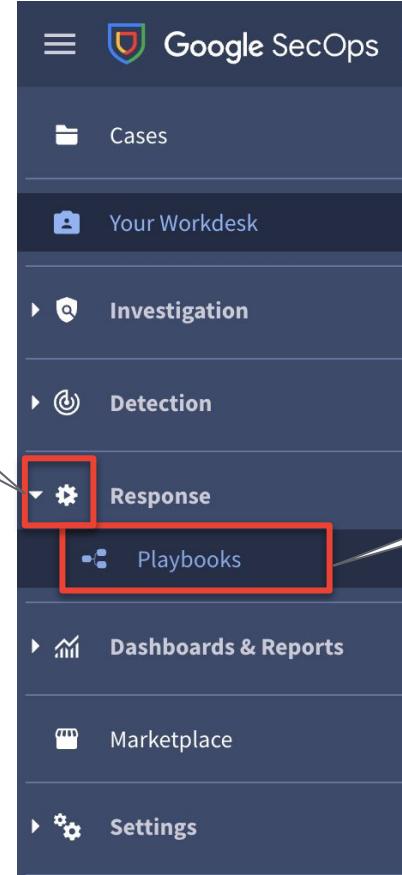


Google SecOps

# Playbook Walk Through



# Navigating to Playbooks





# Selecting Our Playbook

The diagram illustrates a two-step process for selecting a playbook:

- Step 1:** Click on the "SOAR Workshop" item in the "Imported Playbooks" section. A callout bubble labeled "Click" points to the item, which is highlighted with a red border.
- Step 2:** Click on the "Case Management Workshop - Malware Found" playbook. A callout bubble labeled "Click" points to the playbook, which is highlighted with a red border. The playbook details are visible: Created by: Secops Joonix, Last modified: 2023-12-08 14:40:22.

**Left Screenshot (Step 1):**

- Show All
- Search...
- Default
- Imported Playbooks
- SOAR Workshop** (highlighted with a red border)
- Case Management Work... (Workshop 10)
- Case Management Work... (Workshop 10)
- Initial Severity Block (All Environments)
- Playbook Workshop - Pr... (All Environments)

**Right Screenshot (Step 2):**

- Show All
- Search...
- Default
- Case Management Workshop - Malware Found (highlighted with a red border)
  - Created by: Secops Joonix
  - Last modified: 2023-12-08 14:40:22
- Case Management Work... (Workshop 10) (highlighted with a red border)
- Case Management Work... (Workshop 10)
- Initial Severity Block (All Environments)
- Playbook Workshop - Pr... (All Environments)



# Playbook Familiarization

This playbook is used in the Case Management Workshop and is triggered by an alert from the rule sw\_malware\_win\_lokibot\_c2

Case Management W... View only SOAR Workshop Workshop 10 2023-11-29 07:42:40 26 Simulator Save ?

Playbook Alert View

Double Click

The screenshot shows a 'Case Management' interface with a 'Playbook' tab selected. A speech bubble points to a specific step in the workflow with the text 'Double Click'. A red box highlights the first step in the sequence. The workflow consists of several steps connected by arrows, including 'Initial Alert', 'Malware Analysis', 'Containment', 'Remediation', and 'Post-Incident Review'. Some steps are purple, indicating they are part of a conditional branch or a different phase of the process.



# Playbook Review - Trigger

 Custom trigger X

This will trigger the playbook on each alert containing conditions based on data in the case.

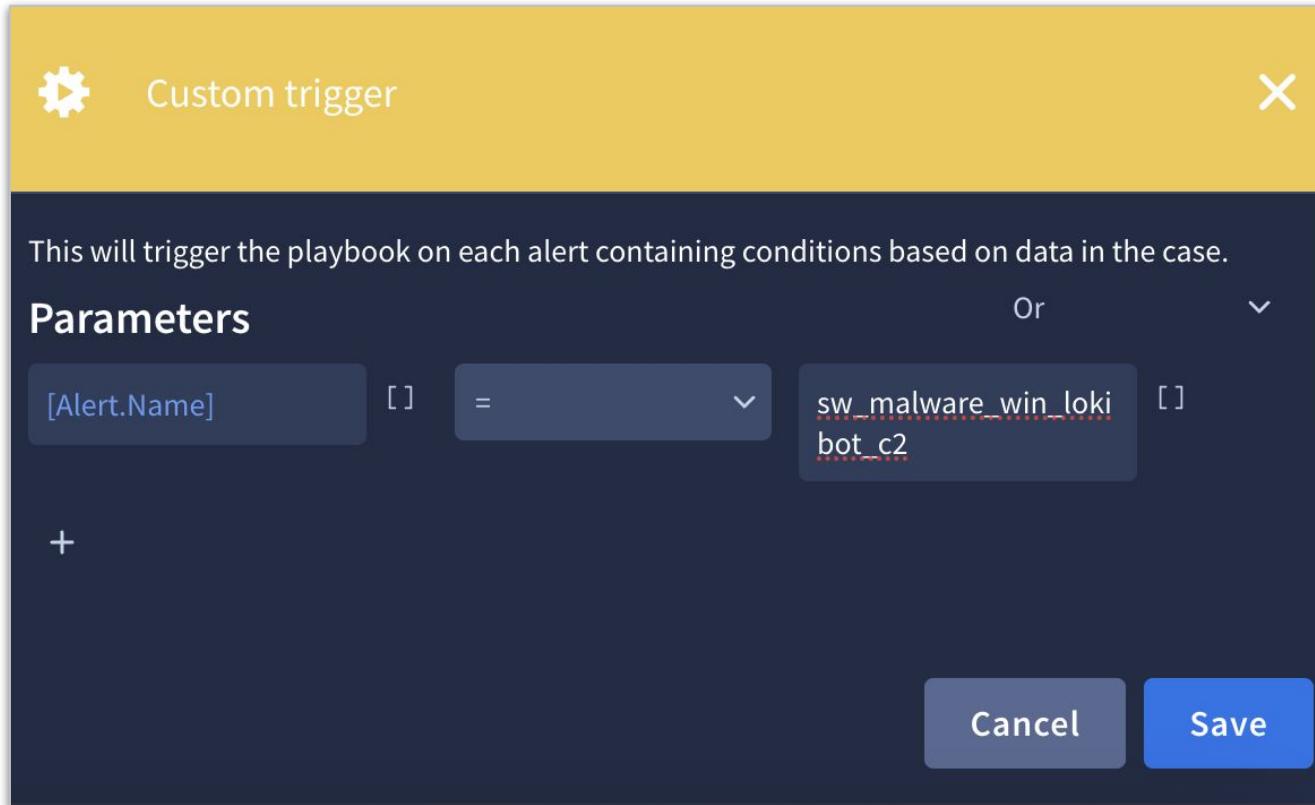
**Parameters**

[Alert.Name] [ ] = Or [ ]

[sw\_malware\_win\_loki]  
bot\_c2

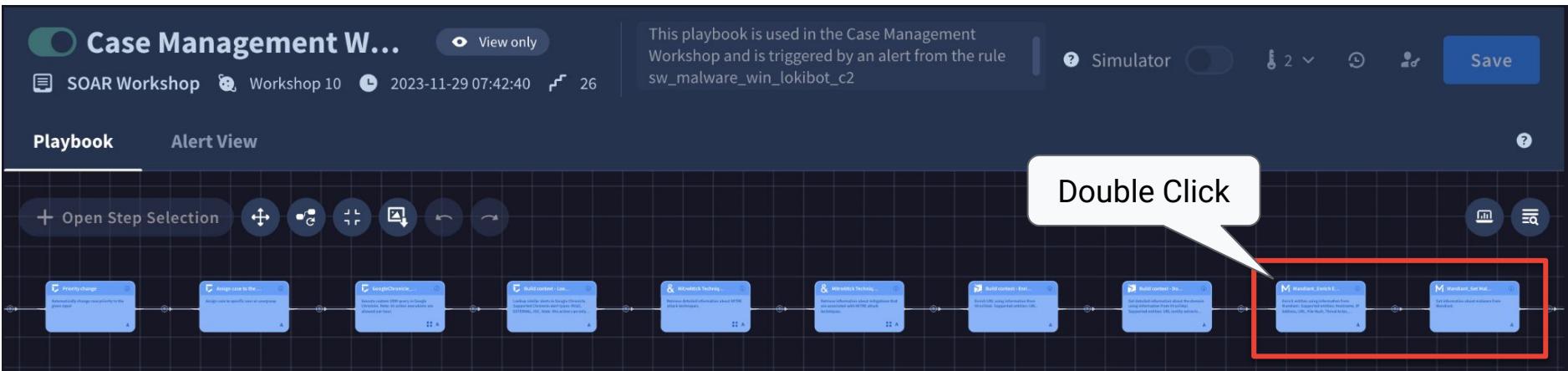
+

Cancel Save





# Playbook Action Blocks



Change Priority

Assign Case

Execute UDM Search

Look for Similar Alerts

MITRE ATT&CK Technique Details

MITRE ATT&CK Technique Mitigations

VirusTotal Enrich URL

VirusTotal Get Domain Details

Mandiant Threat Intelligence Enrich Entities

Mandiant Threat Intelligence Get Malware Details



Google SecOps

# Action Details

M MandiantThreatIntelligence - Enrich Entities X

## MandiantThreatIntelligence\_Enrich Entities\_1

Enrich entities using information from Mandiant. Supported entities: Hostname, IP Address, URL, Domain, File Hash, Threat Actor, Vulnerability. Note: only MD5, SHA-1 and SHA-256 are supported.

**Parameters** **Settings** **Sample Output**

Choose Instance \* ⓘ Shared\_MandiantThreatIntelligence

Entities ⓘ Destination entities

Severity Score Threshold \* ⓘ 15

Create Insight ⓘ

Only Suspicious Entity In... ⓘ

Parameters Settings **Sample Output**

Action Result ⓘ

is\_success

JSON Result (Example) ⓘ

```
Search... < >
```

```
> 0 : Object {2}
> 1 : Object {2}
< 2 :
  Entity : "173.254.xx.xx"
  < EntityResult :
    first_seen : "2022-03-22T21:46:43.000Z"
    last_seen : "2022-05-22T00:58:48.000Z"
    > sources : Array [1]
    mscore : 100
    < attributed_associations :
      < 0 :
        id : "malware--f1151a22-9d9c-589d-90ad-xxxxxx"
        name : "EMOTET"
        type : "malware"
      > misp : Object {74}
        id : "ipv4--da5b1f26-cf25-5a61-9c93-xxxx"
        type : "ipv4"
        value : "173.254.xx.xx"
        is_publishable : true
        last_updated : "2022-05-22T01:04:46.098Z"
        report_link : "https://advantage.mandiant.com/indicator/ipv4/ipv4--da5b1f26-xxxx-5a61-"
```

Google



# Action Details

M MandiantThreatIntelligence - Get Malware Details X

## MandiantThreatIntelligence\_Get Malware Details\_1

Get information about malware from Mandiant.

**Parameters**    **Settings**    **Sample Output**

Choose Instance \* i Shared\_MandiantThreatIntelligence

Entities i All entities

Malware Names \* i [Mandiant\_Enrich Entities\_1.JsonResult]  
"EntityResult.attributed\_associations.name"]

Create Insight i

Fetch Related IOCs i

Max Related IOCs To Return i 100



# Action Details

Insert Placeholder

Search...

Event

Dynamic Environment Parameters

Approval Links

Playbook

Click

Mandiant\_Enrich Entities\_1.is\_success

Mandiant\_Enrich Entities\_1.JsonResult

Build context - Domain Details.is\_success

Build context - Domain Details.JsonResult

Insert Placeholder

Json Sample  
The sample below is for example purposes, actual data may vary.

Entity 173.254.xx.xx

EntityResult {12}

attributed\_associations [1]

0 {3}

id malware-f1151a22-9d9c-589d-91

name EMOTET

type malware

first\_seen 2022-03-22T21:46:43.000Z

Add Functions

- first
- last
- min
- max
- filter
- dateFormat
- count
- orderBy
- toLower
- toUpper
- replace
- distinct

Expression

```
| "EntityResult.attributed_associations.name"
```

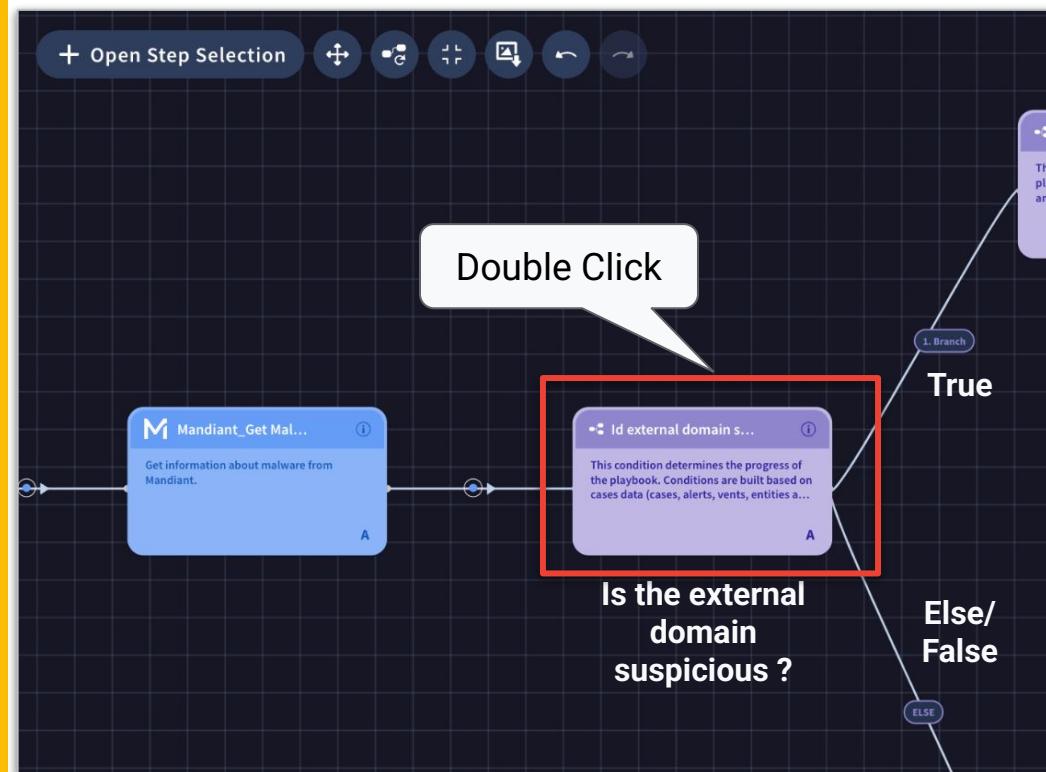
Run

Results

EMOTET

Cancel Insert

# Flow - Condition



**Condition**

**Id external domain suspicious ?**

This condition determines the progress of the playbook. Conditions are built based on cases data (cases, alerts, vents, entities and environment properties) as-well as data that comes back from previous playbook steps.

**Parameters** **Settings**

Entities \* **All entities**

**Parameters** **+ Add Branch**

**Branch**  
This branch was selected **5** out of **5** runs

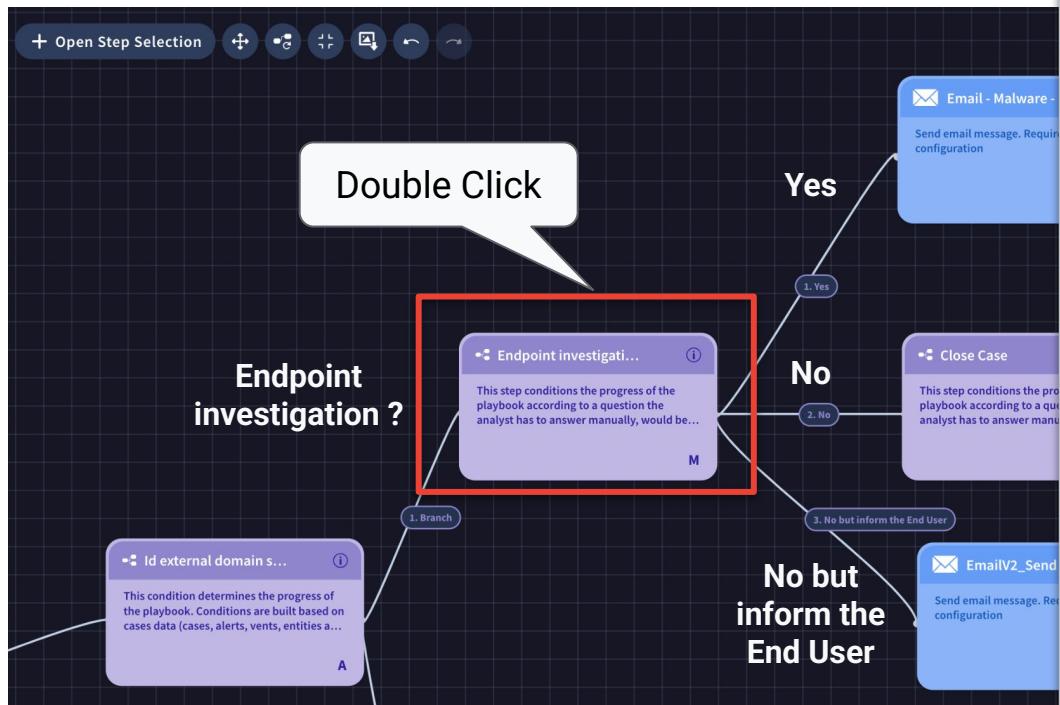
Logical Operator **And**

[Build context - Domain Details.is\_success] = True

**Branch "Else"**



# Flow - Multi-Choice Question



## Multi-Choice Question

**Endpoint investigation ?**

This step conditions the progress of the playbook according to a question the analyst has to answer manually, would be used most for questions which can't be answered automatically

**Parameters** **Settings**

### Question

The external entities (domain and URL) are suspicious. Do you want to request a full investigation of the endpoint ?

### Answers

+ Add answer

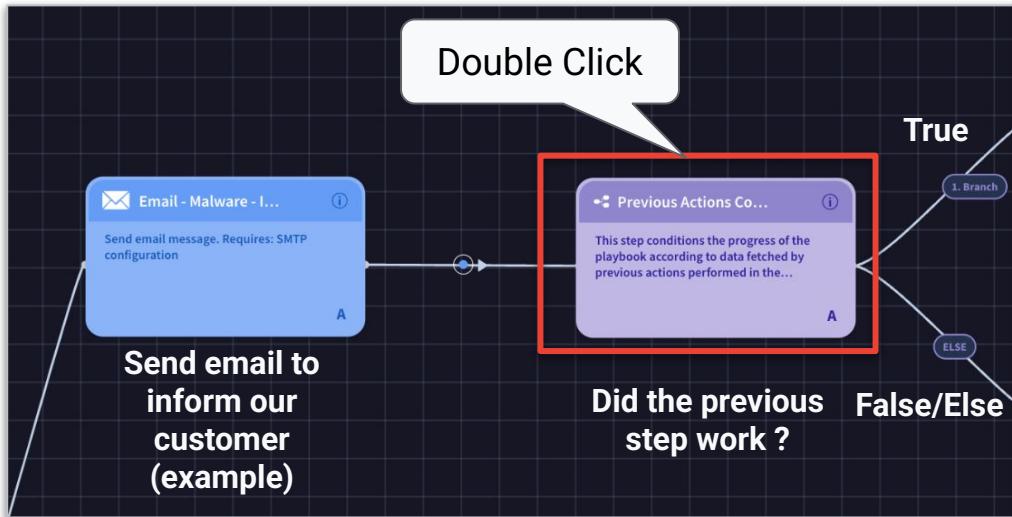
- ① Yes
- ② No
- ③ No but inform the End User



# Playbook - Answered No



# Playbook - Answered Yes



**Condition**

## Previous Actions Conditions\_1

This step conditions the progress of the playbook according to data fetched by previous actions performed in the playbook, for example: report data, action's success or enrichment data

**Parameters**

Entities \* All entities

**Parameters**

1 Branch

Email - Malware - Investigate.is\_success Logical Operator And

Email - Malware - Investi... = true

E Branch "Else"



Google SecOps

# Alert Views

# Alert View



Admins can define default Alert (and Case) Views that include a standard set of widgets in Settings - Case Data - Views

Chronicle | SOAR Settings - Views

Save View

### Settings

- > Organization
- < Case Data
  - Tags
  - Case stages
  - Case close root cause
  - Case name
- < Views
  - Views
  - > Advanced
  - > Data Configuration
  - > Ontology
  - > Environments
  - > Incident Manager
  - > Ingestion

General Predefined

- Entities Highlights
- Events Table
- HTML
- Free Text
- Key Value
- Entities Graph
- Insights
- Pending Actions

### Default Alert View ⓘ

Created at 2023-10-06 20:37:38 PM

Alert Details

No Description

Pending Actions ⓘ

This Widget lists all playbook actions waiting for user input

Events ⓘ

This widget displays all Alert events and their properties

Insights ⓘ

This widget contains all the Insights from the Playbook insights actions, general insights and any other insights you have added. They will be presented in HTML format

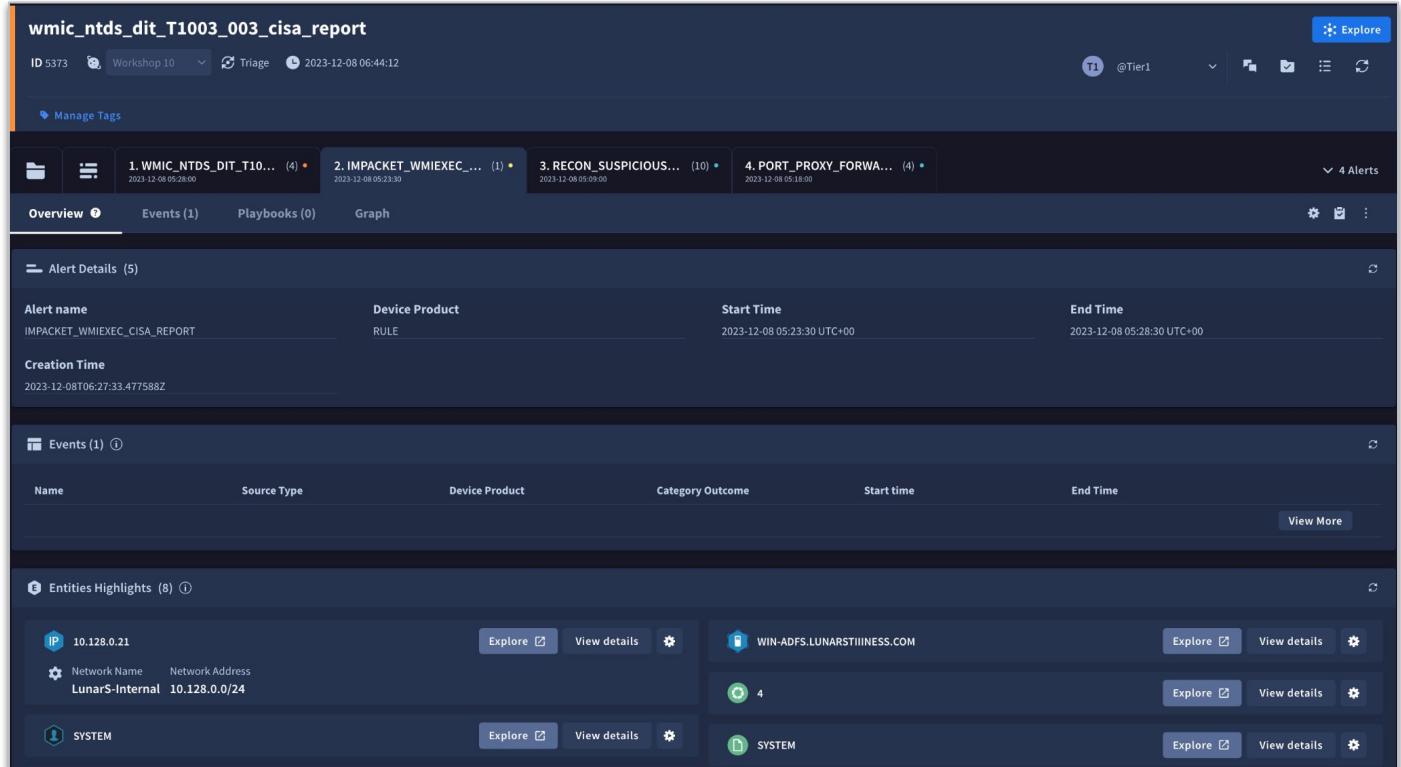
Entities Highlights ⓘ

This widget displays the highlighted fields for each entity

# Default Alert View

If the widget has values, they will display, otherwise they will not

Pending Actions and Insights do not have data, therefore they are not displayed



The screenshot shows the Google SecOps alert view for an alert named "wmic\_ntds\_dit\_T1003\_003\_cisa\_report".

**Alert Details:**

- Alert name:** IMPACKET\_WMIEXEC\_CISA\_REPORT
- Device Product:** RULE
- Start Time:** 2023-12-08 05:23:30 UTC+00
- End Time:** 2023-12-08 05:28:30 UTC+00
- Creation Time:** 2023-12-08T06:27:33.47758Z

**Events (1):**

Name	Source Type	Device Product	Category Outcome	Start time	End Time

**Entities Highlights (8):**

- IP 10.128.0.21: Network Name - LunarS-Internal, Network Address - 10.128.0.0/24. Actions: Explore, View details, Settings.
- WIN-ADFS.LUNARSTIIINESS.COM: Actions: Explore, View details, Settings.
- 4: Actions: Explore, View details, Settings.
- SYSTEM: Actions: Explore, View details, Settings.



Google SecOps

# Playbook Alert View

Case Management W... View only

SOAR Workshop Workshop 10 2023-11-29 07:42:40 26

This playbook is used in the Case Management Workshop and is triggered by an alert from the rule sw\_malware\_win\_lokibot\_c2

Simulator 2 Save

Playbook **Alert View**

General Predefined

This widget is already in the view

MitreAttck Technique Mitigations

Build context - Enrich URL

GoogleChronicle\_Execute UDM

Mandiant\_Enrich Entities\_1

MitreAttck Technique Details

Mandiant\_Get Malware Details\_1

Build context - Lookup for Similar Alerts

Build context - Domain Details

Events Table

This widget displays all Alert events and their properties.

Alert View A T T +3 Created at 2023-11-08 15:48:50 PM

Events Table

Insights

Similar Alerts

Similar Alerts over the Past Week

GoogleChronicle\_Execute UDM QL

This widget highlights the most important items in Execute UDM Query - Google Chronicle.

MitreAttck Technique Details

This widget highlights the most important items in MitreAttck - Get Techniques Details

MitreAttck\_Get Techniques Mitiga

This widget highlights the most important items in MitreAttck - Get Techniques Mitigations

Google



Google SecOps

# Alert with Playbook Specific Widgets

**sw\_malware\_win\_lokibot\_c2**

ID 5315 Workshop 10 Triage 2023-12-08 06:24:21

Manage Tags

**Similar Alerts** 9 SIMILAR ALERTS FOUND

9 alerts reviewed - run time 0.52 sec

Pivot Entity	Alert Name	Product	Target	First Seen	Last Seen
--------------	------------	---------	--------	------------	-----------

**MitreAttck Technique Details** T1071.001

**Web Protocols** ID T1071.001 MITRE

Tactics: Command And Control  
Domains: Enterprise attack  
Platforms: Linux, macOS, Windows  
Data Sources: Network Traffic: Network Traffic Content, Network Traffic...  
Creation Time: 2020-03-15T16:13:46.151Z  
Modification Time: 2023-09-29T20:22:37.414Z

Description

**GoogleChronicle\_Execute UDM Query\_1** 1 EVENT FOUND

EVENT TYPE	TIMESTAMP	PRODUCT	PRINCIPAL	TARGET
NETWORK_HTTP	2023-12-08T05:48:40Z	NSS	{ "hostname": "win-adfs.lunarstiiness.com", "assetId": "WIN-ADFS\$", "user": { "username": "alpha" } }	{ "hostname": "alphas", "ip": [ "185.189.112.157" ] }

**MitreAttck\_Get Techniques Mitigations\_1** T1071.001 T1071.001 & 1 MITIGATION

EXTERNAL ID	MITIGATION	DESCRIPTION
M1031	Network Intrusion Prevention	Use intrusion detection signatures to block traffic at network boundaries.

Google



**Case Management W...**

**View only**

This playbook is used in the Case Management Workshop

SOAR Workshop Workshop 10 2023-11-29 07:42:40 26

Simulator

Save

Playbook **Alert View**

+ Open Step Selection

Click



Google SecOps

General      Predefined

JSON Result

Entities Highlights

Events Table

HTML

Free Text

Key Value

Entities Graph

Insights

Pending Actions

**Click**

General      Predefined

Search... MitreAttck Technique Mitigations ⓘ

Build context - Enrich URL ⓘ

GoogleChronicle\_Execute UDM ... ⓘ

M Mandiant\_Enrich Entities\_1 ⓘ **Click**

Mandiant\_Get Malware Details\_1 ⓘ

Build context - Lookup for Simila... ⓘ

Build context - Domain Details ⓘ

& MitreAttck Techniq... ⓘ

Retrieve detailed information about MITRE attack techniques.

Includes predefined widget

**A**

M Mandiant

M Enrich Entities

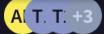
M Enrich IOCs

M Get Malware Details

M Get Related Entities

Google

# Alert View



Created at 2023-11-08 15:48:50 PM



Google SecOps

## Events Table

This widget displays all Alert events and their properties.

## Insights

This widget contains all the Insights from the Playbook Insights actions, general Insights added. They will be presented in HTML format

## Similar Alerts

Similar Alerts over the Past Week

## GoogleC

This widget highlights Execute UDM Query - Google Chronicle.

## Insights

**Widget Title \***

Insights

**Widget Description**

This widget contains all the Insights from the Playbook Insights actions, general Insights and any other Insights you have added. They will be presented in HTML format

**Widget Width**

100%

## MitreAtt

Predefined



This widget highlights the most important items in MitreAttck - Get Techniques Details

## MitreAtt

Predefined



This widget highlights the most important items in MitreAttck - Get Techniques Mitigations

Google



# Exercise: Explore the Alert View Configuration

What fields are used to populate the Alert Details widget?

Can the Pending Actions widget be set to display even if there are no actions?

What fields are displayed in the Events Table widget?

How many predefined widgets are being used in our Alert View?

How many widgets have html exposed in them?

# Exercise: Explore the Alert View Configuration

What fields are used to populate the Alert Details widget?

Can the Pending Actions widget be set to display even if there are no actions?

What fields are displayed in the Events Table widget?

How many predefined widgets are being used in our Alert View? 3

How many widgets have html exposed in them? 4

Keys	Value
Alert name	[Alert.Name]
Product	[Alert.Product]
Start Time	[Alert.StartTime]
End Time	[Alert.EndTime]

Display widget when empty  

Event Field  
You can only add up to 6 fields

Column Name	Value
metadata.event_type	[Event.event_type]
metadata.vendor_n...	[Event.event_metadata_vendorName]
ingested_timestamp	[Event.event_metadata_ingestedTimestamp]
principal.ip	[Event.event_principal_ip]
principal.userid	[Event.event_principal_user_userid]



Google SecOps

# Playbook Simulator



# Playbook Simulator

Provides a way to test playbooks and their associated actions without impacting existing alerts and cases

Requires an alert to be ingested as a test case

Does not change the existing cases or alerts

Simulator processes the steps and provides results for review

The screenshot shows the Playbook Simulator interface with the following details:

- Choose Case:** A dropdown menu currently set to "5786# wmic\_ntds\_dit\_T1003\_003\_cisa\_report - 202...".
- Run Button:** A blue button labeled "Run" with a play icon.
- Entities:** A link to view entities.
- Test Cases:** Three entries listed:
  - MultiChoiceQuestion\_1** (status: yellow box labeled "Manual Action")  
Created: 2023-12-11 20:22:22
  - Siemplify\_Case Tag\_1** (status: green checkmark)  
Created: 2023-12-11 20:22:22  
Actions: View Results, i
  - Siemplify\_Assign Case\_1** (status: green checkmark)  
Created: 2023-12-11 20:22:22  
Actions: View Results, i



# Ingest Alert as Test Case

Chronicle | Cases

4 Cases

Case Name

- W1 Suspicious Microsoft Office Download - win-server.lunarstiiness.com
- W1 wmic\_ntds\_dit\_T1003\_003\_cisa\_report
- W1 recon\_suspicious\_commands\_cisa\_report
- W1 sw\_malware\_win\_lokibot\_c2

Case Queue Filter

Parameters

Time Frame Choose

Logical Operator AND

Alerts names IS

+ Add Criteria

WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT

RECON\_ENVIRONMENT\_ENUMERATION\_SYSTEM\_CISA\_REPORT

RECON\_SUSPICIOUS\_COMMANDS\_CISA\_REPORT

SW\_MALWARE\_WIN\_LOKIBOT\_C2

SW\_SUSPICIOUS\_DOWNLOAD\_OFFICE

WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT

Reset

Click Apply

Select Alert names

Select wmic\_ntds\_dit....

WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT



# Ingest Alert as Test Case

The screenshot shows the Google SecOps interface for managing alerts. On the left, a sidebar displays '1 Cases' and a search bar for 'Case Name'. The main area shows an alert titled 'wmic\_ntds\_dit\_T1003\_003\_cisa\_report' with ID 5892, created on 2023-12-12 at 06:45:30, and assigned to 'Workshop 10' and 'T1 @Tier1'. Below the title, there are four event items: 1. WMIC\_NTDS\_DIT\_T10... (4), 2. IMPACKET\_WMIEXEC\_..., 3. RECON\_SUSPICIOUS..., and 4. PORT\_PROXY\_FOR... (4 Alerts). The first event is highlighted with a red box. A context menu is open on the right side of the screen, with the 'Ingest alert as test case' option highlighted by a red box and a callout bubble labeled 'Click'.

Alert name: WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT

Device Product: RULE

Start Time: 2023-12-12 05:28:00 UTC+00

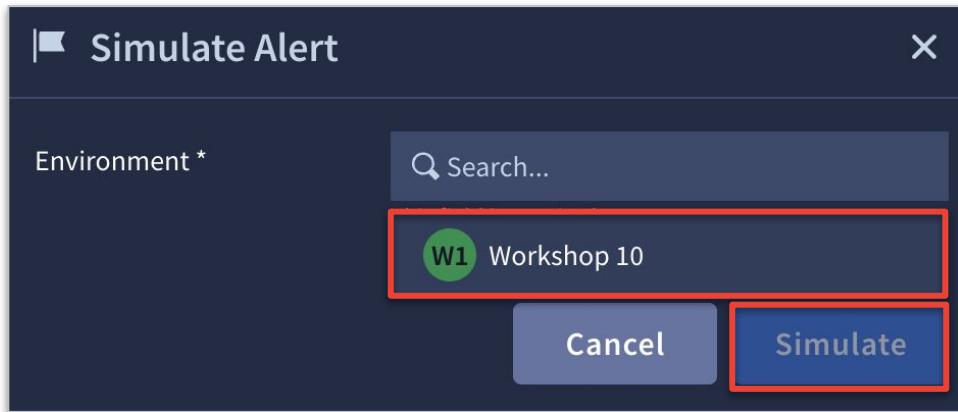
End Time: 2023-12-12 05:33:00 UTC+00

Creation Time: 2023-12-12T06:30:00.412787Z

Events (4)

- Move Alert
- Change Priority
- Add Entity
- View Other Alerts From The Rule
- Manage Alert Detection Rule
- Close Alert

# Ingest Alert as Test Case



The screenshot shows the "Google SecOps" interface. At the top, it displays "5 Cases" and various navigation icons. A search bar is present with the placeholder "Search Case Name". Below the search bar is a list of five test cases, each represented by a card:

- W1 wmic\_ntds\_dit\_T1003\_003\_cis... (1 T1)
- W1 Suspicious Microsoft Office ... (3 SU)
- W1 wmic\_ntds\_dit\_T1003\_003\_cis... (4 T1)
- W1 recon\_suspicious\_commands\_... (2 T1)
- W1 sw\_malware\_win\_lokibo... (1 SU)

The first test case in the list is also highlighted with a red rectangular box.



Google SecOps

wmic\_ntds\_dit\_t100...

Playbook Workshop Exercise

Simulator

+ Add View

⚠️ Playbook

+ Close Step Selection

Drag a trigger over here

Drag a step over here

Choose Case 5786# wmic\_ntds\_dit\_T1003\_003\_cisa\_report - 202... ▶ Run Entities

Google



# Running a Playbook Simulation

Playbook

+ Add View ?

+ Close Step Selection

Simulator is on

Custom Trigger [Alert.Name] Equal wmic\_ntds\_dit\_t1003\_003\_cisa\_report

Playbook Workshop ... This block is for the playbook workshop to prep the alert and case with a standard set of information before additional...

Choose Case 5786# wmic\_ntds\_dit\_T1003\_003\_cisa\_report - 202... ▶ Run

Entities

Output\_1 2023-12-11 20:00:38 View Results

MitreAttack\_Get Techniques Mitigations\_1 2023-12-11 20:00:38 View Results

MitreAttack\_Get Techniques Details\_1 2023-12-11 20:00:38 View Results

Drag a step over here

```
graph LR; CT[Custom Trigger] --> PW[Playbook Workshop ...]; subgraph Entities [ ]; OR1[Output_1 2023-12-11 20:00:38]; OR2[MitreAttack_Get Techniques Mitigations_1 2023-12-11 20:00:38]; OR3[MitreAttack_Get Techniques Details_1 2023-12-11 20:00:38]; end;
```

# View Results



Google SecOps

**Siemplify\_Update Case Description\_1**  
2023-12-11 20:00:47

**Results**      **Technical Details**

**Scope**  
All entities

**Parameters**

NAME	VALUE
Description	This case contains a critical alert around Windows Directory Services being accessed on system win-adfs.lunarstiiness.com

**Return Values**

**Script Result**

is_success	true
------------	------

**JSON Result**  
No JSON result

**& MitreAttck\_Get Techniques Details\_1**  
2023-12-11 20:00:49

MitreAttck\_Get Techniques Details  
Shared\_MitreAttck

**Results**      **Technical Details**

**Scope**  
All entities

**Parameters**

NAME	VALUE
Technique Identifier	T1003.003
Identifier Type	External ID

**Return Values**

**Script Result**

is_success	true
------------	------

**JSON Result**

```
0 [2]
Entity T1003.003
EntityResult [22]
created 2020-02-11T18:42:35.572Z
created_by_ref identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
description Adversaries may attempt to access or create a copy of the Active Directory domain database in order
```

Google



# Case Data

**Case Data**

This case contains a critical alert around Windows Directory Services being accessed on system win-adfs.lunarstiiness.com

Action & MitreAttck\_Get Techniques Details

Time 2023-12-11 20:00:38

Case Alert Events Entity Details

Search...

Field Name	Value
Case Name	wmic_ntds_dit_T1003_003_cisa_report
Case ID	5787
Case Description	This case contains a critical alert around Windows Directory Services being accessed on system win-adfs.lunarstiiness.com
Priority	CRITICAL
Assignee	@Tier1
Environment	Workshop 10
Is Incident	false
Is Important	true
Tags	Simulated Case
Case Modification Time	2023-12-11 20:00:48
Case Creation Time	2023-12-11 20:00:38

Shows the case data of the simulation case at the point where this step finished

**View Results** 

Google

# Manual Action

Choose Case 5786# wmic\_ntds\_dit\_T1003\_003\_cisa\_report - 202... ▾ Run

Entities

 MultiChoiceQuestion_1 2023-12-11 20:22:22	<span>Manual Action</span>
 Siemplify_Case Tag_1 2023-12-11 20:22:22	<span>View Results</span> <span>i</span>
 Siemplify_Assign Case_1 2023-12-11 20:22:22	<span>View Results</span> <span>i</span>

Manual Action X

Instance Action Parameters

Do you want to check VirusTotal for IOCs from the alert?

Yes

No

Cancel Execute

# Pin Results

Choose Case 5786# wmic\_ntds\_dit\_T1003\_003\_cisa\_report - 202... ▶ Run Entities

 Instruction_1 2023-12-11 20:40:58	<a href="#">View Results</a> 
 VirusTotalV3_Get Related URLs_1 2023-12-11 20:40:58	<a href="#">Pin Results</a> <a href="#">View Results</a> 
 GoogleChronicle_List Assets_1 2023-12-11 20:40:58	<a href="#">Pin Results</a> <span style="border: 2px solid red; padding: 2px;">Pin Results</span> <a href="#">View Results</a> 

Choose Case 5916# wmic\_ntds\_dit\_T1003\_003\_cisa\_report - 202... ▶ Run Entities

Instruction\_1  
Step ran in simulate mode and returned simulation data

 GoogleChronicle_List Assets_1 2023-12-12 15:36:58	<a href="#">View Results</a> 
 Siemplify_Case Comment_1 2023-12-12 15:36:58	<a href="#">View Results</a> 



# Simulate - Action Step

GoogleChronicle - Execute UDM Query X

**GoogleChronicle\_Execute UDM Query\_1** Simulate Toggle

Execute custom UDM query in Google Chronicle. Note: 120 action executions are allowed per hour.

Action Results Enrichment

**Script Results**

Key	Value
is_success *	true

**JSON Result** Load sample Edit

```
1 [ {  
2   "events": [  
3     {  
4       "name": "00000007955f792b88143d25467ec84b31cab500000000500000"  
5       "udm": {  
6         "metadata": {  
7           "productLogId": "efhlu4ftgtvh9",  
8           "eventTimestamp": "2023-12-11T04:59:44.761072660Z",  
9           "collectedTimestamp": "2023-12-11T04:59:51.182789425Z",  
10          "eventType": "NETWORK_CONNECTION",  
11          "rendezvous": "Google Cloud Platform"  
12        }  
13      }  
14    ]  
15  }  
16 ]
```

GoogleChronicle - Execute UDM Query X

**GoogleChronicle\_Execute UDM Query\_1** Simulate Toggle

Execute custom UDM query in Google Chronicle. Note: 120 action executions are allowed per hour.

Action Results Enrichment

**Script Results**

Key	Value
is_success *	true

**JSON Result** Load sample Edit

```
1 [ {  
2   "events": [  
3     {  
4       "name": "00000007955f792b88143d25467ec84b31cab500000000500000"  
5       "udm": {  
6         "metadata": {  
7           "productLogId": "efhlu4ftgtvh9",  
8           "eventTimestamp": "2023-12-11T04:59:44.761072660Z",  
9           "collectedTimestamp": "2023-12-11T04:59:51.182789425Z",  
10          "eventType": "NETWORK_CONNECTION",  
11          "rendezvous": "Google Cloud Platform"  
12        }  
13      }  
14    ]  
15  }  
16 ]
```



Google SecOps

# Building Your Own Playbook



# Brainstorming Playbooks

Whiteboard and Notes are good options

- Color-coding actions versus decision points can also be helpful

Tabletop exercises responding to a specific alert is another method to identify workflow and potential gaps



# Exercise - Building a Playbook

Use the wmic\_ntds\_dit\_t1003\_003\_cisa\_report alert as the trigger for a playbook

Ingest this alert as a test case

- We stepped through this earlier

The playbook will gather information from VirusTotal and automate a set of analyst actions

- In production, additional mitigation steps to the active directory server may be in order as well but that is beyond the scope of our playbook building today

Once we have built and tested our playbook using Simulator mode, create an alert view to accompany this playbook

If you want to enhance the playbook further, go ahead!

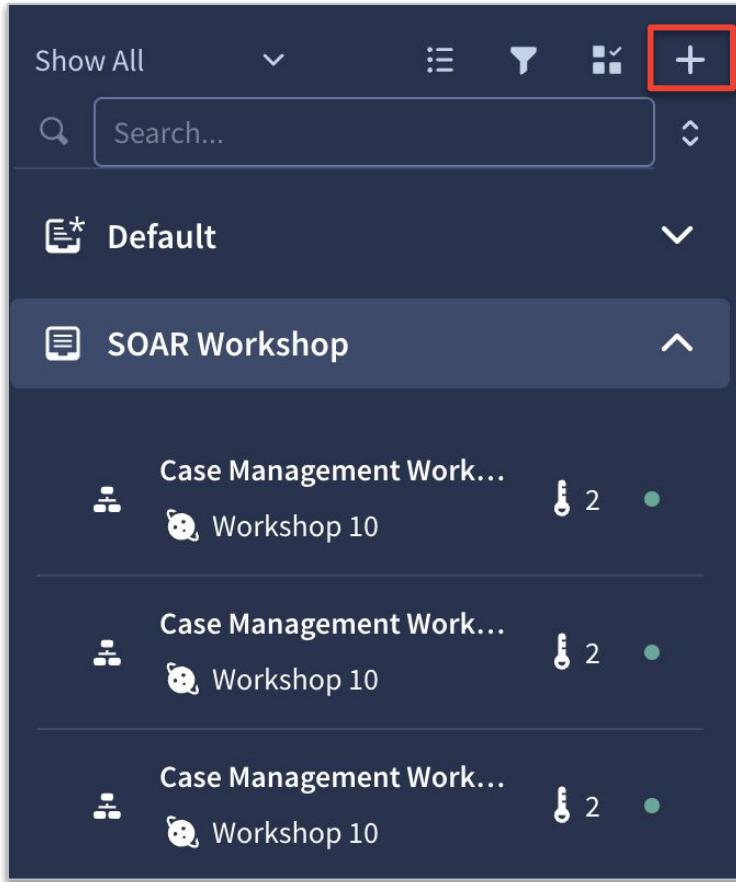
The exercise guide provides detailed steps to be built into our playbook



Google SecOps

# Playbook Exercise Review

# Creating Our Playbook



The screenshot shows the SOAR platform's playbooks list. At the top, there are filters (Show All, Search bar, and three icons), a plus sign icon (highlighted with a red box), and a dropdown menu set to 'Default'. Below this, a folder named 'SOAR Workshop' is expanded. Inside the folder, there are three items, each representing a playbook:

- Case Management Work... (Workshop 10, 2 runs)
- Case Management Work... (Workshop 10, 2 runs)
- Case Management Work... (Workshop 10, 2 runs)

Create New

Type  Playbook  Block

Choose Folder \* SOAR Workshop

Environment \* Workshop 10

**Create**

wmic\_ntds\_dit\_t100...

Playbook Workshop Exercise

Simulator

Save

Playbook

+ Close Step Selection

Simulator is on

Drag a trigger over here

Drag a step over here

Choose Case

5786# wmic\_ntds\_dit\_T1003\_003\_cisa\_report - 202...

Run

Entities

This screenshot shows the SOAR Playbook Workshop Exercise interface. At the top left, there's a red box around the session identifier 'wmic\_ntds\_dit\_t100...'. To its right is another red box around the 'Playbook Workshop Exercise' title and a 'Simulator' toggle switch, which is turned on. Below the title, there are several small icons and a 'Save' button. In the center, under the heading 'Playbook', there's a green banner with the text 'Simulator is on'. The main workspace features two large dashed boxes: one on the left labeled 'Drag a trigger over here' and one on the right labeled 'Drag a step over here', connected by a horizontal arrow. At the bottom, there's a red box around the 'Choose Case' dropdown menu, the 'Run' button, and the 'Entities' tab.



Google SecOps

Google



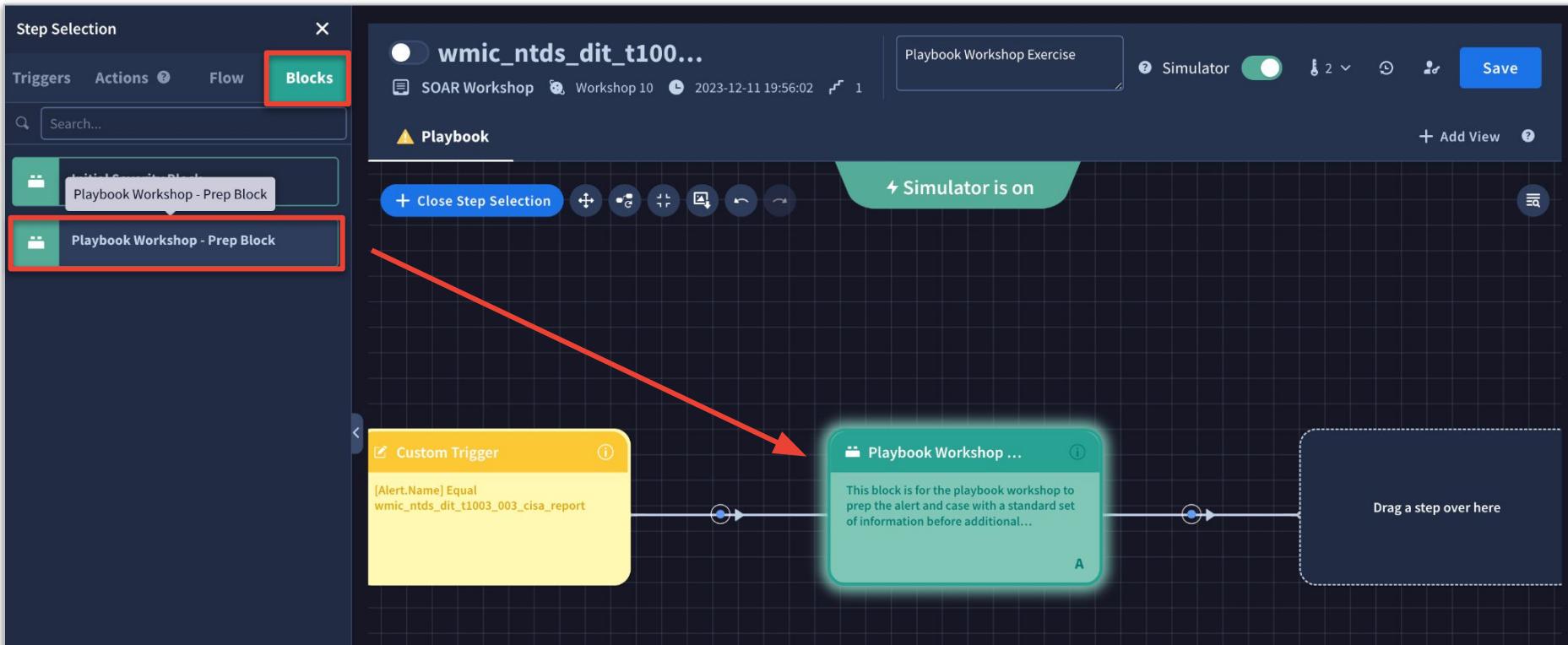
# Trigger

The screenshot shows the Chronicle Step Selection interface. On the left, there is a sidebar with various filter options: Step Selection, Triggers (highlighted with a red box), Actions, Flow, and Blocks. Below these are several dropdown menus: Alert Trigger Value, Alert Type, All, Custom List, Custom Trigger (highlighted with a red box), Network Name, Product Name, and Tag Name. A red arrow points from the 'Custom Trigger' option in the sidebar to a 'Custom Trigger' node in the main canvas area.

In the center, there is a 'wmic\_ntds\_dit\_t100...' step, which is a Playbook. Below it, there is a 'Custom Trigger' node with the text 'No conditions set'. To the right of the 'wmic\_ntds\_dit\_t100...' step, a 'Custom trigger' configuration dialog is open. It contains the text: 'This will trigger the playbook on each alert containing conditions based on data in the case.' Under the heading 'Parameters', there is a dropdown menu with the value '[Alert.Name] = wmic\_ntds\_dit\_t1003\_003\_cisa\_report'. This entire configuration dialog is also highlighted with a red box.



# Block





# Action - Assign Case

The screenshot shows the Chronicle Playbook editor interface. On the left, the 'Step Selection' sidebar is open, with the 'Actions' tab selected and a search bar containing 'case'. A red box highlights the 'Assign Case' step in the list. In the center, a grid of playbooks is shown, with one specific playbook titled 'wmic\_ntds\_dit\_t100...' highlighted. On the right, a detailed view of the 'Assign Case' step is displayed in a modal window titled 'Simplify - Assign Case'.

**Simplify - Assign Case**

**Simplify\_Assign Case\_1**

Assign case to specific user or usergroup

**Parameters**   **Settings**   **Sample Output**

Choose Instance \*  

Entities  

Assigned User \*  

The 'Assigned User' field is also highlighted with a red box. A red arrow points from the 'Assign Case' step in the Step Selection sidebar to the 'Assigned User' field in the detailed view.

# Action - Tag the Case

**Insert Placeholder**

**Json Sample**  
The sample below is for example purposes, actual data may vary.

```

{
  "0": [
    {
      "Entity": "course-of-action--4f170666-7edb-4489-8f",
      "EntityResult": [
        {
          "created": "2017-05-31T21:30:30.26Z",
          "created_by_ref": "identity--c78cb6e5-0c4b-46",
          "description": "Data is encrypted before being",
          "external_references": [
            {
              "0": [
                {
                  "external_id": "T1022",
                  "source_name": "mitre-attack",
                  "url": "https://attack.mitre.org/technic"
                }
              ]
            }
          ]
        }
      ]
    }
  ]
}
  
```

**Add Functions**

- first
- last
- min
- max
- filter
- dateFormat
- count
- orderBy
- toLower
- toUpper
- replace
- distinct

**Expression**

```
| "EntityResult.external_references.external_id"
```

**Results**

T1022

**Cancel** **Insert**

**Siemplify - Case Tag**

## Siemplify\_Case Tag\_1

Add given tag to the case the current alert is grouped to

Parameters	Settings	Sample Output
Choose Instance *	(i) Shared_Siemplify_1	
Entities	(i) All entities	
Tag *	(i) [Playbook Workshop - Prep Block_1.MitreAttck_Get Techniques Details_1.JsonResult] "EntityResult.external_references.external_id"]	



# Flow - Multi-Choice Question

The screenshot shows the Chronicle Playbook editor interface. On the left, a sidebar lists "Step Selection" categories: Triggers, Actions, Flow (which is highlighted with a red box), Blocks, Condition, MultiChoiceQuestion (also highlighted with a red box), and Previous Actions Conditions. The main workspace displays a flow diagram. A "wmic\_ntds\_dit\_t100..." step (SOAR Workshop, Workshop 10, 2023-12-12 17:09:01) is connected to a "Simplify\_Case Ta..." step (Add given tag to the case the current alert is grouped to). This leads to a "MultiChoiceQuestion" step (MultiChoiceQuestion\_1). A red arrow points from the "MultiChoiceQuestion" step in the editor to the "MultiChoiceQuestion" step in the flow diagram.

Chronicle | Playbooks

Step Selection

Triggers Actions ? Flow Blocks

Condition

MultiChoiceQuestion

Previous Actions Conditions

wmic\_ntds\_dit\_t100...

SOAR Workshop Workshop 10 2023-12-12 17:09:01

Playbook

+ Close Step Selection

MultiChoiceQuestion

MultiChoiceQuestion\_1

This step conditions the progress of the playbook according to a question the analyst has to answer manually, would be used most for questions which can't be answered automatically

Parameters Settings

Question

Do you want to check VirusTotal for IOCs from the alert?

Answers + Add answer

① Yes

② No



# Answer: Yes, VT Enrichment, Related IP/URLs

Chronicle | Playbooks

wmic\_ntds\_dit\_t100...

SOAR Workshop | Workshop 10 | 2023-12-12 17:09:01 | 7

Playbook Workshop Exercise

Playbook

+ Close Step Selection

Simulator is on

MultiChoiceQuestion...  
This step conditions the progress of the playbook according to a question the analyst has to answer manually, would be...

1...Yes

2...No

Drag a step over here

VirusTotalV3 - Enrich Hash

X

**VirusTotalV3\_Enrich Hash\_1**

Simulate

Enrich Hash using information from VirusTotal. Supported entities: Filehash. Note: only MD5, SHA-1 and SHA-256 are supported.

**Parameters** **Settings** **Sample Output**

Choose Instance \*  Shared\_VirusTotal

Entities  All entities

Engine Threshold  20

Engine Percentage Threshold

Engine Whitelist

Resubmit Hash

Resubmit After (Days)  30

Retrieve Comments

Retrieve Sigma Analysis

Sandbox  VirusTotal Jujubox

Retrieve Sandbox Analysis

Google



# Answer: Yes, Related IP/URLs Only Suspicious Entities

The screenshot shows a SOAR platform interface with a dark theme. At the top, there is a navigation bar with a shield icon and the text "Google SecOps". Below the navigation bar, the title "wmic\_ntds\_dit\_t100..." is displayed, along with "SOAR Workshop", "Workshop 10", "2023-12-12 17:09:01", and a file count of "7".

The main area is titled "Playbook" and contains a "Simulate" button. Below the simulate button is a "Close Step Selection" button and several small circular icons.

Two blue rounded rectangular boxes represent actions:

- The first action is labeled "VirusTotalV3\_Get Related URLs\_1". It has a tooltip: "Get related IPs to the provided entities from VirusTotal. Note: this action requires a VT Enterprise token. Supported entities: URL...".
- The second action is labeled "VirusTotalV3\_Get Related URLs\_2". It has a tooltip: "Get related urls to the ... from VirusTotal. Note: VT Enterprise token. S...".

A horizontal arrow points from the first action to the second. The second action is labeled with a circled letter "A".

To the right of the second action, a modal window titled "VirusTotalV3 - Get Related URLs" is open. It includes a close button ("X") and tabs for "Parameters", "Settings", and "Sample Output".

The "Parameters" tab is active, showing the following fields:

- "Choose Instance": A dropdown menu set to "Shared\_VirusTotal".
- "Entities": A dropdown menu showing a list of options:
  - All entities
  - All entities
  - Internal entities
  - External entities
  - Source entities
  - Destination entities
  - All entities marked suspicious
  - All enriched entities
  - All users
  - Internal usersThe option "All entities marked suspicious" is highlighted with a blue background.
- "Results": A dropdown menu showing a list of options:
  - All entities
  - Internal entities
  - External entities
  - Source entities
  - Destination entities
  - All entities marked suspicious
  - All enriched entities
  - All users
  - Internal users
- "Max URLs To Return": A dropdown menu set to "50".

At the bottom right of the modal window is a "Simulate" button with a toggle switch that is currently off.



# Answer: Yes, Query Joiner

Insert Placeholder

Json Sample  
The sample below is for example purposes, actual data may vary.

EntityResults [2]

ips [5]

- 0 72.21.xx.xx
- 1 23.54.xx.xx
- 2 169.254.xx.xx
- 3 169.254.xx.xx
- 4 192.168.xx.xx

Add Functions

- first
- last
- min
- max
- filter
- dateFormat
- count
- orderBy
- toLower
- toUpper
- replace
- distinct

Expression

| "ips"

Run

Results

72.21.xx.xx,23.54.xx.xx,169.254.xx.xx,169.254.xx.xx,192.168.xx.xx

Insert Placeholder

Search...

VirusTotalV3\_Get Related URLs\_1.JsonResult

VirusTotalV3\_Get Related IPs\_1.is\_success

VirusTotalV3\_Get Related IPs\_1.JsonResult

VirusTotalV3\_Enrich Hash\_1.is\_success

SiemplifyUtilities - Query Joiner

SiemplifyUtilities\_Query Joiner\_1

Form query string from given parameters.

Parameters    Settings    Sample Output

Choose Instance \*    Shared\_SiemplifyUtilities\_1

Entities    All entities

Values \*    [VirusTotalV3\_Get Related IPs\_1.JsonResult| "ips"]

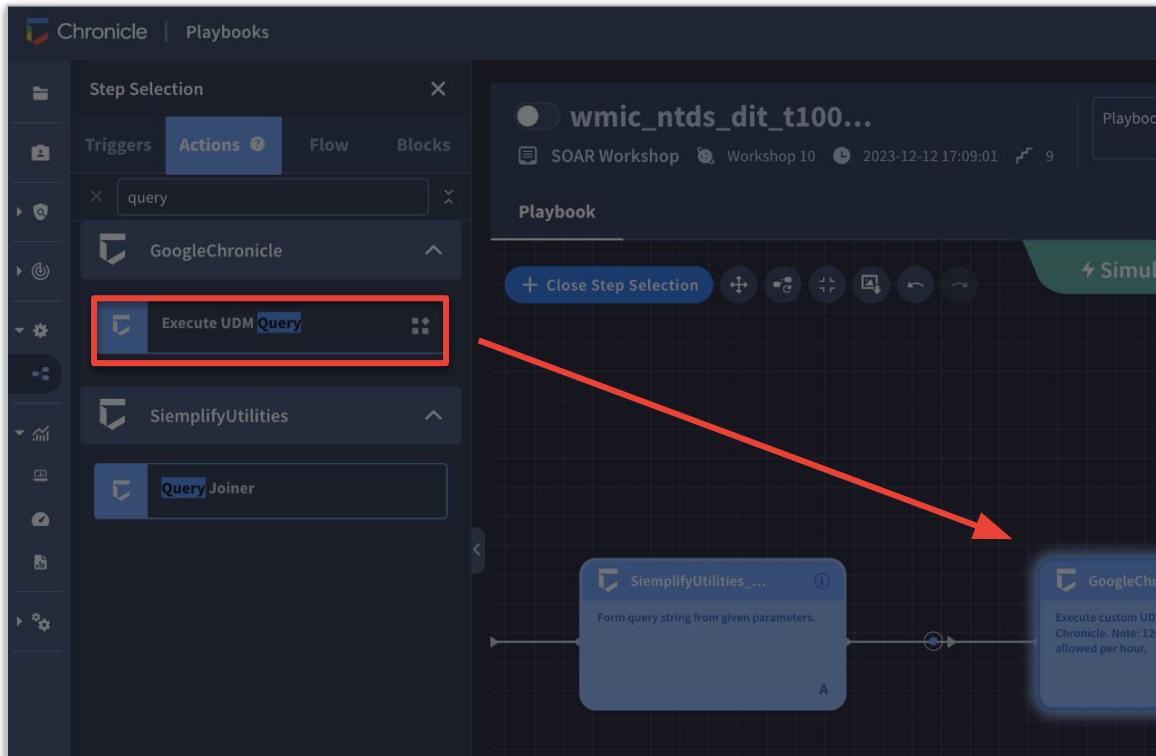
Query Field \*    ip

Query Operator \*    OR

Add Quotes   

Add Double Quotes

# Answer: Yes, Google Chronicle UDM Query



The screenshot shows the Chronicle Playbooks interface. On the left, the Step Selection sidebar is open, showing various actions like 'Execute UDM Query' (which is highlighted with a red box). The main area displays a workflow titled 'wmic\_ntds\_dit\_t100...'. This workflow starts with a 'SimplifyUtilities\_Query Joiner' step (which also has a red box around it), followed by a connector arrow pointing to a 'GoogleChronicle\_Execute UDM Query' step. A large red arrow points from the 'Execute UDM Query' step in the sidebar to the same step in the workflow.

**GoogleChronicle - Execute UDM Query**

**GoogleChronicle\_Execute UDM Query\_1**  Simulate

Execute custom UDM query in Google Chronicle. Note: 120 action executions are allowed per hour.

**Parameters** **Settings** **Sample Output**

Choose Instance \*  Shared\_GoogleChronicleSecops

Entities  All entities

Query \*  [SimplifyUtilities\_Query Joiner\_1.query]

Time Frame  Last Week

Start Time

End Time

Max Results To Return  50



# Answer: No, Case Comment

The screenshot illustrates the Chronicle Playbooks interface. On the left, a sidebar shows available tools: Chronicle, Triggers, Actions (selected), Flow, and Blocks. A search bar is present above the tool list. The main area displays a "Step Selection" dialog for the action "comment". The "Actions" tab is selected, and the search term "comment" is entered. The results list includes "Simplify" and "Case Comment", with "Case Comment" highlighted by a red rectangle. A large red arrow points from this selection towards the right side of the screen.

**wmic\_ntds\_dit\_t100...**

SOAR Workshop Workshop 10 2023-12-12 17:09:01 10

Playbook

+ Close Step Selection

VirustotalV3

Enrich Hash using info from VirusTotal. Supported note: only MD5, SHA-1

MultiChoiceQuestion

This step conditions the progress of the playbook according to a question the analyst has to answer manually, would be...

1. Yes

2. No

M

Simplify - Case Comment

Siemplify - Case Comment

**Siemplify\_Case Comment\_1**

Add a comment to the case the current alert has been grouped to

**Parameters** **Settings** **Sample Output**

Choose Instance \* Shared\_Siemplify\_1

Entities All entities

Comment \* Analyst declined to research hashes using VirusTotal

```
graph TD; Start(( )) --> MultiChoice[MultiChoiceQuestion]; MultiChoice --> Yes1((1. Yes)); MultiChoice --> No2((2. No)); Yes1 --> Siemplify[Siemplify_Case Comment]; No2 --> VirusTotal[VirustotalV3]
```



# Action - Google Chronicle List Assets

The screenshot illustrates the configuration of a playbook step to list assets in Google Chronicle.

**Step Selection:** On the left, under the "Actions" tab, the "List Assets" step is selected and highlighted with a red box. A red arrow points from this selection to the detailed configuration dialog on the right.

**Playbook Step Configuration:** The central area shows a step titled "wmic\_ntds\_dit\_t100..." which is part of a "Playbook". The "GoogleChronicle\_List Assets\_1" step is highlighted with a blue box. The configuration details are as follows:

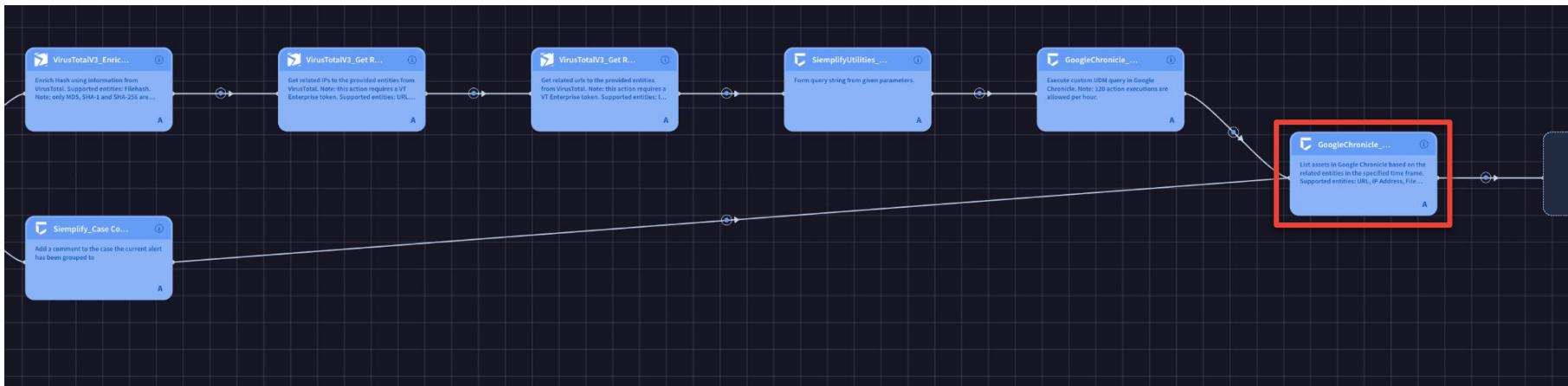
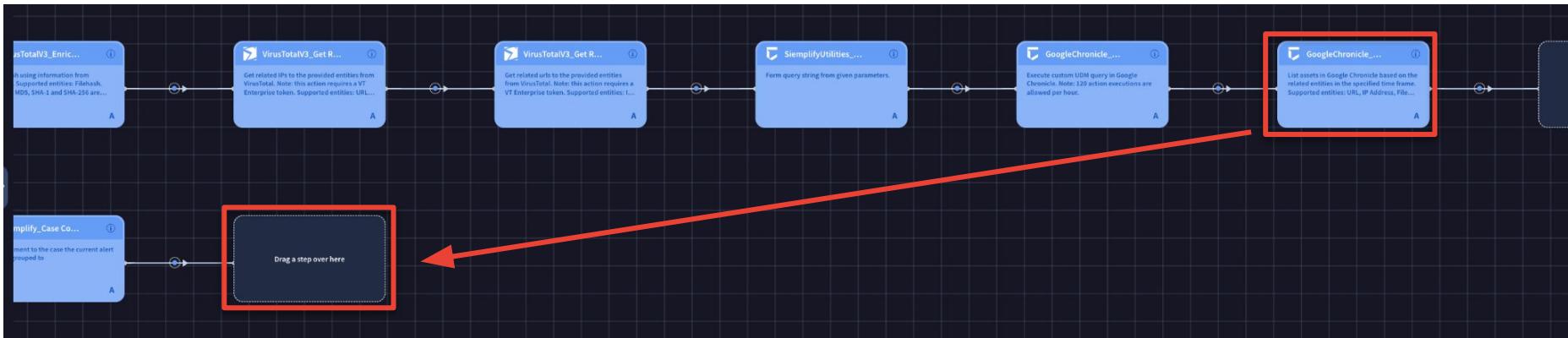
- Parameters:** Choose Instance: Shared\_GoogleChronicleSecops
- Entities:** All entities
- Max Hours Backwards:** 72 (highlighted with a red box)
- Time Frame:** Max Hours Backwards
- Start Time:** (unspecified)
- End Time:** (unspecified)
- Max Assets To Return:** 50

**Note:** The "List Assets" step has a note: "Execute custom UDM query in Google Chronicle. Note: 120 action executions are allowed per hour."



Google SecOps

# Merging Paths





# Action - Instruction

The screenshot shows the Chronicle Playbooks interface. On the left, there's a sidebar with sections like Step Selection, Triggers, Actions (which is selected), Flow, and Blocks. Under Actions, there are two 'Instruction' steps highlighted with a red box. The main area shows a workflow diagram with nodes: 'wmic\_ntds\_dit\_t100...' (trigger), 'GoogleChronicle...', and 'Instruction\_1' (action). A red arrow points from the 'Instruction' step in the sidebar to the 'Instruction\_1' node in the diagram. The right side of the screen displays the detailed configuration for 'Instruction\_1'. It includes fields for 'Assign To' (Soar User 10), 'Message to assignee' (Review the information gathered to date), 'Time to respond' (0 Days, 0 Hours, 5 Minutes), 'Approval link' (disabled), and a note: 'Based on the findings, determine whether this should be escalated to tier 3 for incident response.'

Chronicle | Playbooks

Step Selection

Triggers Actions ? Flow Blocks

instruction

Flow

Instruction

Siemplify

Instruction

wmic\_ntds\_dit\_t100...

SOAR Workshop Workshop 10 2023-12-12 17:09:01 12

Playbook

+ Close Step Selection

Simula

GoogleChronicle...

List assets in Google Chronicle based on the related entities in the specified time frame. Supported entities: URL, IP Address, File...

A

Instruction\_1

Instruct the analyst to do a specific action which can't be run from Siemplify, for example: Call the SOC manager, or go physically to his office to notify him regarding an issue

Instruction \*

Assign To: Soar User 10

Message to assignee: Review the information gathered to date

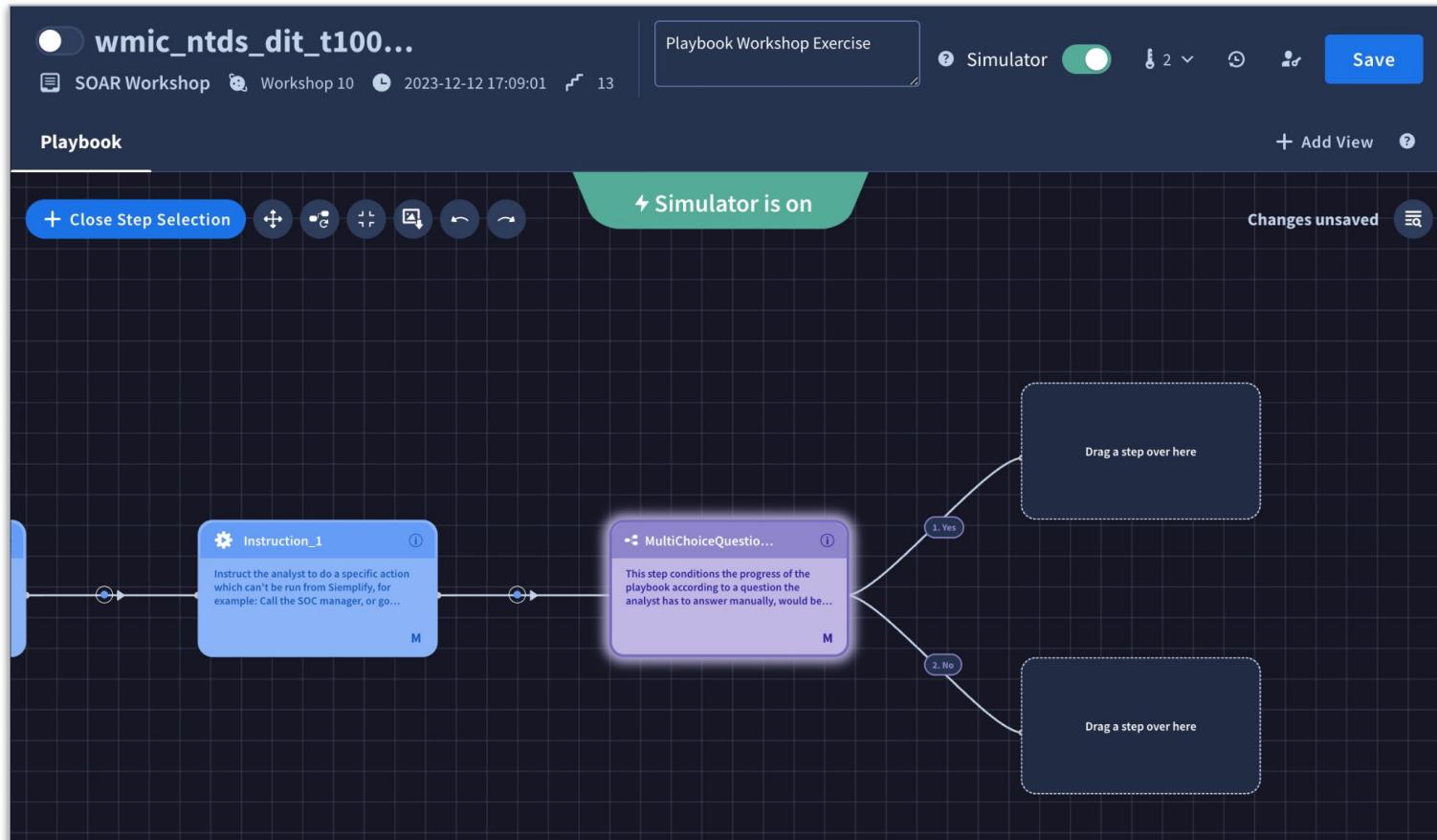
Time to respond: 0 Days, 0 Hours, 5 Minutes

Approval link: (disabled)

Based on the findings, determine whether this should be escalated to tier 3 for incident response.



# Flow - Multi-Choice Question



# Yes/No Action Paths

Chronicle | Playbooks

**Step Selection**

- Triggers
- Actions** ⓘ
- Flow
- Blocks

comment

Siemplify

Case Comment

Tools

Add Comment to Entity Log

VirusTotalV3

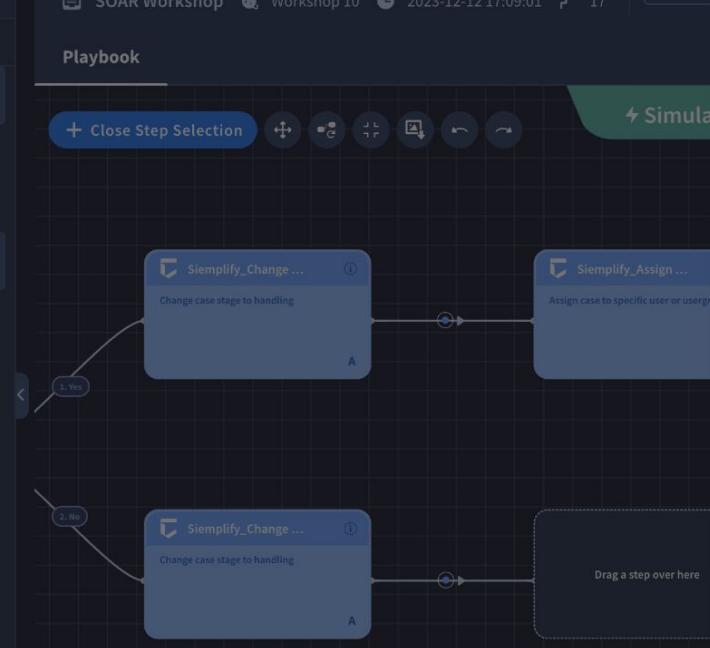
wmic\_ntds\_dit\_t100...

SOAR Workshop Workshop 10 2023-12-12 17:09:01 17

Playbook

+ Close Step Selection

Simulate



**Siemplify - Case Comment**

**Siemplify\_Case Comment\_2**

Add a comment to the case the current alert has been grouped to

**Parameters**

Choose Instance \* ⓘ Shared\_Siemplify\_1

Entities ⓘ All entities

Comment \*

ⓘ This case has been escalated to tier3 for system [Event.event\_principal\_hostname]

# Testing Our Playbook



# Google SecOps

The screenshot shows the SOAR Playbook Workshop Exercise interface. At the top left, there's a toggle switch labeled "wmic\_ntds\_dit\_t100..." and a status bar with "SOAR Workshop", "Workshop 10", "2023-12-12 19:55:21", and "17". The main area is titled "Playbook Workshop Exercise" and contains a "Simulator" toggle switch which is turned on. A green callout bubble says "Simulator is on". Below the title is a "Playbook" section with a "Close Step Selection" button and several small circular icons. The central part of the screen displays a complex workflow diagram on a grid. The diagram consists of numerous blue rectangular boxes representing steps, connected by arrows indicating flow. Some steps have additional text or icons below them. At the bottom, there are buttons for "Choose Case" (containing the value "5916# wmic\_ntds\_dit\_T1003\_003\_cisa\_report - 202..."), "Run" (with a play icon), and "Entities" (with a hexagon icon). On the right side, there are additional buttons for "Add View" and "Save".



# Simulating our Case/Alert

The screenshot shows the SOAR Platform interface during a 'Playbook Workshop Exercise'. The top navigation bar includes 'wmic\_ntds\_dit\_t100...', 'SOAR Workshop', 'Workshop 10', '2023-12-12 19:56:37', and '17' items. A 'Simulator' toggle is turned on, indicated by a green button and a message 'Simulator is on'.

A central 'Manual Action' dialog box is open, asking 'Do you want to check VirusTotal for IOCs from the alert?'. It contains two radio button options: 'Yes' (selected) and 'No'. Below the dialog are 'Cancel' and 'Execute' buttons.

The main workspace displays a process flow diagram with various nodes and connections. On the left, a list of recent actions is shown:

- MultiChoiceQuestion\_1 (2023-12-12 19:57:45)
- Siemplify\_Case Tag\_1 (2023-12-12 19:57:45)
- Siemplify\_Assign Case\_1 (2023-12-12 19:57:45)
- Output\_1 (2023-12-12 19:57:45)

On the right, there are three cards labeled 'Manual Action' with 'View Results' buttons.



# Adding a View

wmic\_ntds\_dit\_t100...

SOAR Workshop Workshop 10 2023-12-12 19:56:37 17

Playbook Workshop Exercise

Simulator  2 Save

Playbook

+ Add View

+ Open Step Selection

Simulator is on

Create View

View name \* AlertView

Roles \* Administrator, Tier1, Tier2, Ti...

Predefined widgets  Include all predefined playbook widgets in this view

Cancel Add





# Alert View

**General**    **Predefined**

- JSON Result
- Entities Highlights
- Events Table**
- HTML
- Free Text
- Key Value
- Entities Graph
- Insights
- Pending Actions

## AlertView A T T +3

Created at 2023-12-12 20:05:24 PM

**Pending Actions** i Predefined

This Widget lists all playbook actions waiting for user input.

**VirusTot** i Predefined

This widget returns information about the Hashes that were enriched by VirusTotal.

**GoogleC** i Predefined

This widget highlights the most important items in Execute UDM Query - Google Chronicle.

**MitreAtt** i Predefined

This widget highlights the most important items in MitreAttack - Get Techniques Details

**MitreAtt** i Predefined

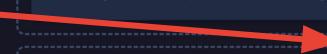
This widget highlights the most important items in MitreAttack - Get Techniques Mitigations

**Insights** i

This widget contains all the Insights from the Playbook Insights actions, general Insights and any other Insights you have added. They will be presented in HTML format

**Entities Highlights** i

This widget displays the highlighted fields for each entity.





# Modifying a Widget

**Events Table** ⓘ

This widget displays all Alert events and their properties.

Delete icon Settings icon (highlighted with a red box)

## Events Table

**Widget Title \*** Events Table

**Widget Description** This widget displays all Alert events and their properties.

**Widget Width** 100%

**Event Field**  
You can only add up to 6 fields

Column Name	Value
principal.hostname	[Event.event_principal_hostname]
principal.userid	[Event.event_principal_user_userid]
principal.sha256	[Event.event_principal_process_file_sha256]
p.commandLine	[Event.event_principal_process_commandLine]
t.commandLine	[Event.event_target_process_commandLine]
target.sha256	[Event.event_target_process_file_sha256]



Google SecOps

# HTML Widget

**HTML**

**Basic Settings**

**Widget Title \*** Chronicle Related Assets

**Widget Description** Description

**Widget Width** 100%

**Advanced Settings**

**HTML Code**

Preset

- Empty
- Clock
- Map
- Table
- Video
- Score
- Number**
- Bar Chart

A large red arrow points from the "Number" preset in this window to the "Number" card in the main interface.

**HTML**

Video Score Number Bar Chart

Conversation Gallery Layout 1 Layout 2

Layout 3 Layout 4 Layout 5 Layout 6

Layout 7

Show Less ^

A red box highlights the "Number" card, which displays the value "76". A red box also highlights the bottom right corner of the entire interface.

```
1 <!DOCTYPE html>
2 <html>
3
4 <link href="https://fonts.googleapis.com/css?family=Open+Sans:400,400i,700,700i" rel="stylesheet">
5 <link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">
6 <link href="https://www.siemplify.co/wp-content/themes/siemplify/assets/fonts/stylesheets.css?version=996" rel="stylesheet">
7 <style>
8 .cardContainer{
9   float: left;
10  width: 100%;
```

Google



# HTML Widget - Code Editor

HTML Code editor

HTML Code

```
354     </div>
355     <div class="cntRightSide">
356         <div class="cusWdgNumberTitle" id="field2"></div>
357         <div class="cusWdgNumberText" id="field3"></div>
358     </div>
359   </div>
360 </div>
361 <script src="https://code.jquery.com/jquery-3.5.1.min.js"></script>
362 <script>
363 $(document).ready(function(){
364
365     /*Update below variable value with placeholder*/
366     var field1 = [GoogleChronicle_List Assets_1.JsonResult| "EntityResult.assets" | count()];
367     var field2 = 'Related Assets';
368     var field3 = 'Total Related Assets found in Chronicle over the past 72 hours';
369
370     /*End*/
371     $("#field1").html(field1);
372     $("#field2").html(field2);
373     $("#field3").html(field3);
374 });
375 </script>
376 </body>
377 </html>
```

Update below variable value with placeholder

HTML Preview



# Preparing Our Playbook

The screenshot shows a SOAR platform interface for creating a new playbook. The top bar displays the title "wmic\_ntds\_dit\_t100..." and the category "SOAR Workshop - Workshop 10". It also shows the creation date and time as "2023-12-12 20:35:41" and a count of 17 items. The main area is titled "Playbook Workshop Exercise" and contains a "Simulator" toggle switch, which is highlighted with a red box. A "Save" button is also highlighted with a red box. Below this, there are tabs for "Playbook" and "AlertView", with "AlertView" being the active tab. The "General" view is selected under "AlertView". The alert view has a title "AlertView" and a status badge showing "ATT.T +3". It was created at "2023-12-12 20:35:41 PM". On the far right of the interface, there are standard edit and delete icons.



# Manual Action - Attach Playbook to Alert

wmic\_ntds\_dit\_T1003\_003\_cisa\_report

ID 5892    Workshop 10    Triage    2023-12-12 06:45:30    T1    @Tier1

Manage Tags

1. WMIC\_NTDS\_DIT\_T10... (4) • 2023-12-12 05:28:00  
2. IMPACKET\_WMIEXEC\_... (1) • 2023-12-12 05:23:30  
3. RECON\_SUSPICIOUS... (10) • 2023-12-12 05:09:00  
4. PORT\_PROXY\_FORW... (1) alerts

Manual Action

Overview (4)    Events (4)    Playbooks (0)    Graph

More Options

The screenshot shows a security alert titled 'wmic\_ntds\_dit\_T1003\_003\_cisa\_report' with ID 5892. It includes fields for 'Workshop 10' (selected), 'Triage' status, and a timestamp of '2023-12-12 06:45:30'. A 'T1' indicator and '@Tier1' location are also present. Below the title, there's a 'Manage Tags' link. The main content area displays four event cards: 1. WMIC\_NTDS\_DIT\_T10... (4) • (timestamp: 2023-12-12 05:28:00), 2. IMPACKET\_WMIEXEC\_... (1) • (timestamp: 2023-12-12 05:23:30), 3. RECON\_SUSPICIOUS... (10) • (timestamp: 2023-12-12 05:09:00), and 4. PORT\_PROXY\_FORW... (1) alerts (timestamp: 2023-12-12 05:18:00). A 'Manual Action' button is highlighted with a red box and a tooltip. At the bottom, there are tabs for 'Overview' (selected), 'Events (4)', 'Playbooks (0)', and 'Graph', along with a 'More Options' menu.



# Manual Action - Attach Playbook to Alert

**Manual Action**

**Siemplify**

**Attach Playbook to Alert**  
Attach a specific playbook to an alert

Choose Instance \*

Run on Alerts \*

**Entities**

Group

Specific

Playbook Name \*

Actions:

- Add Entity Insight
- Add General Insight
- Add Tags To Similar Cases
- Add to Custom List
- Assign Case
- Attach Playbook to Alert**
- Case Comment
- Case Tag
- Change Alert Priority
- Change Case Stage
- Change Priority
- Close Alert

**Close** **Execute**

# Pending Action

Chronicle | Cases

### wmic\_ntds\_dit\_T1003\_003\_cisa\_report

ID 5892 Workshop 10 Investigation 2023-12-12 20:48:07

T1003.003 X Manage Tags

Overview Events (4) Playbooks (1) Graph

Pending Actions (1) [i](#)

Failed Pending

MultiChoiceQuestion\_1 4 minutes ago

Target Entities

- IP 10.128.0.21
- User TIM.SMITH\_ADMIN
- URL HTTPS://ATTACK.MITRE.ORG/VERSIONS/V13/T...
- 64BITS
- LOLBIN
- 8204

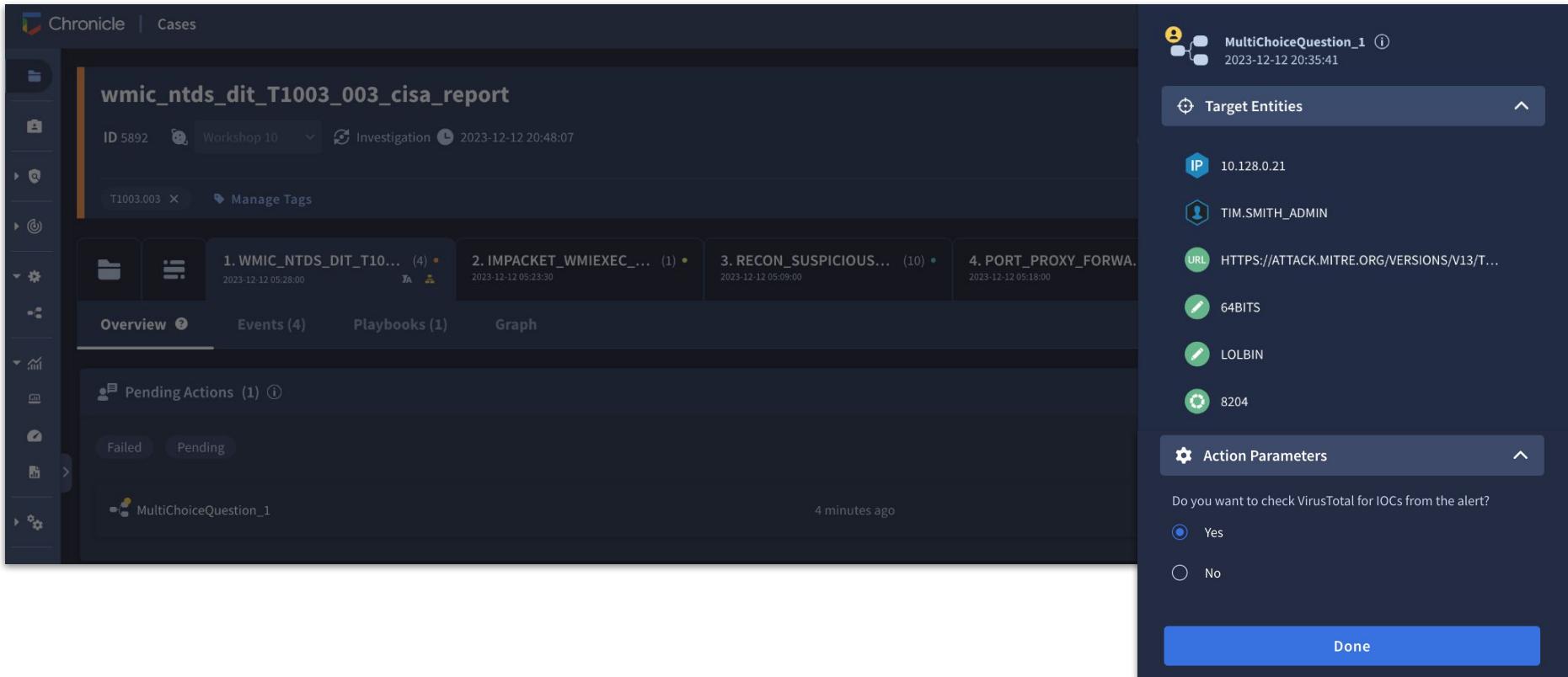
Action Parameters

Do you want to check VirusTotal for IOCs from the alert?

Yes

No

Done



# Instructions

 **Instruction\_1** ⓘ  
2023-12-12 20:35:41

 **Time to respond**  
0 hours 4 minutes left

 **Message to Assignee** ^

Review the information gathered to date

 **Target Entities** ^

- # EB71EA69DD19F728AB9240565E8C7EFB59821...
- # A3204D81E5F06EB3ACDB44EA8B342B6FDFDA...
- # A9AB5725D4E96E39F5001B4982B1C81F868A0...
- IP 10.128.0.21
- 👤 TIM.SMITH\_ADMIN
- URL <HTTPS://ATTACK.MITRE.ORG/VERSIONS/V13/T...>

 WIN-ADFS.LUNARSTIIINESS.COM

 **Action Parameters** ^

Based on the findings, determine whether this should be escalated to tier 3 for incident response.

**Done**



Google SecOps

# Alert View

### wmic\_ntds\_dit\_T1003\_003\_cisa\_report

ID 5892 Workshop 10 Incident 2023-12-12 20:55:07 T3 @Tier3

Manage Tags

principal.hostname	principal.userid	principal.sha256	p.commandLine	t.commandLine
WIN-ADFS.LUNARSTIIINESS.COM	TIM.SMITH_ADMIN	# A9AB5725D4E96E39F5001B-	C:\DISKUTIL.EXE	"cmd.exe" /c wmic process call create 'ntdsutil "ac i ntc
WIN-ADFS.LUNARSTIIINESS.COM	TIM.SMITH_ADMIN	# 1792731E030B7FE35A7EB21	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	ntdsutil "ac i ntds" ifm "create full C:\Windows\Temp\p
WIN-ADFS.LUNARSTIIINESS.COM	TIM.SMITH_ADMIN	# DE9396D630A198FCE8EBC9	ntdsutil "ac i ntds" ifm "create full C:\Windows\Temp\pro\	
WIN-ADFS.LUNARSTIIINESS.COM	TIM.SMITH_ADMIN	# EB71EA69DD19F728AB9240	"cmd.exe" /c wmic process call create 'ntdsutil "ac i ntds" ifm "cre...	wmic process call create 'ntdsutil "ac i ntds" ifm "cre...

### VirusTotalV3\_Enrich Hash\_1

Detections: 52 / 72

IoCs: a9ab5725d4e96e39f5001b4982b1c81f868a081f25e60383  
a3204d81e5f06eb3ac...  
eb71ea69dd19f728a...  
1792731e030b7fe35a...

Attribution: trojan.msl/gruntstager

### GoogleChronicle\_Execute UDM Query\_1

18 EVENTS FOUND

Google

# Alert View

 Chronicle Related Assets

# 23

## Related Assets

Total Related Assets found in Chronicle over the past 72 hours

 Insights ⓘ

 VirusTotalV3

Expand

# EB71EA69DD19F728AB9240565E8C7EFB59821E19E3788E289301E...

Detected: 0 Threshold: 20

 VirusTotalV3

Expand

# A3204D81E5F06EB3ACDB44EA8B342B6FDFDA471AAFA205AE16D8...

Detected: 0 Threshold: 20

 VirusTotalV3

Expand

# A9AB5725D4E96E39F5001B4982B1C81F868A081F25E603832709D...

Detected: 52 Threshold: 20

# Case Wall

wmic\_ntds\_dit\_T1003\_003\_cisa\_report

ID 5892 Workshop 10 Incident 2023-12-12 20:56:08

T3 @Tier3

Explore

T1003.003 X Manage Tags

2023-12-12 20:54:31 2.WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT

U Automation left a comment  
This case has been escalated to tier3 for system win-adfs.lunarstiiness.com

2023-12-12 20:54:31 2.WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT

Siemplify\_Case Comment\_2 | Comment added to case: This case has been escalated to tier3 f... View More

2023-12-12 20:54:31 2.WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT ★

Case assigned to @Tier3 by System

2023-12-12 20:54:30 2.WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT

Siemplify\_Assign Case\_2 | The case was successfully assigned to Tier3. View More

2023-12-12 20:54:30 2.WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT

Case stage set to Incident by System

2023-12-12 20:54:30 2.WMIC\_NTDS\_DIT\_T1003\_003\_CISA\_REPORT

Siemplify\_Change Case Stage\_1 | Case stage was successfully changed to Incident. View More

Google

4

Click

# Export (and Import)

Playbooks can be exported (and imported into other instances)

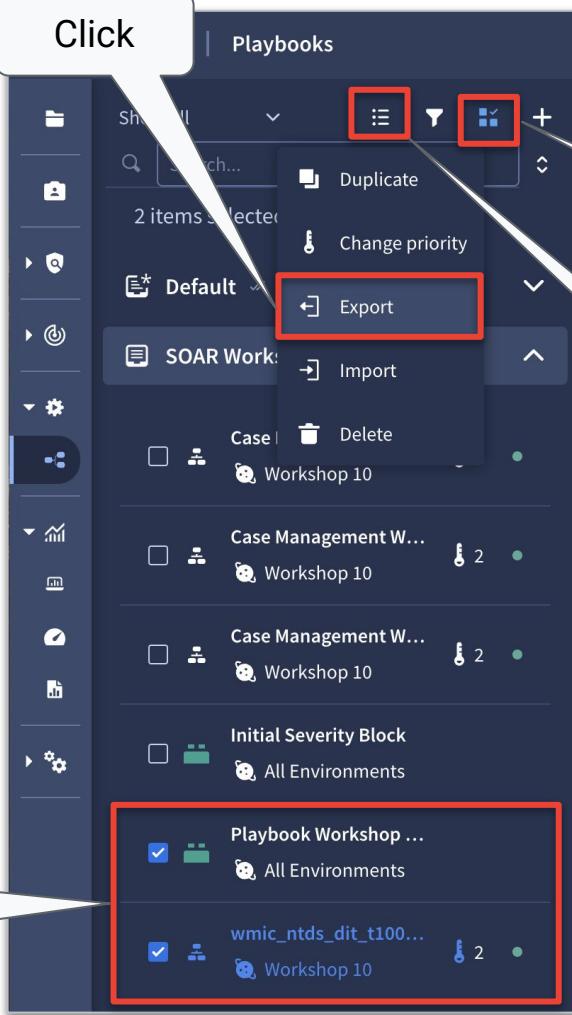
Blocks must also be exported and imported for a playbook that calls a block to successfully load

Exported files are stored as multiple jsons (one per playbook or block) within a zip

Playbooks saved in json must be compressed to zip for import

Select both the Block and Playbook

2



Google SecOps

1

Click

3

Click

Google



# Summary

Playbooks are a series of steps that include a trigger, actions, flows and blocks

Blocks can be used to streamline repetitive sets of flows and action in a build once use many paradigm

Simulator mode provides a way to test playbooks without creating action in production alerts

Alert View provides a per playbook view for analysts to consume information

A playbook can be triggered via manual action by attaching a playbook to an alert

Playbooks can be exported and imported across instances



# Handy Links

Playbooks:

<https://cloud.google.com/chronicle/docs/soar/respond/working-with-playbooks/whats-on-the-playbooks-screen>

Playbook Simulator:

<https://cloud.google.com/chronicle/docs/soar/respond/working-with-playbooks/working-with-playbook-simulator>

Custom Alert Views:

<https://cloud.google.com/chronicle/docs/soar/respond/working-with-playbooks/define-customized-alert-views-from-playbook-designer>

Marketplace Integrations: <https://cloud.google.com/chronicle/docs/soar/marketplace-integrations>

SecOps Community: <https://secopscommunity.com>

# Thank You