Google

Google SecOps

Building Playbooks in Google SecOps

Using Playbooks in Security Operations

January 2024

Using goo.gle/secops-workshop

Agenda

Google SecOps

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

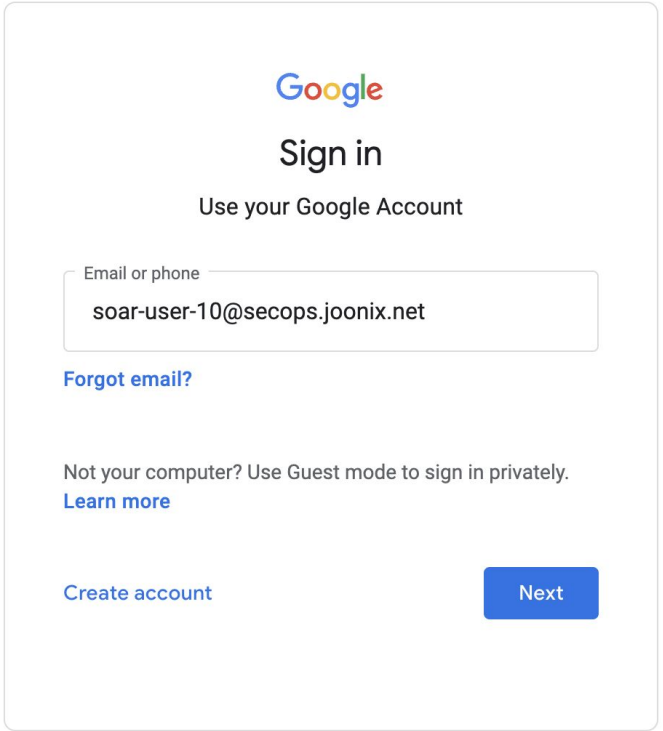
Login Instructions (1)

Google SecOps

1) Open a new Incognito Window in your Chrome Browser

2) Navigate to the Google SecOps instance URL: **https://goo.gle/secops-workshop**

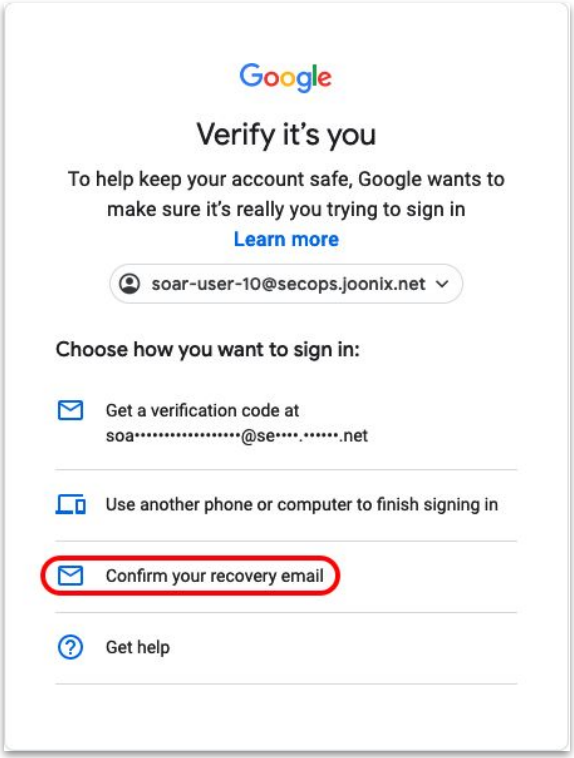
3) Use the account assigned to you by your instructor that uses Google Workspace as Identity Provider



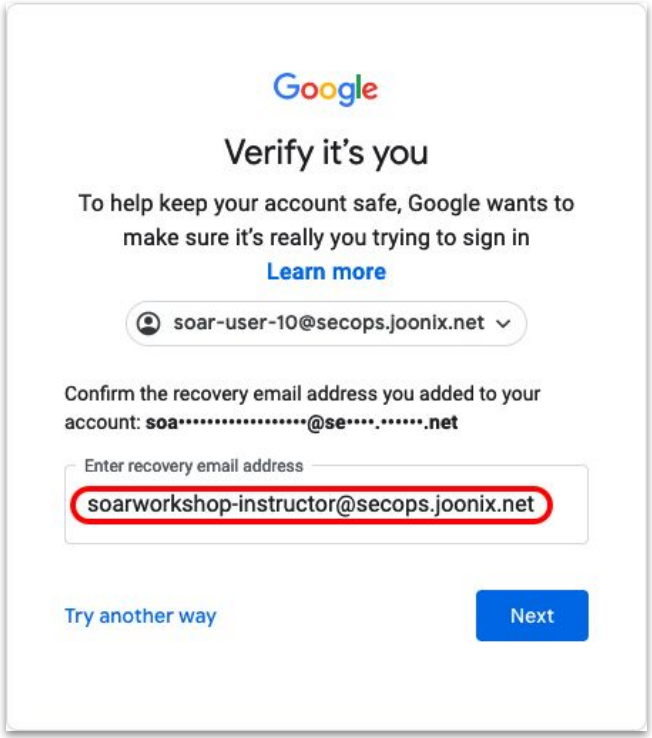
Login Instructions (2)

Google SecOps

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



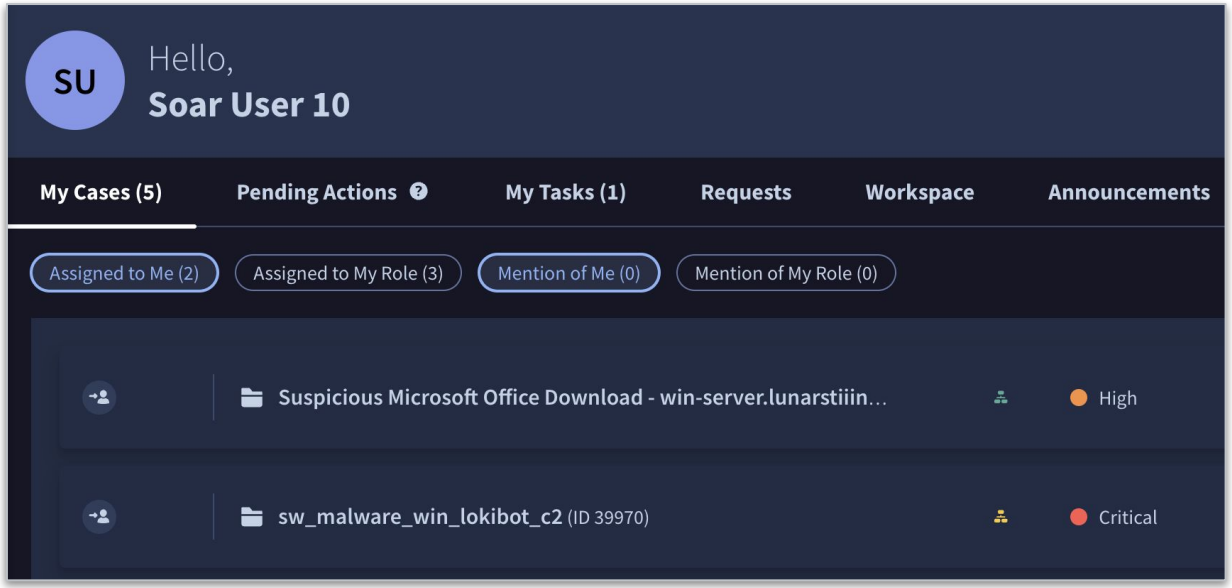
5) Type “soarworkshop-instructor@secops.joonix.net” as the recovery email and click Next



Login Instructions (3)

Google SecOps

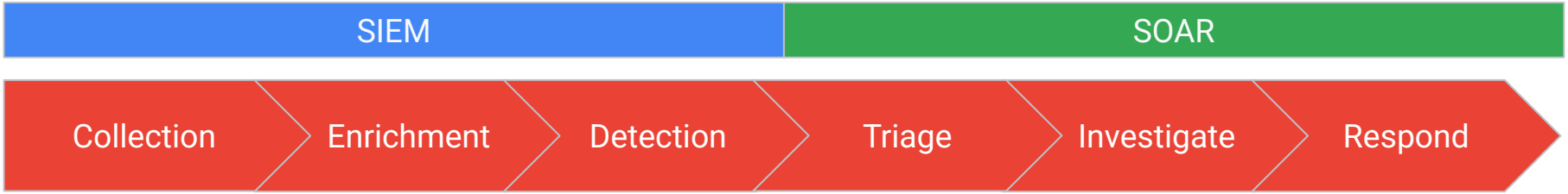
6) We are now logged into Google SecOps with a view similar to this



SecOps Overview

Google SecOps

Google's Security Operations Platform



- Data Ingest
- Parsing
- Indexing

- Attaching Context to Events
- Calculating Prevalence

- YARA-L Rules
- Curated Detections
- UEBA
- IOC Matching

- Alert Prioritization
- Grouping Alerts

- Case Management
- Collaboration

- Actions
- Playbooks

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

Google SecOps

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

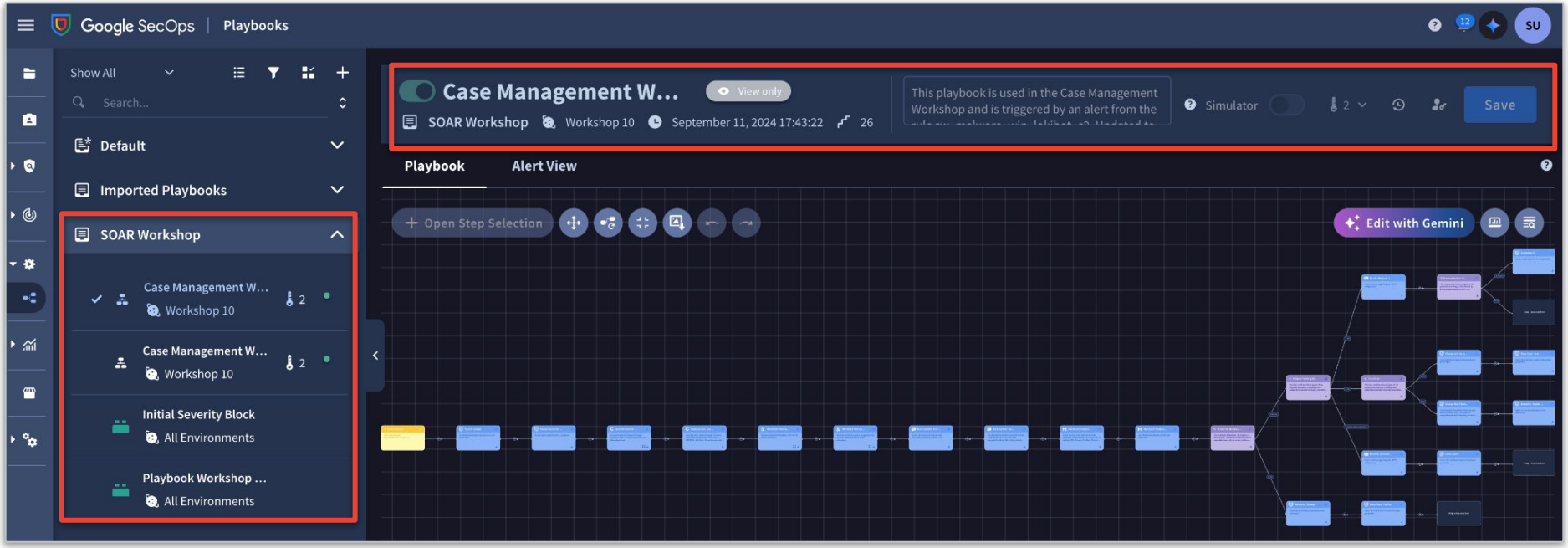
Inject specific analyst inputs into the process and then allow the system to go down other paths based on the input provided

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

The Basics

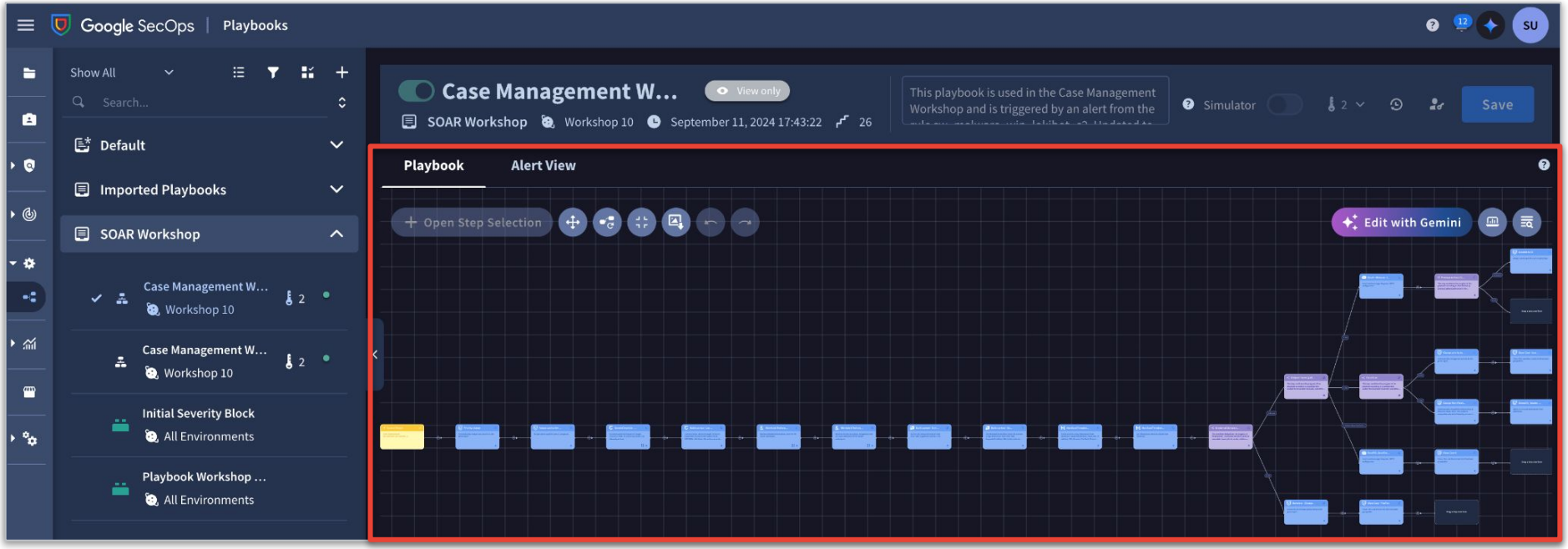
Playbook Editor

Google SecOps



Playbook Editor

Google SecOps



Playbook Tool Grouping

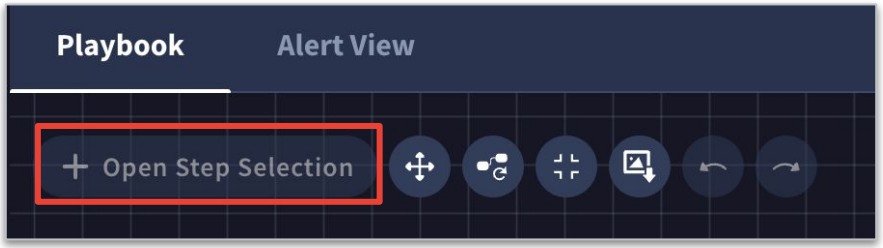
Google SecOps

Conditions to start the execution of a Playbook

Conditions (if), and multiple choices questions

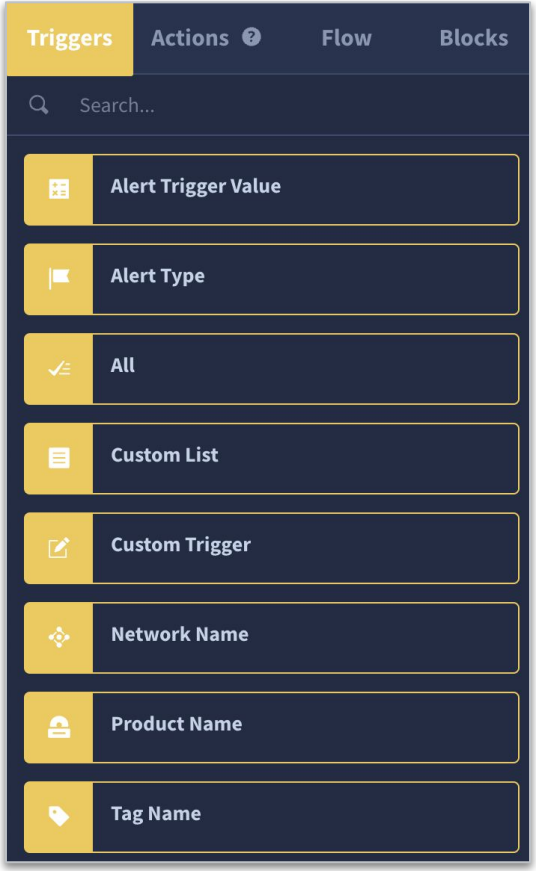
Enrichments, Data collection, Allow/Block and much more...
(Installed from Marketplace, Configured in Response - Integrations Setup)

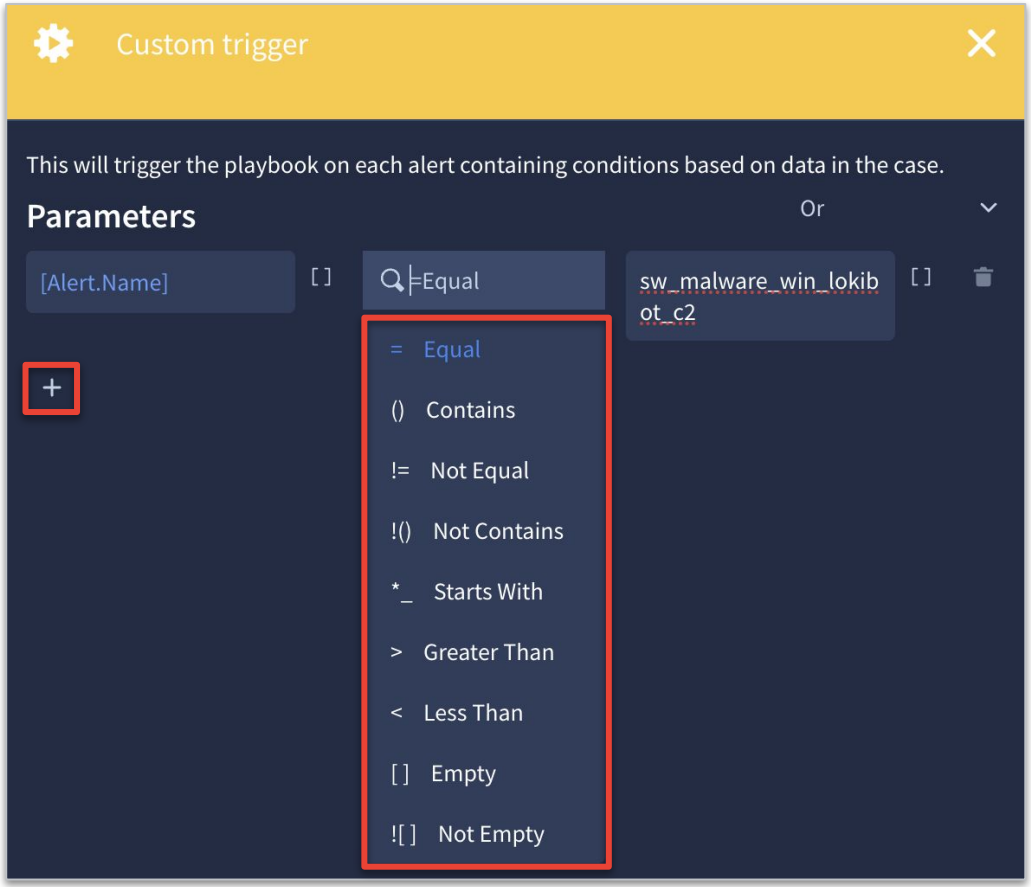
Sub-playbooks; actions and flow



Google

Triggers

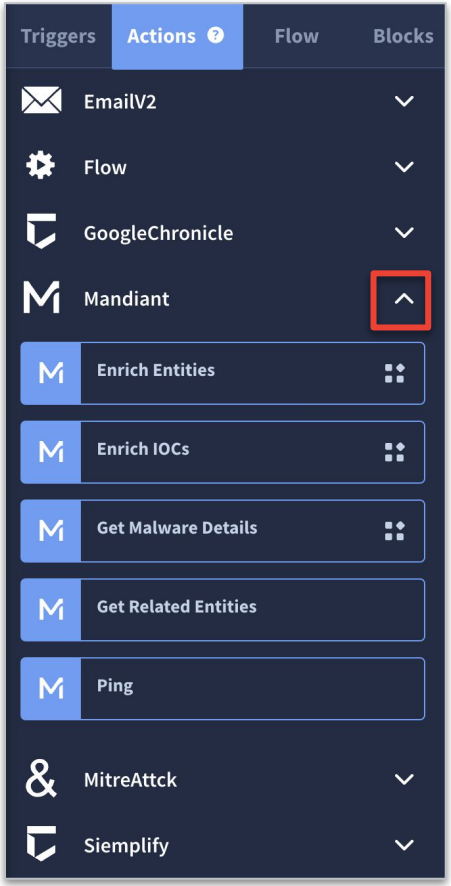


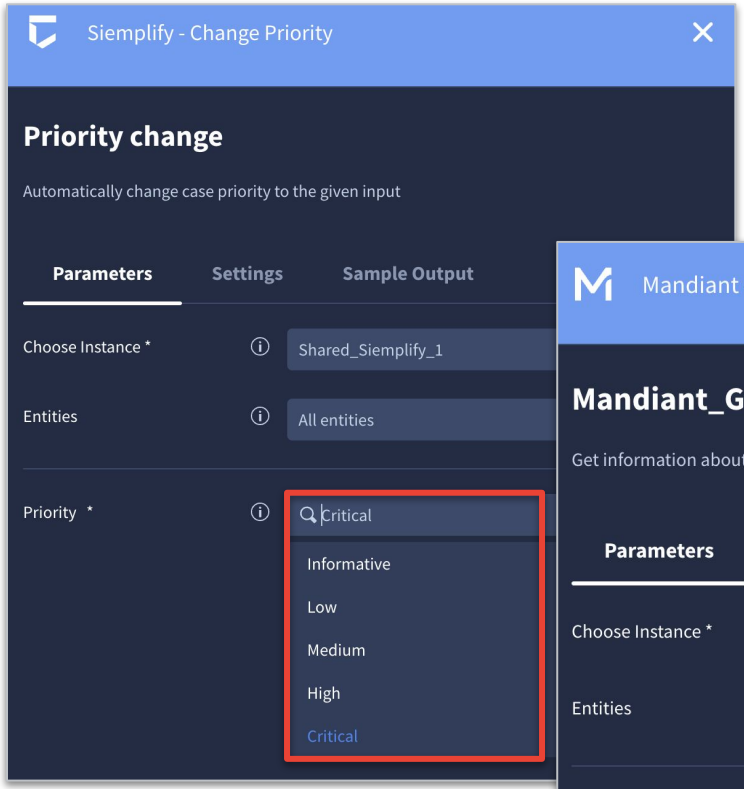


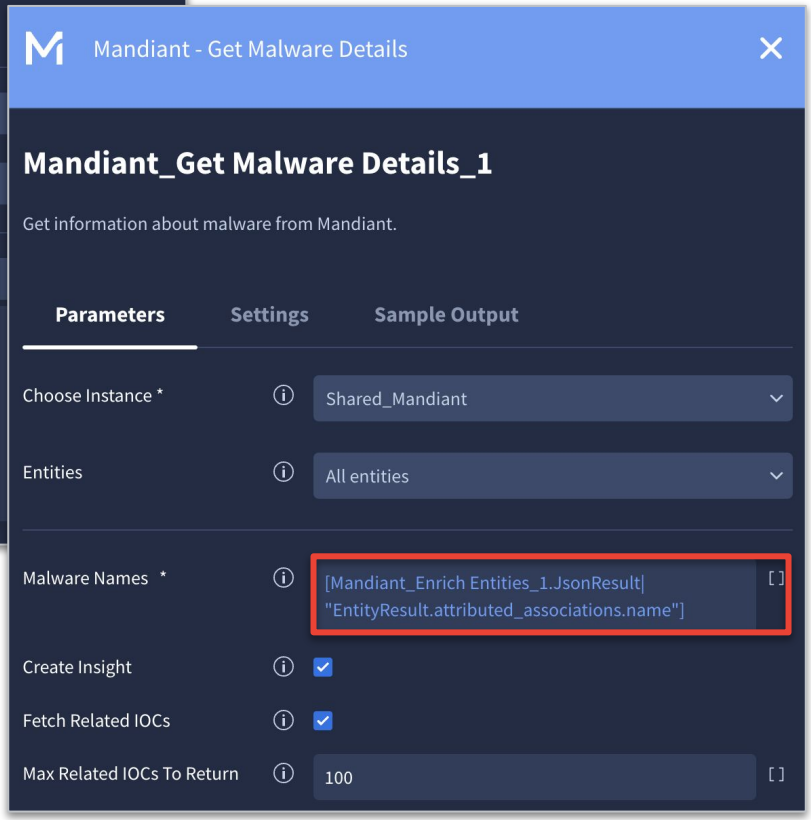
Google SecOps

Google

Actions

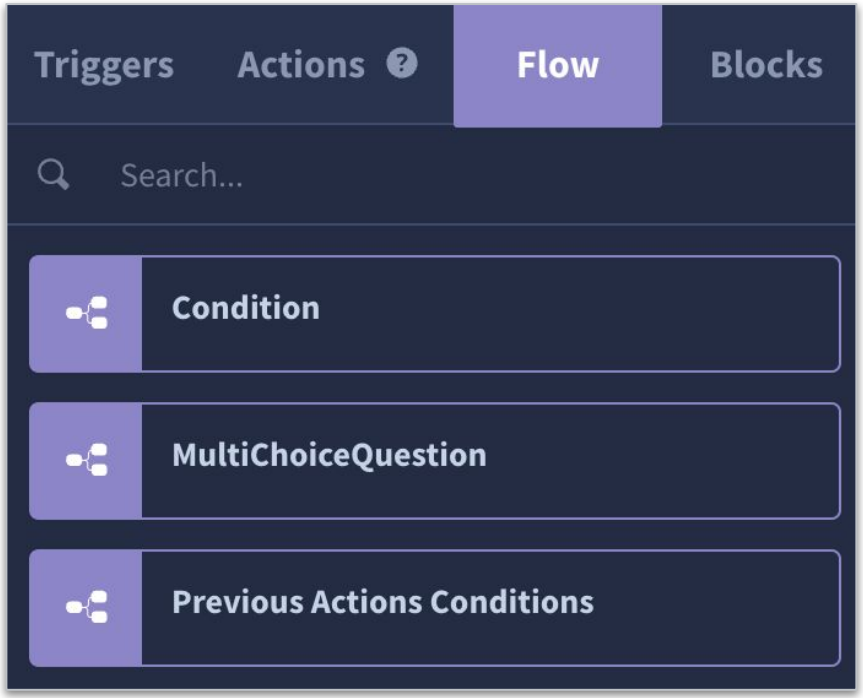


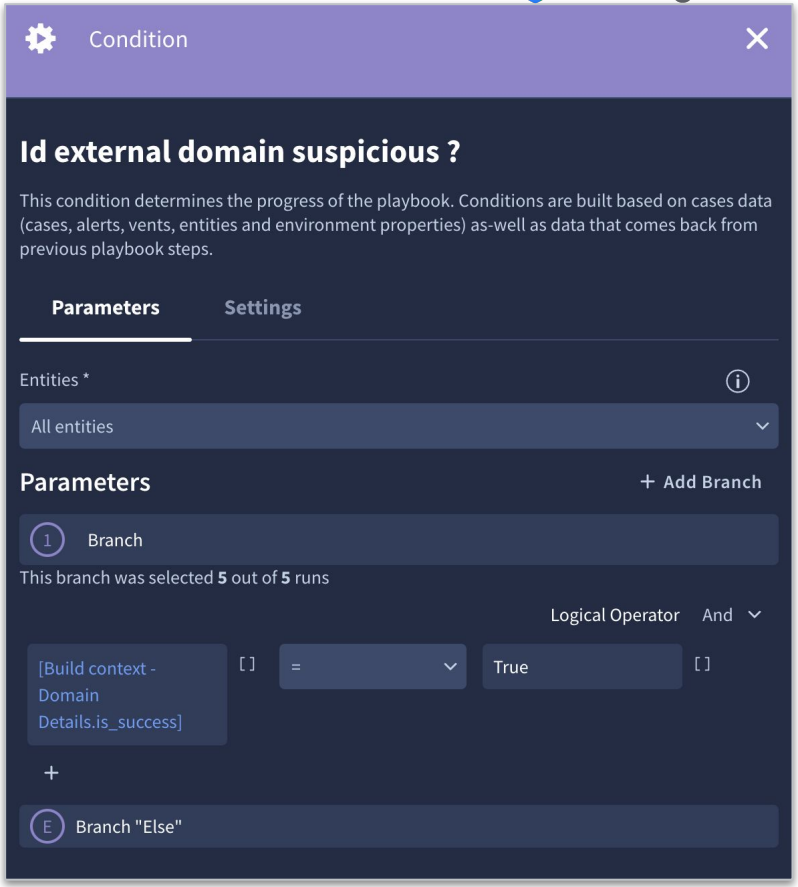




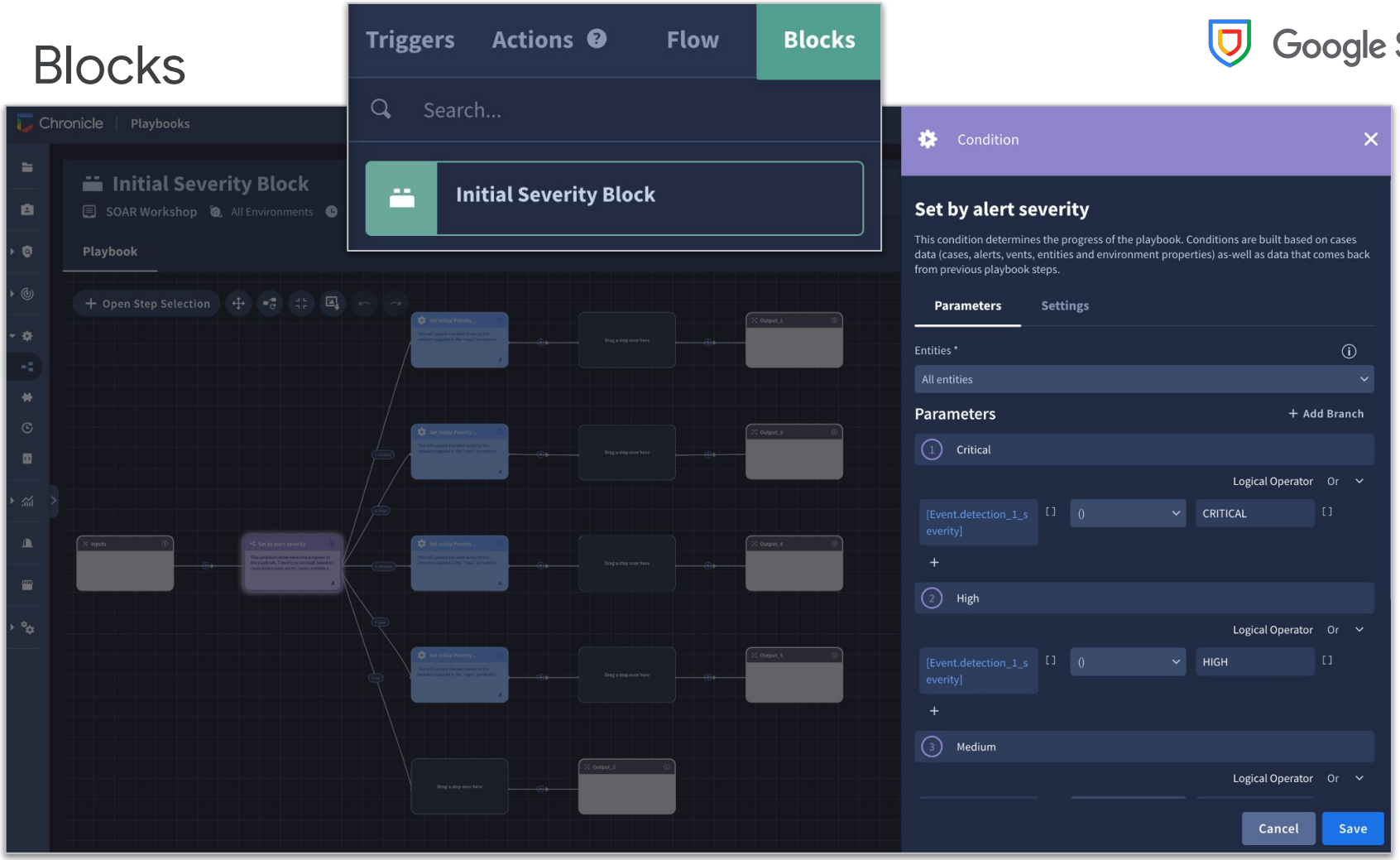
Google SecOps

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 *
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



Google SecOps

Google

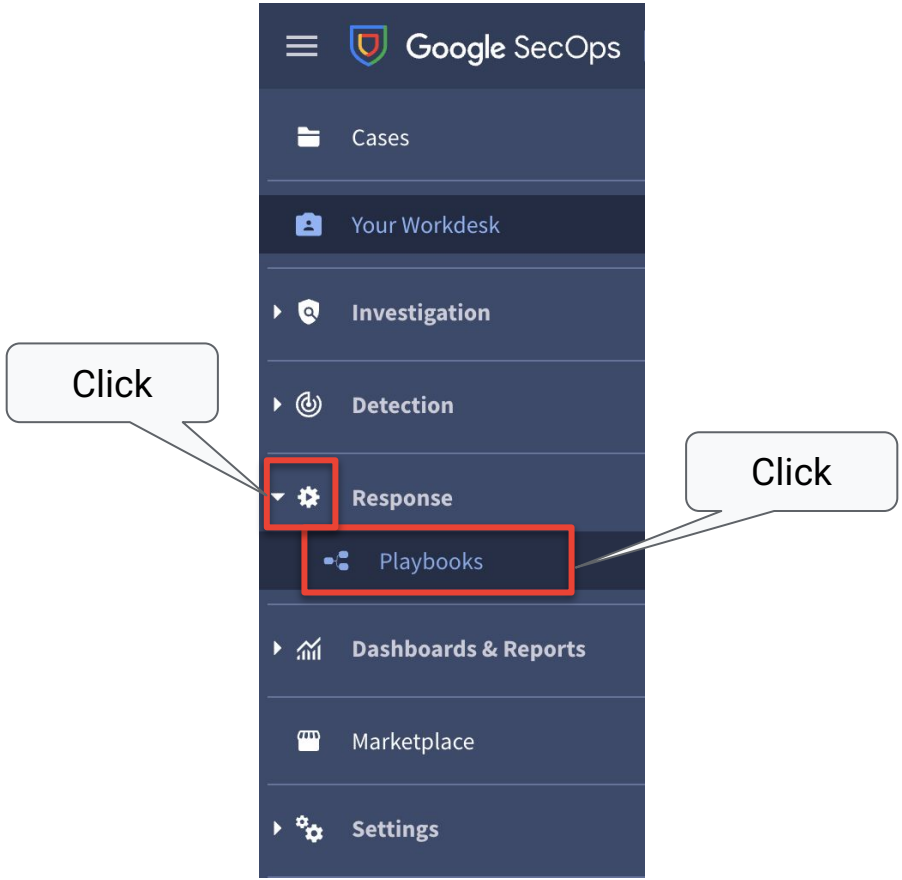
Google SecOps

Playbook Walk Through

Google

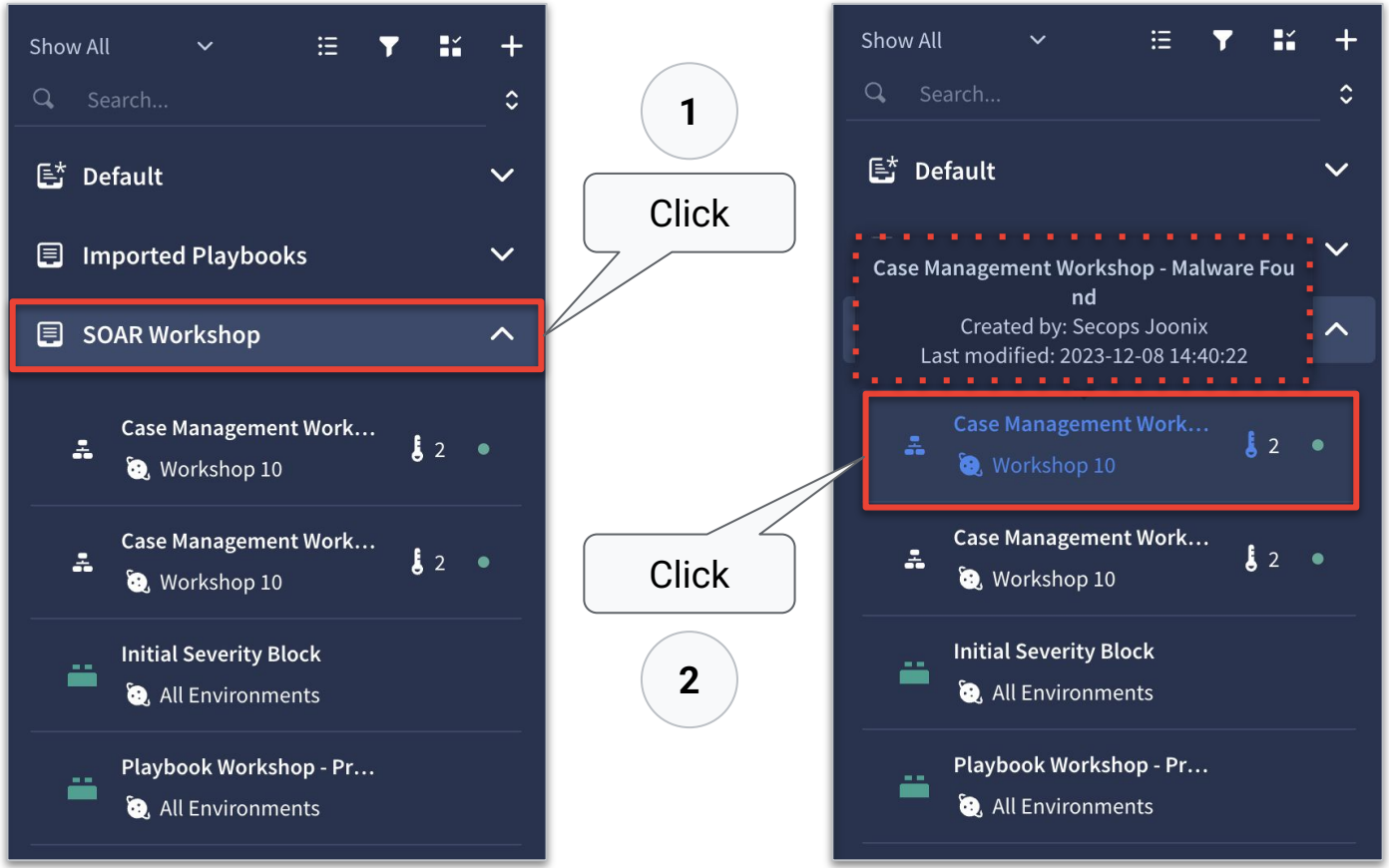
Navigating to Playbooks

Google SecOps



Selecting Our Playbook

Google SecOps

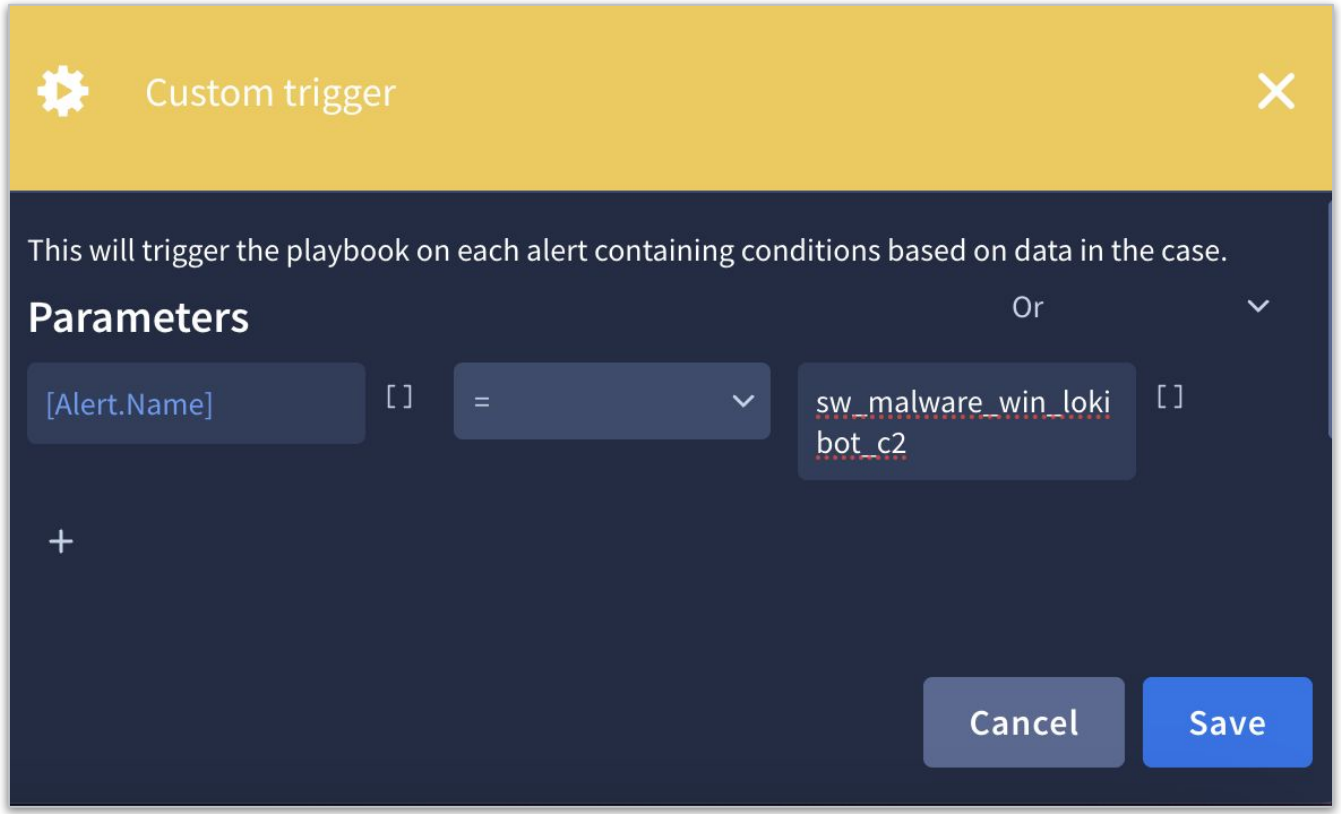


Playbook Familiarization

Google SecOps

Playbook Review - Trigger

Google SecOps



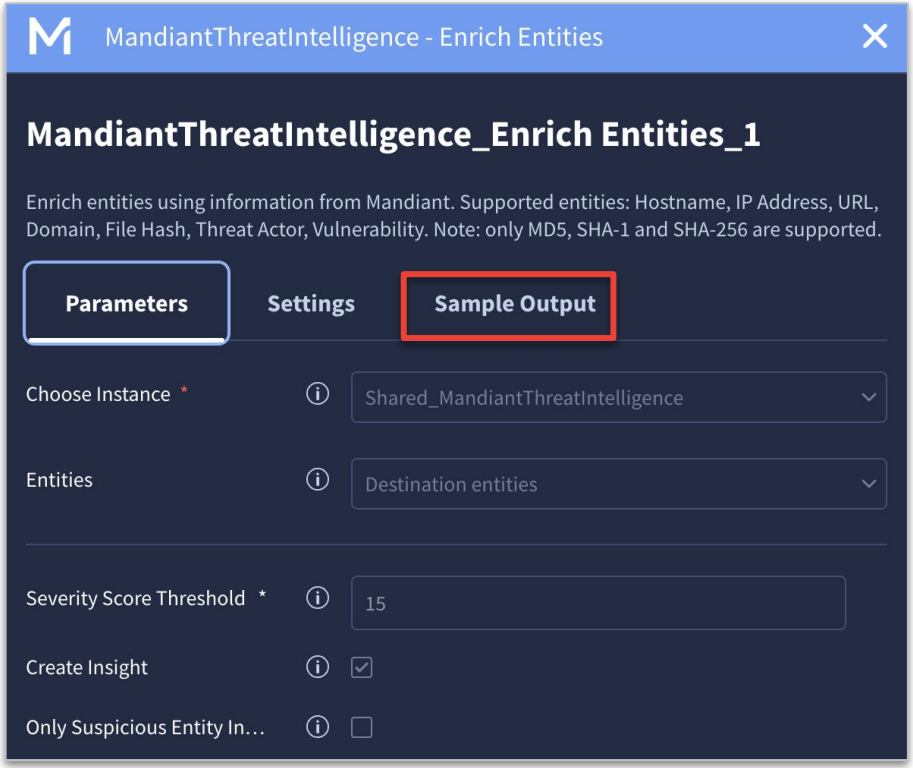
Playbook Action Blocks

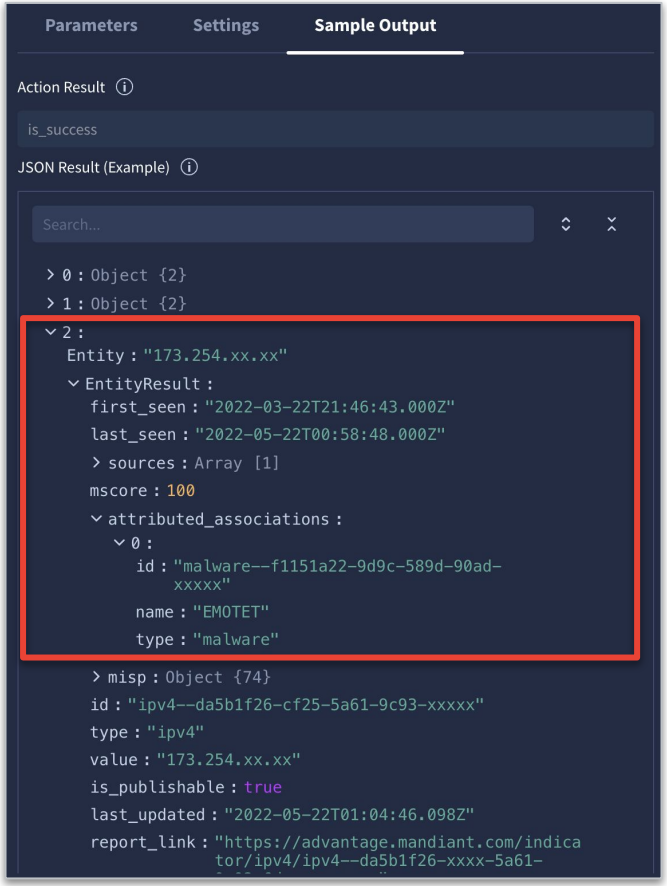
Google SecOps

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

Action Details

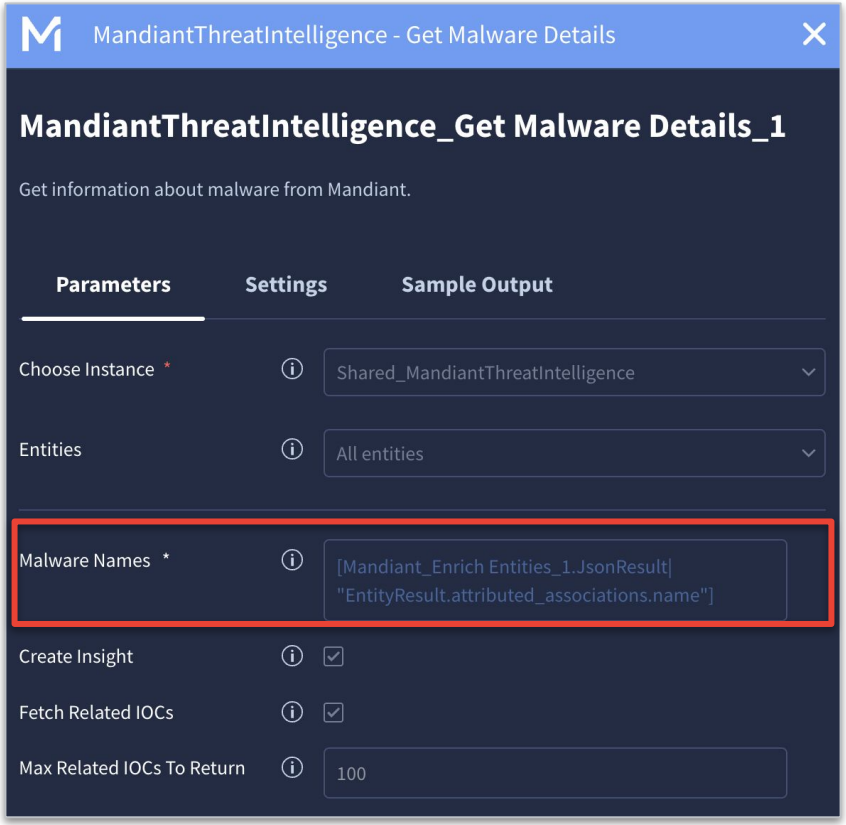
Google SecOps



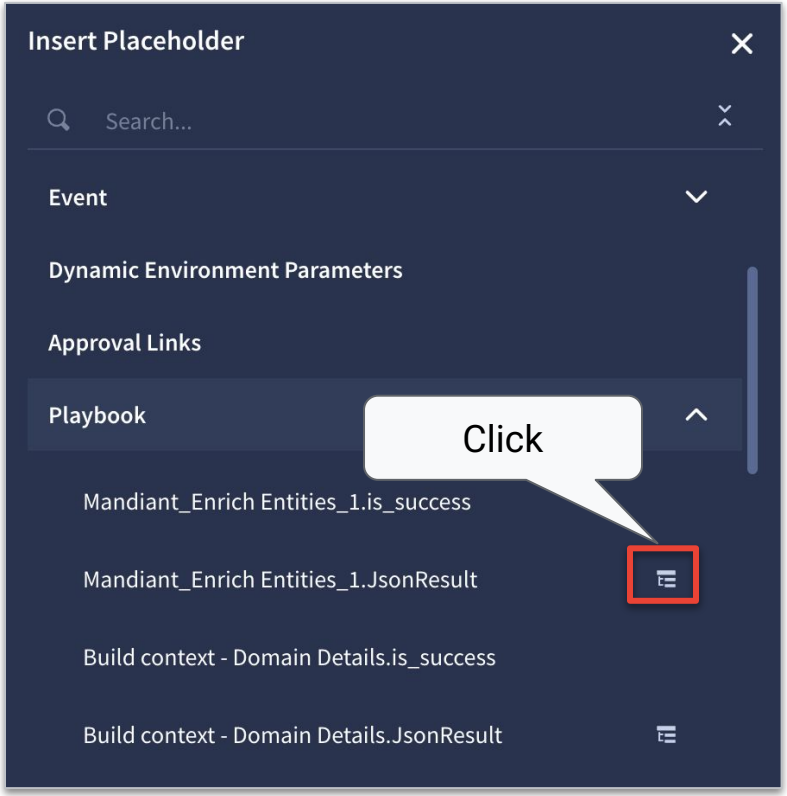


Action Details

Google SecOps

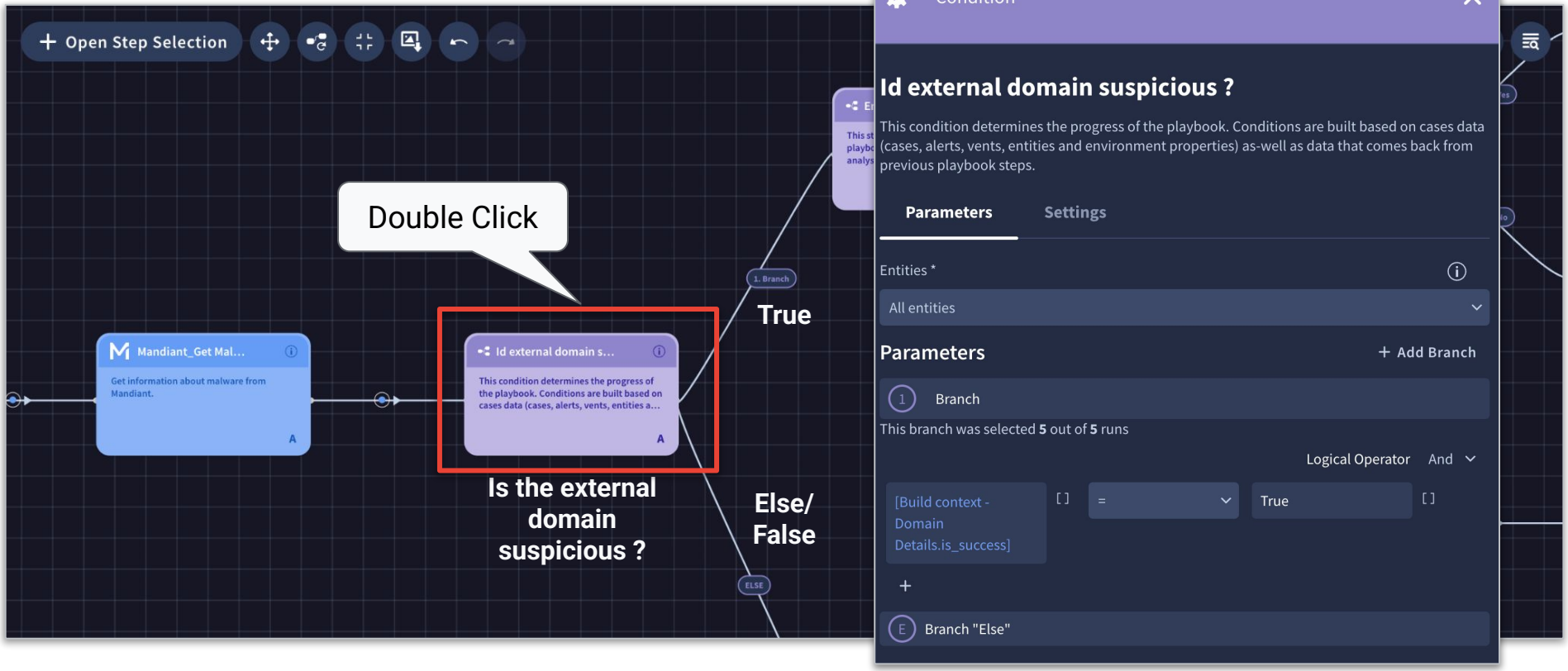


Action Details



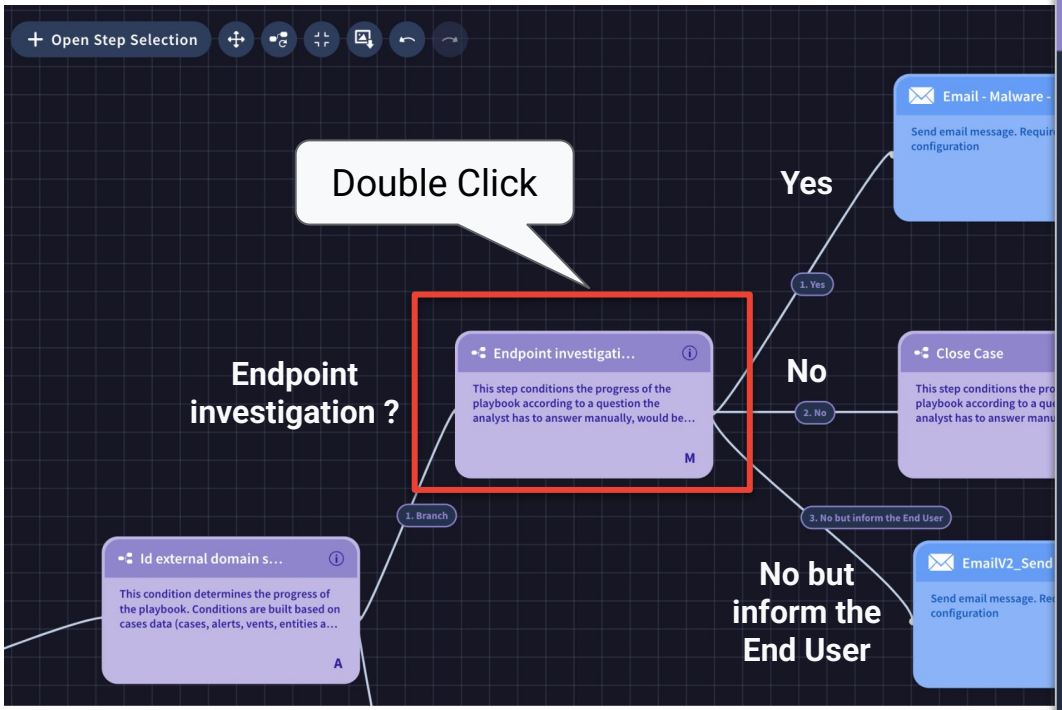
Flow - Condition

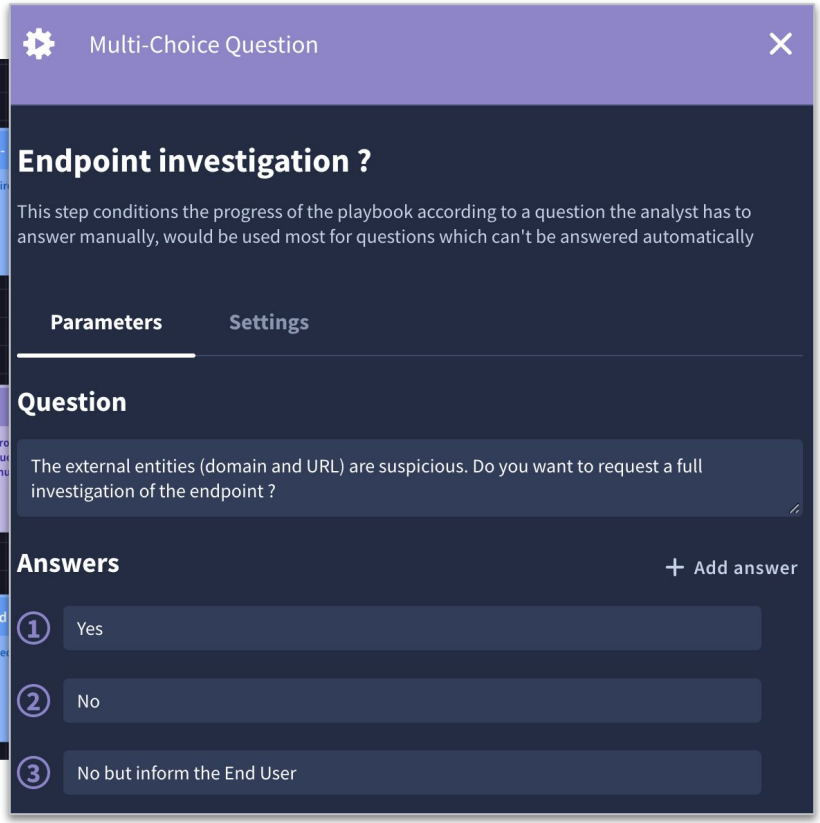
Google SecOps



Flow - Multi-Choice Question

Google SecOps



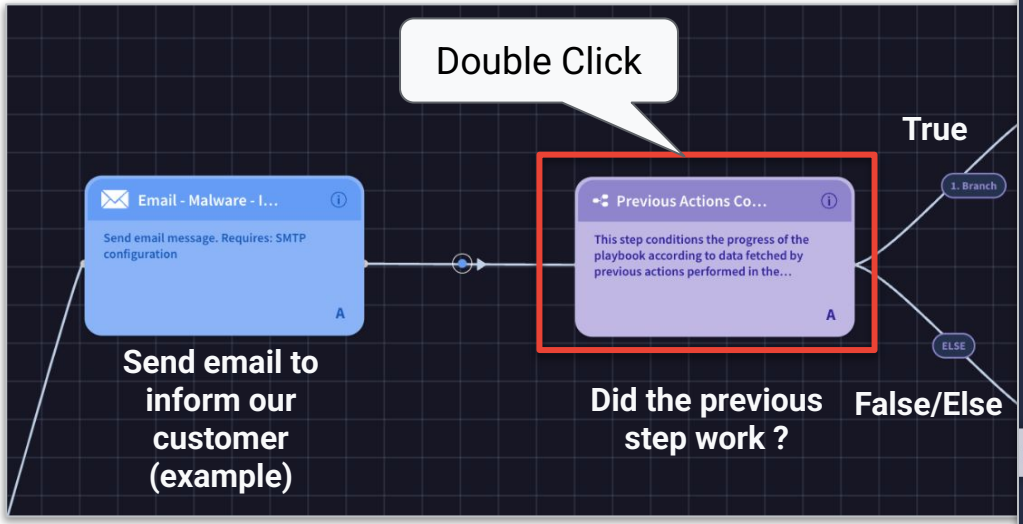


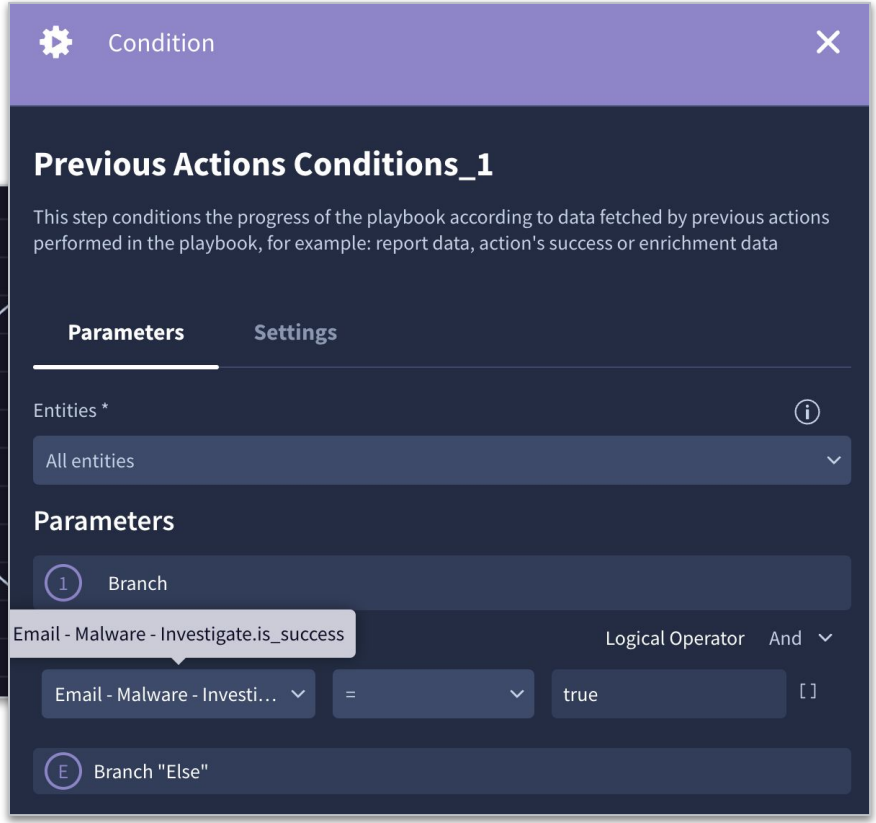
Playbook - Answered No

Google SecOps

Playbook - Answered Yes

Google SecOps





Google

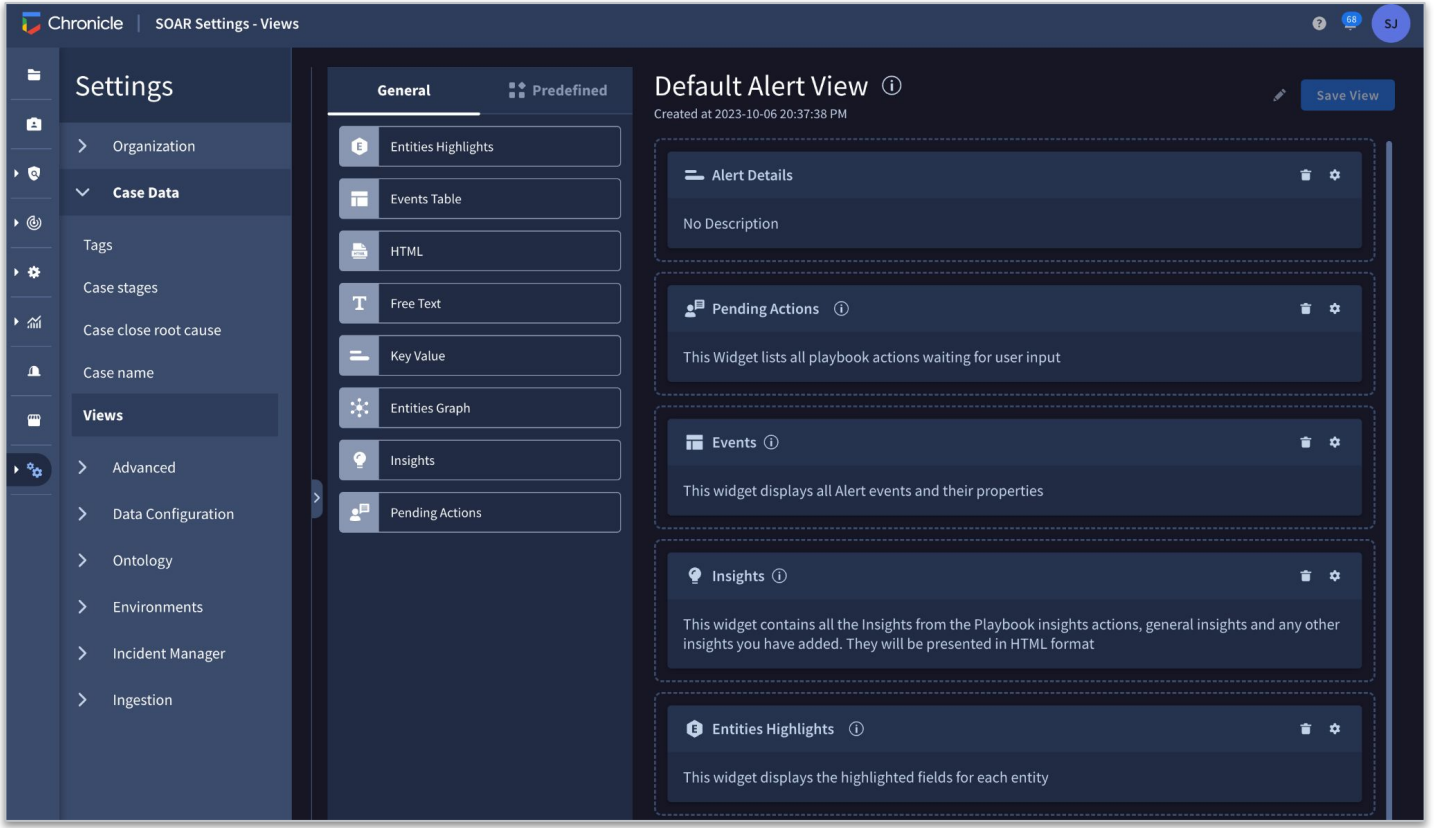
Google SecOps

Alert Views

Google

Alert View

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

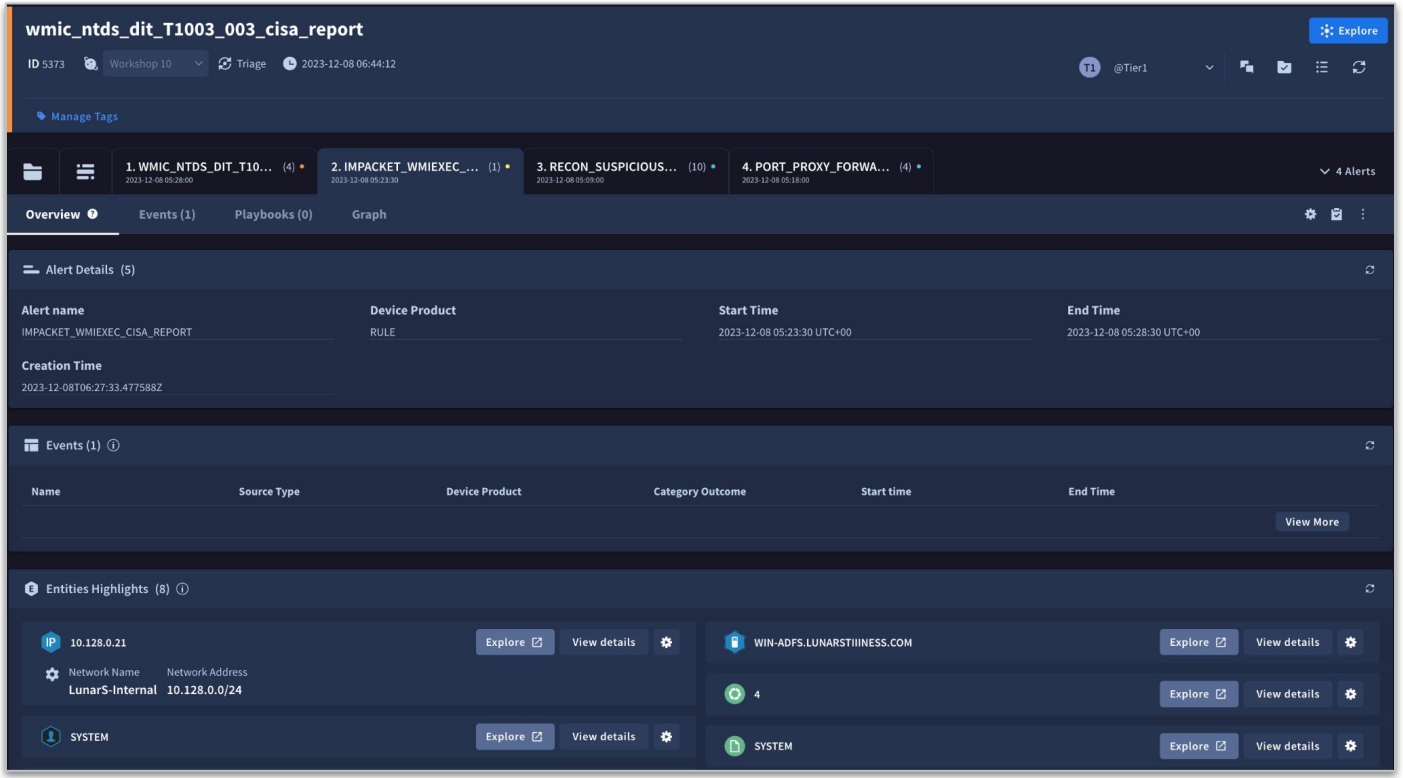


Default Alert View

Google SecOps

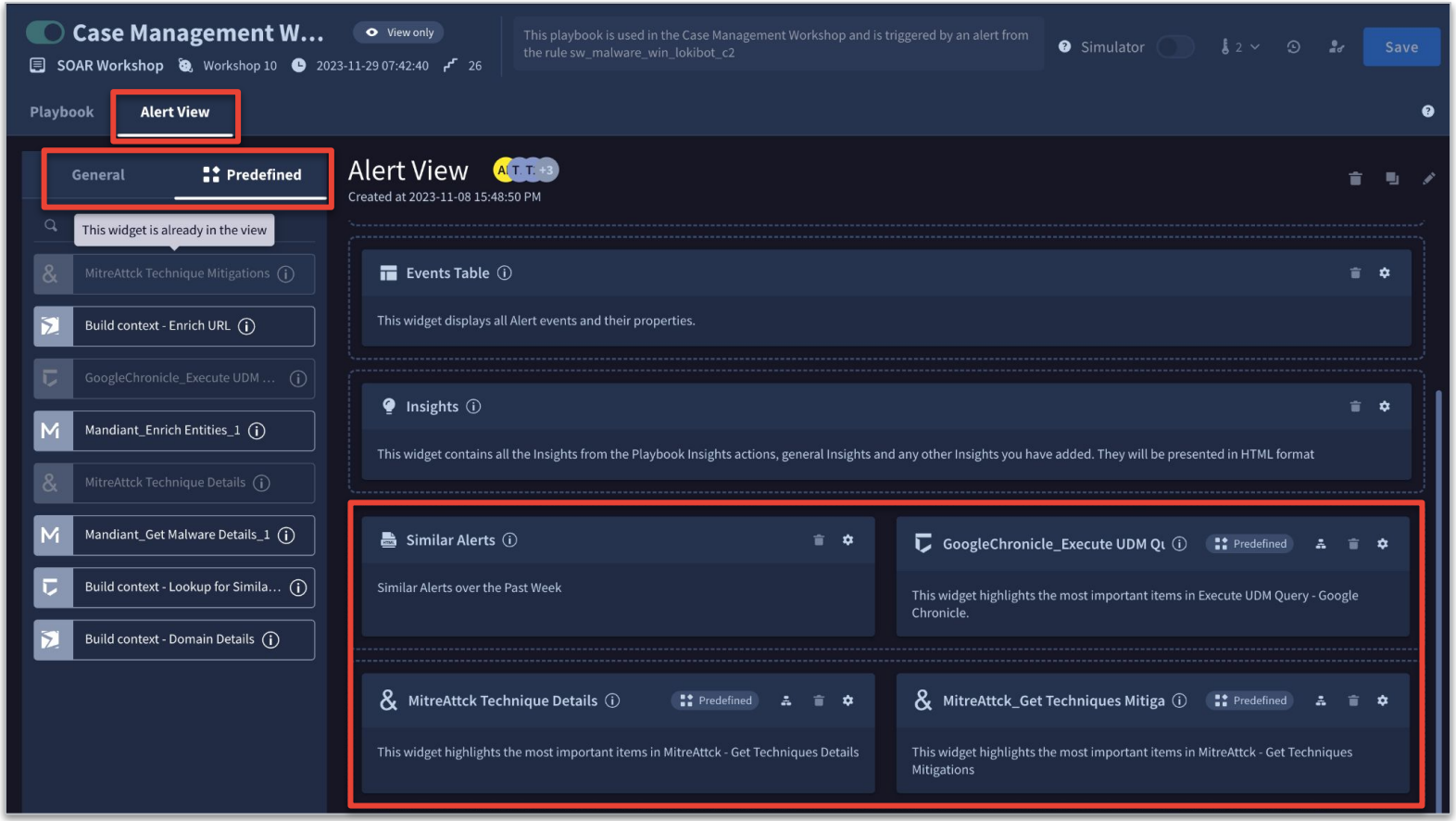
If the widget has values, they will display, otherwise they will not

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



Playbook Alert View

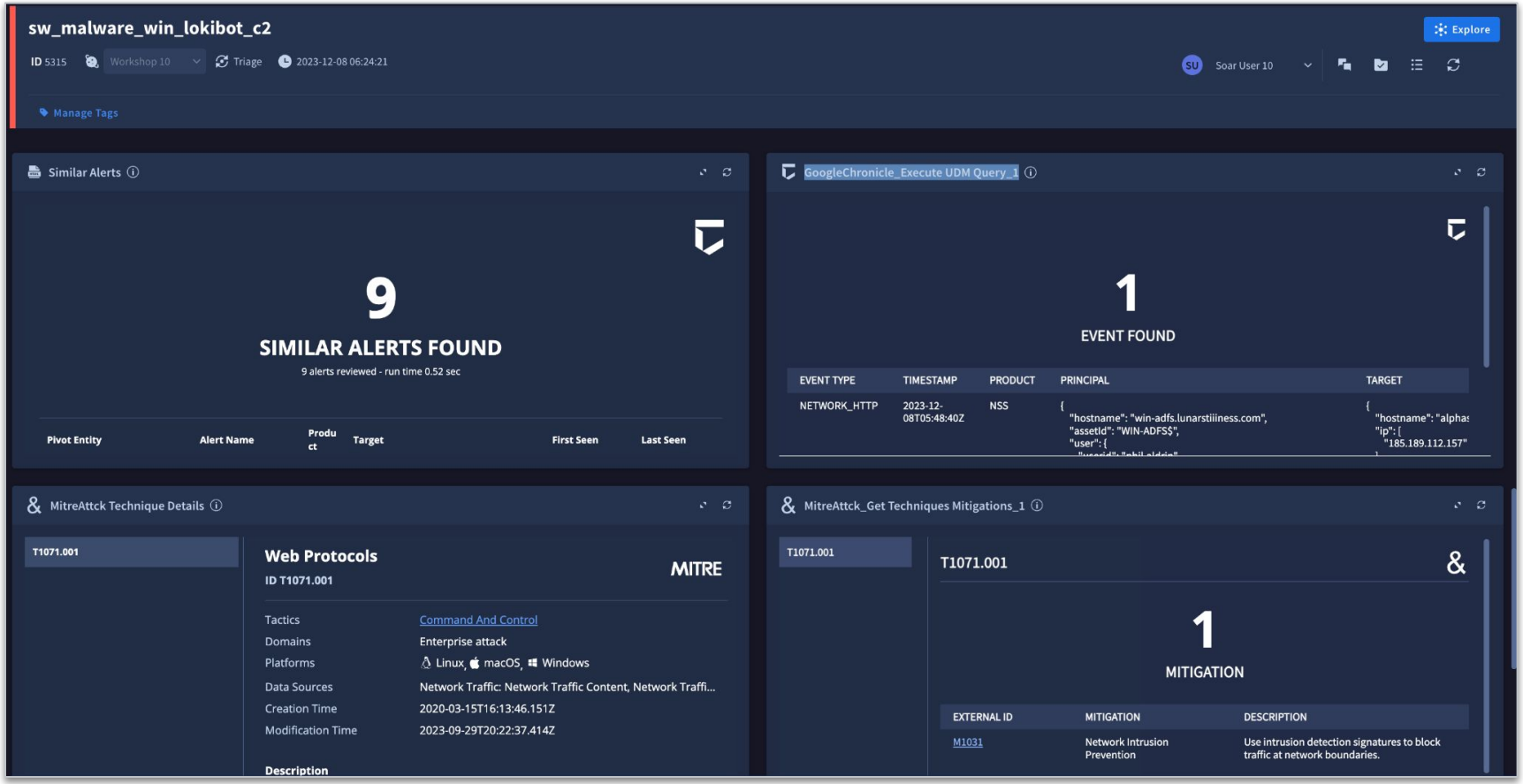
Google SecOps



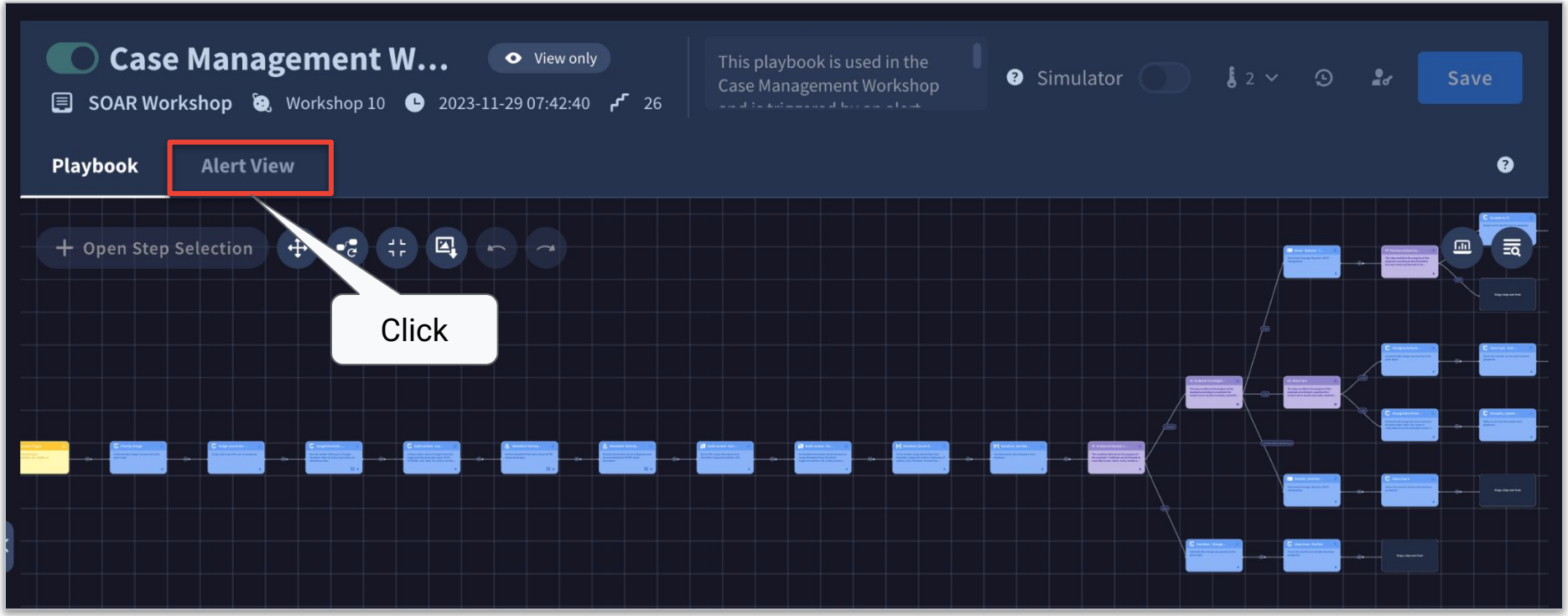
Google

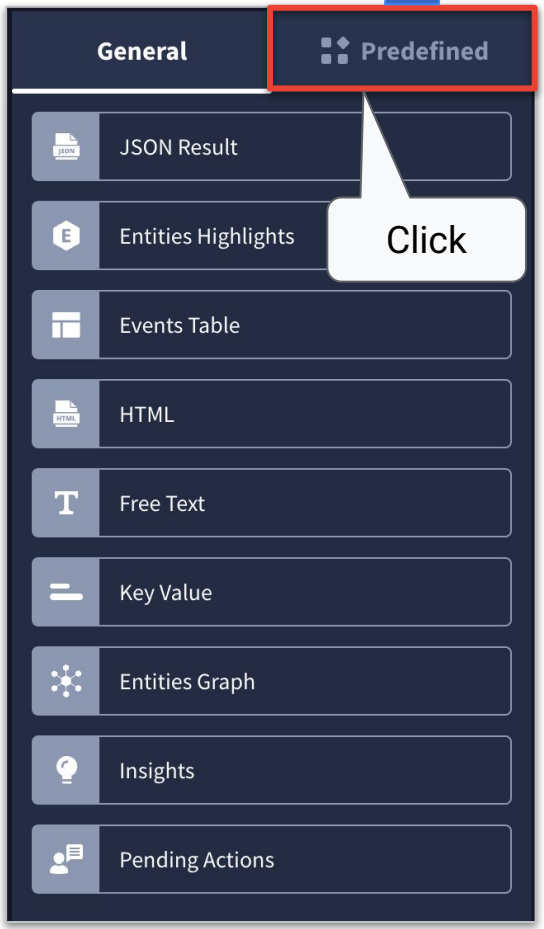
Alert with Playbook Specific Widgets

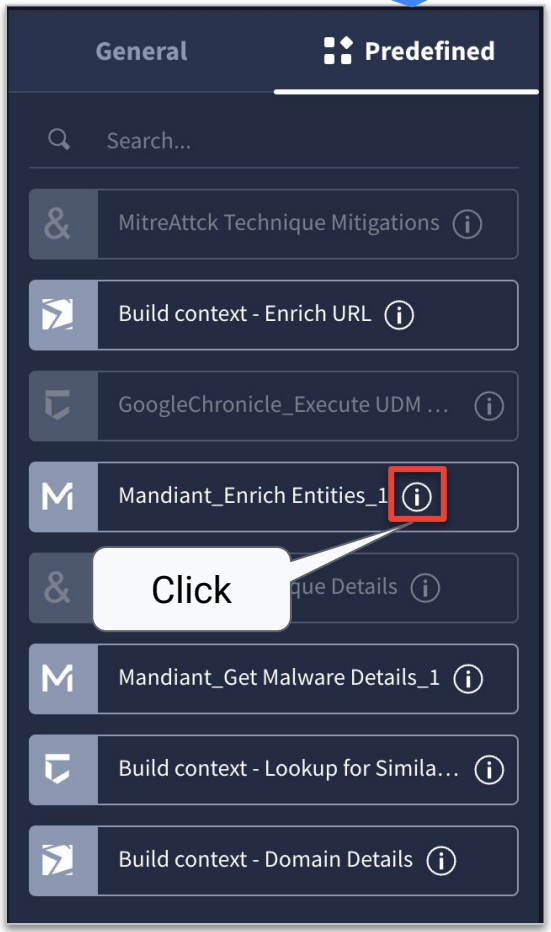
Google SecOps



Google

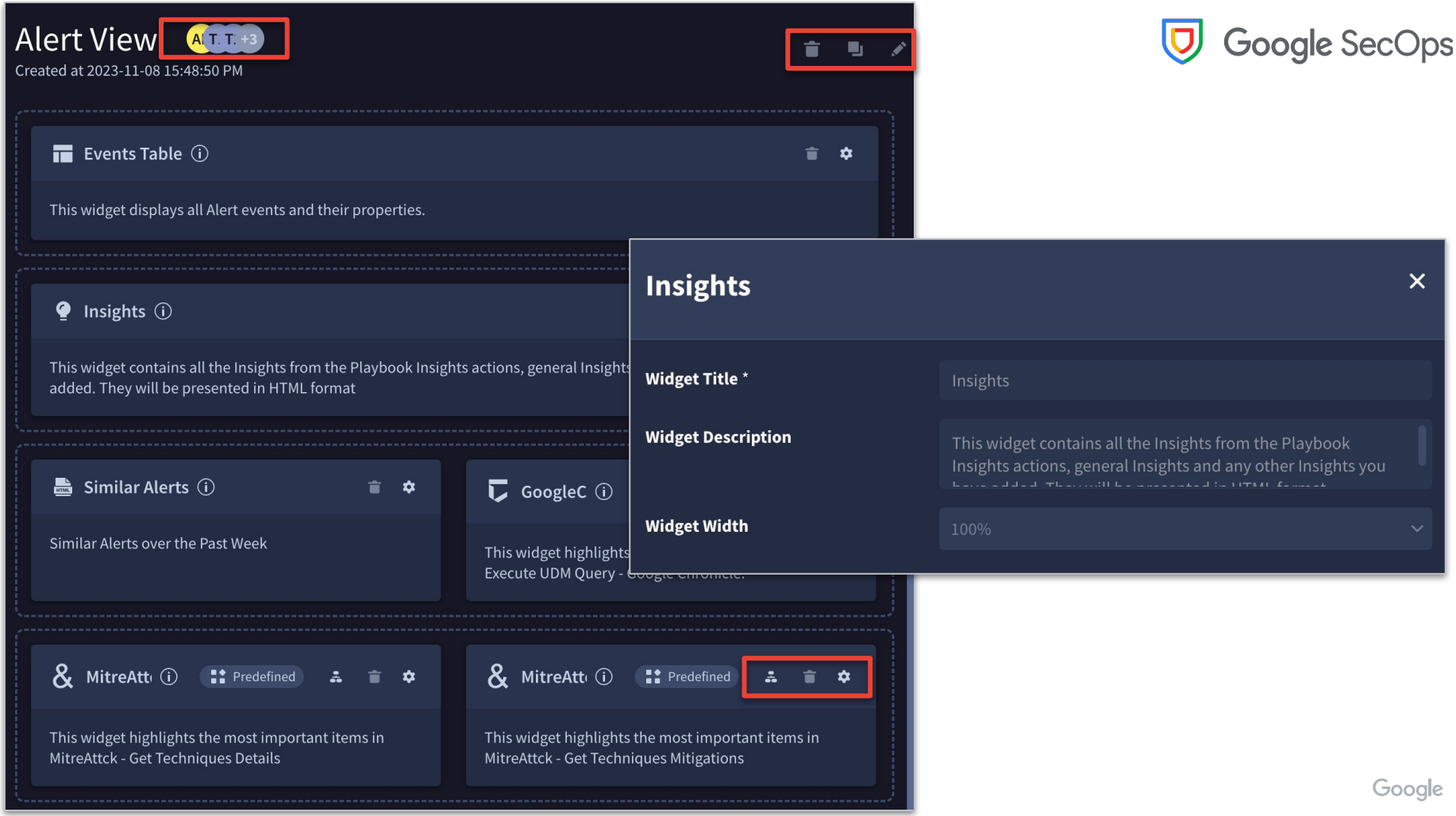

Case Management W...
View only
SOAR Workshop
Workshop 10
2023-11-29 07:42:40
26
This playbook is used in the Case Management Workshop
Simulator
2
Save
Playbook
Alert View
Open Step Selection
Click


General
Predefined
JSON Result
Entities Highlights
Click
Events Table
HTML
Free Text
Key Value
Entities Graph
Insights
Pending Actions


General
Predefined
Search...
MitreAttck Technique Mitigations
Build context - Enrich URL
GoogleChronicle_Execute UDM ...
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


Mandiant
Enrich Entities
Enrich IOCs
Get Malware Details
Get Related Entities



Google SecOps

Google

Exercise: Explore the Alert View Configuration

Google SecOps

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

Google SecOps

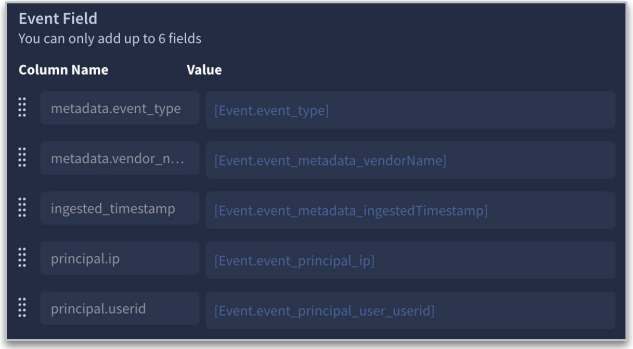
What fields are used to populate the Alert Details widget?

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**



Google SecOps

Playbook Simulator

Google

Playbook Simulator

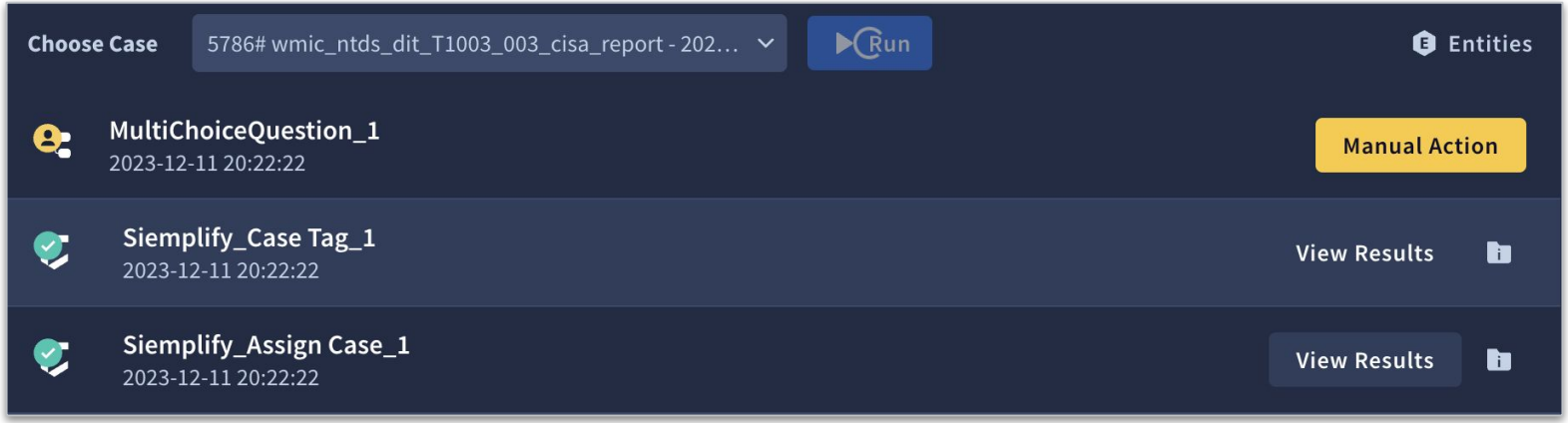
Google SecOps

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

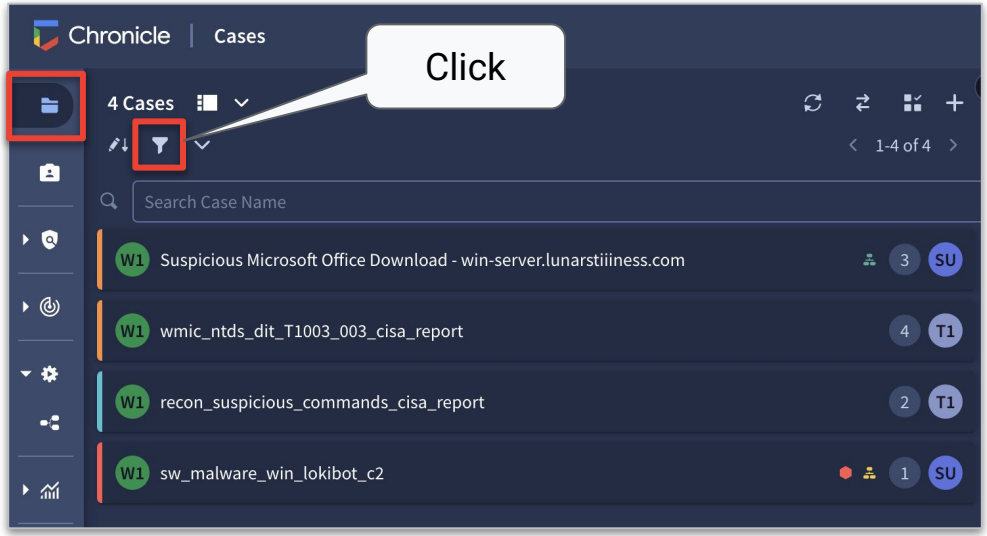
Does not change the existing cases or alerts

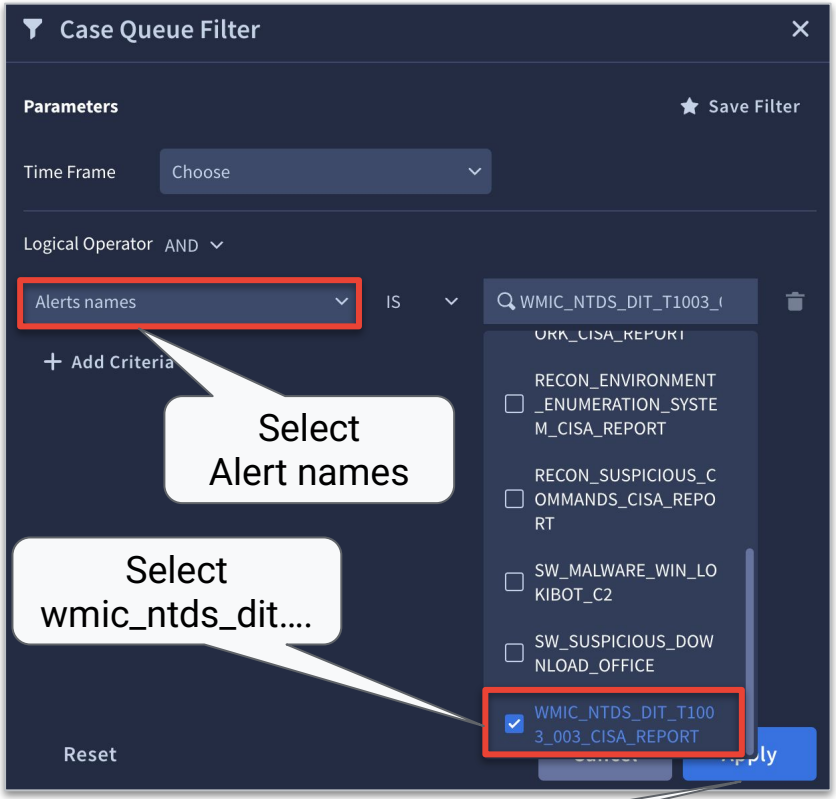
Simulator processes the steps and provides results for review



Ingest Alert as Test Case

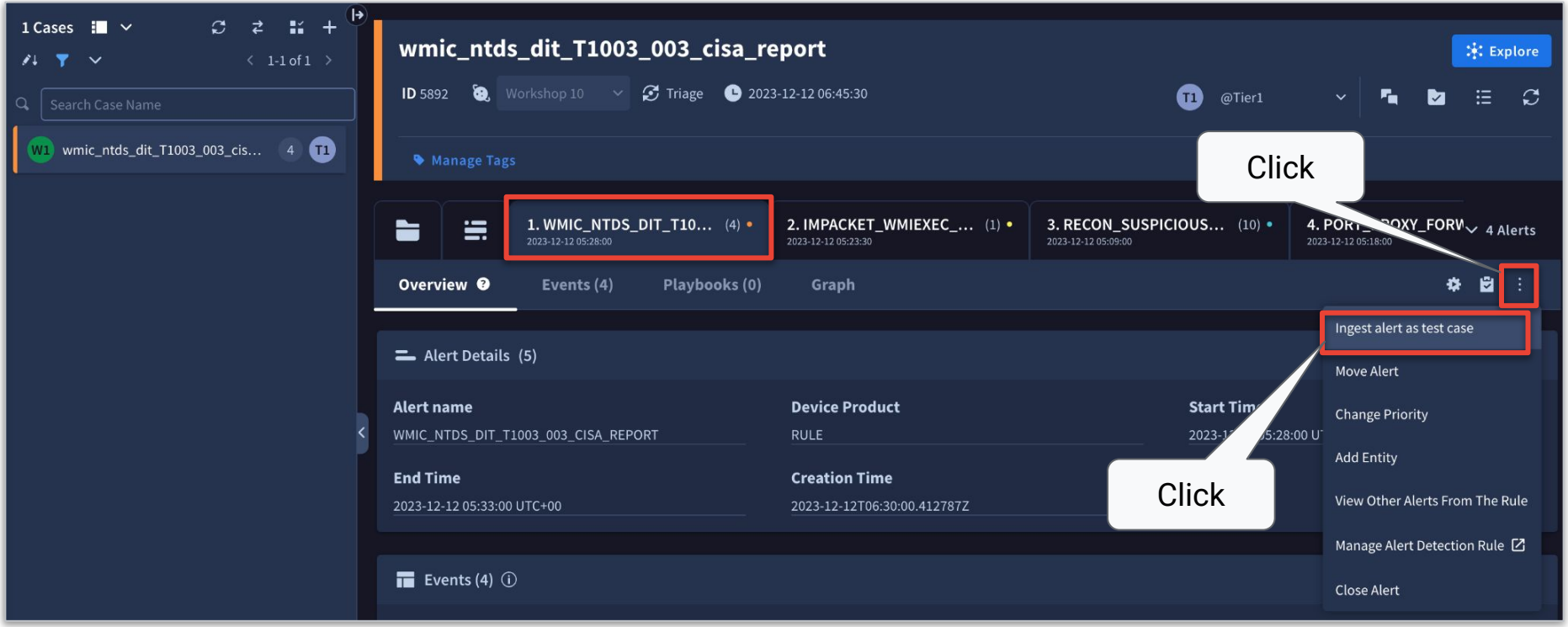
Google SecOps





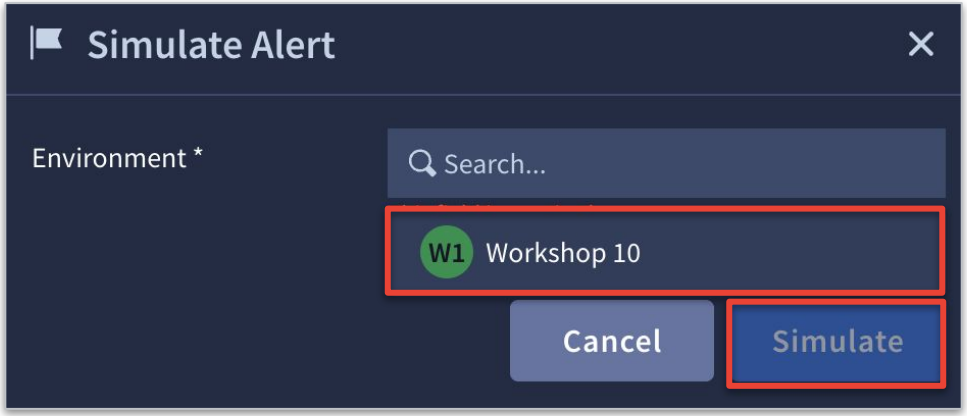
Ingest Alert as Test Case

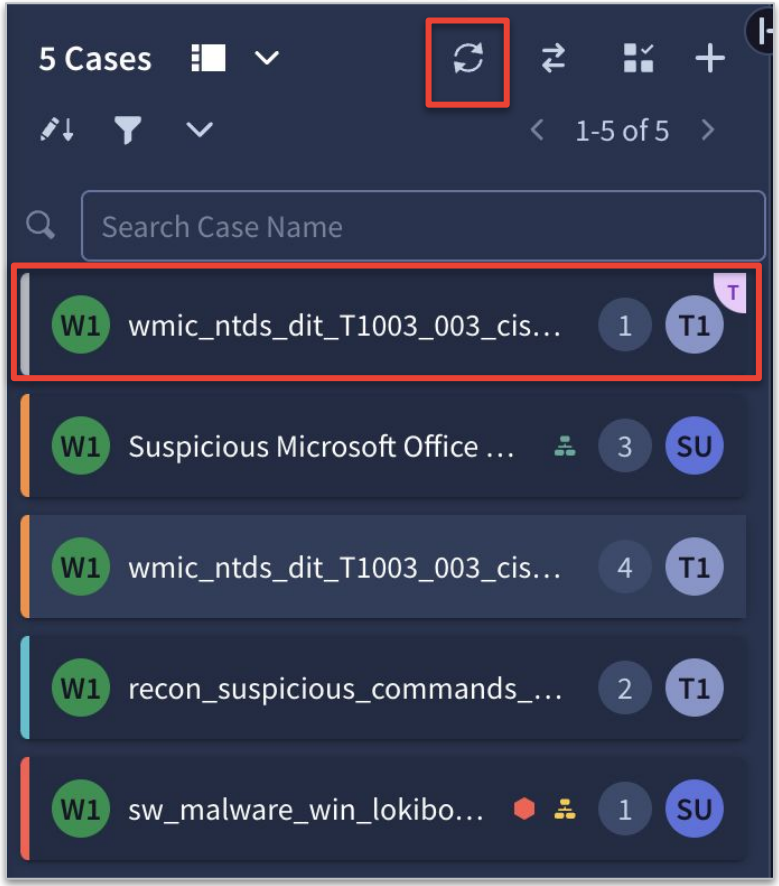
Google SecOps

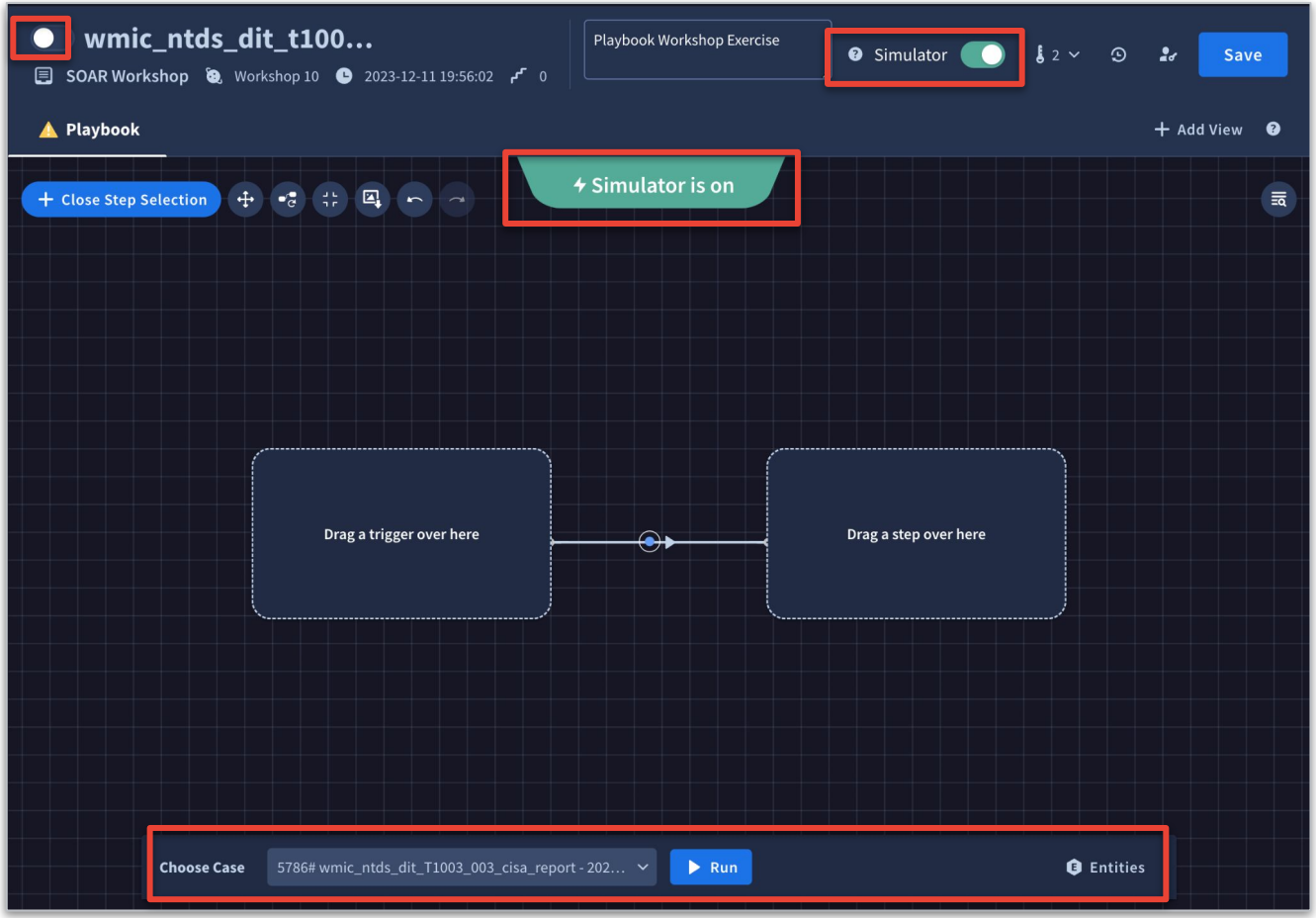


Ingest Alert as Test Case

Google SecOps

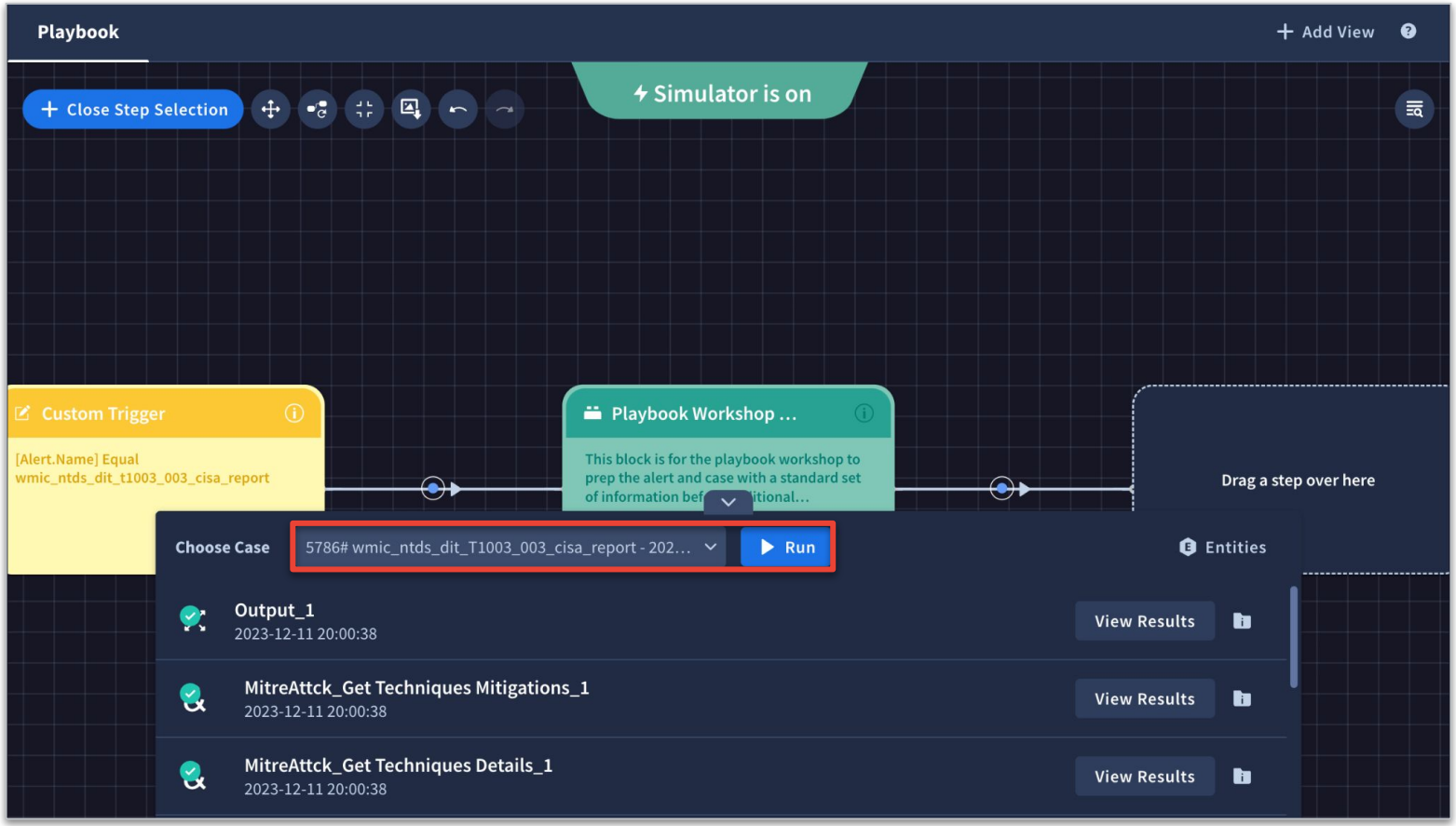





wmic_ntds_dit_t100...
SOAR Workshop
Workshop 10
2023-12-11 19:56:02
0
Playbook Workshop Exercise
Simulator
2
Save
Playbook
Add View
Close Step Selection
Simulator is on
Drag a trigger over here
Drag a step over here
Choose Case
5786# wmic_ntds_dit_T1003_003_cisa_report - 202...
Run
Entities

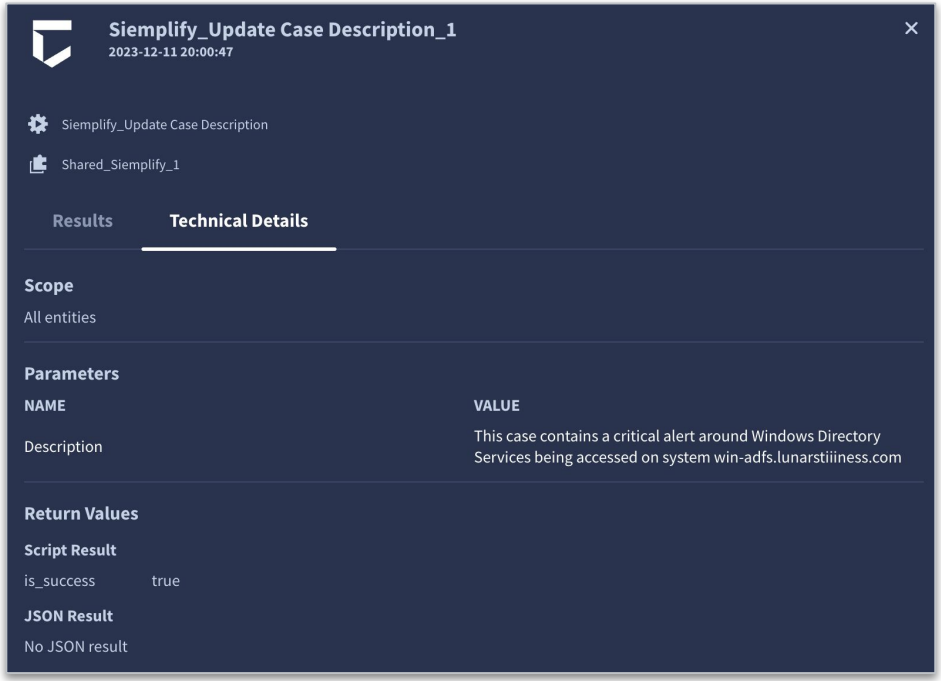
Running a Playbook Simulation

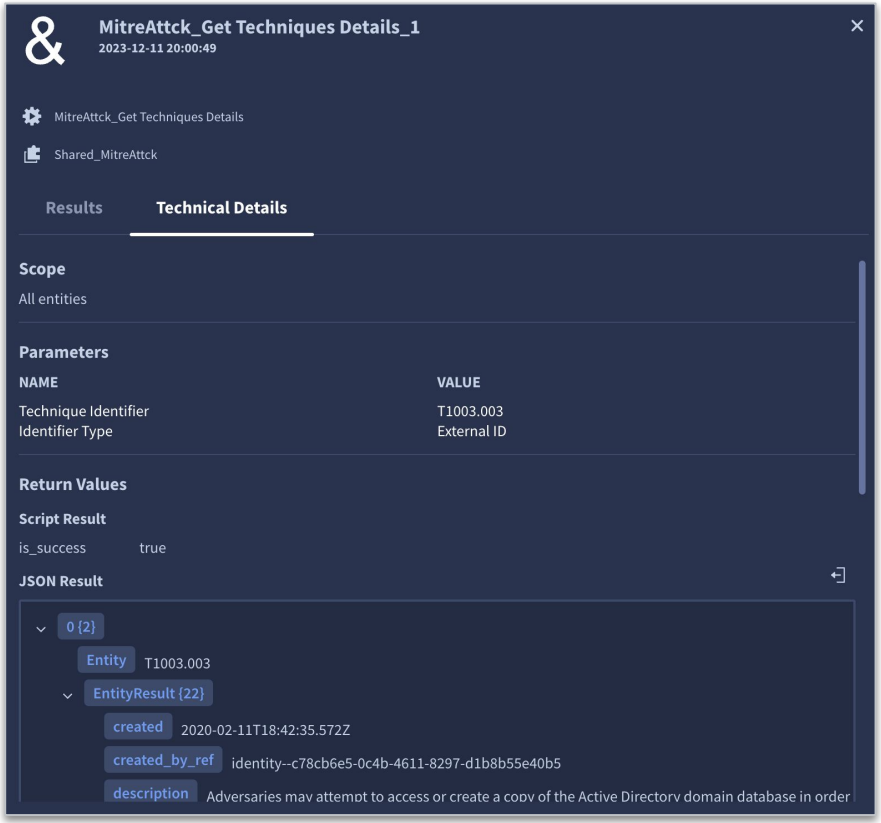
Google SecOps



View Results

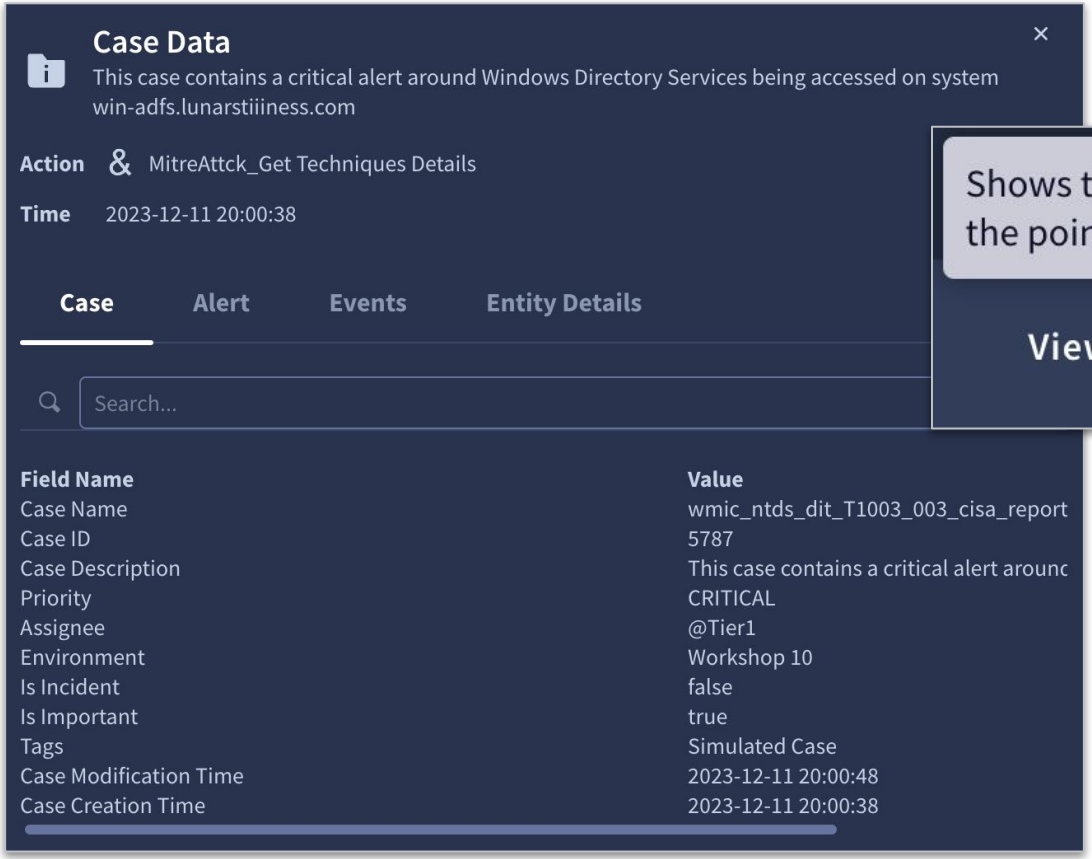
Google SecOps

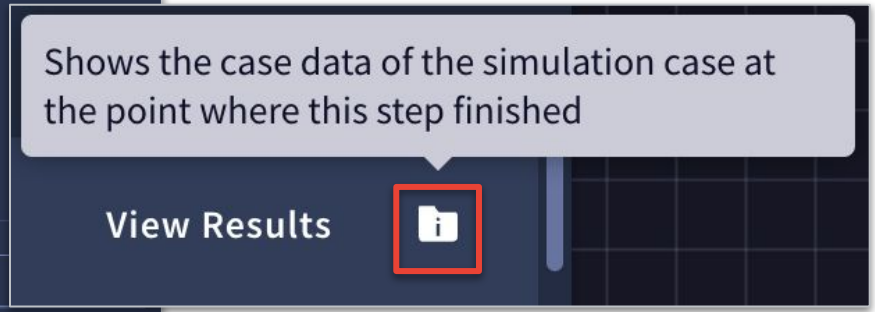




Case Data

Google SecOps

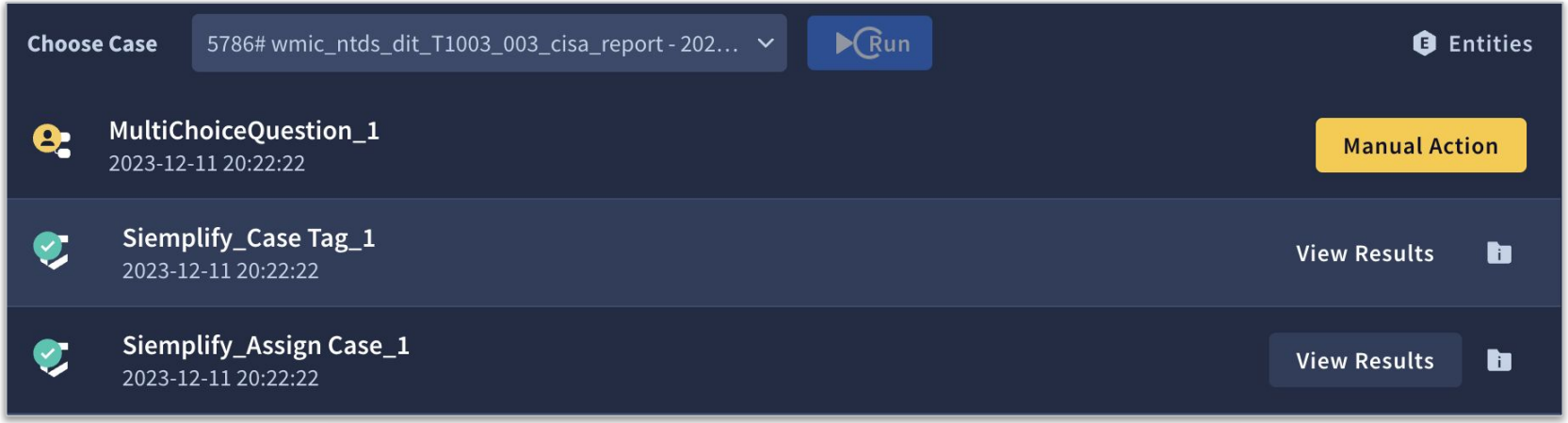


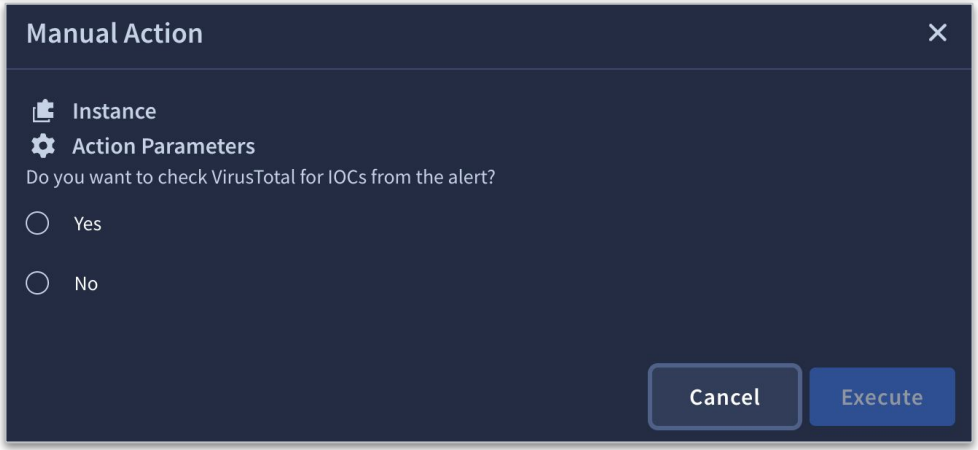


Google

Manual Action

Google SecOps

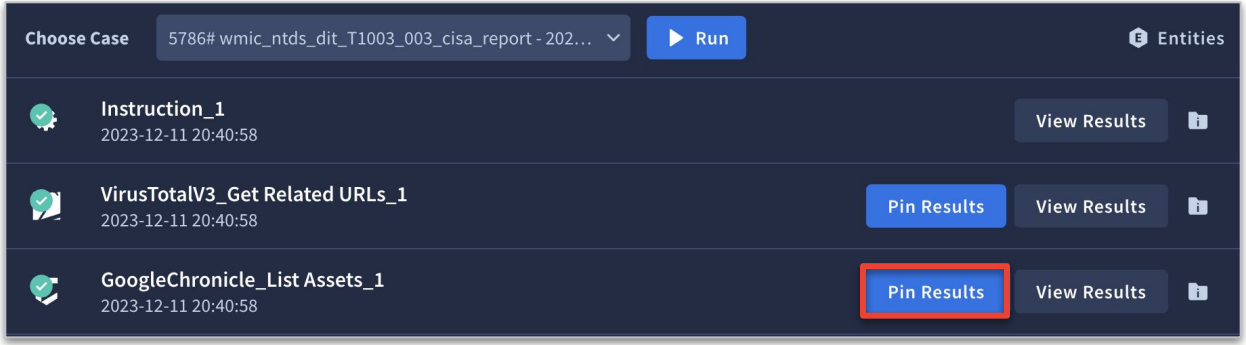


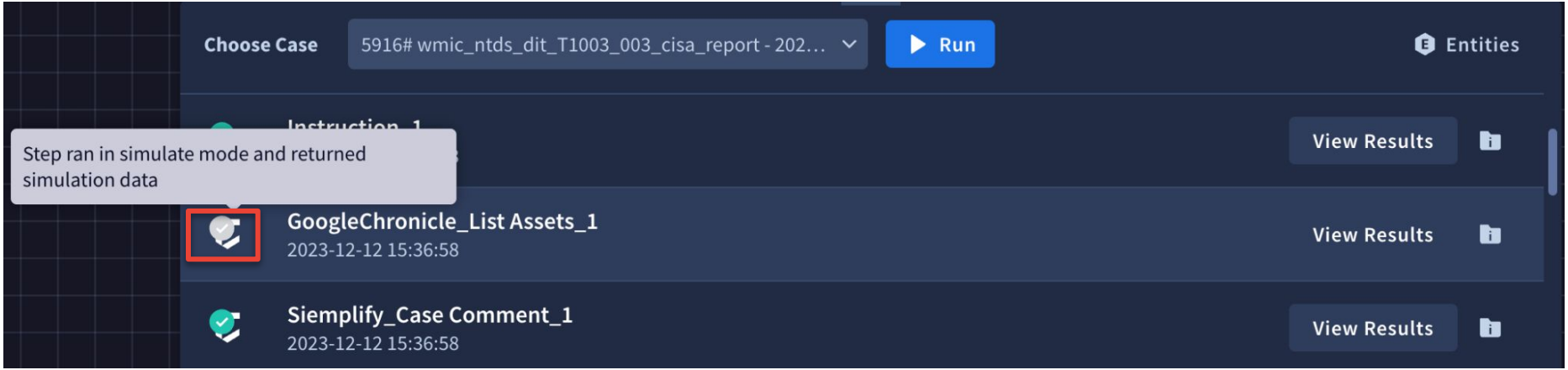


Google

Pin Results

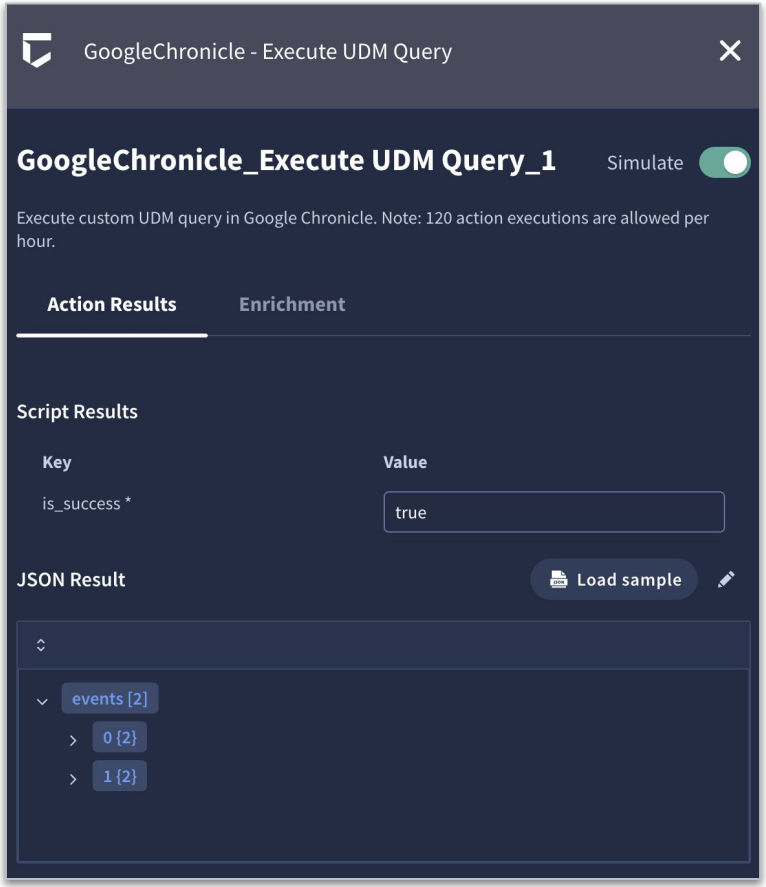
Google SecOps

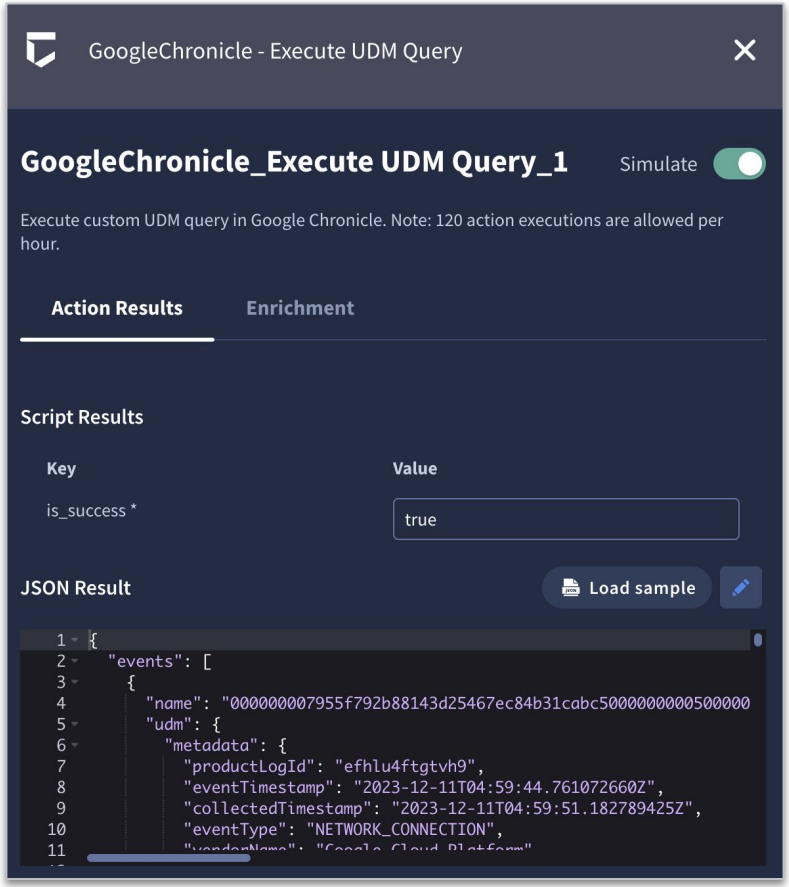




Simulate - Action Step

Google SecOps





Google

Google SecOps

Building Your Own Playbook

Google

Brainstorming Playbooks

Google SecOps

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

Google SecOps

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

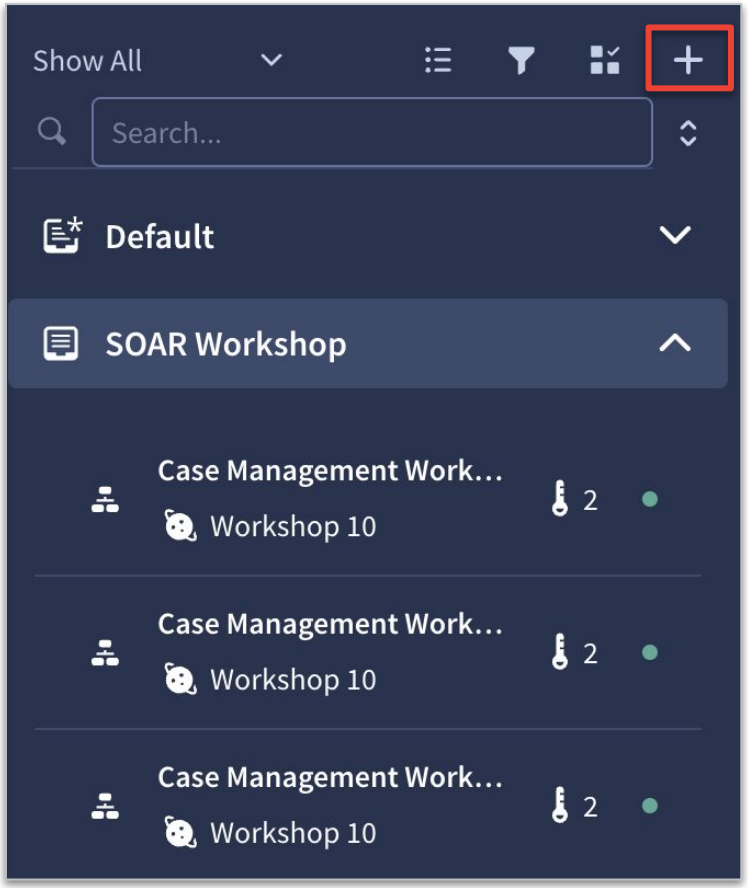
Google SecOps

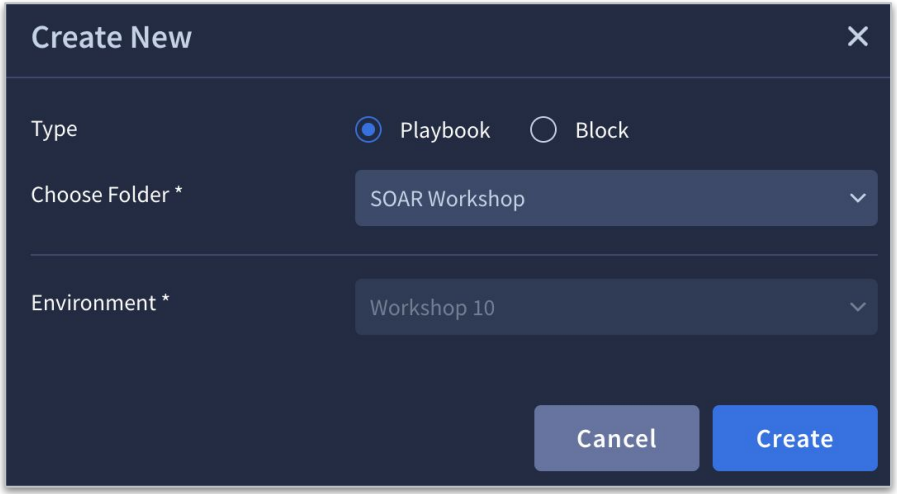
Playbook Exercise Review

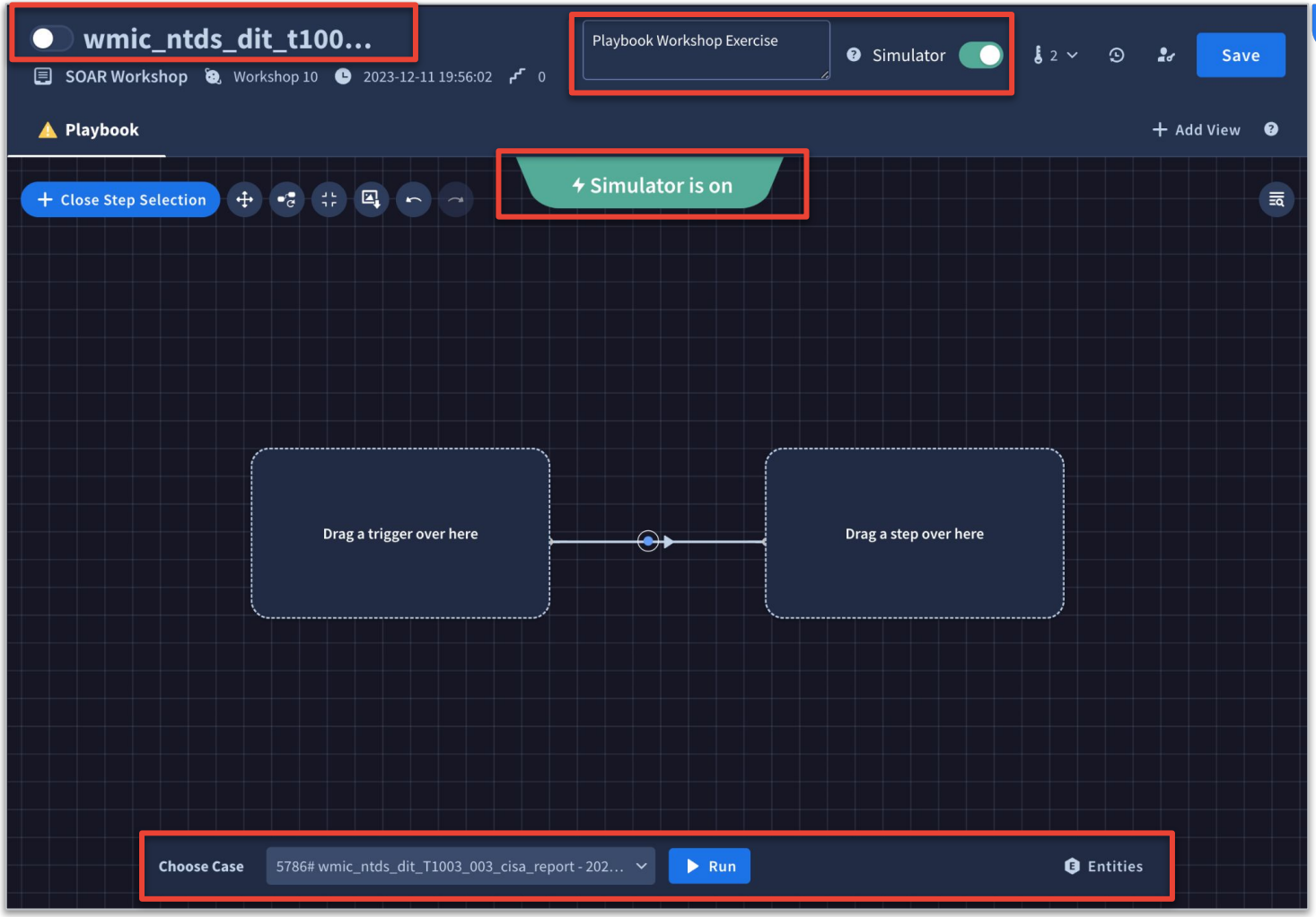
Google

Creating Our Playbook

Google SecOps





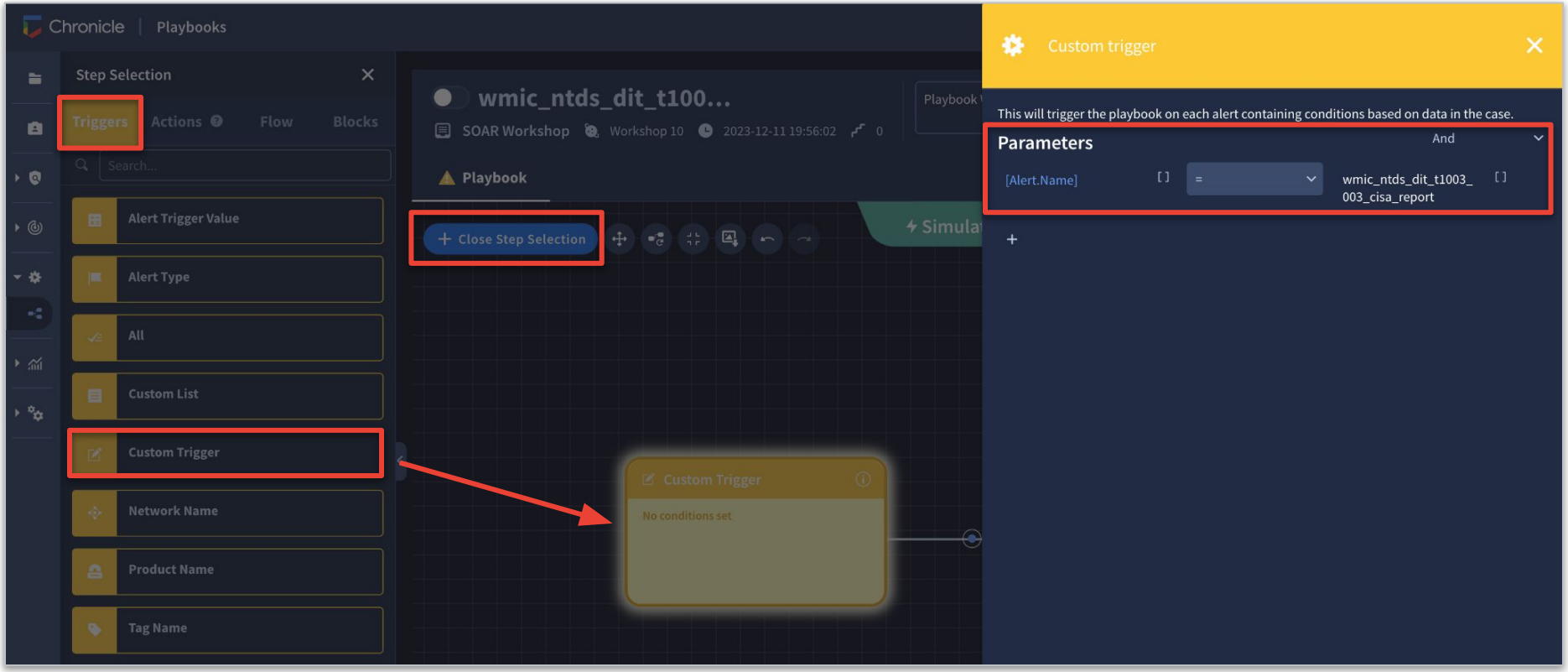


Google SecOps

Google

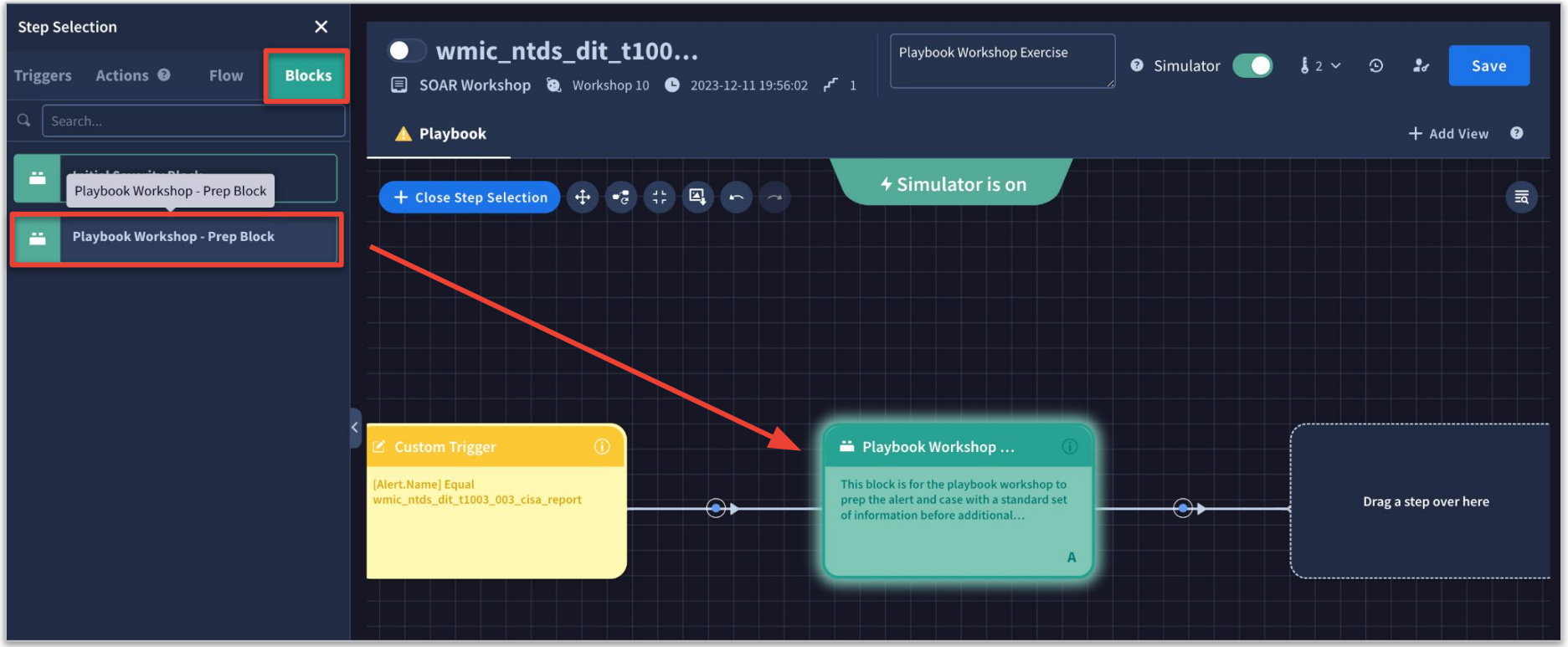
Trigger

Google SecOps



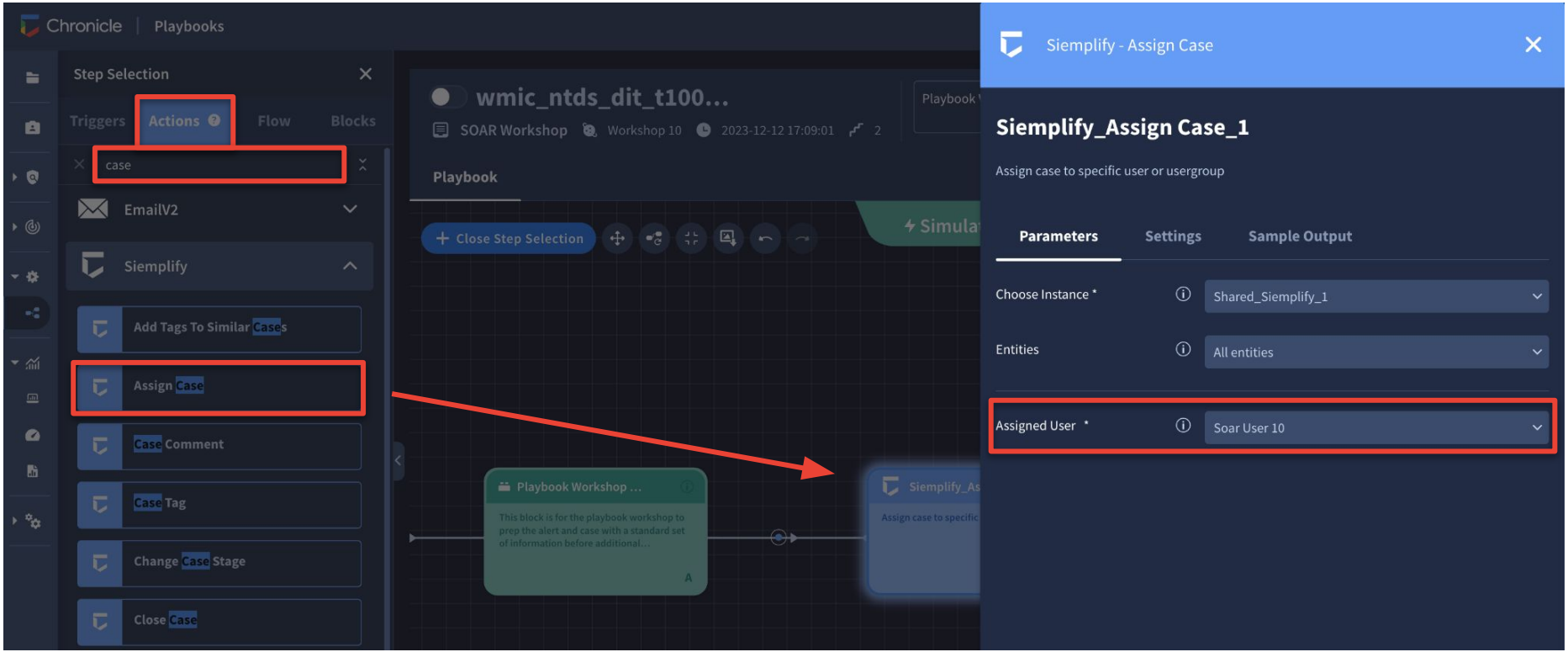
Block

Google SecOps



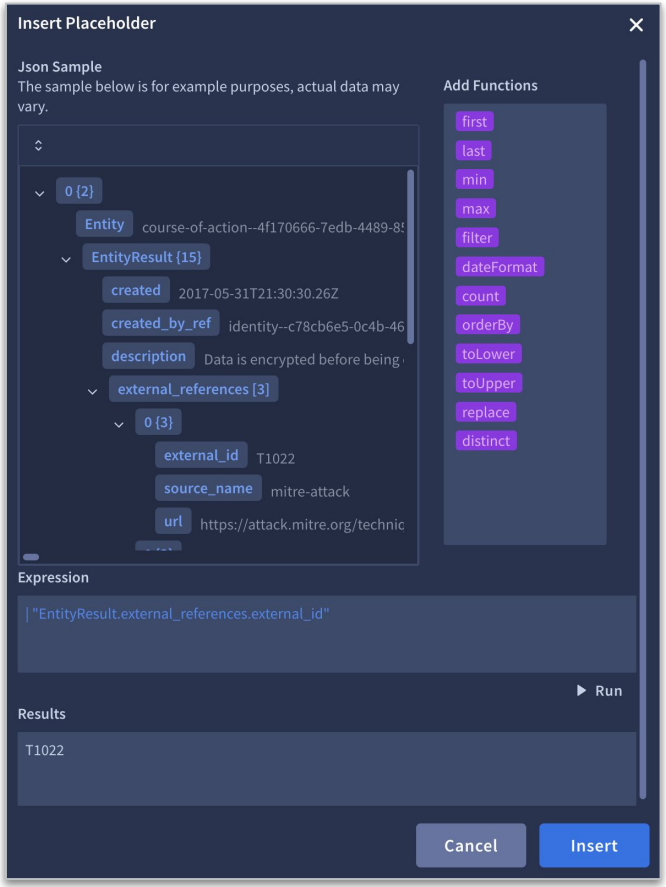
Action - Assign Case

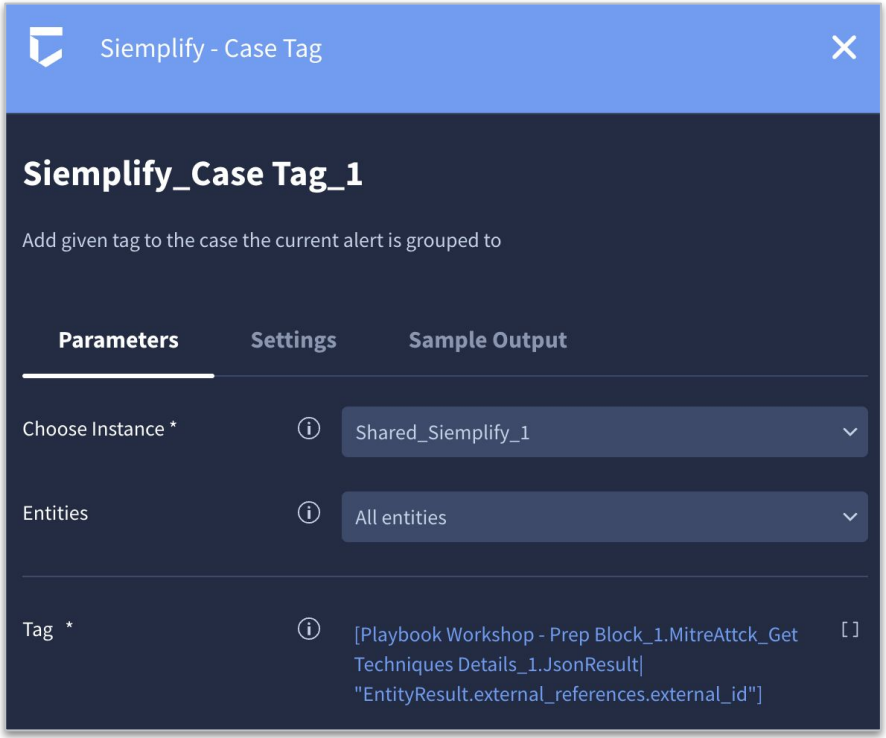
Google SecOps



Action - Tag the Case

Google SecOps

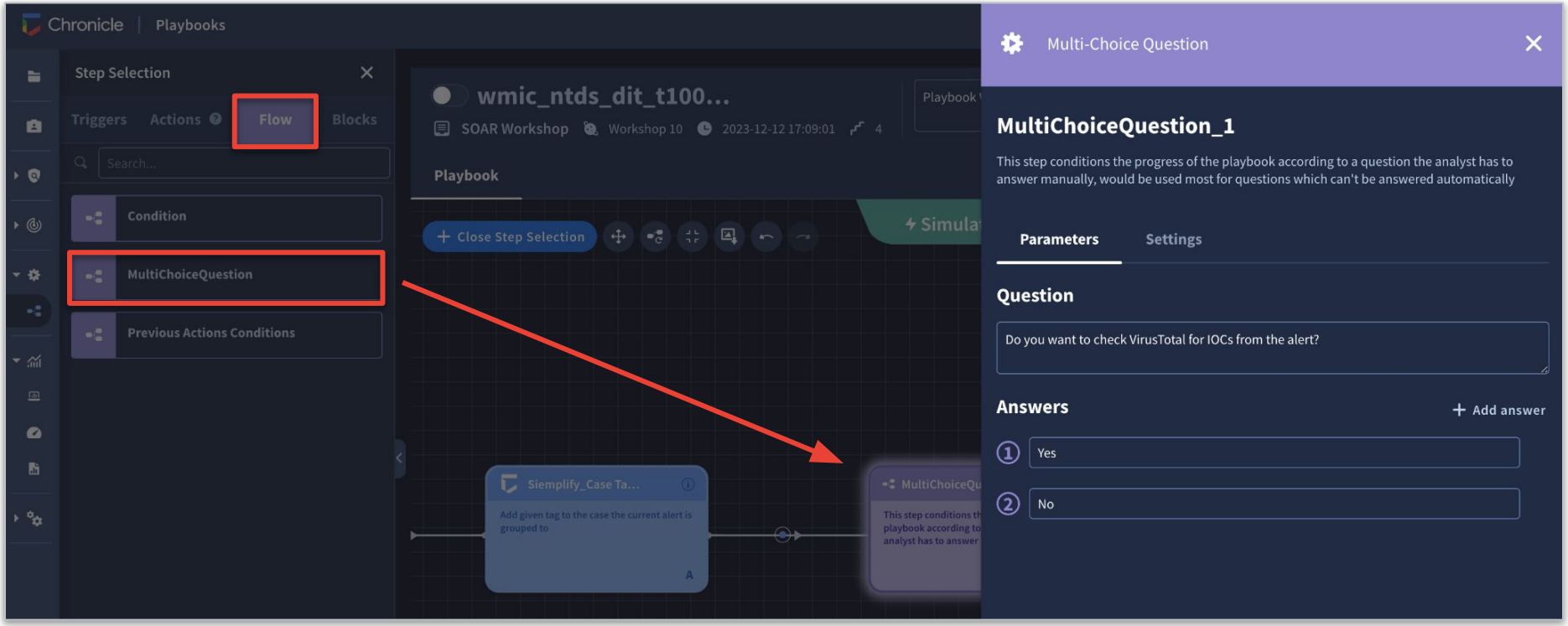




Google

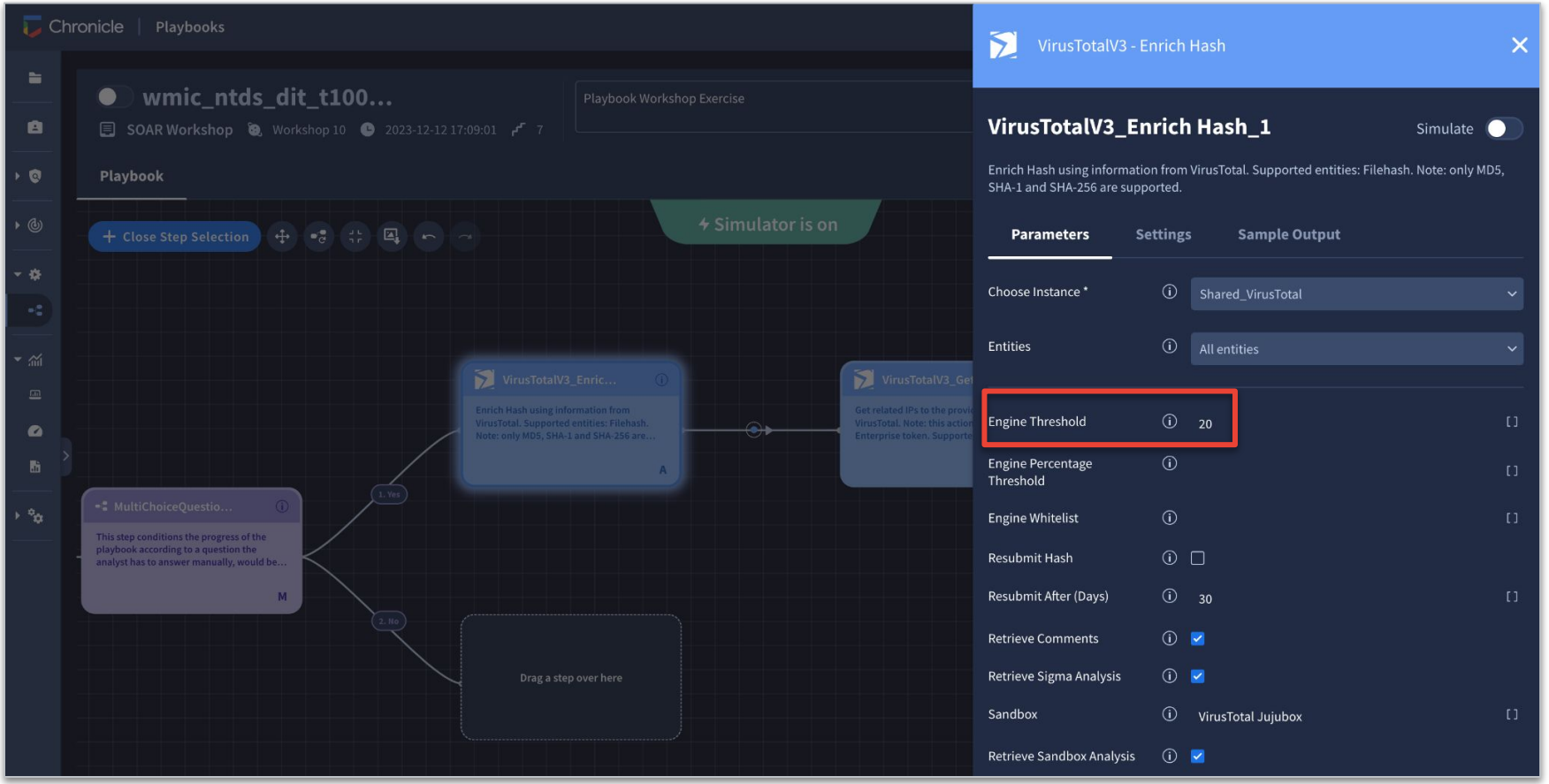
Flow - Multi-Choice Question

Google SecOps



Answer: Yes, VT Enrichment, Related IP/URLs

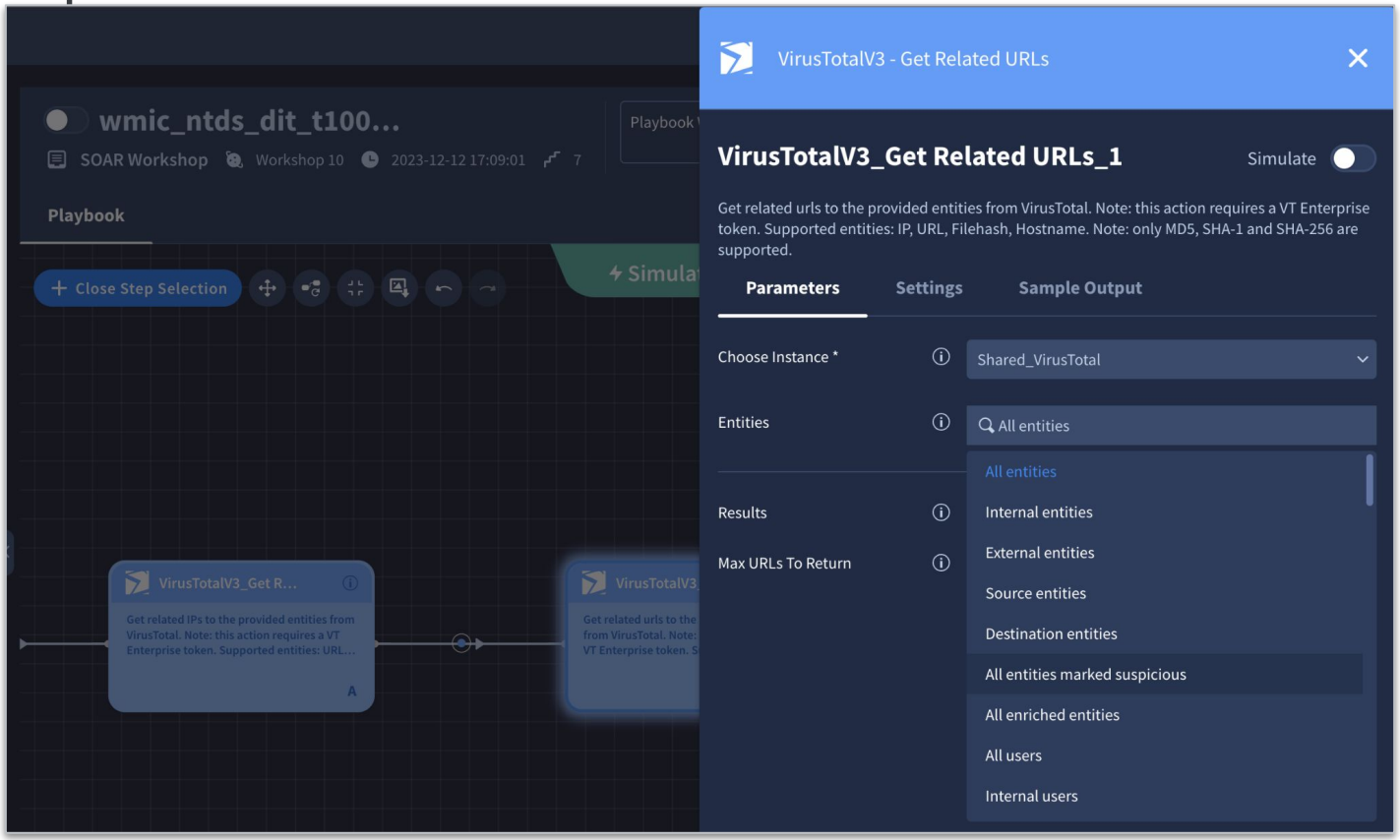
Google SecOps



Google

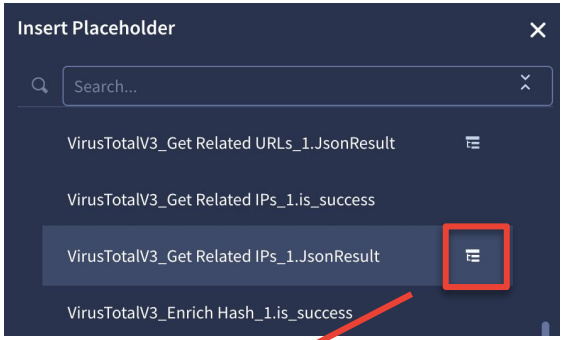
Answer: Yes, Related IP/URLs Only Suspicious Entities

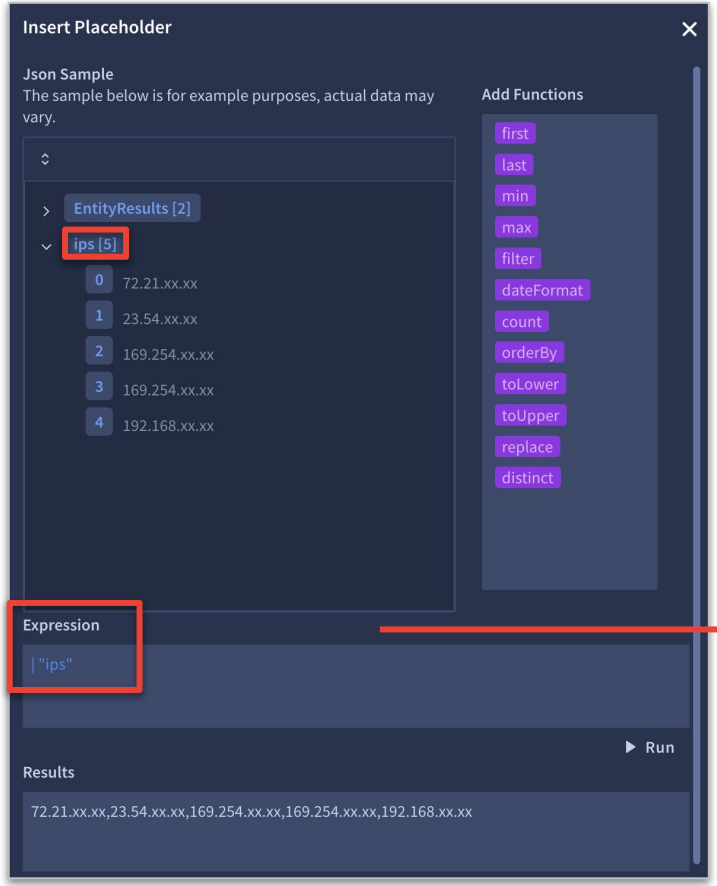
Google SecOps

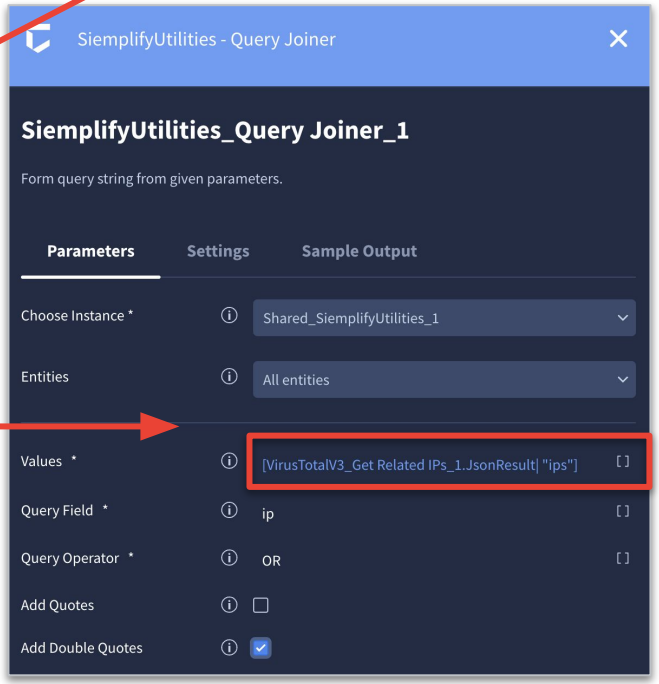


Google

Answer: Yes, Query Joiner

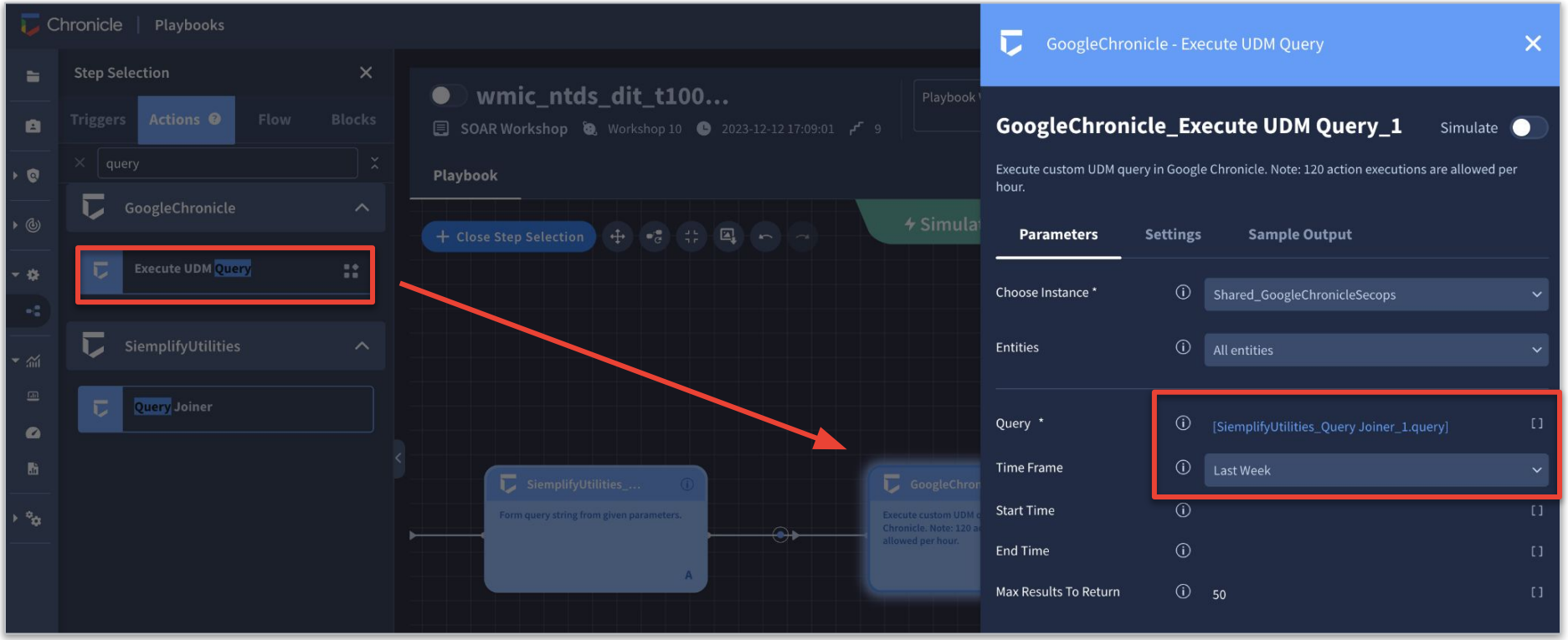






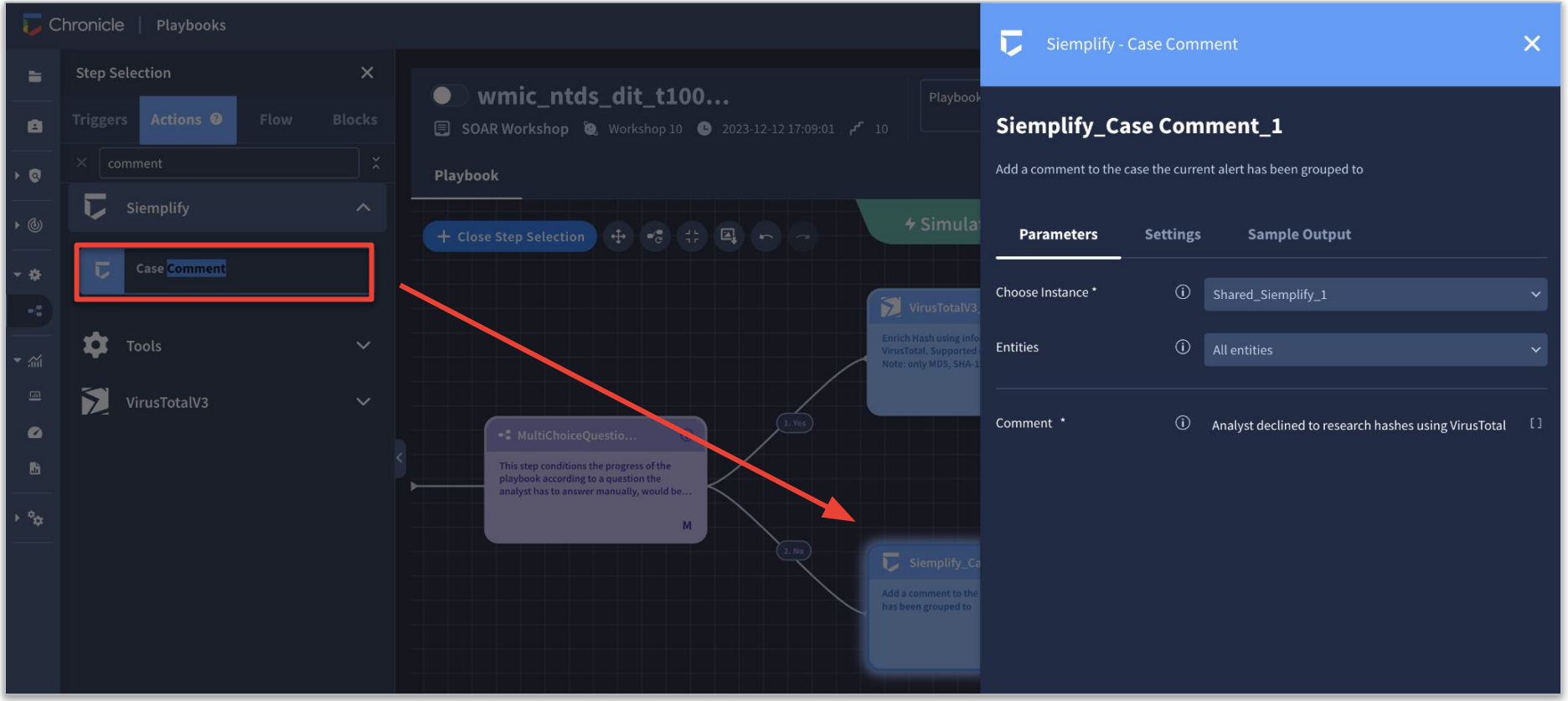
Answer: Yes, Google Chronicle UDM Query

Google SecOps



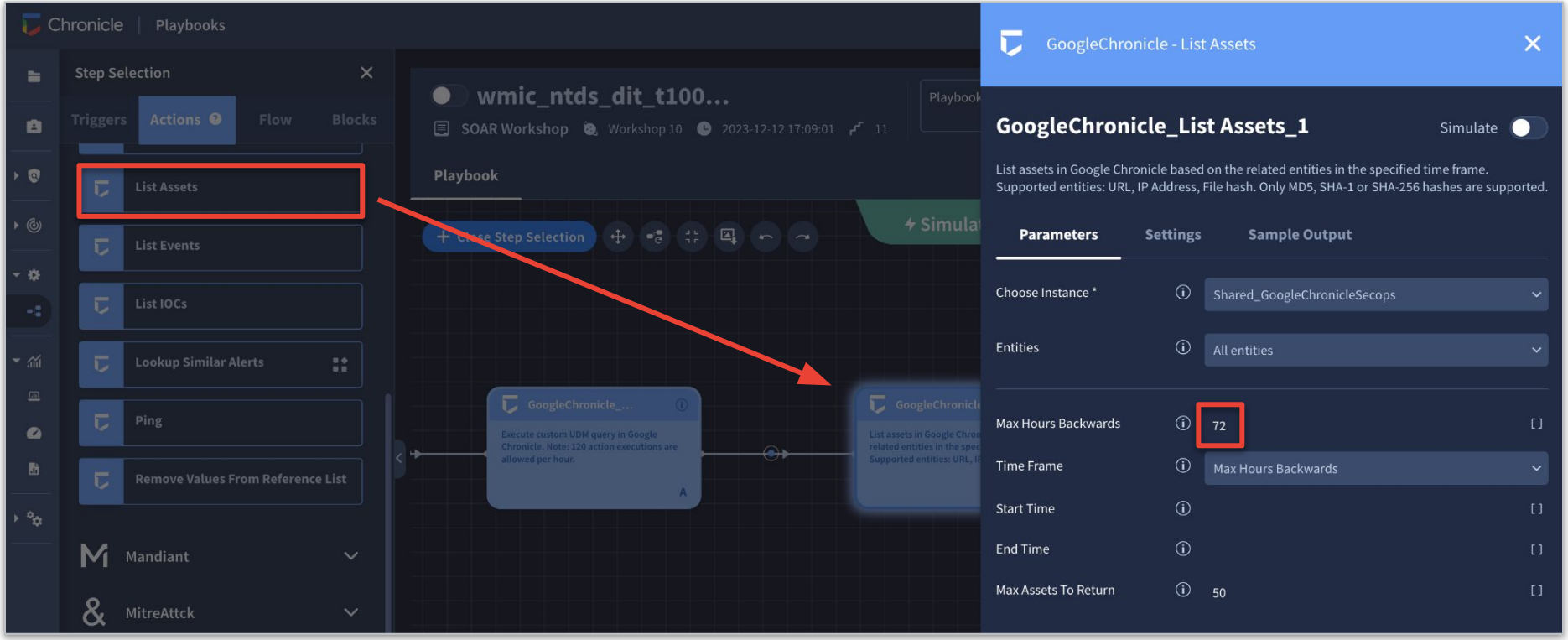
Answer: No, Case Comment

Google SecOps



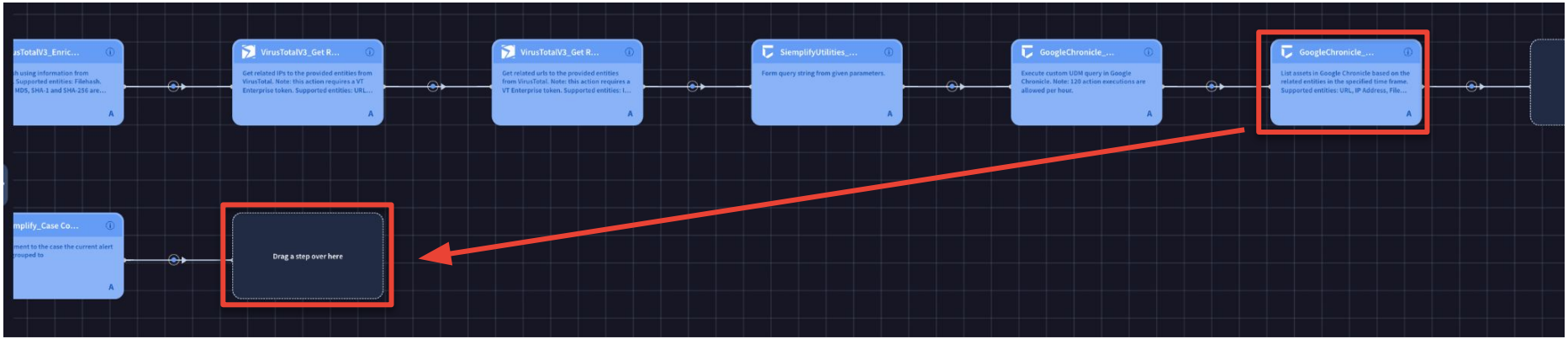
Action - Google Chronicle List Assets

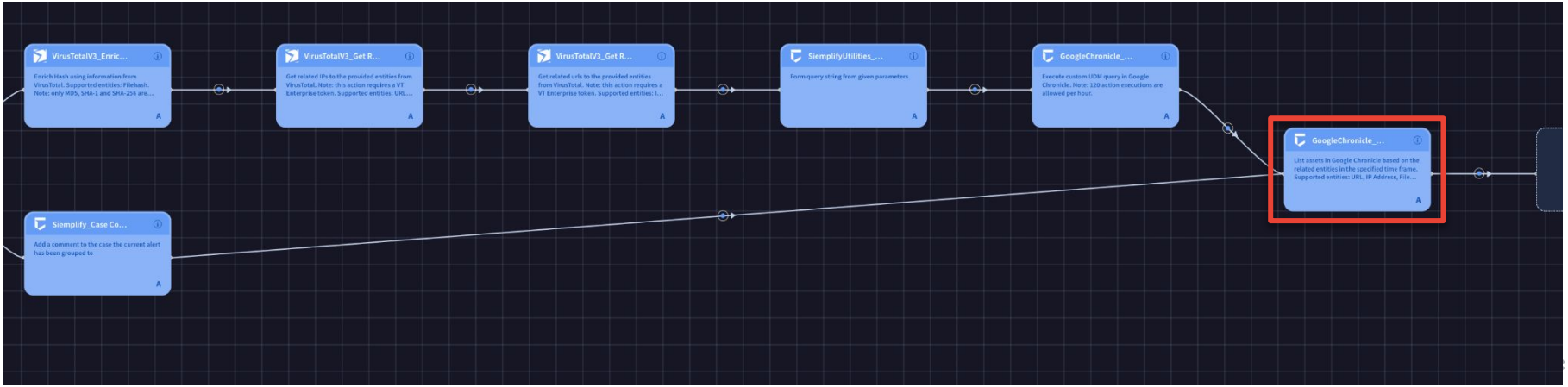
Google SecOps



Merging Paths

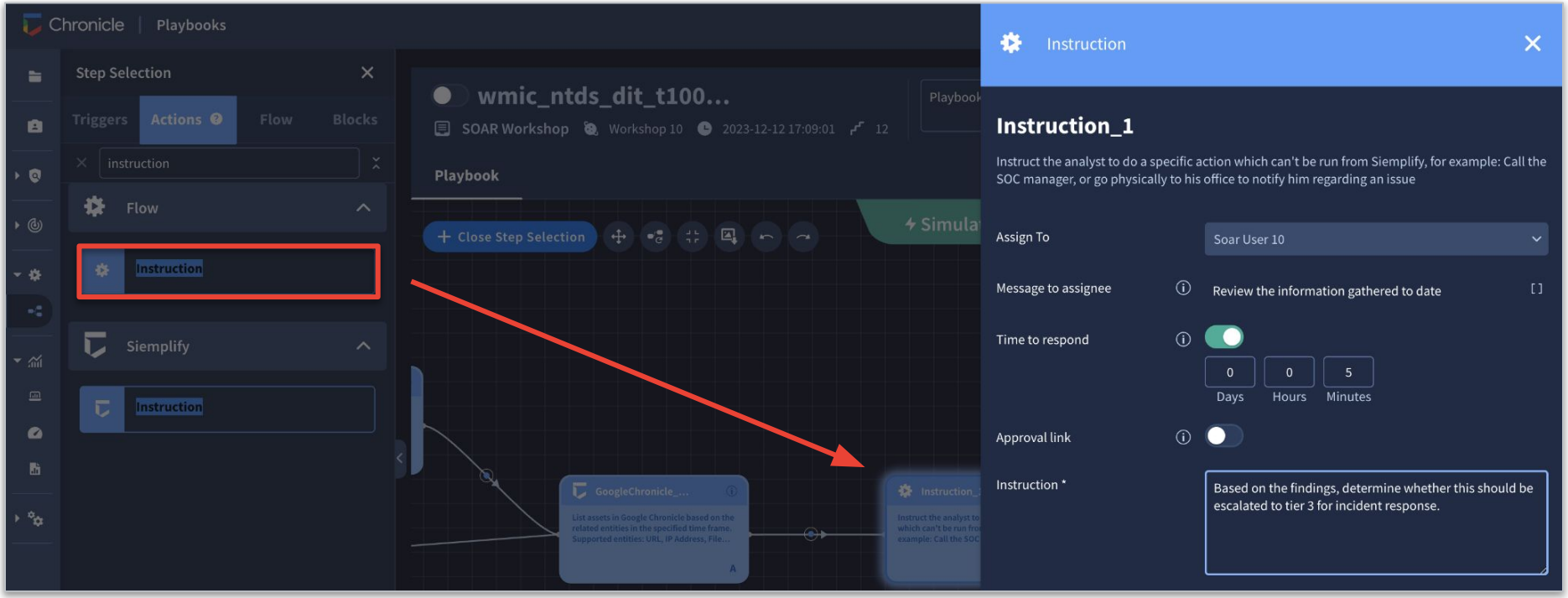
Google SecOps





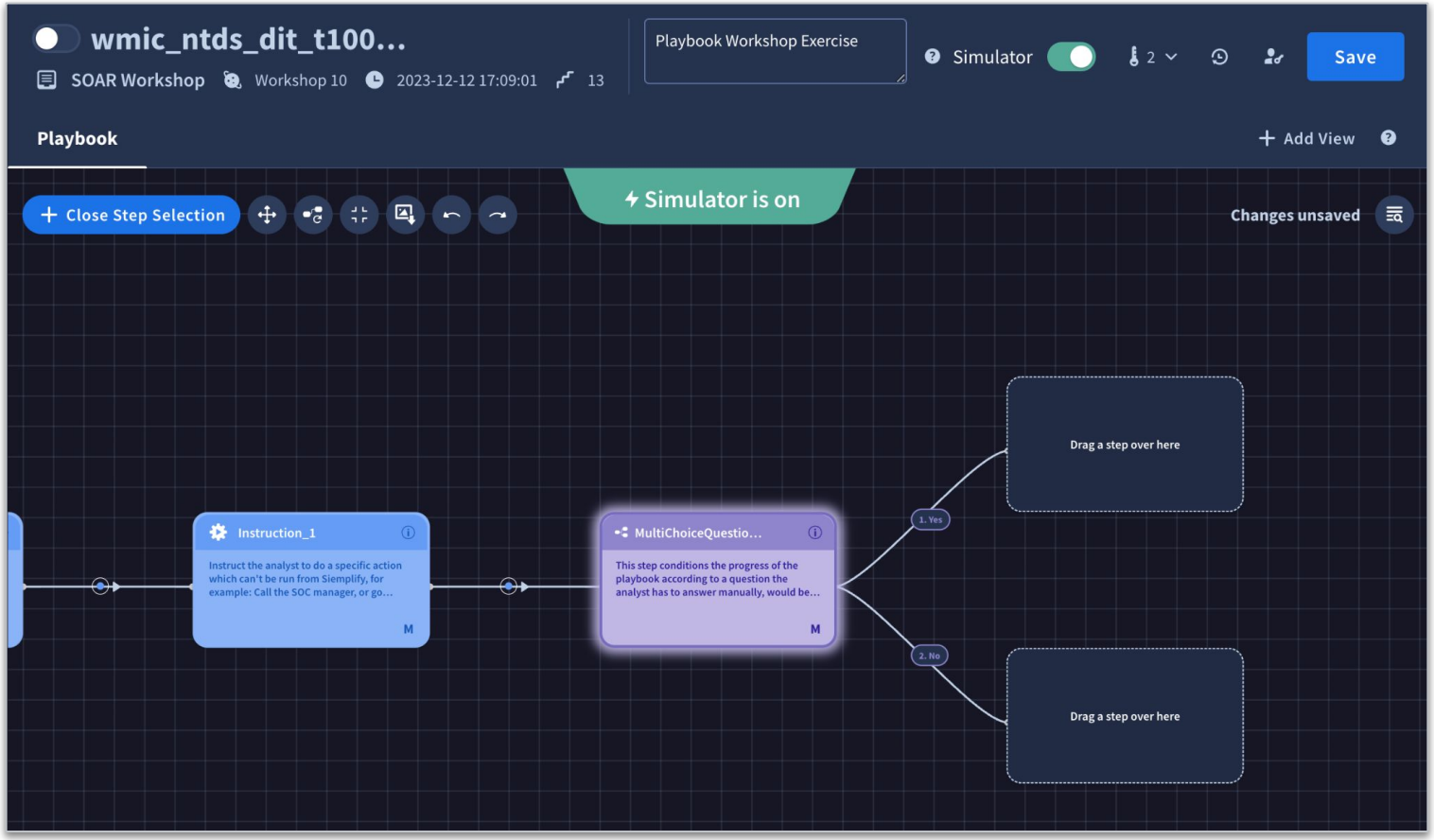
Action - Instruction

Google SecOps



Flow - Multi-Choice Question

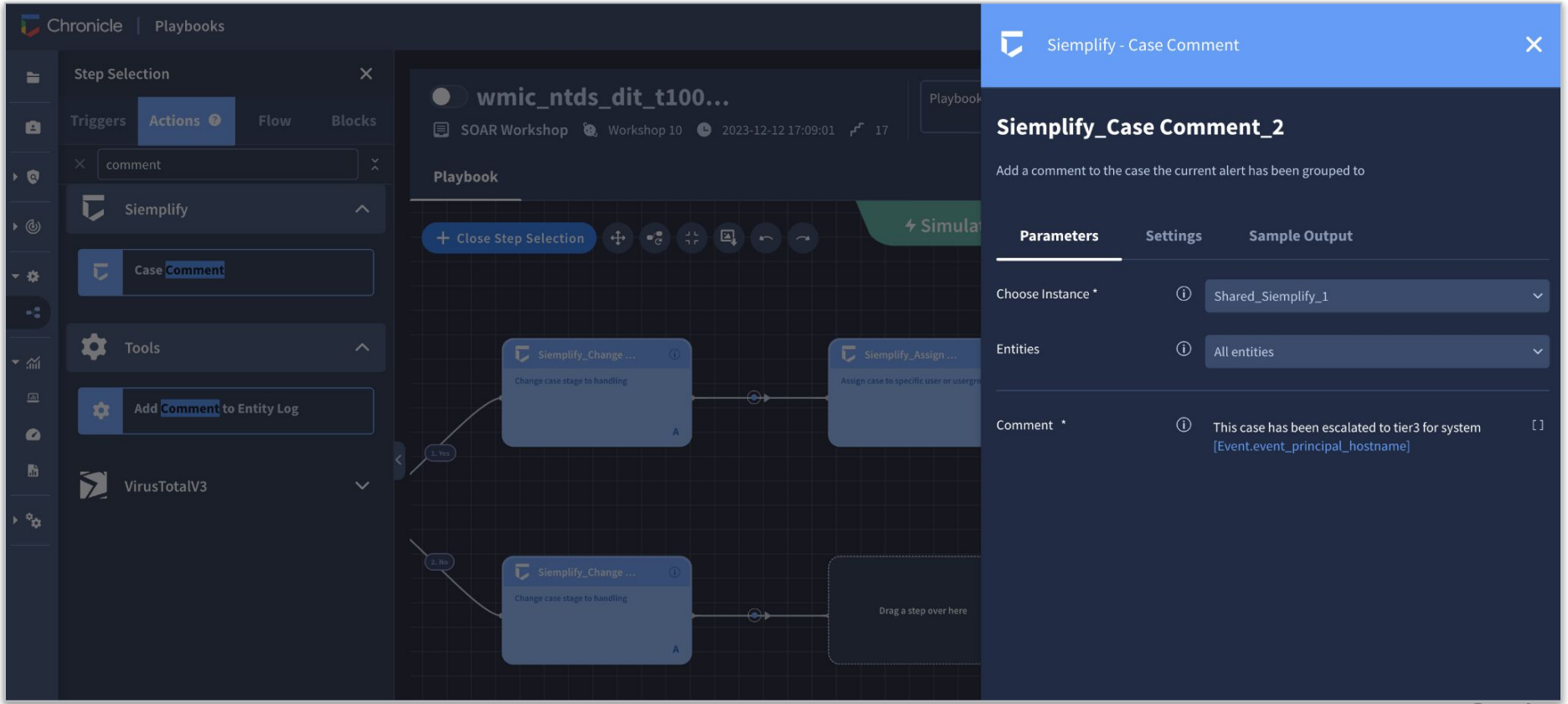
Google SecOps



Google

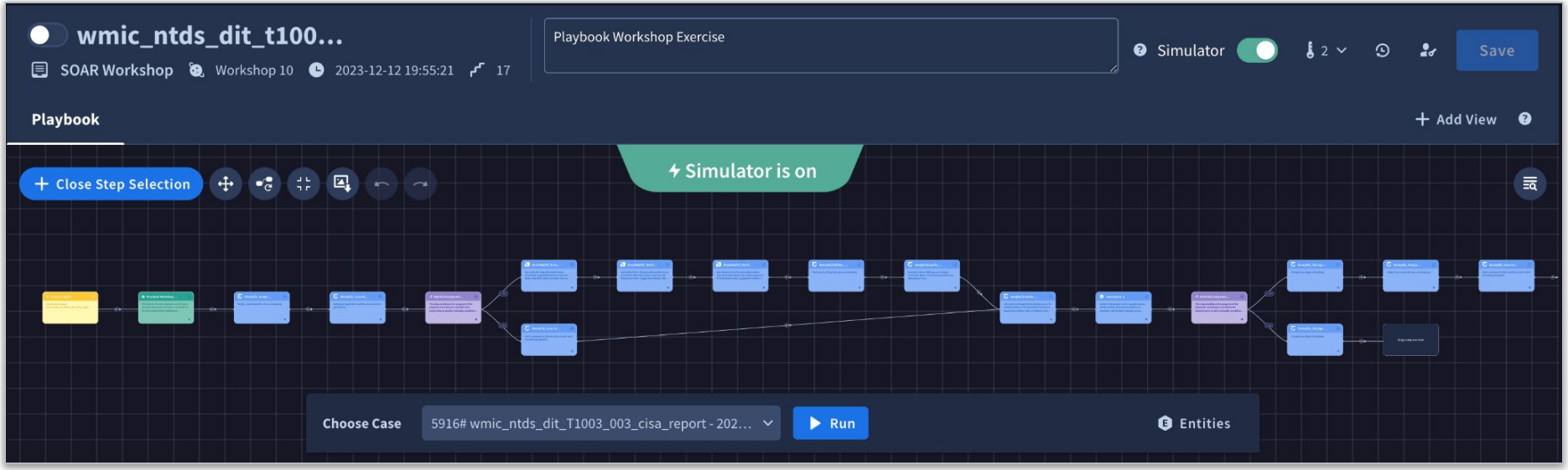
Yes/No Action Paths

Google SecOps



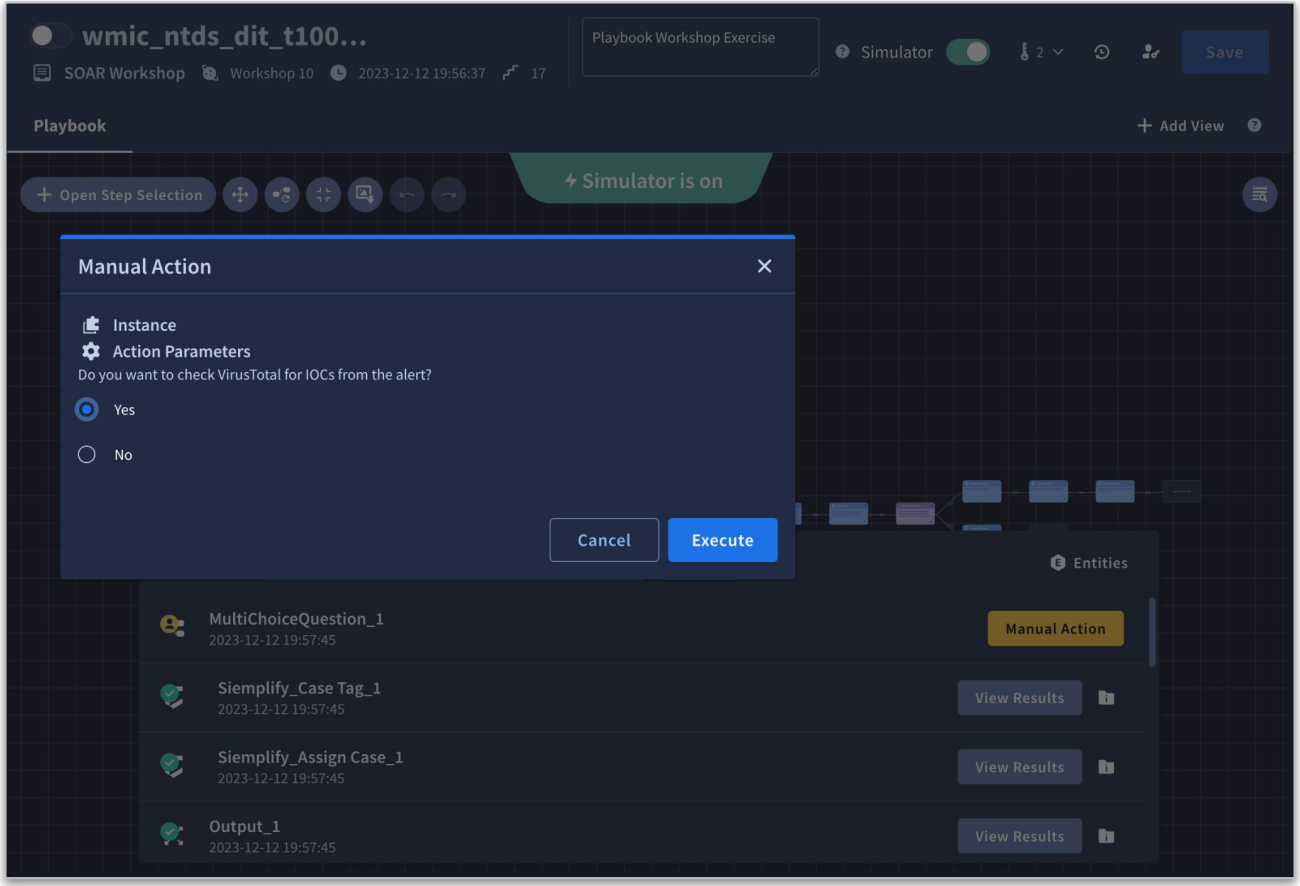
Testing Our Playbook

Google SecOps



Simulating our Case/Alert

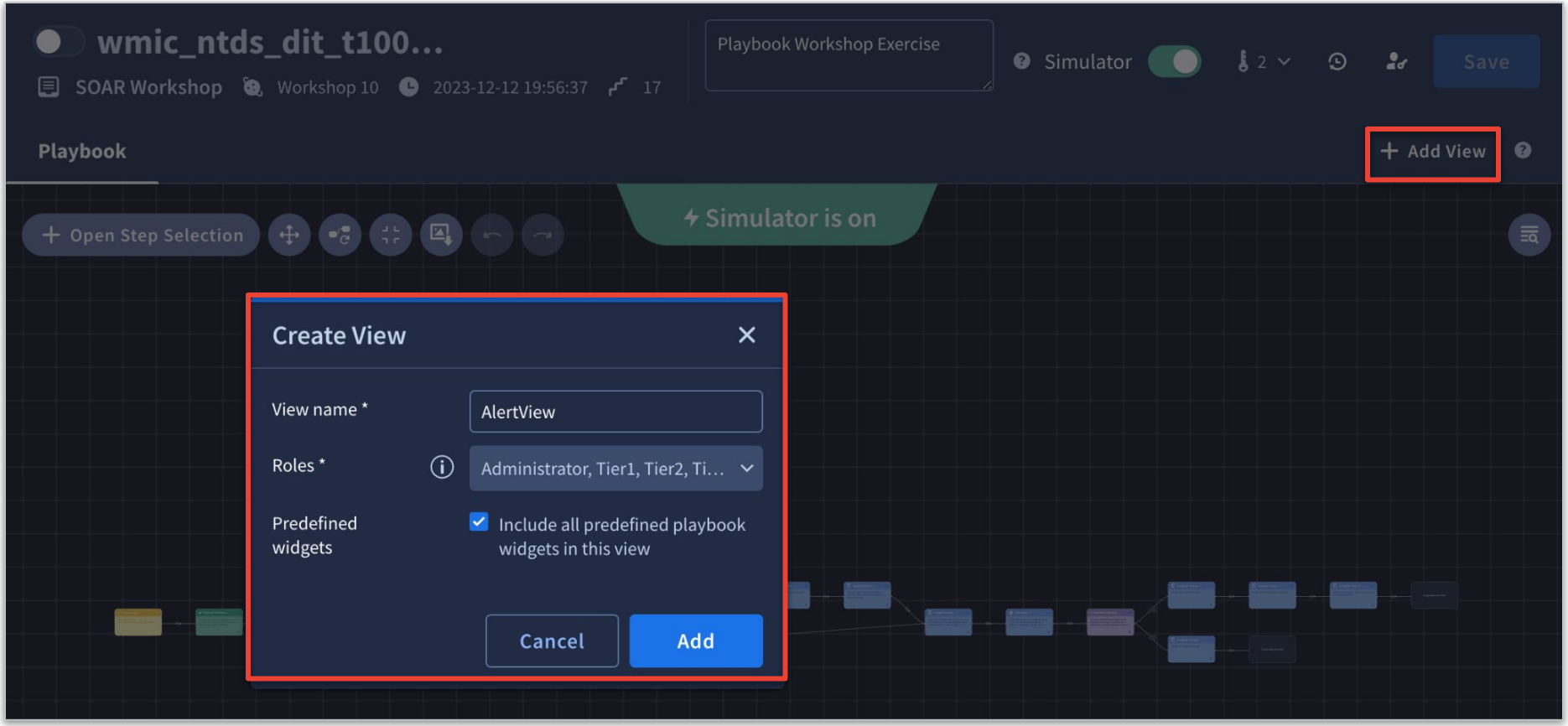
Google SecOps



Google

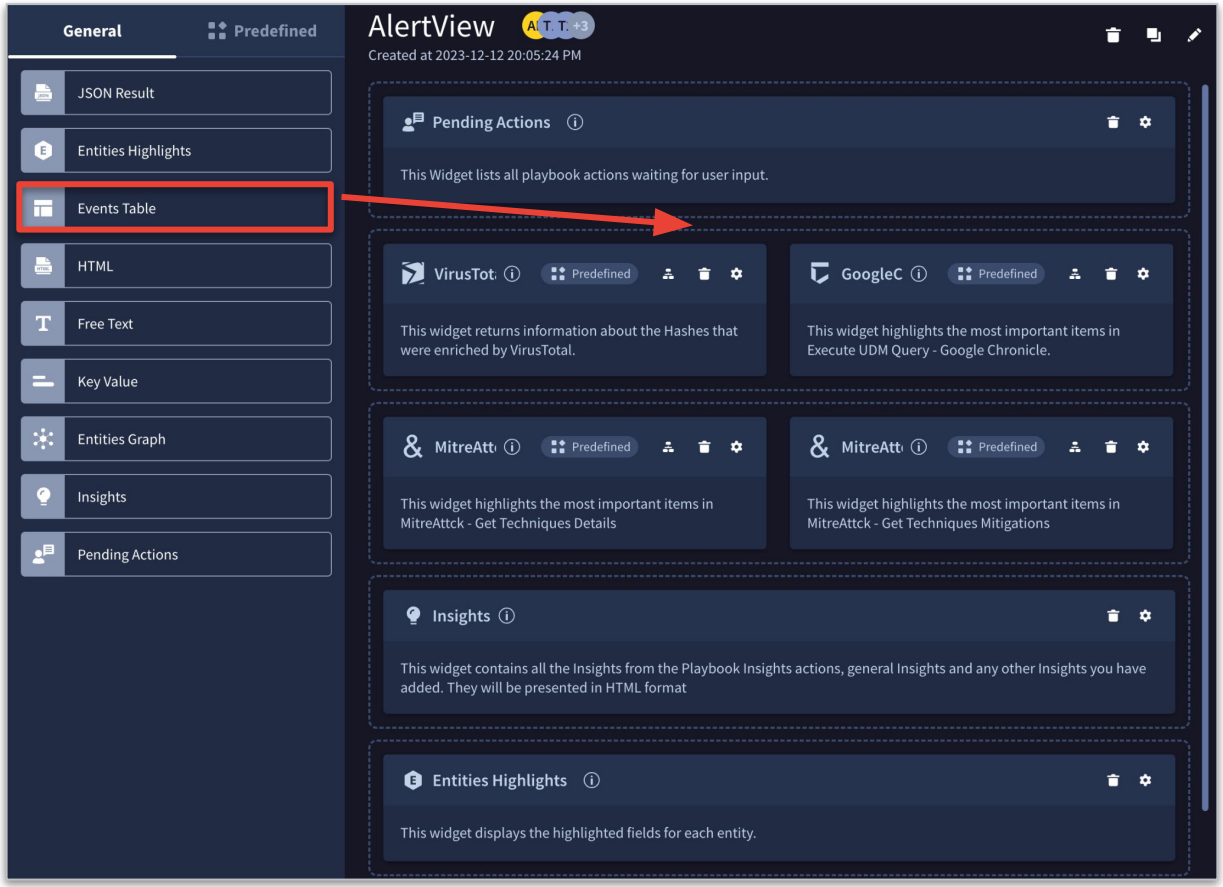
Adding a View

Google SecOps



Alert View

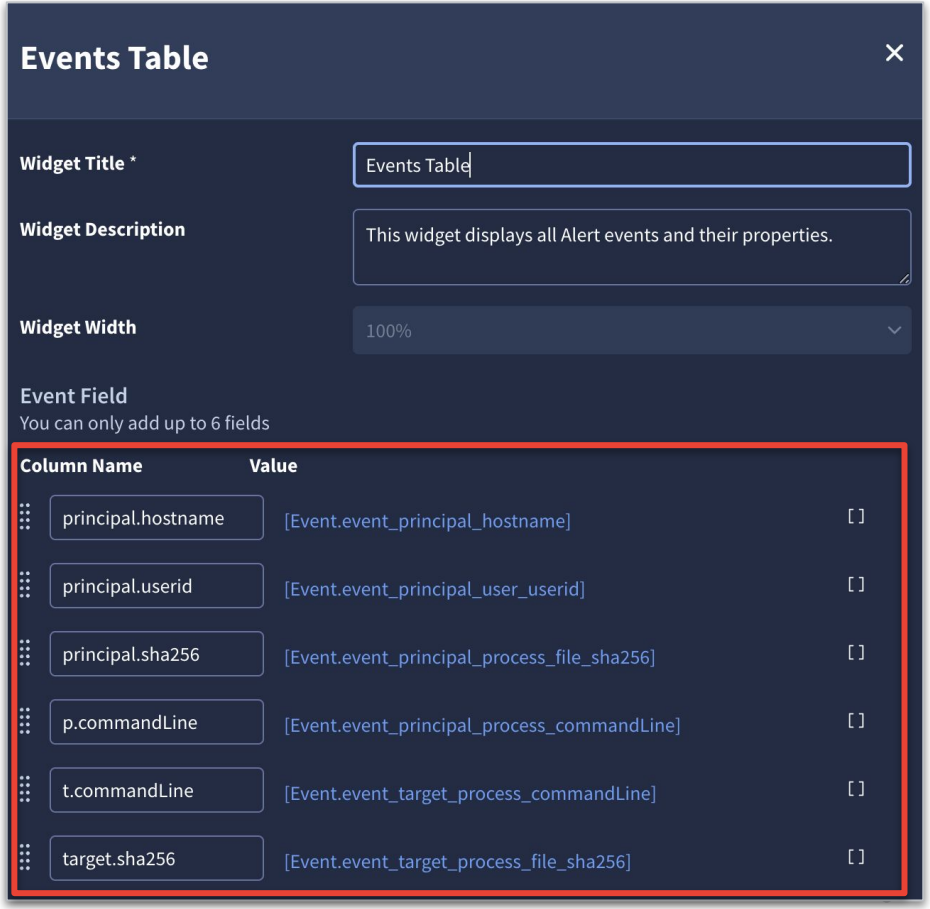
Google SecOps



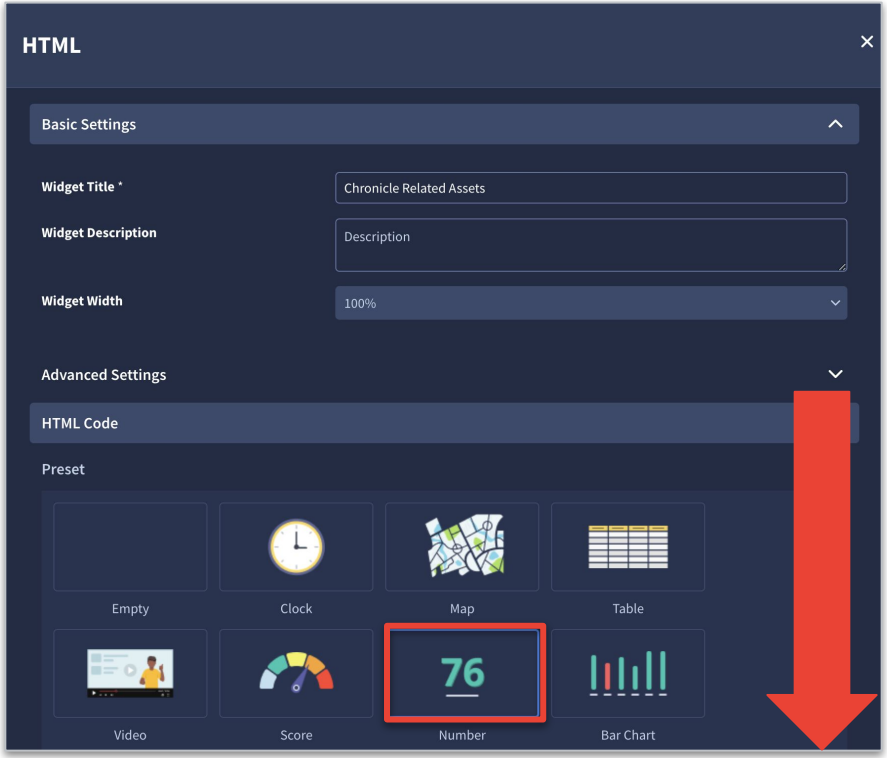
Google

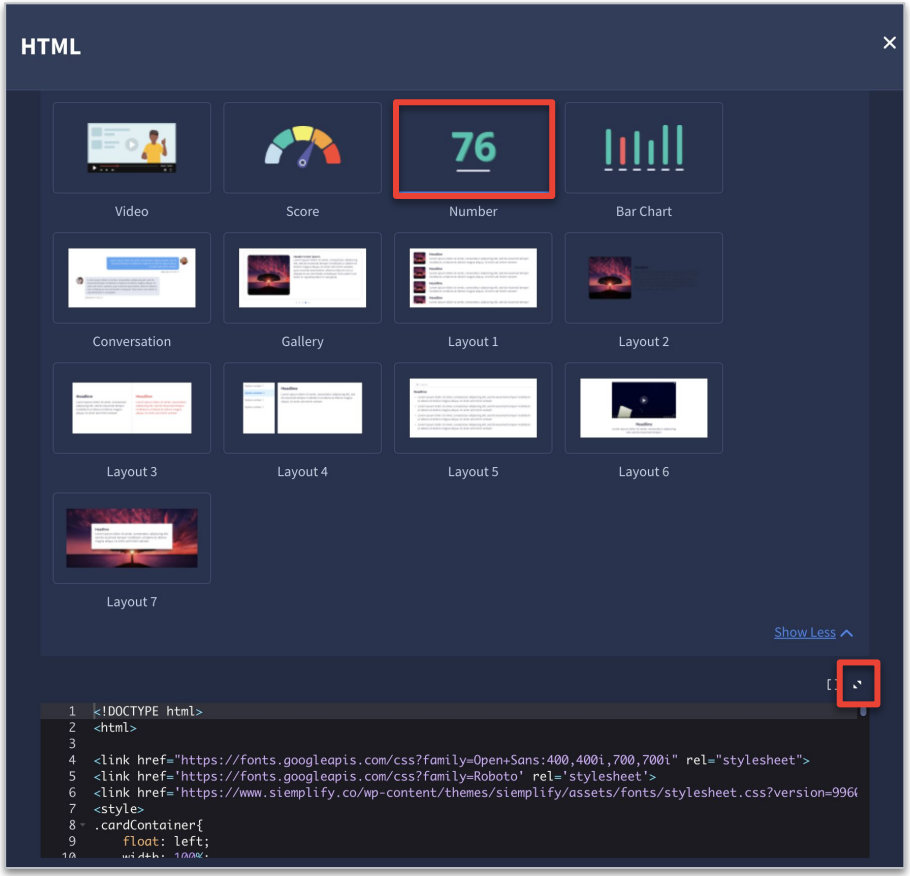
Modifying a Widget

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
76
Number
Bar Chart


HTML
Video
Score
76
Number
Bar Chart
Conversation
Gallery
Layout 1
Layout 2
Layout 3
Layout 4
Layout 5
Layout 6
Layout 7
Show Less
<!DOCTYPE html>
<html>
<link href="https://fonts.googleapis.com/css?family=Open+Sans:400,400i,700,700i" rel="stylesheet">
<link href='https://fonts.googleapis.com/css?family=Roboto' rel='stylesheet'>
<link href='https://www.siemplify.co/wp-content/themes/siemplify/assets/fonts/stylesheet.css?version=996
<style>
.cardContainer{
float: left;

HTML Widget - Code Editor

Google SecOps

HTML Code editor

HTML Code

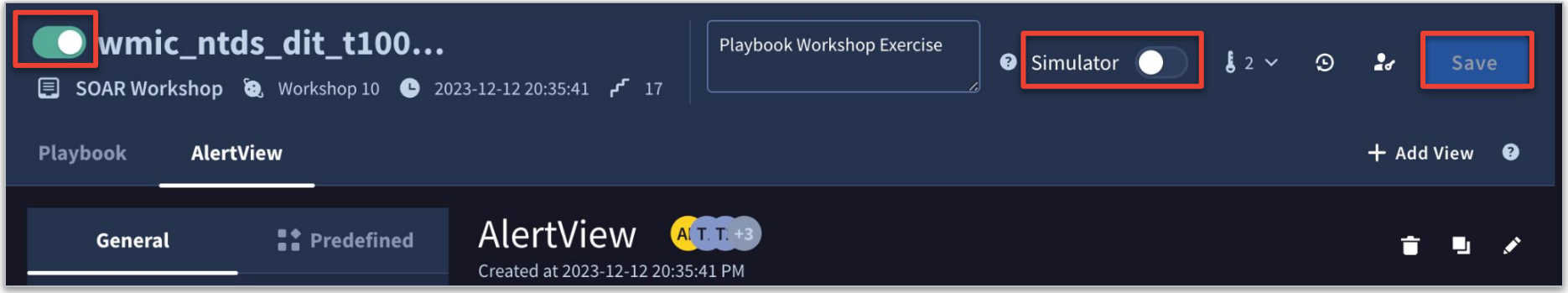
```
354     </div>
355     <div class="cntRightSide">
356         <div class="cusWdgNumberTitle" id="field2"></div>
357         <div class="cusWdgNumberText" id="field3"></div>
358     </div>
359   </div>
360 </div>
361 <script src="https://code.jquery.com/jquery-3.5.1.min.js"></script>
362 <script>
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 placeh

HTML Preview

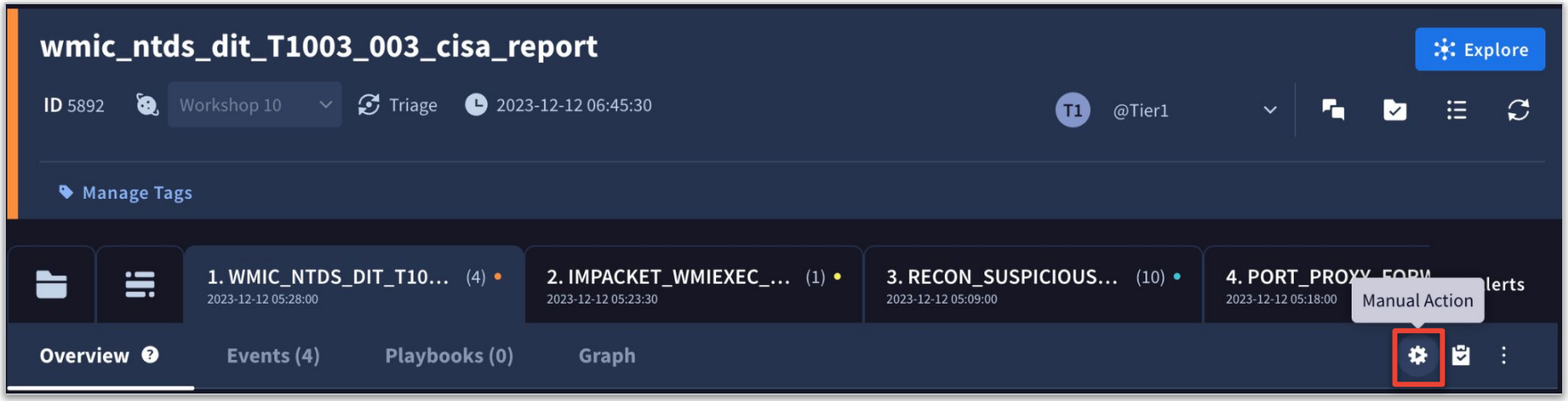
Preparing Our Playbook

Google SecOps



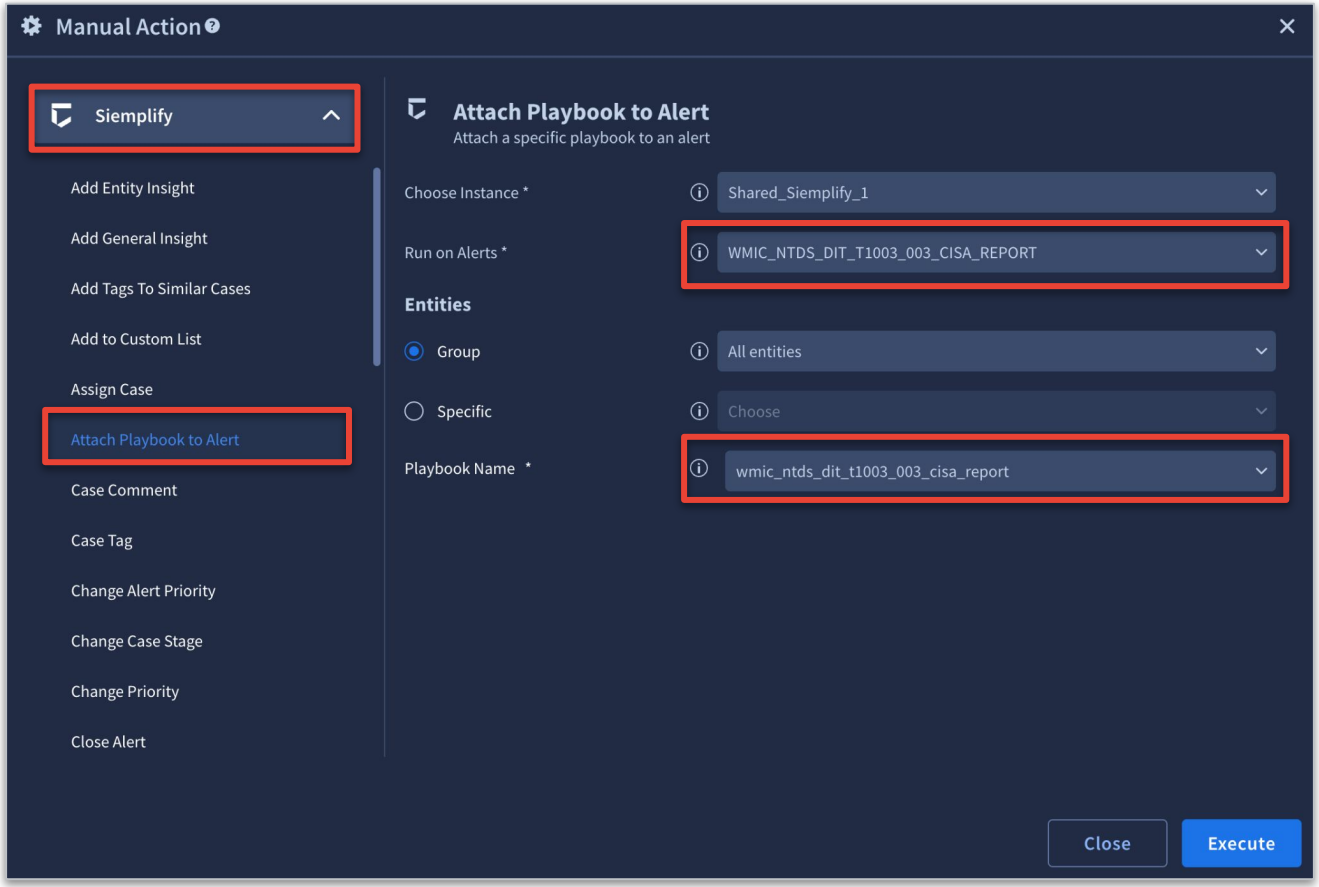
Manual Action - Attach Playbook to Alert

Google SecOps



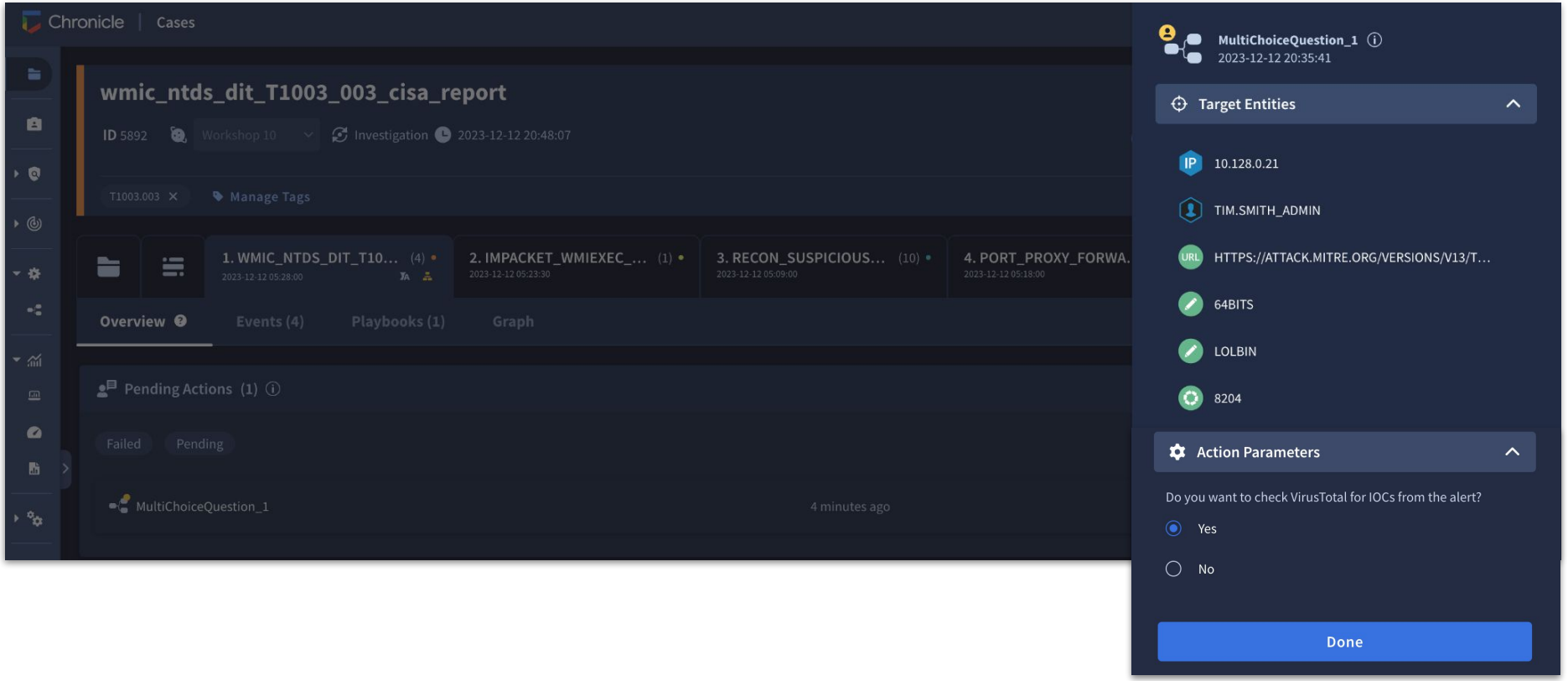
Manual Action - Attach Playbook to Alert

Google SecOps



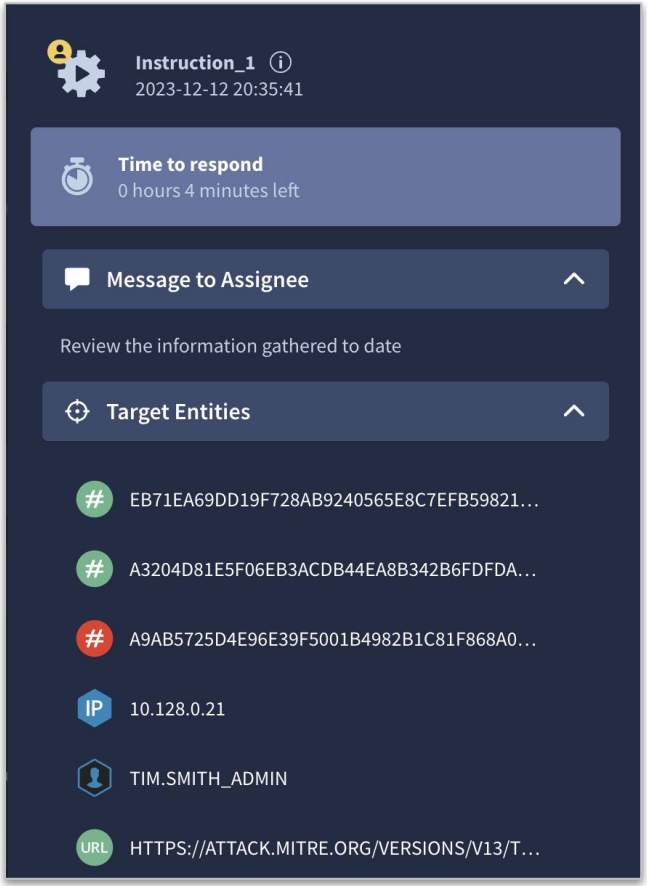
Pending Action

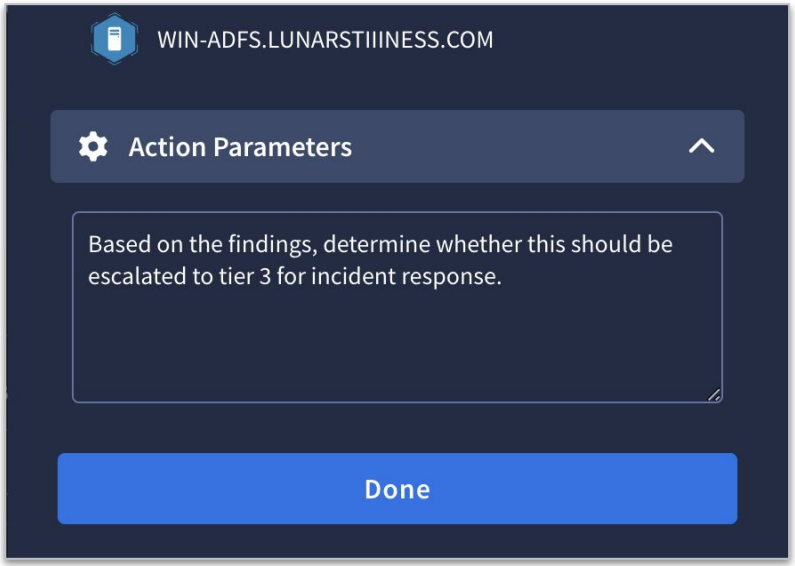
Google SecOps



Instructions

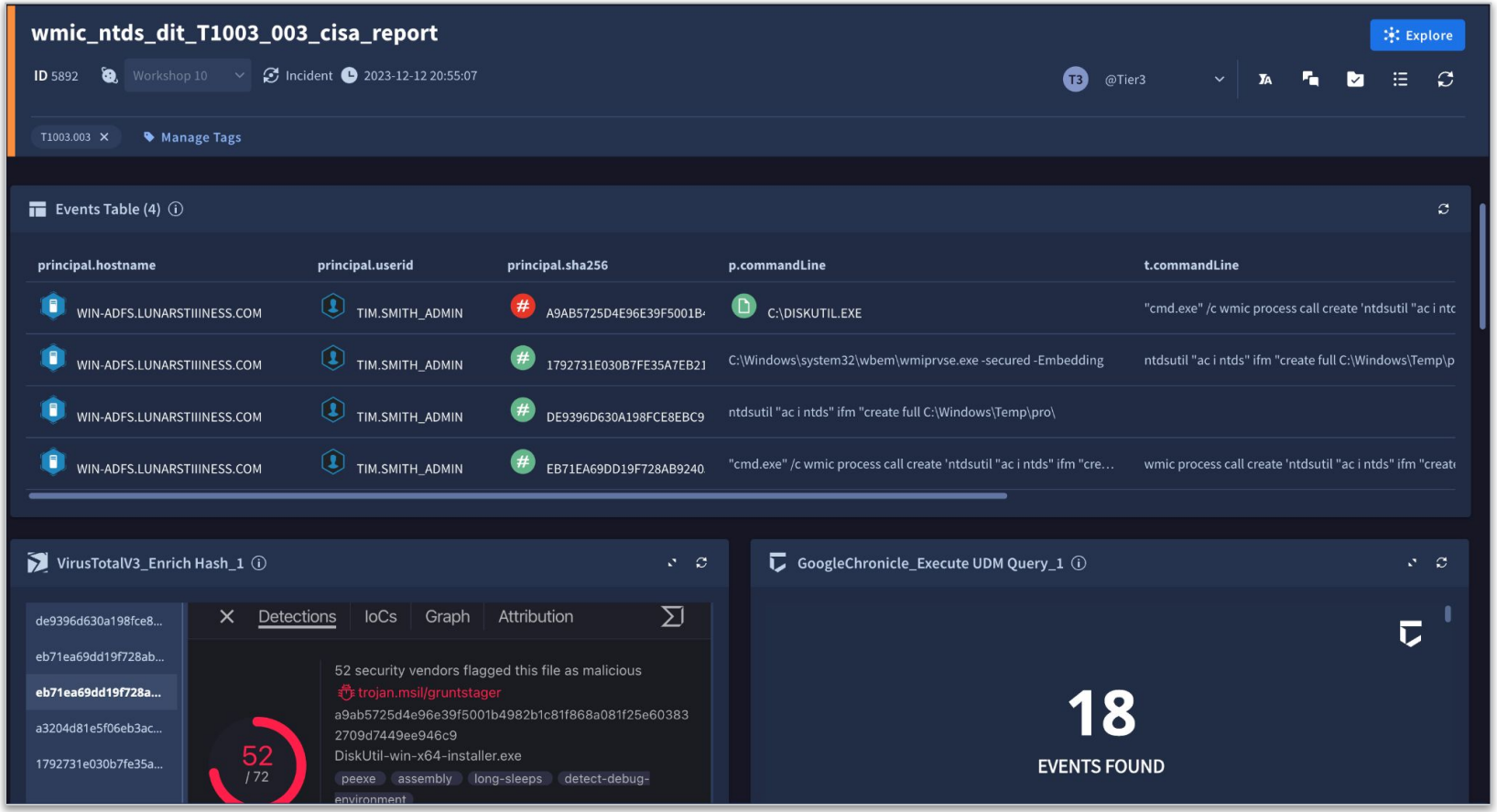
Google SecOps





Alert View

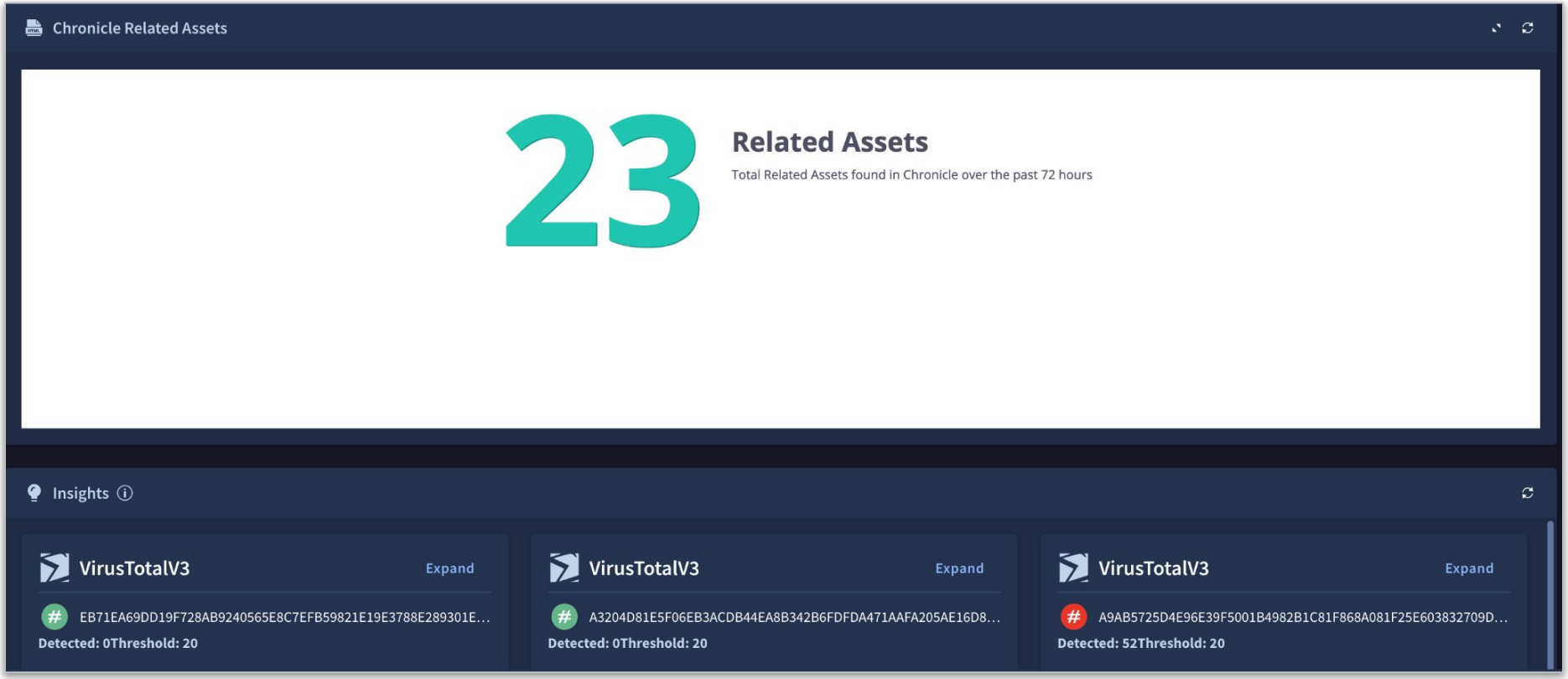
Google SecOps



Google

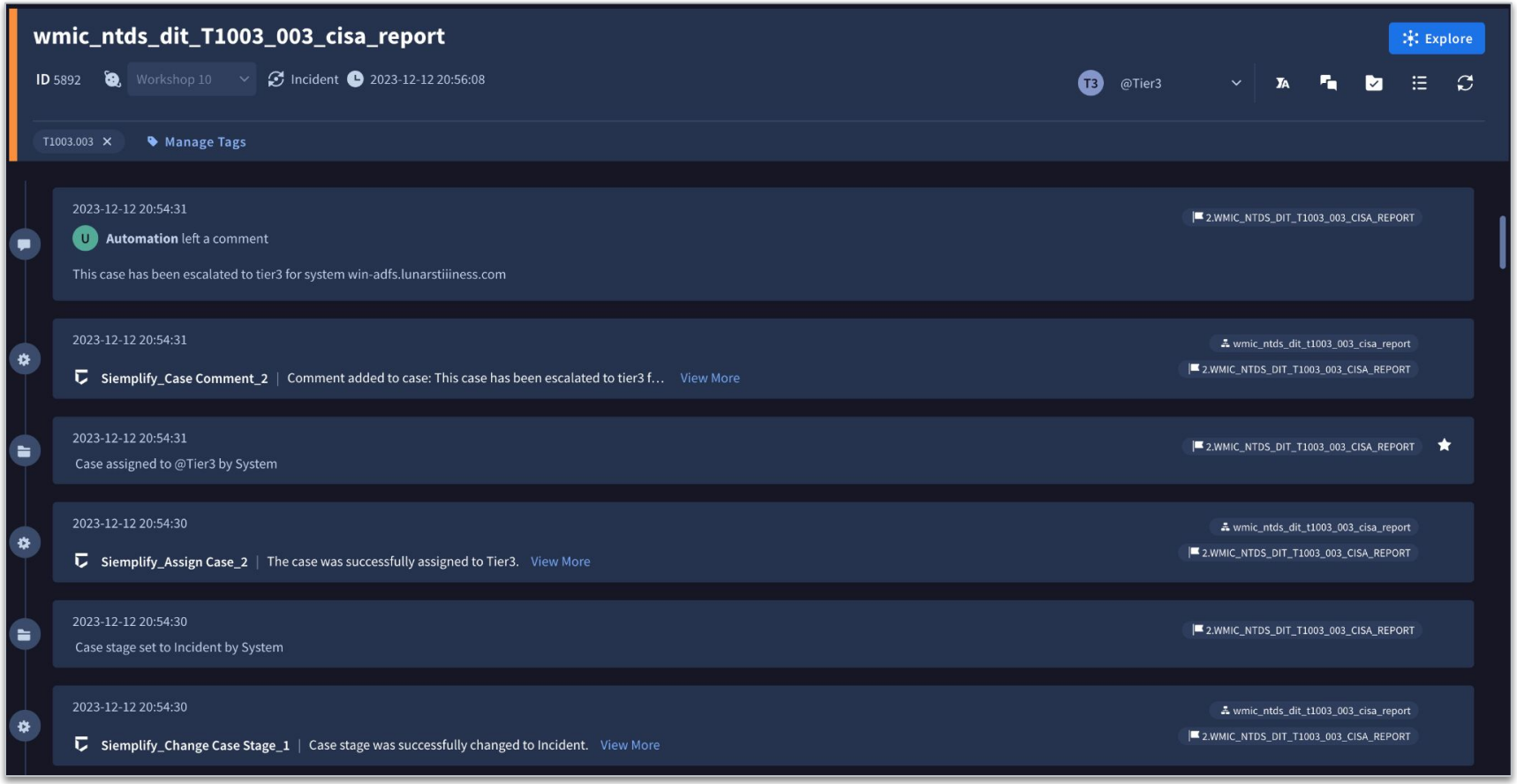
Alert View

Google SecOps



Case Wall

Google SecOps



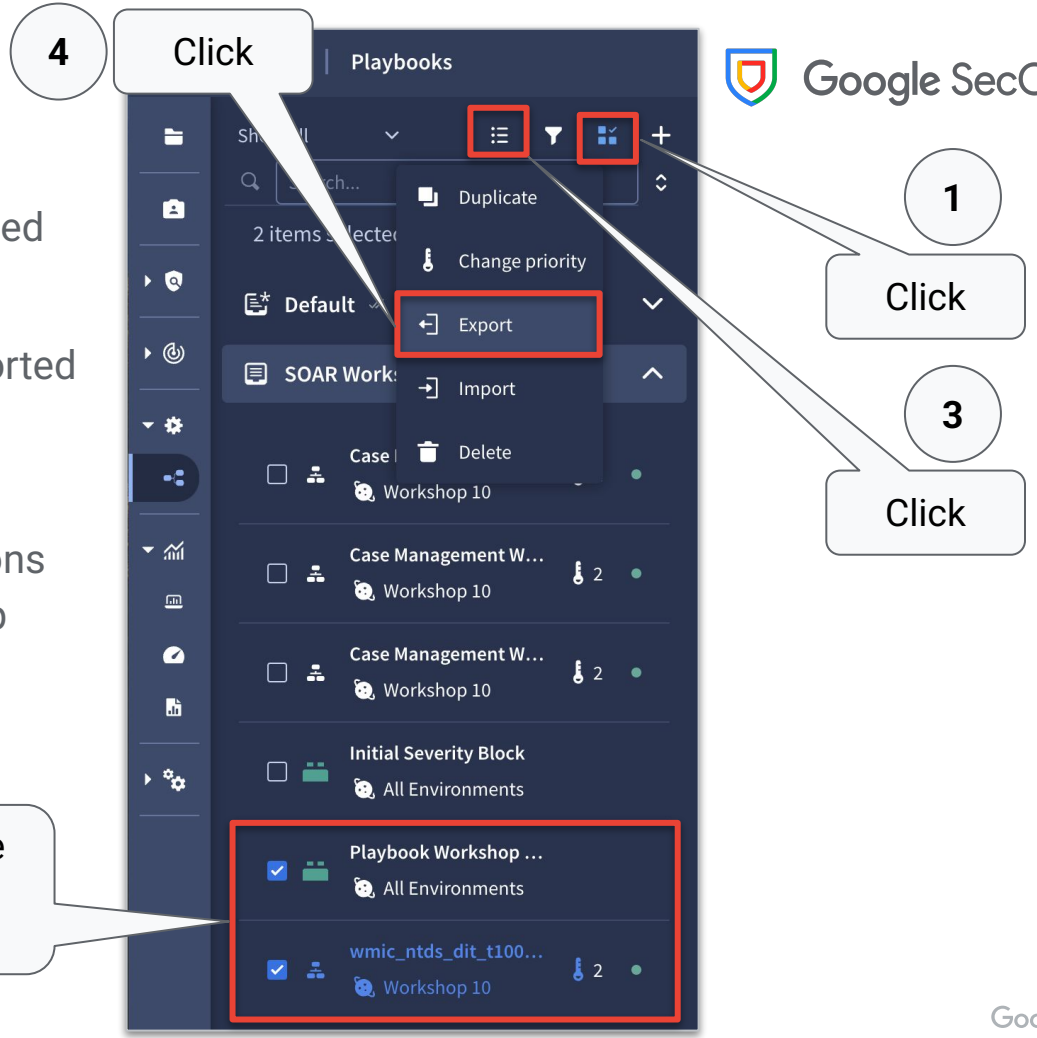
Export (and Import)

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



Google SecOps

Google

Summary

Google SecOps

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

Google SecOps

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