Google

Google SecOps

Managing Cases in Google SecOps

Using Case Management in Security Operations

September 2024

Using goo.gle/secops-workshop

Agenda

Google SecOps

- SecOps Primer
- Case Management Familiarization
- Your Workdesk
- Manual Actions
- Exercise

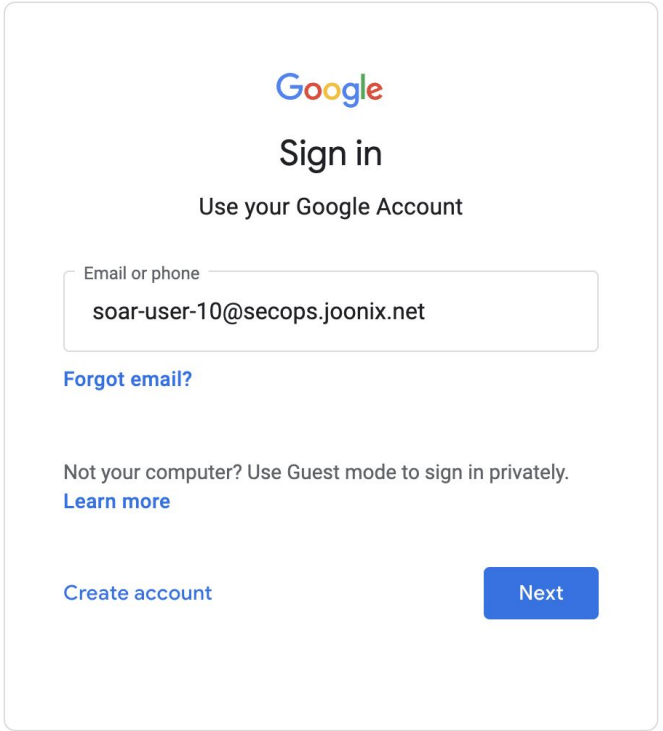
Login Instructions (1)

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**

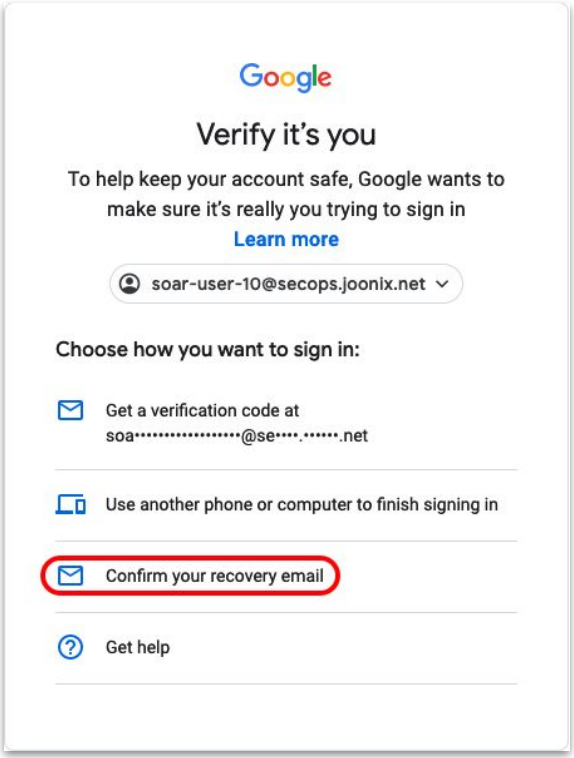
3) Use the account assigned to you by your instructor that uses Google Workspace as Identity Provider



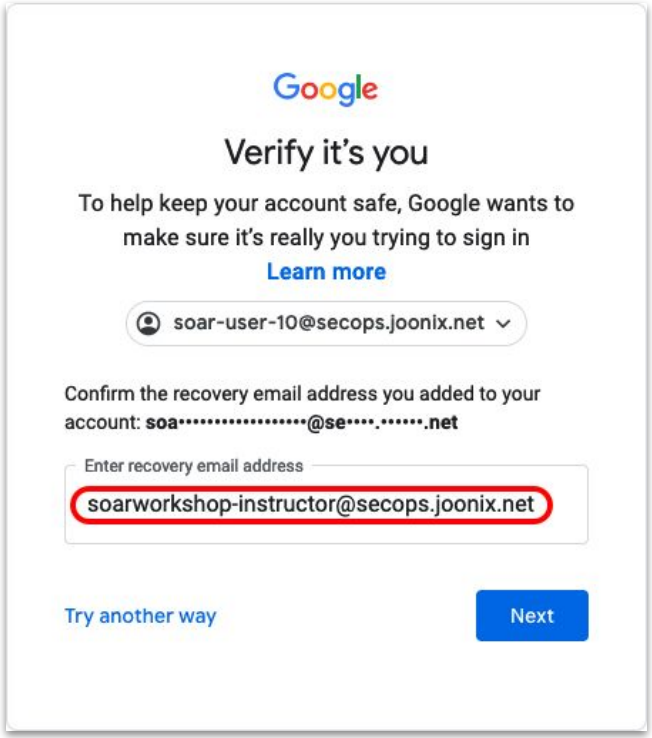
Login Instructions (2)

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

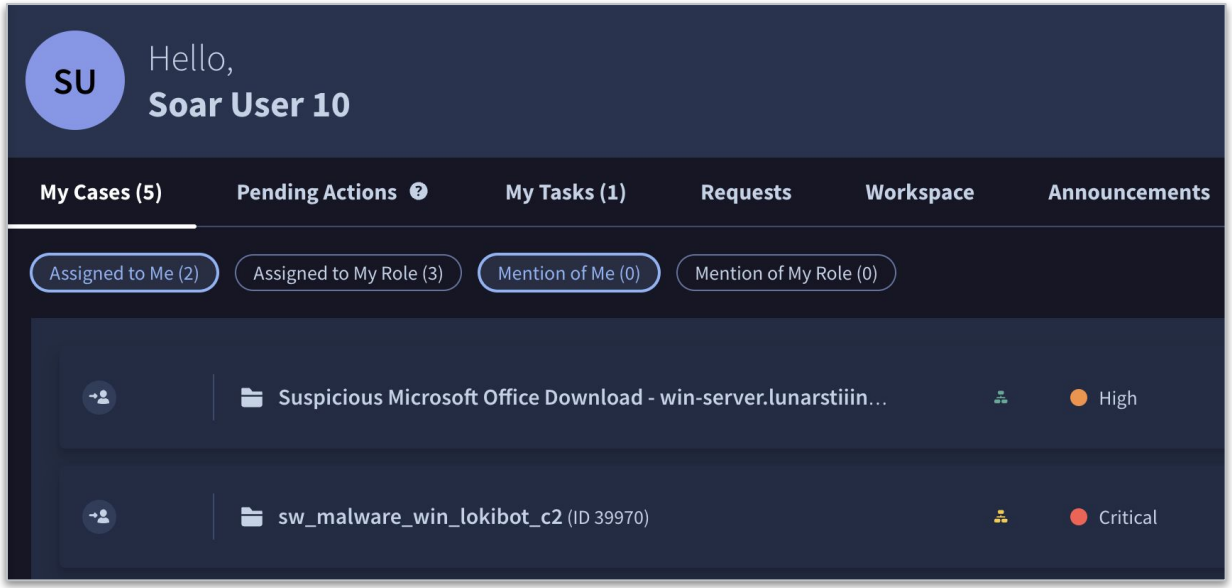


Login Instructions (3)

Google SecOps

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

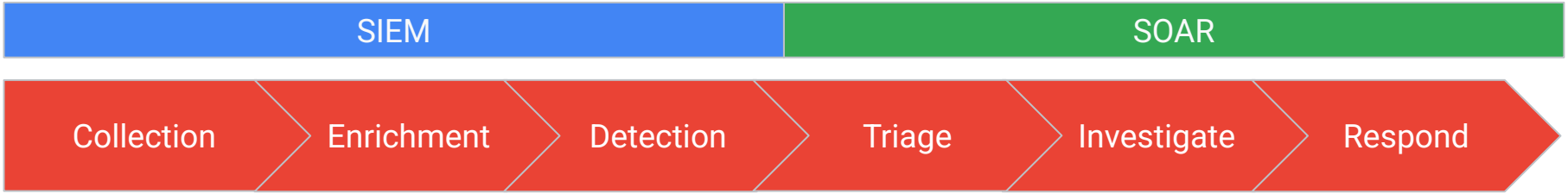
7) Open a new tab in the same Incognito Window and navigate to https://gmail.com/ which we will use during the workshop



SecOps Primer

Google SecOps

Google 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

Orchestration and Automation in SecOps

Google SecOps

SecOps is not just using a SIEM, but bringing automation and orchestration to streamline response

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 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

Case Management Workflow

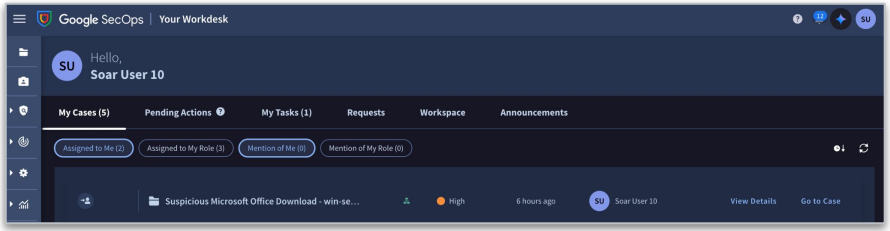
Different approaches

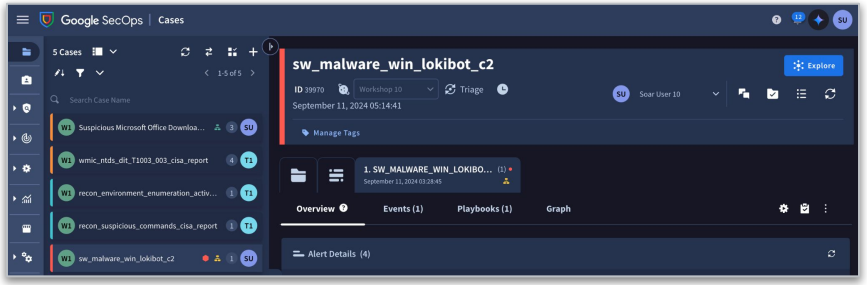
Google SecOps

Workdesk

< not exclusive approaches >

Cases





Analysts are interacting with cases assigned to them, and pending actions :

- [+] well structured and organized SOC team
- [+] better priority management
- [-] requires higher maturity to structure the SOC Team
- [-] lack of visibility to other cases

Analysts are interacting within the global cases list :

- [+] broad view of all cases
- [+] doesn't require additional configuration to structure the processes
- [-] the analyst doesn't see immediately the actions that are pending

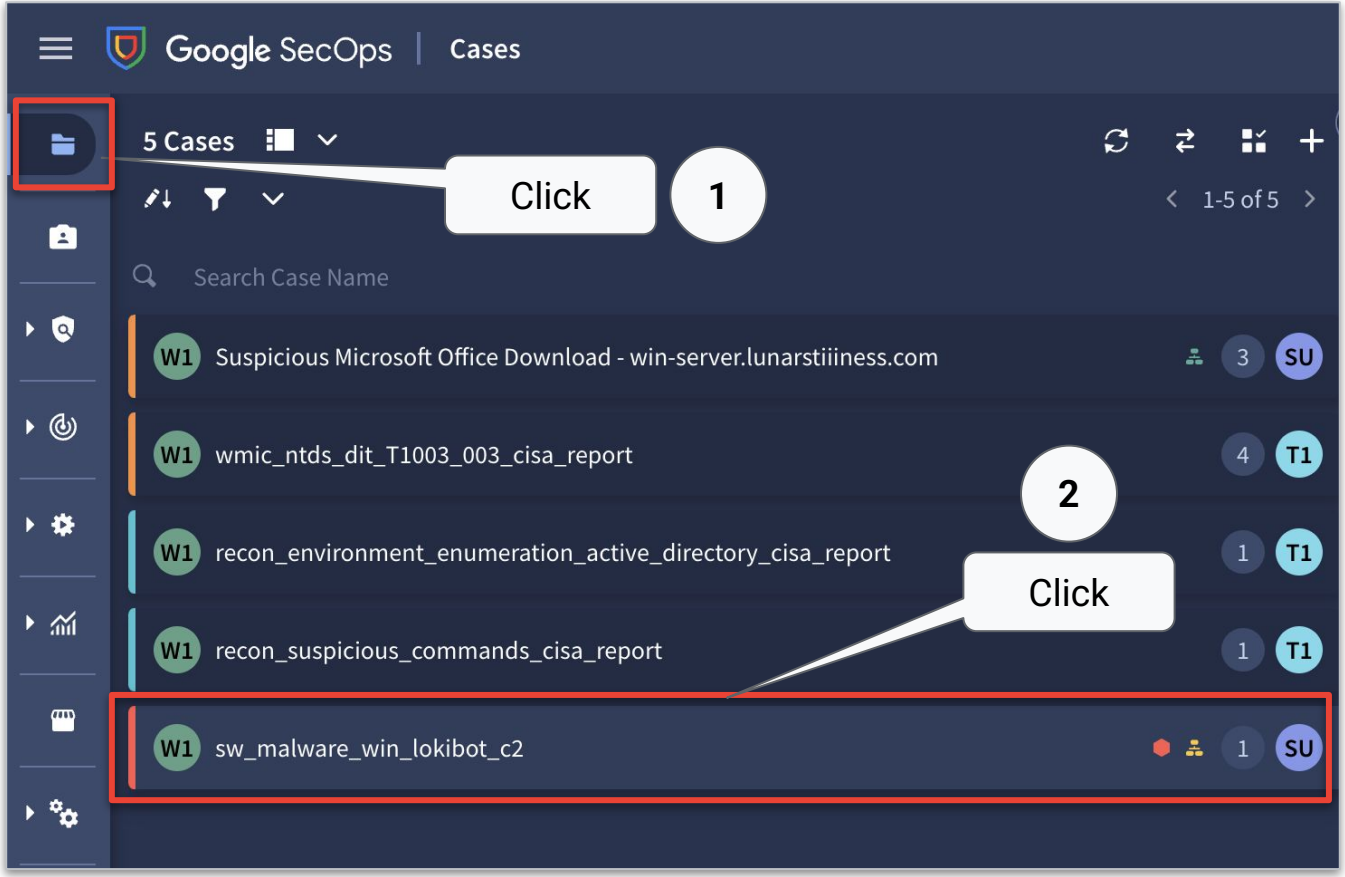
Google

Google SecOps

Familiarization with Case Management

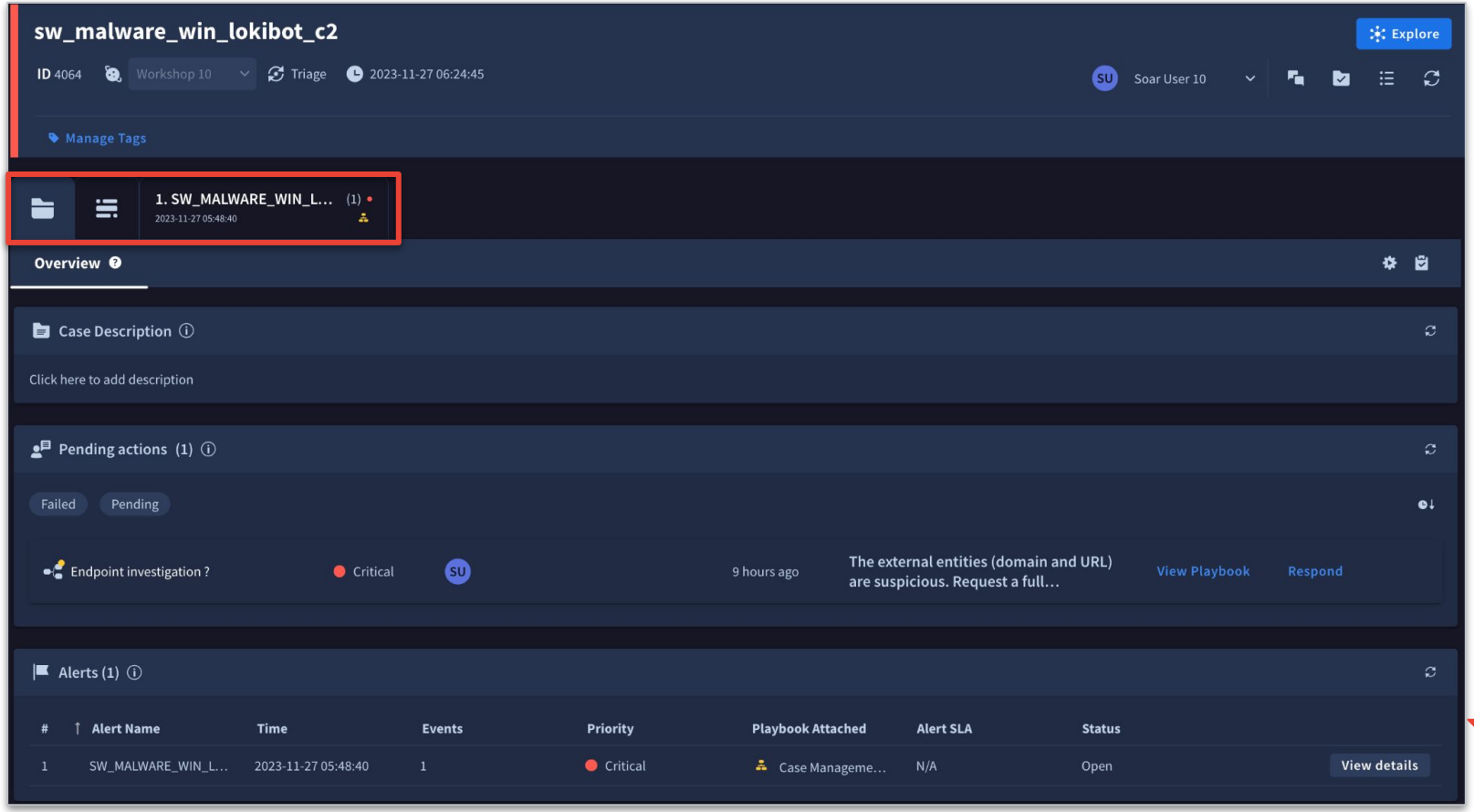
Google

Case List


Google SecOps | Cases
5 Cases
Click
1
1-5 of 5
Search Case Name
W1 Suspicious Microsoft Office Download - win-server.lunarstiiiness.com 3 SU
W1 wmic_ntds_dit_T1003_003_cisa_report 4 T1
2
W1 recon_environment_enumeration_active_directory_cisa_report 1 T1
Click
W1 recon_suspicious_commands_cisa_report 1 T1
W1 sw_malware_win_lokibot_c2 1 SU

Case Overview

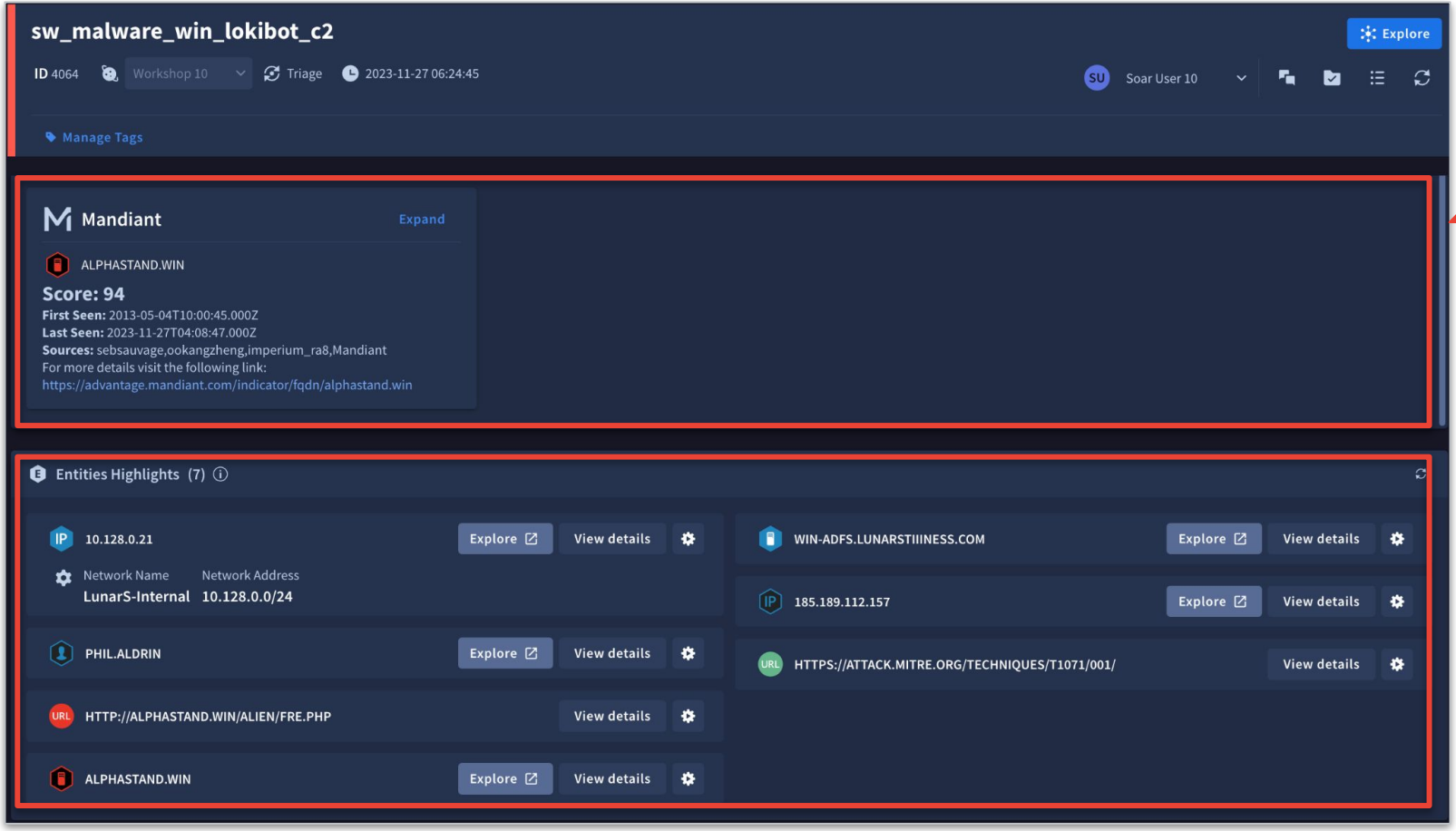
Google SecOps



Google

Case Overview

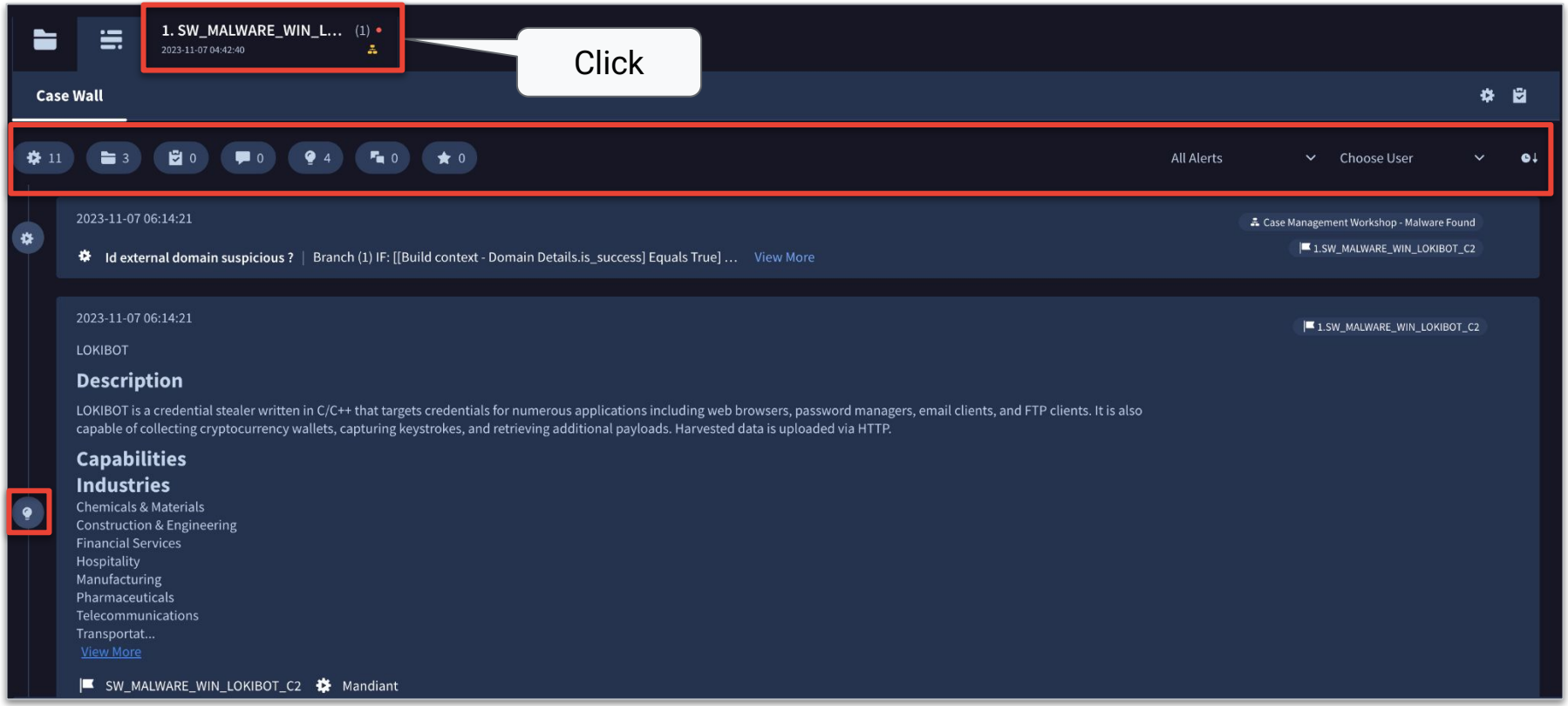
Google SecOps



Google

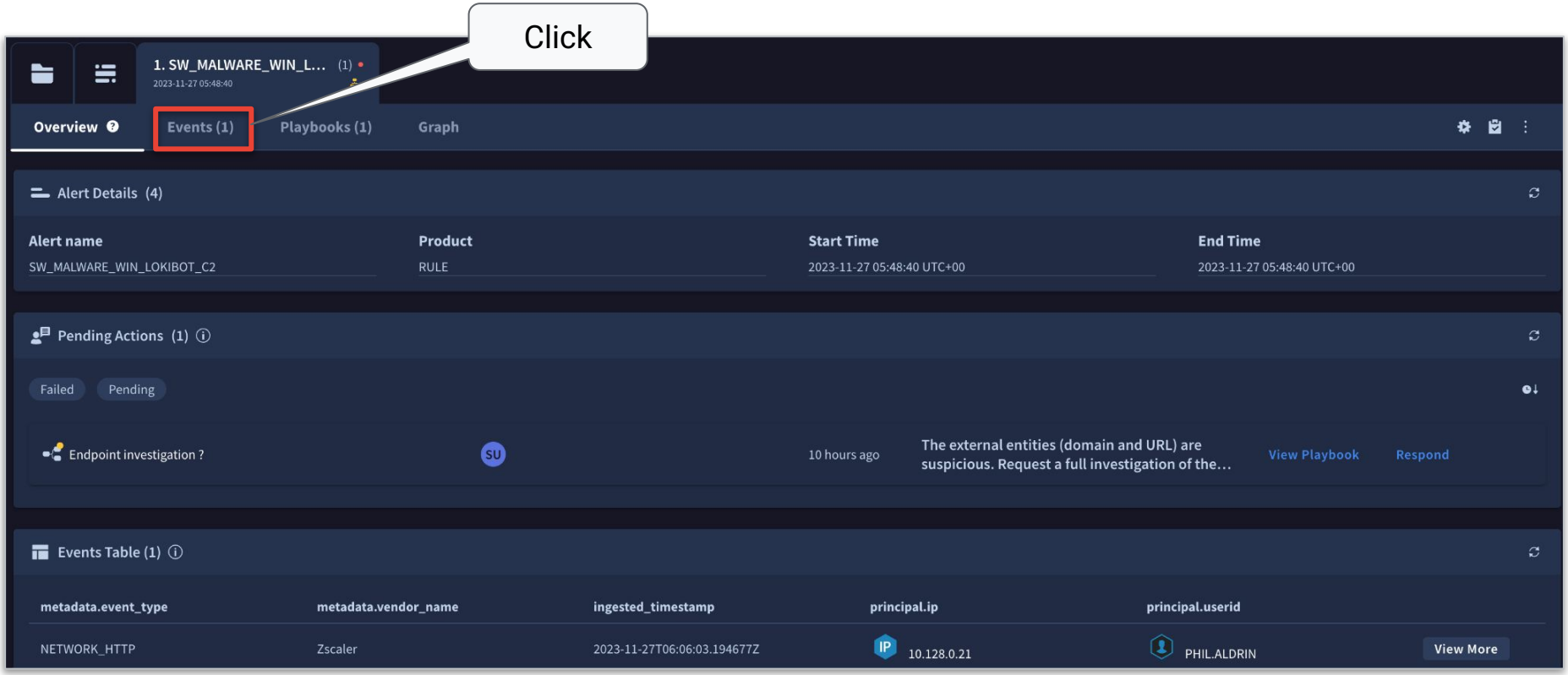
Case Wall - Audit Trail

Google SecOps



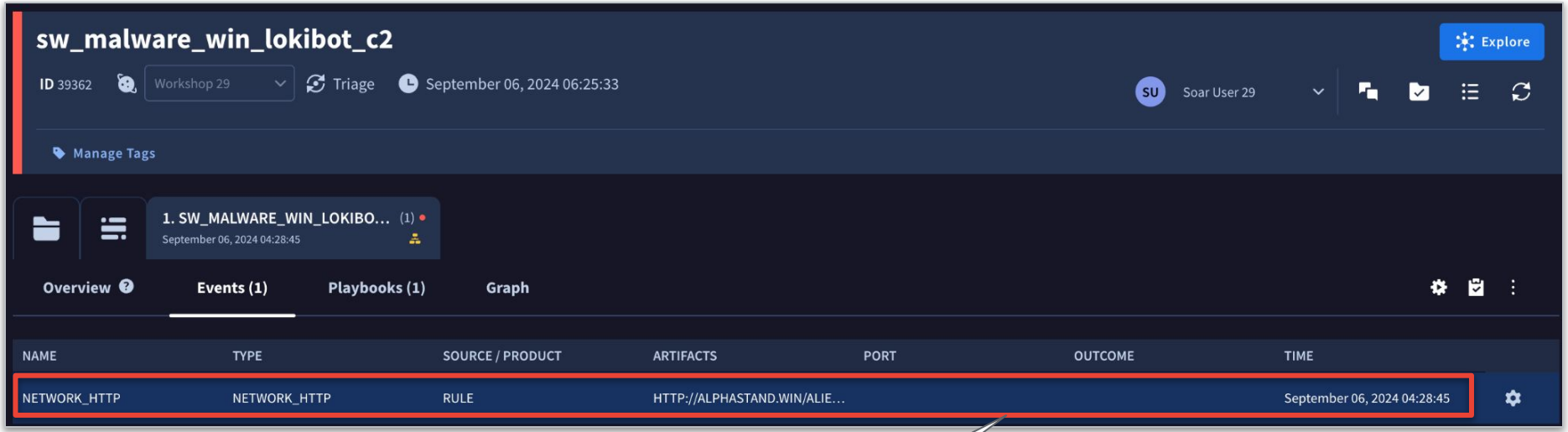
Alert Overview

Google SecOps



Alert - Event View

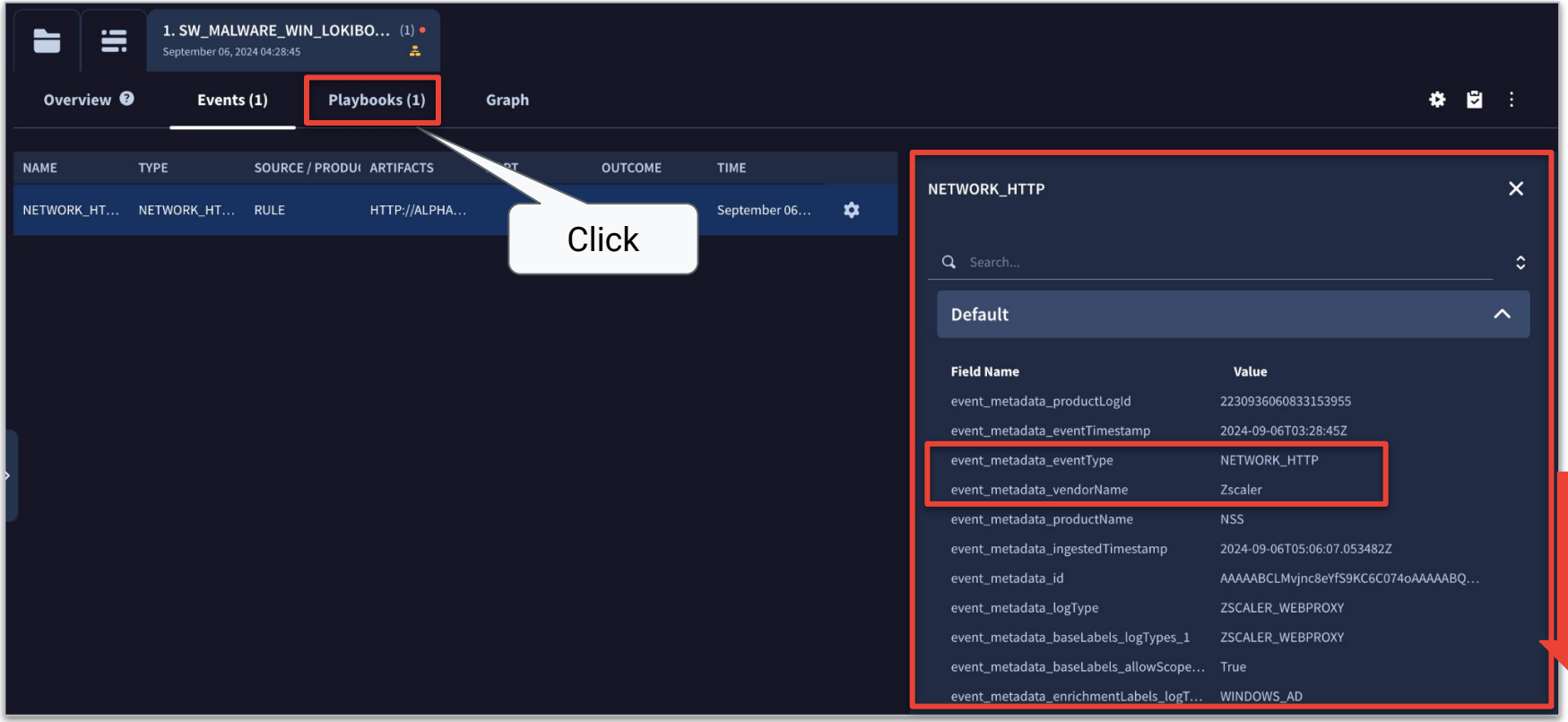
Google SecOps



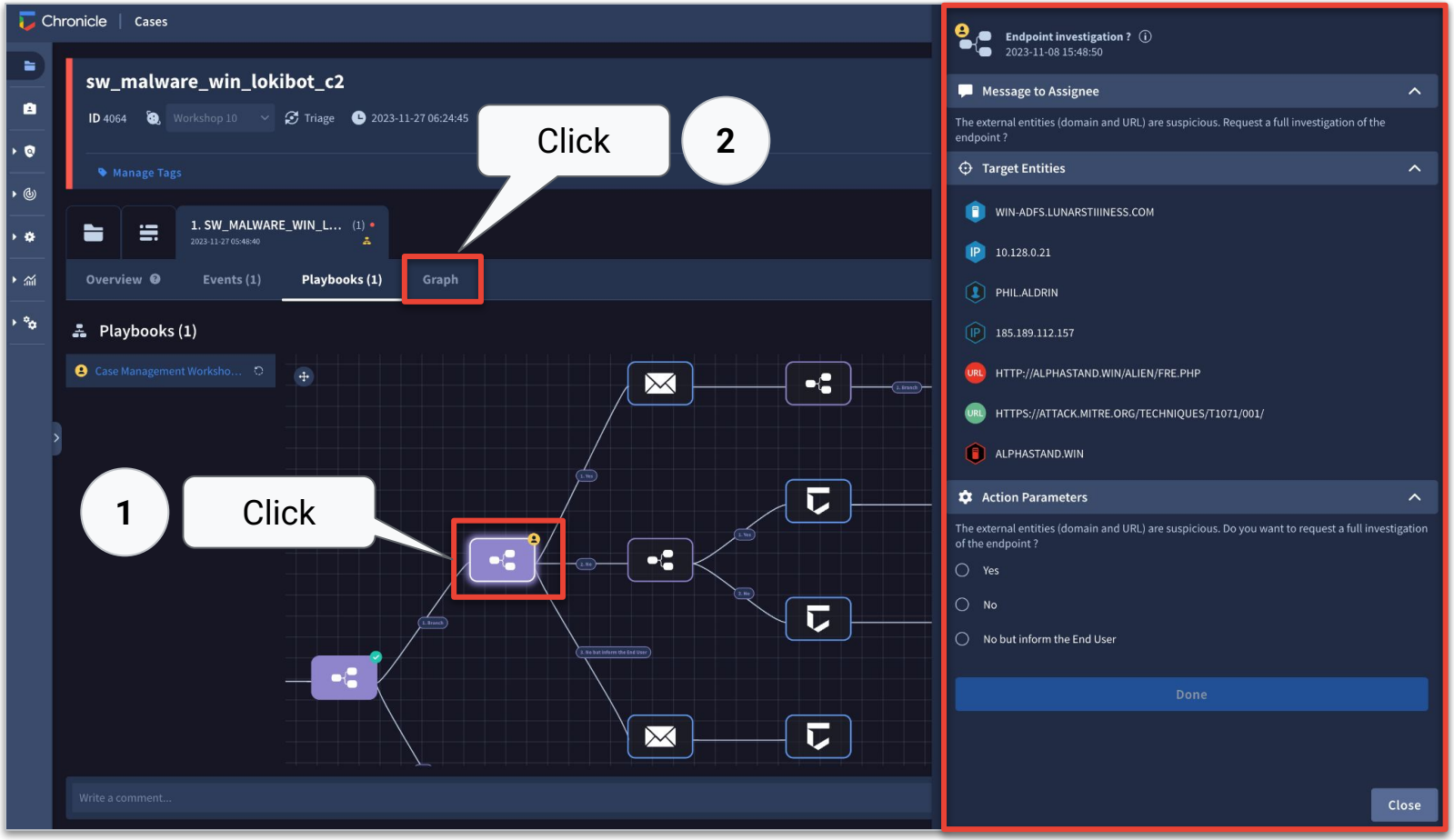
Click

Alert - Event/Detection Details

Google SecOps

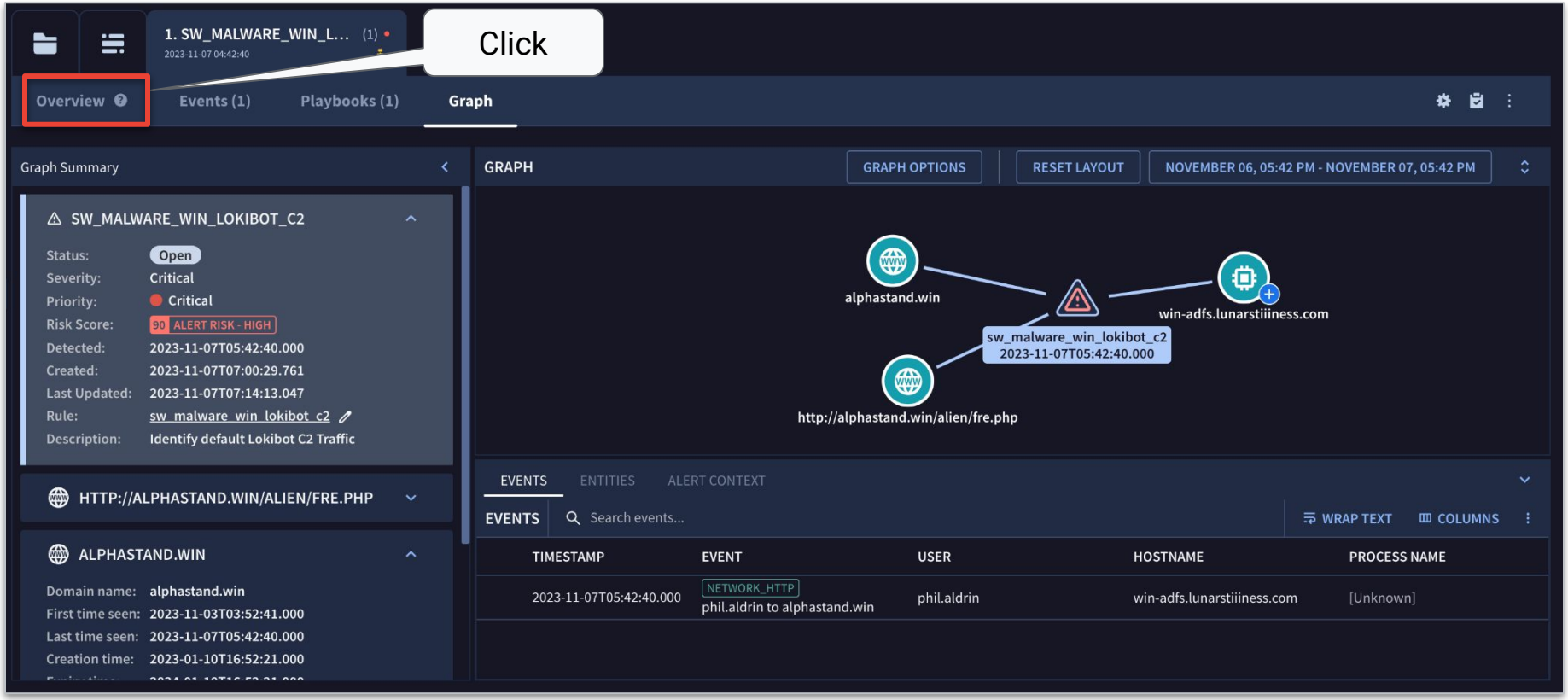


Alert Playbook Status



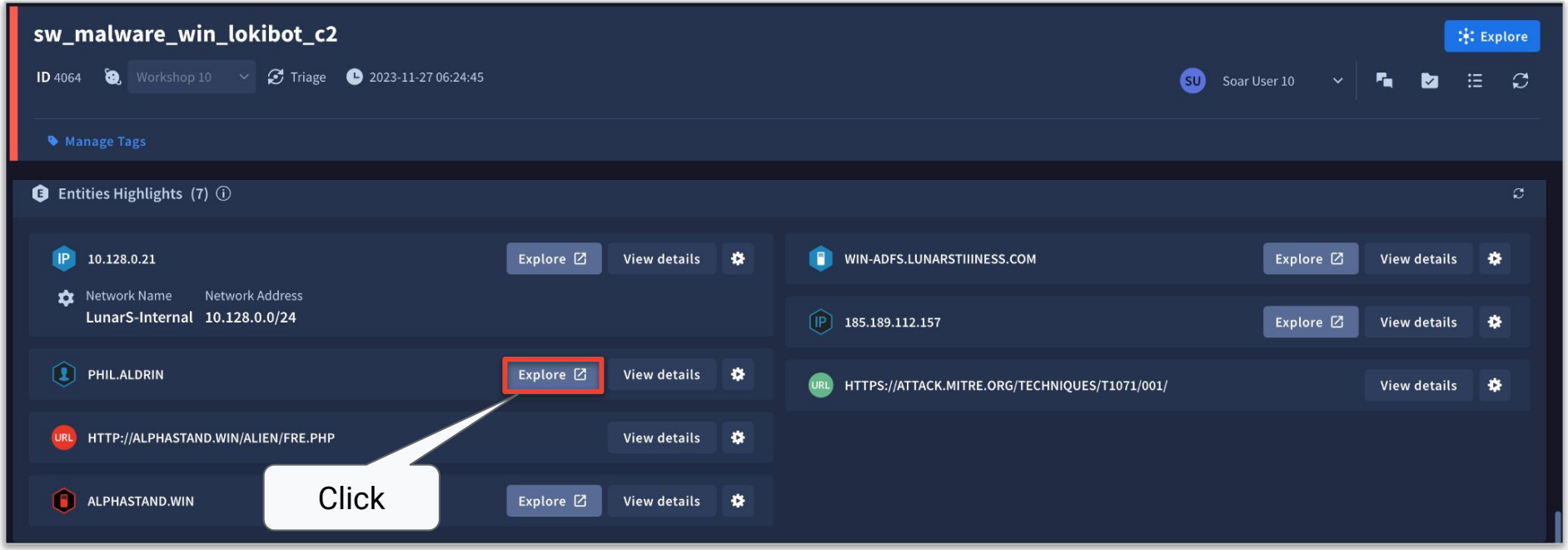
Alert - Graph

Google SecOps



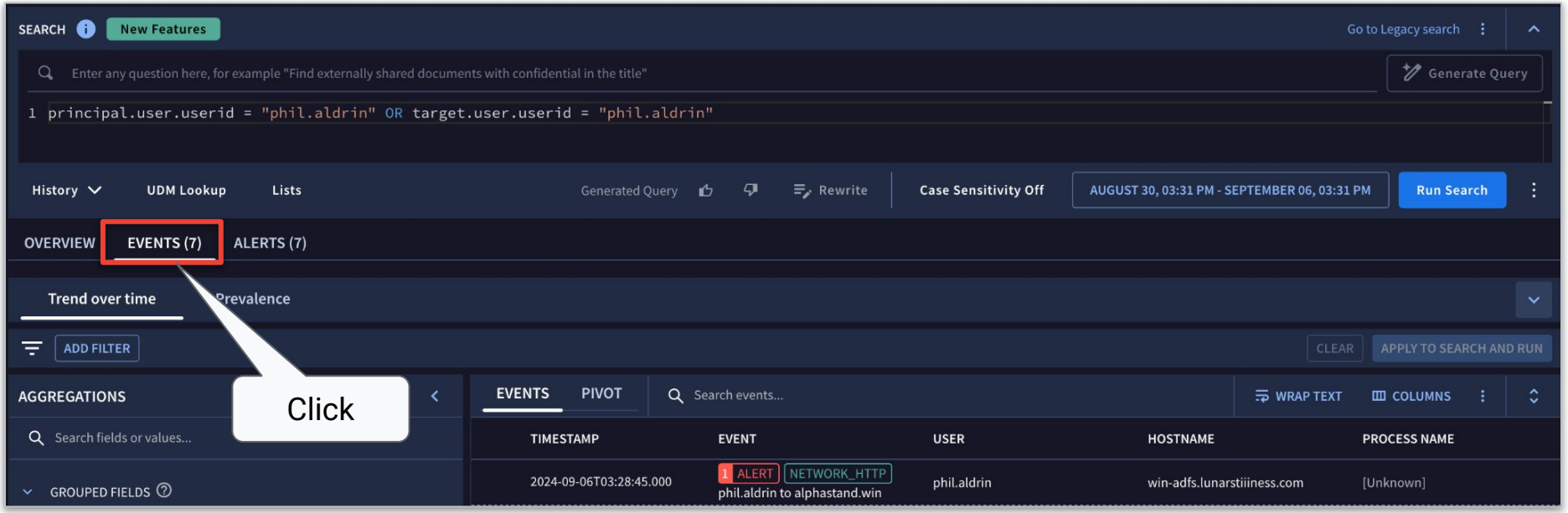
Entity Highlights - Case and Alerts

Google SecOps



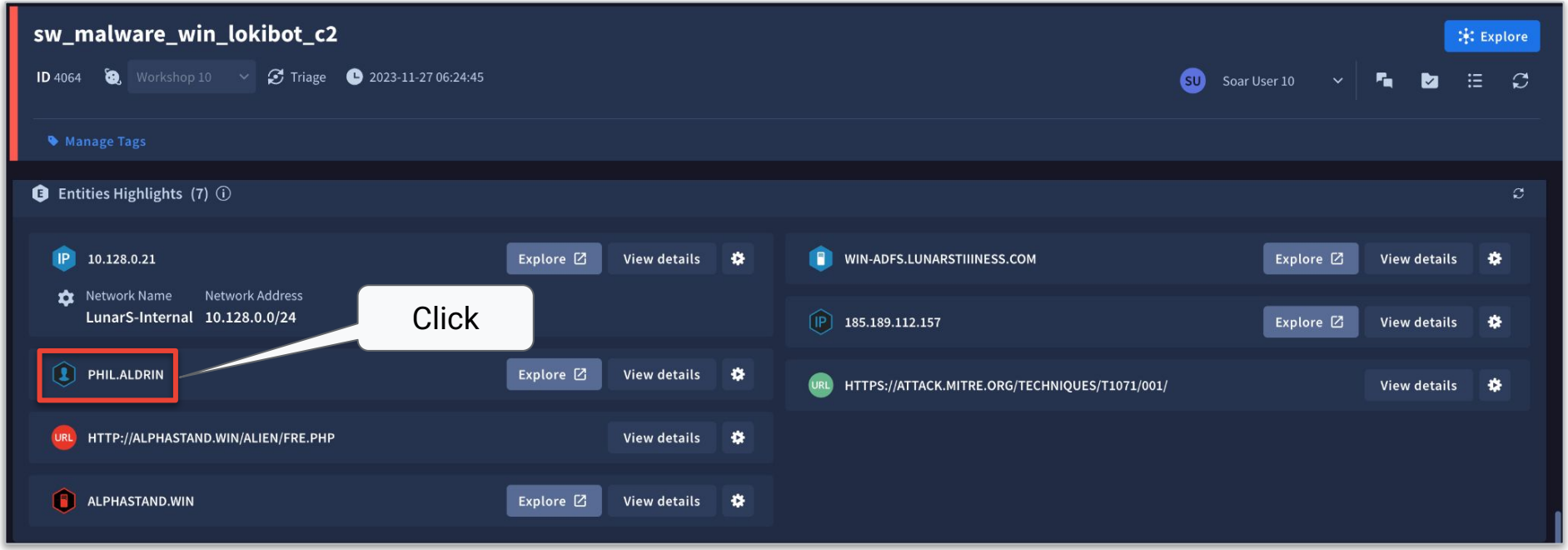
User Overview, Events and Alerts

Google SecOps



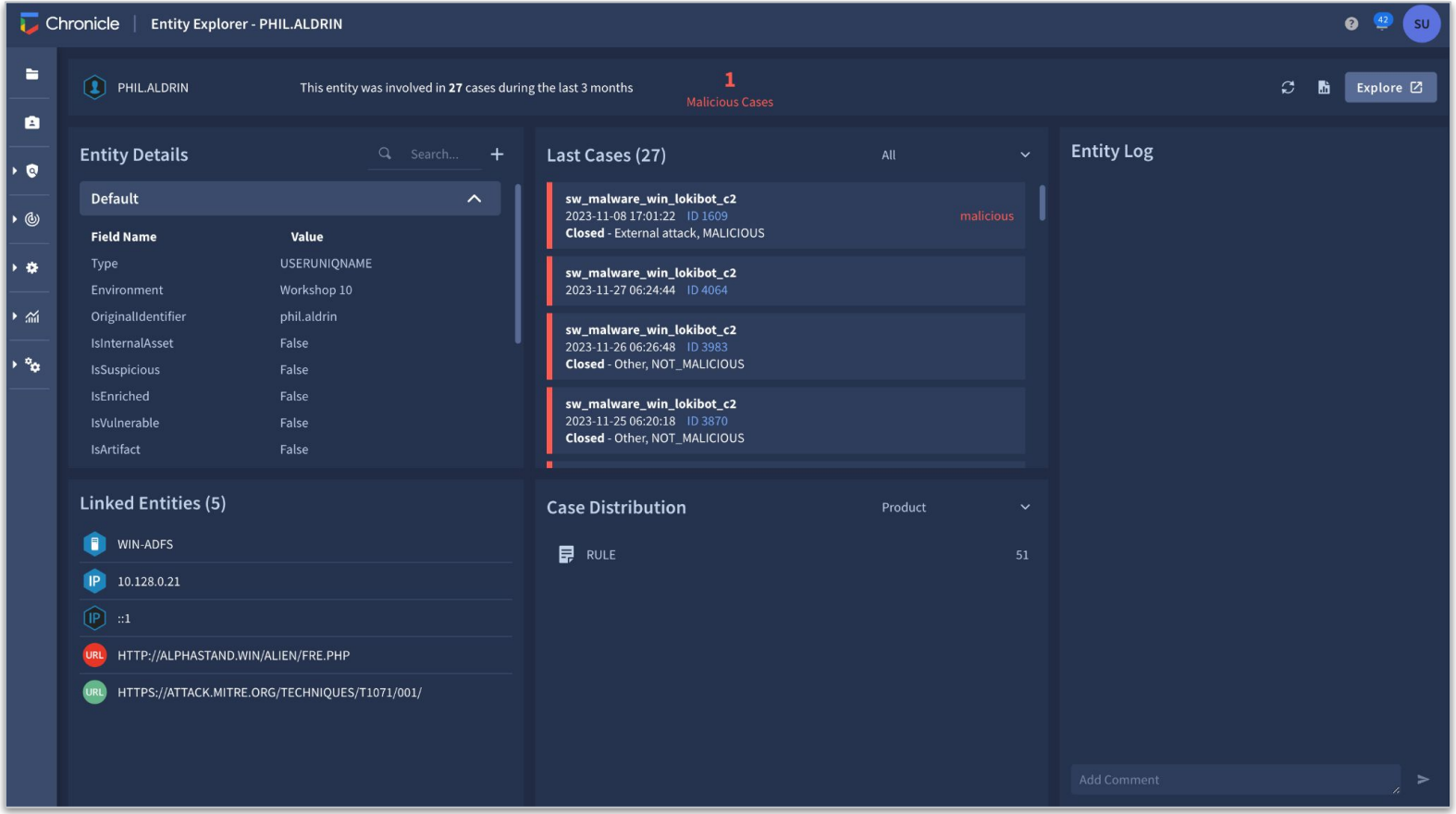
Entity Highlights - Case and Alerts

Google SecOps



Entity Explorer

Google SecOps



Google

Exercise: Exploring Our Case Further

Google SecOps

With a better understanding of how cases and alerts are displayed in Google SecOps, let's further explore this case to answer the following questions

Based on the VirusTotal Insights in the Case Overview tab:

- What does Sophos classify the URL as?
- When was the domain alphastand.win created?

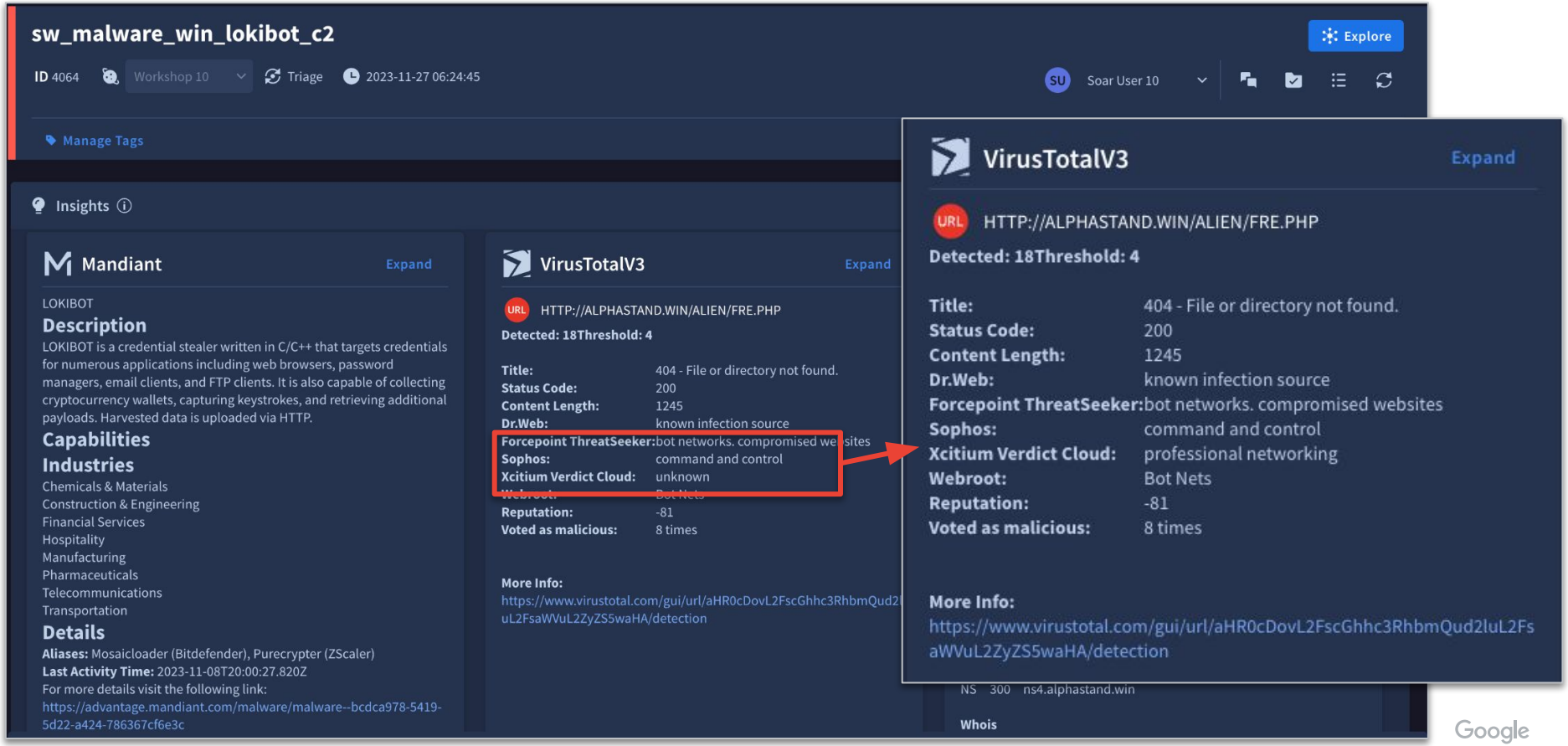
Within the alert, what is the http user agent for the event that triggered the alert?

Pivoting to an IP specific view, is the external IP address in the Entities Highlights section communicating with other systems in our environment?

Are there any specific entities in the highlights that jumped out and make you want to look into them further?

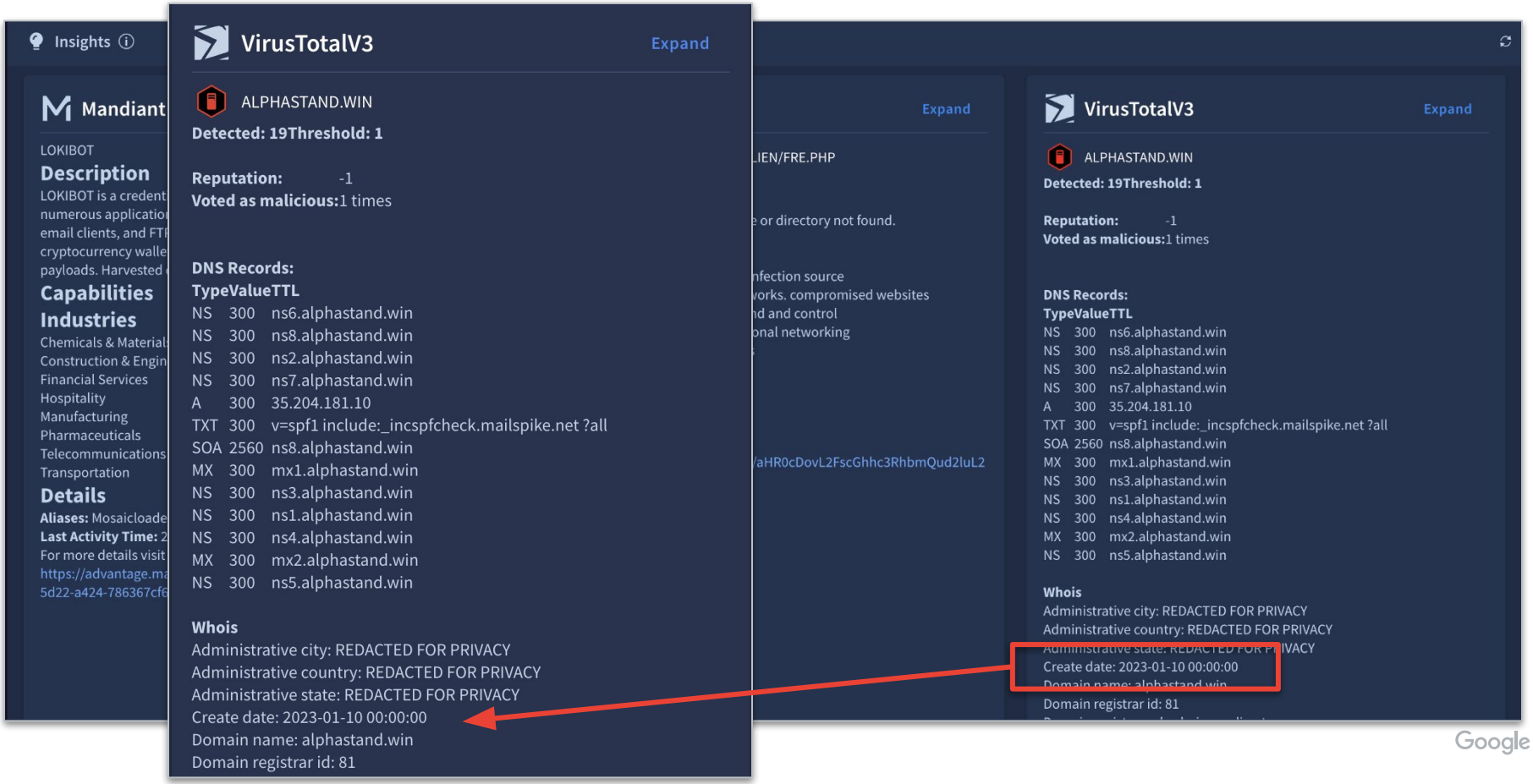
What does Sophos Classify the URL as?

Google SecOps



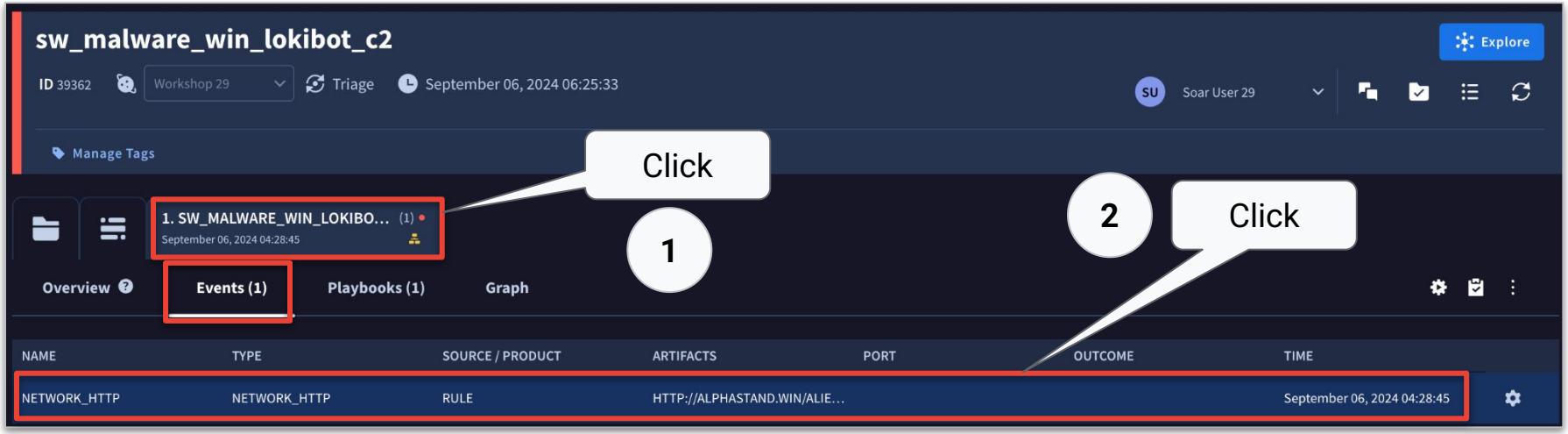
When was the domain alphastand.win created?

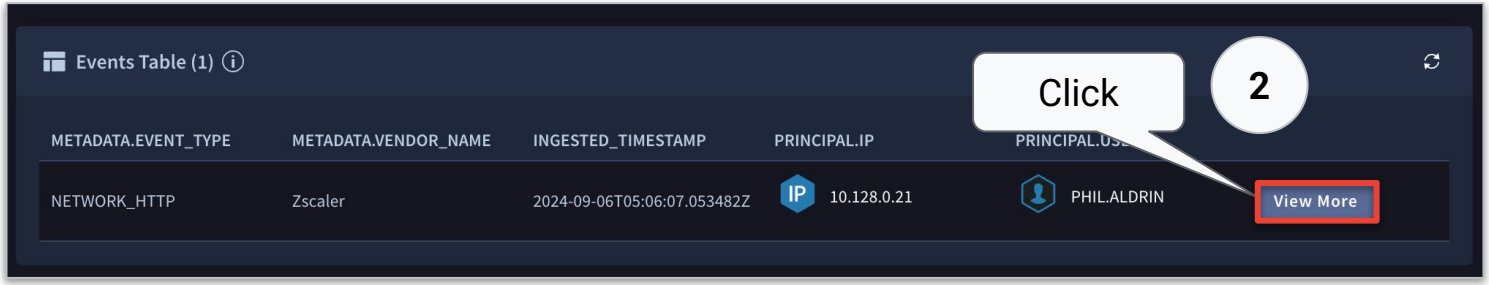
Google SecOps



Within the alert, what is the http user agent for the event that triggered the alert? (1/2)

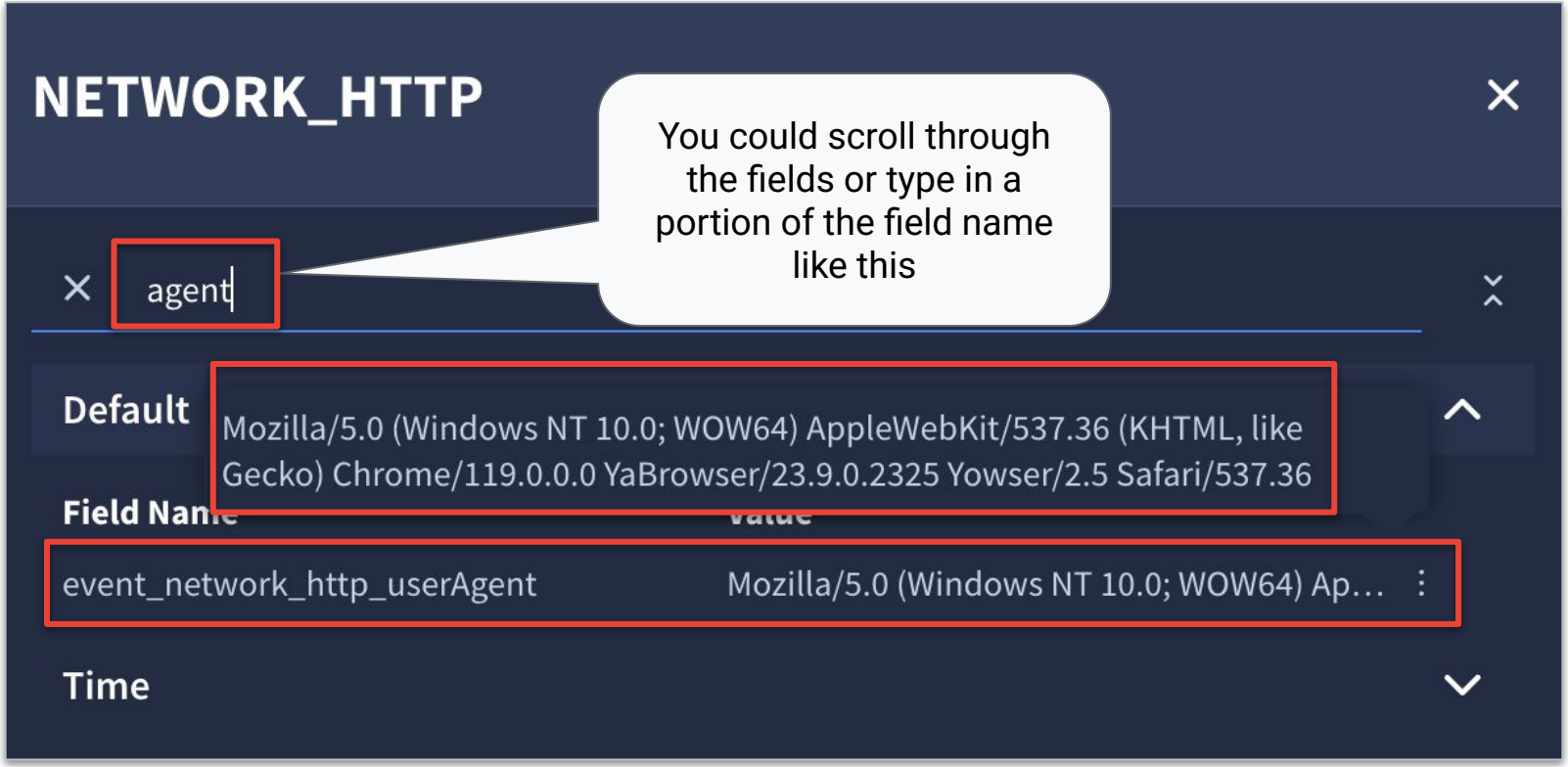
Google SecOps





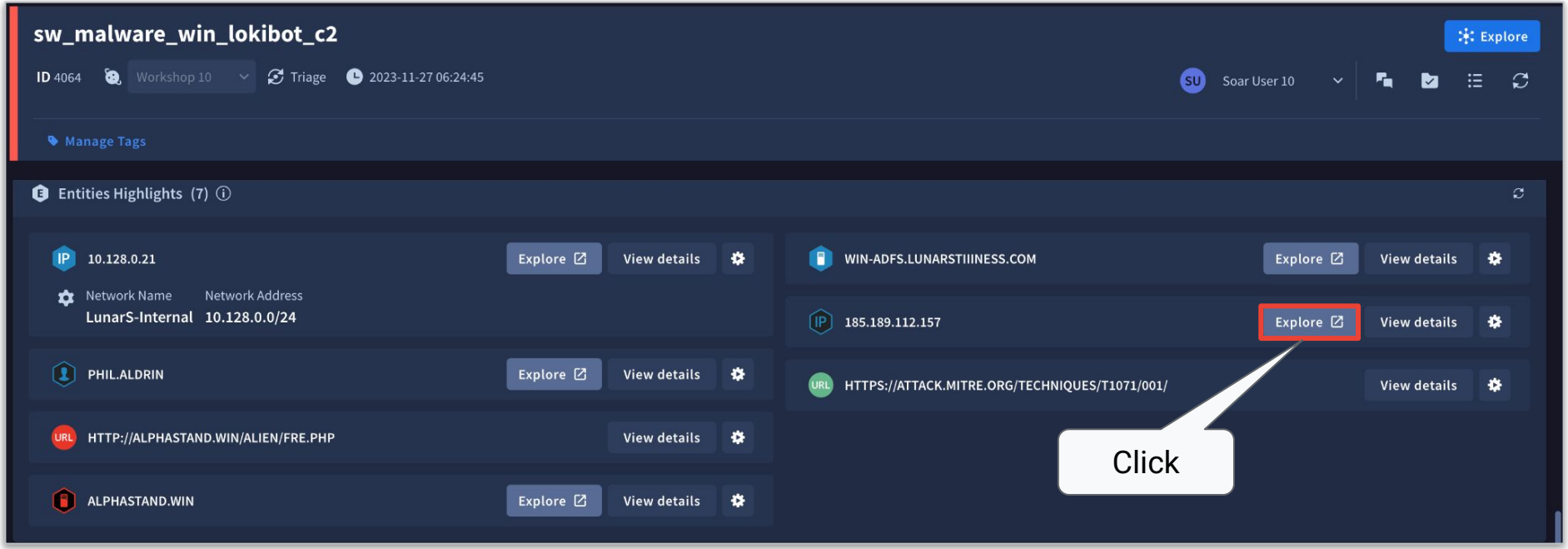
Google

Within the alert, what is the http user agent for the event that triggered the alert? (2/2)



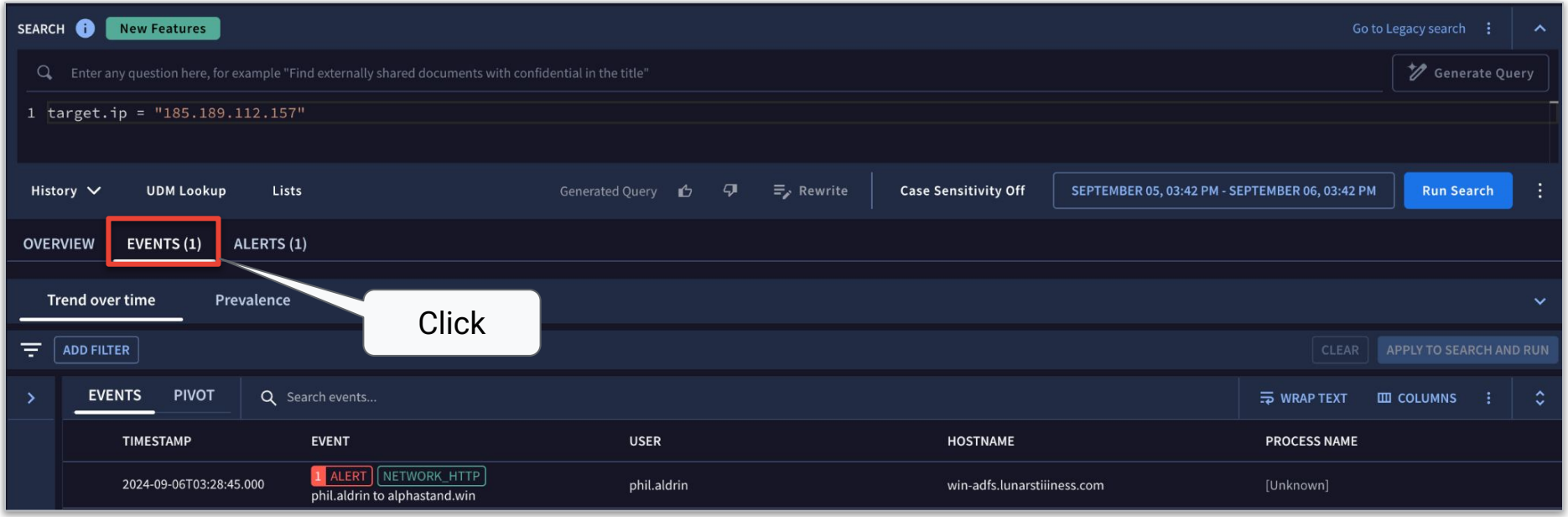
Is the external IP address in the Entities Highlights widget communicating with other systems? (1/2)

Google SecOps



Is the external IP address in the Entities Highlights widget communicating with other systems?(2/2)

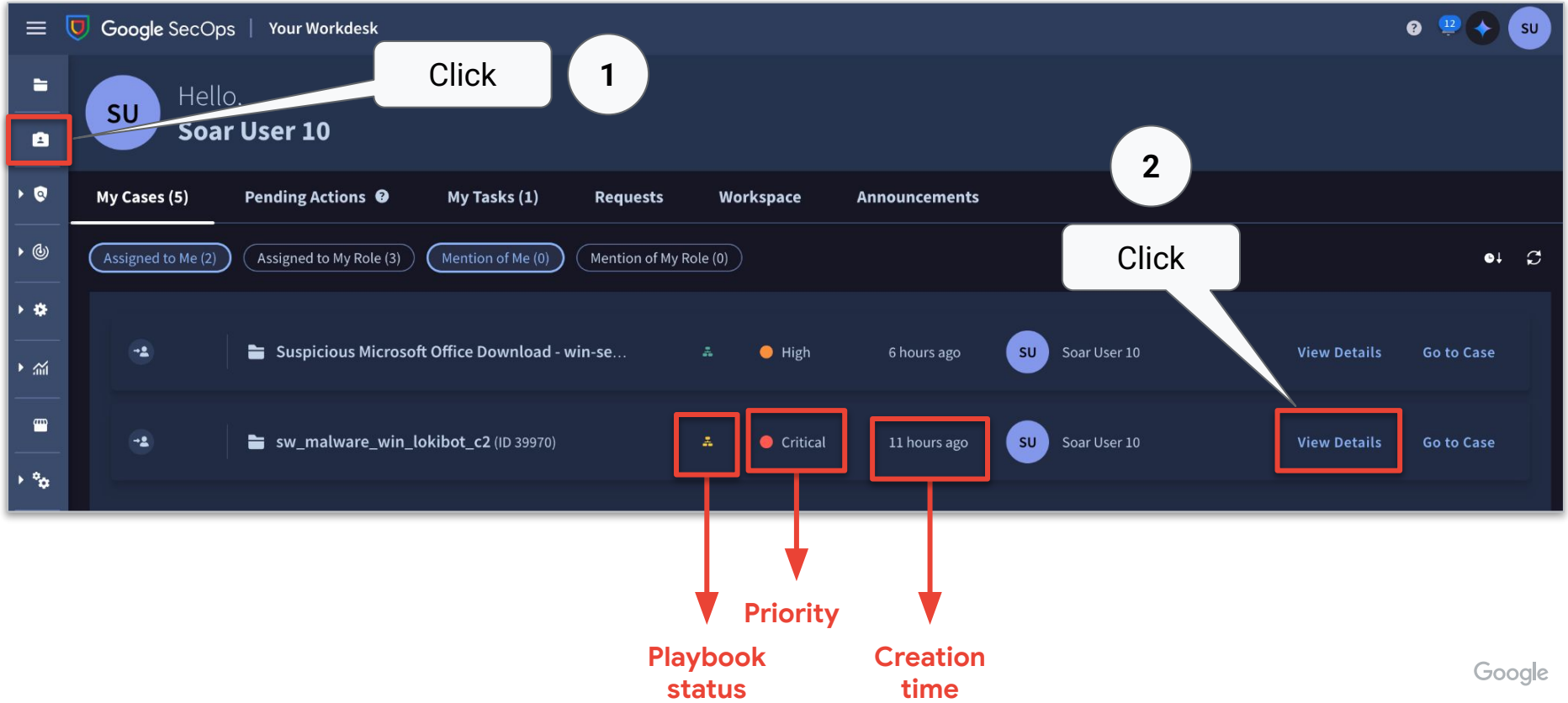
Google SecOps



Your Workdesk

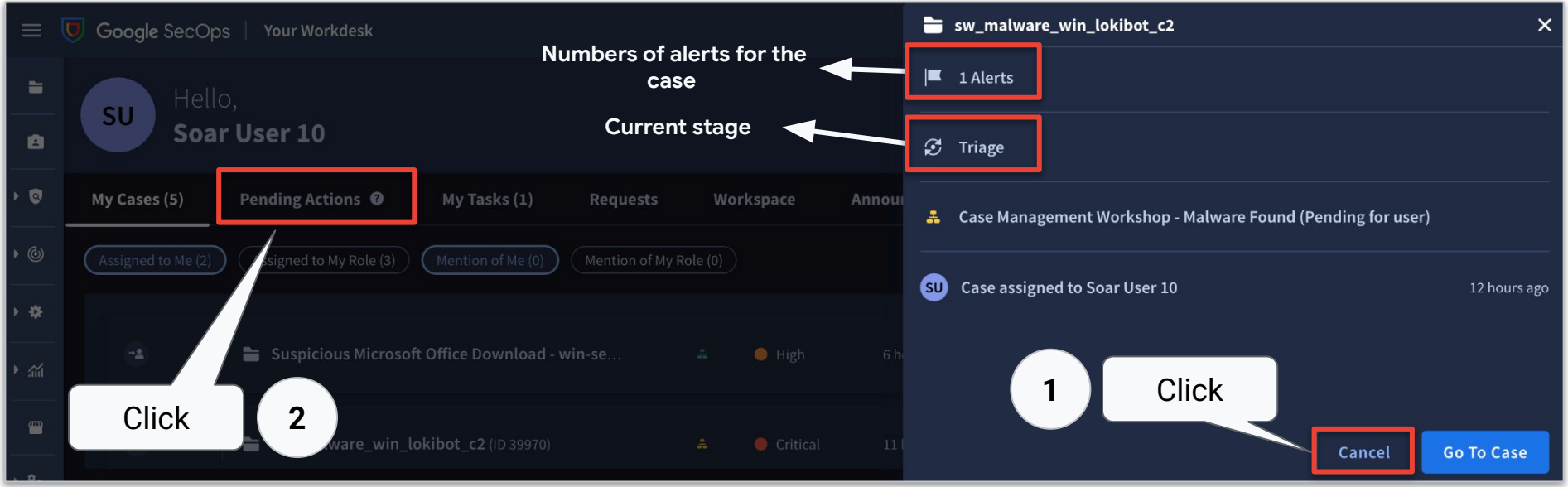
My Cases

Google SecOps



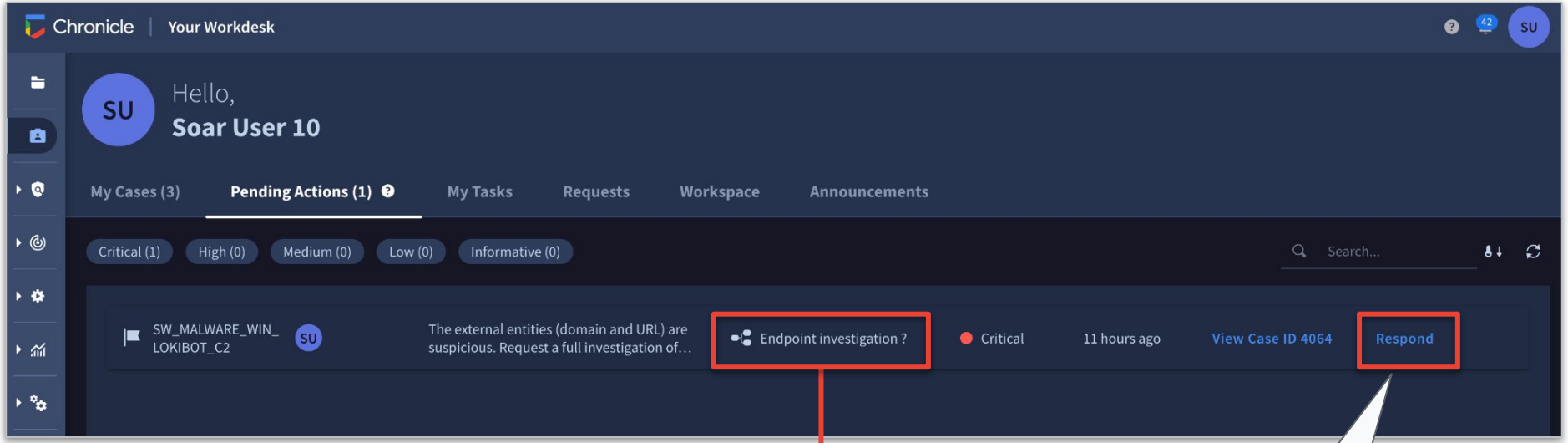
Case Summary Status

Google SecOps



Pending Actions

Google SecOps



Name of the stage/ step in the playbook

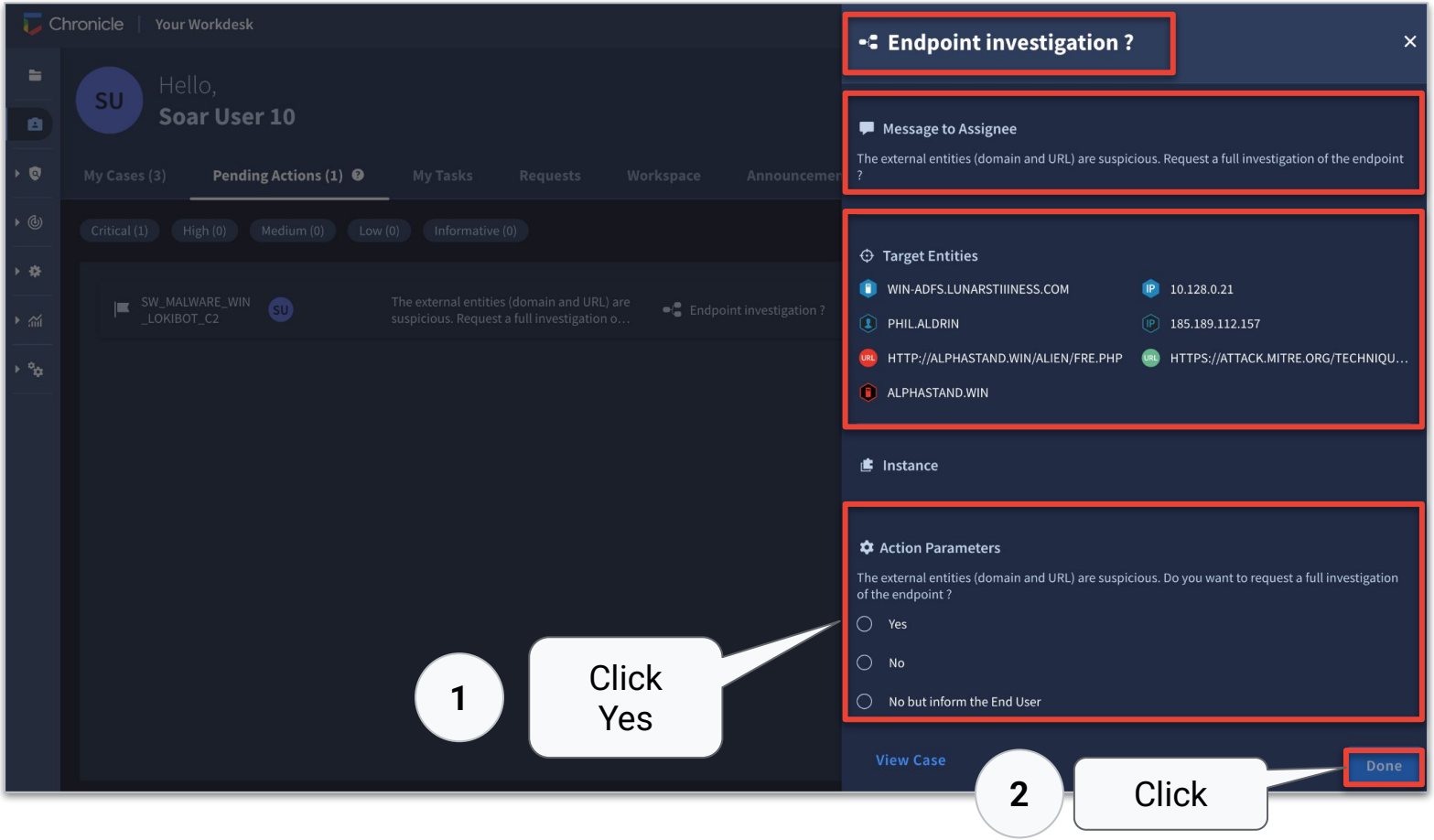
Click

Google

Pending Action Details

Current step in the Playbook

Google SecOps



Additional information:
It is an external threat

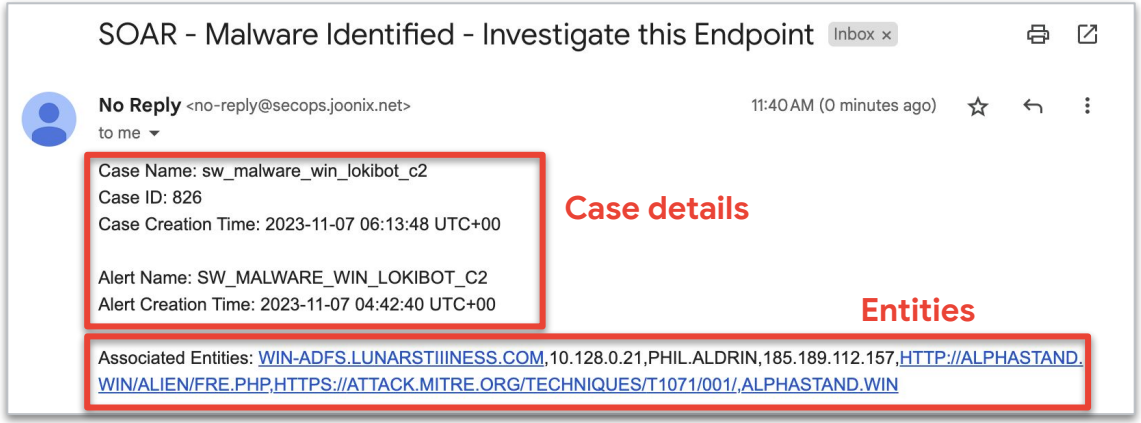
Target Entities:
Malicious Domain
Malicious URL
External IP Address
Username
Hostname
Internal IP Address
MITRE ATT&CK Technique

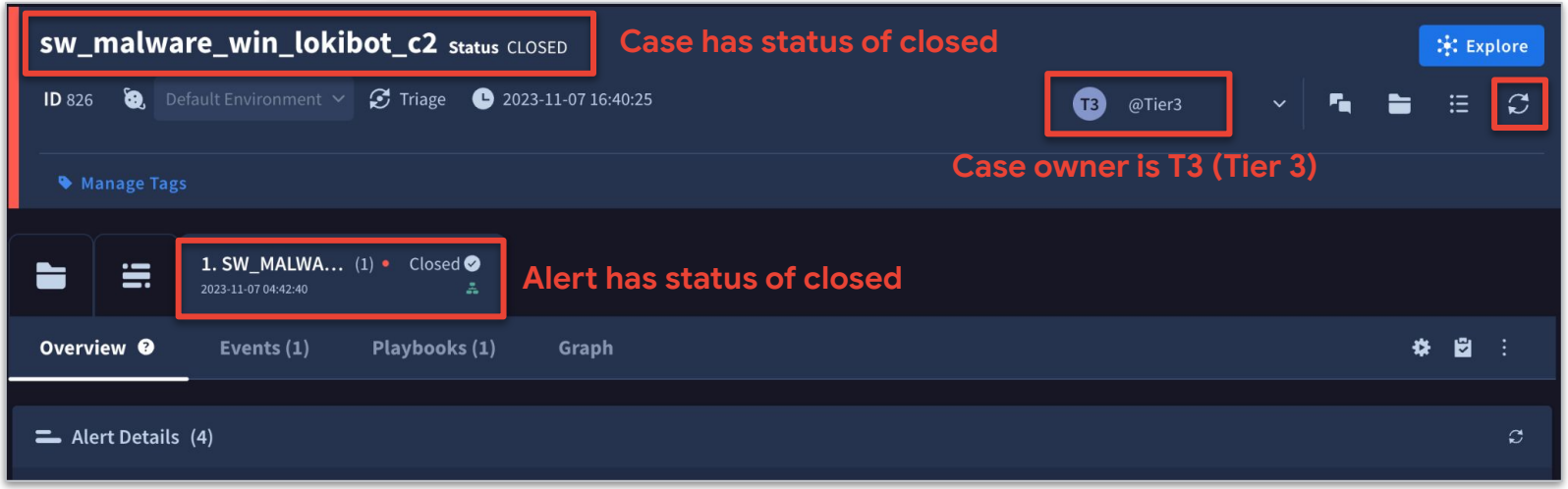
Pending Playbook Action:
Analyst response requested

Google

Responding and Taking Action

Google SecOps





Google

Manual Actions

Manual Actions

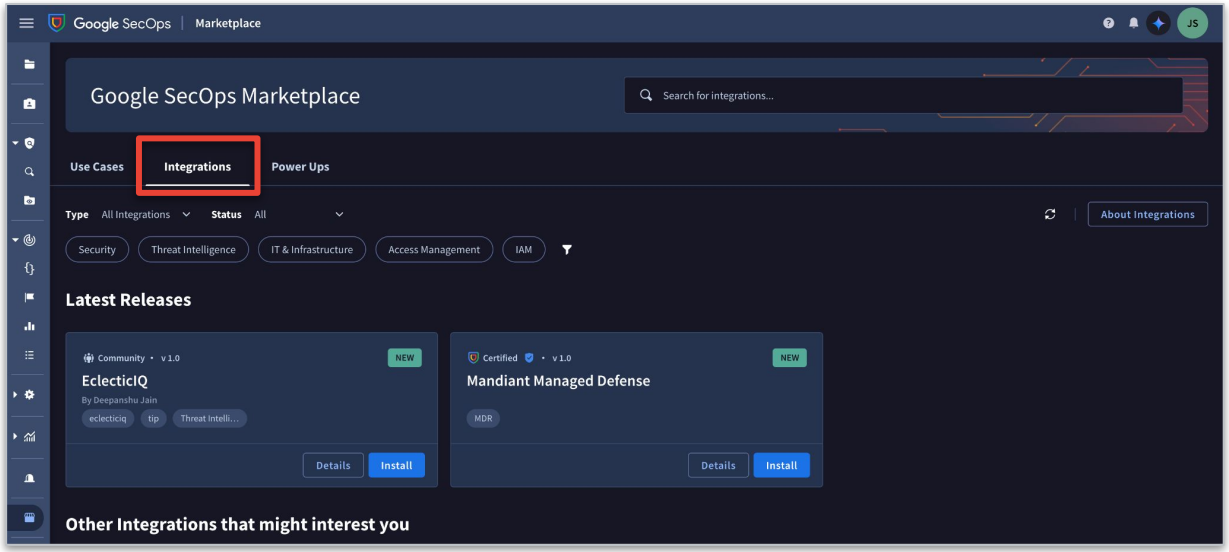
Google SecOps

Can be triggered on a per entity basis

Provides additional context around entities in an alert or case

Dependent upon the integrations installed on your instance

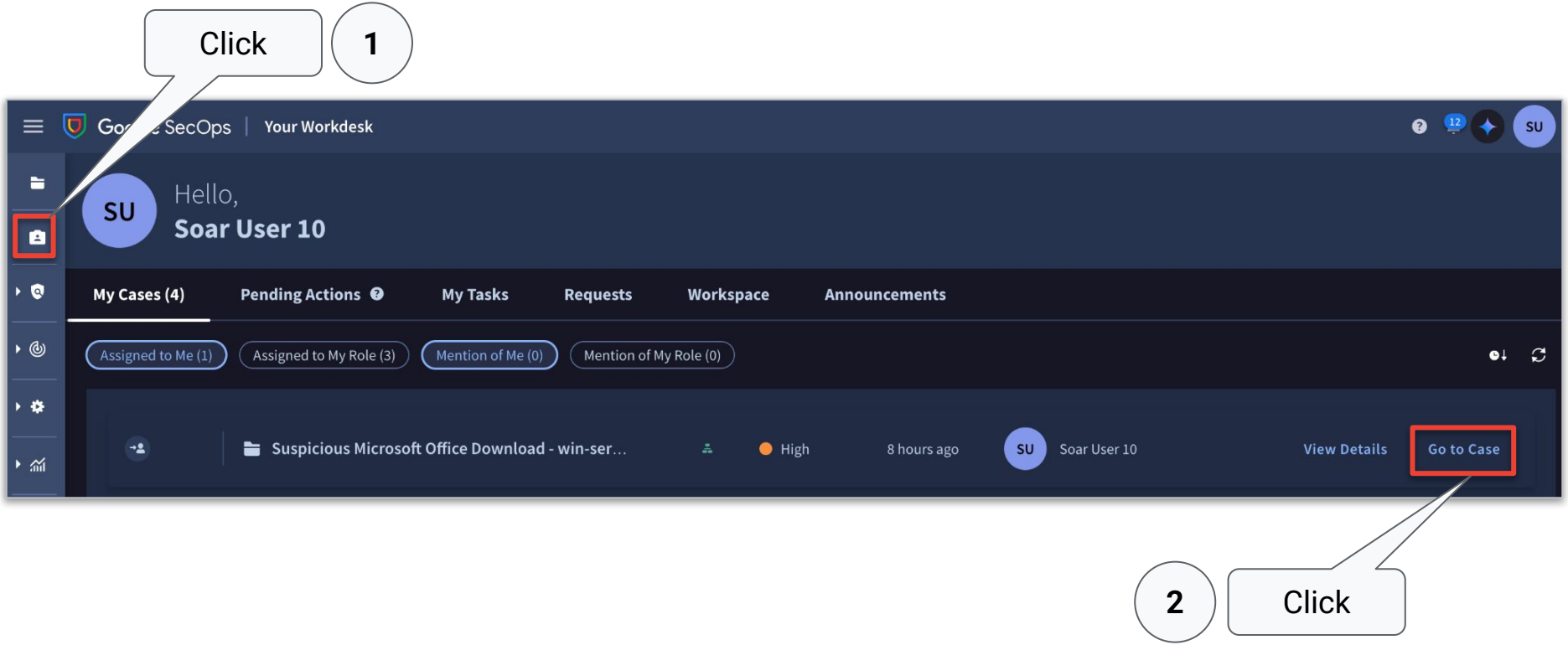
Will highlight Google SecOps, Mandiant and VirusTotal today but additional integrations can be downloaded from the Marketplace



Google

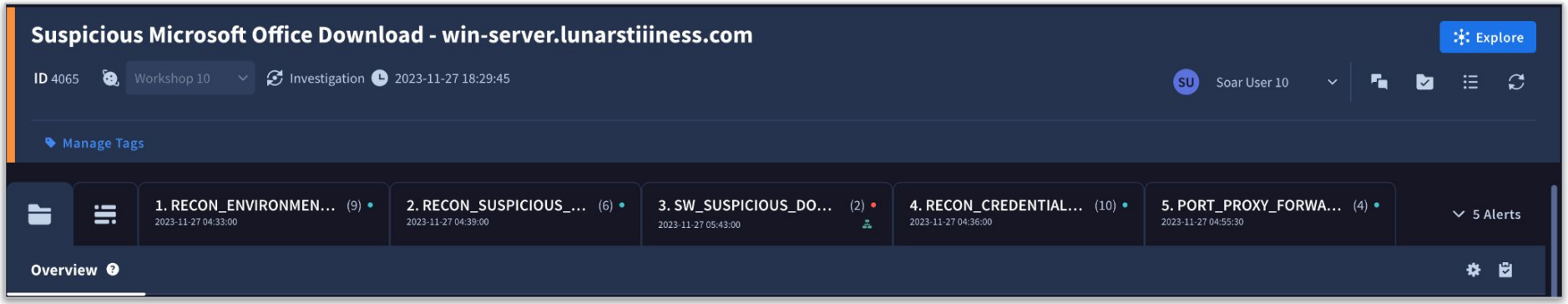
Navigate to a Case from Your Workdesk

Google SecOps



Cases & Alerts Review

Google SecOps



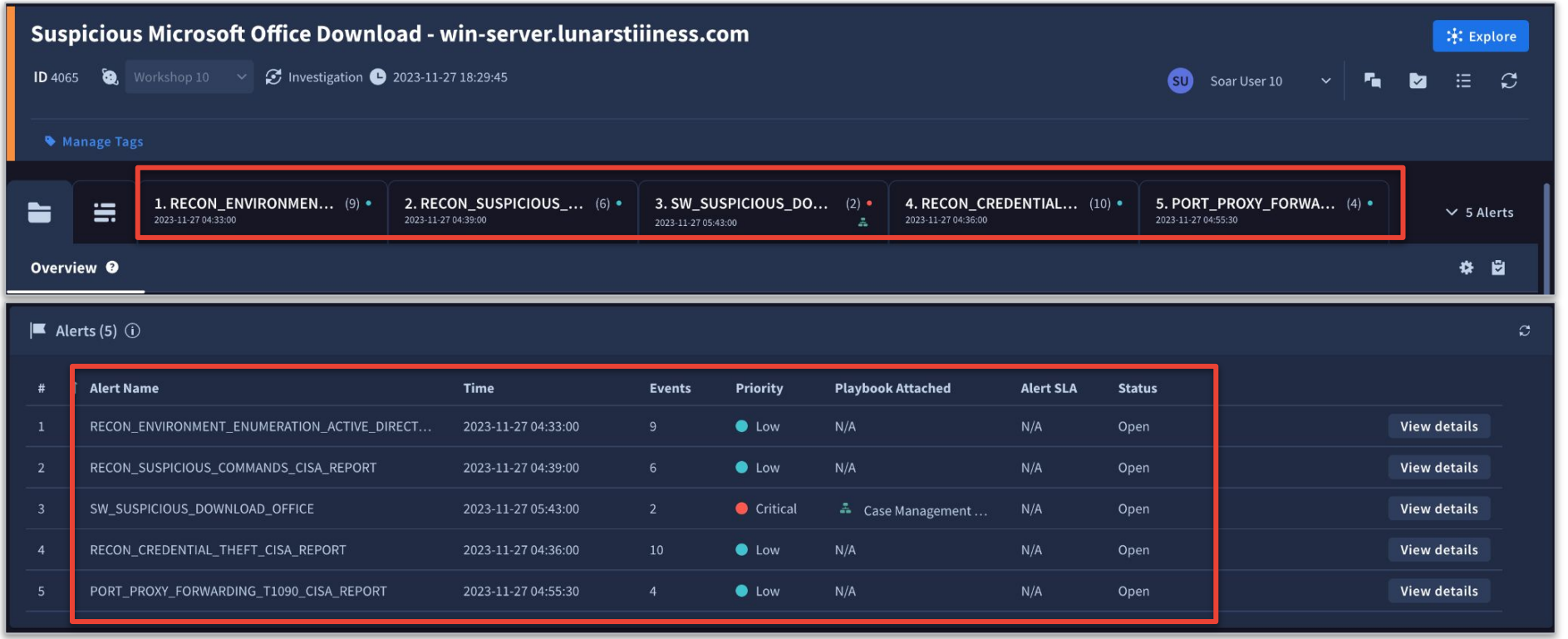
How many alerts are a part of this case?

How many events are part of each alert?

Have playbooks been run on any alerts yet? If so, which ones and what are their current state?

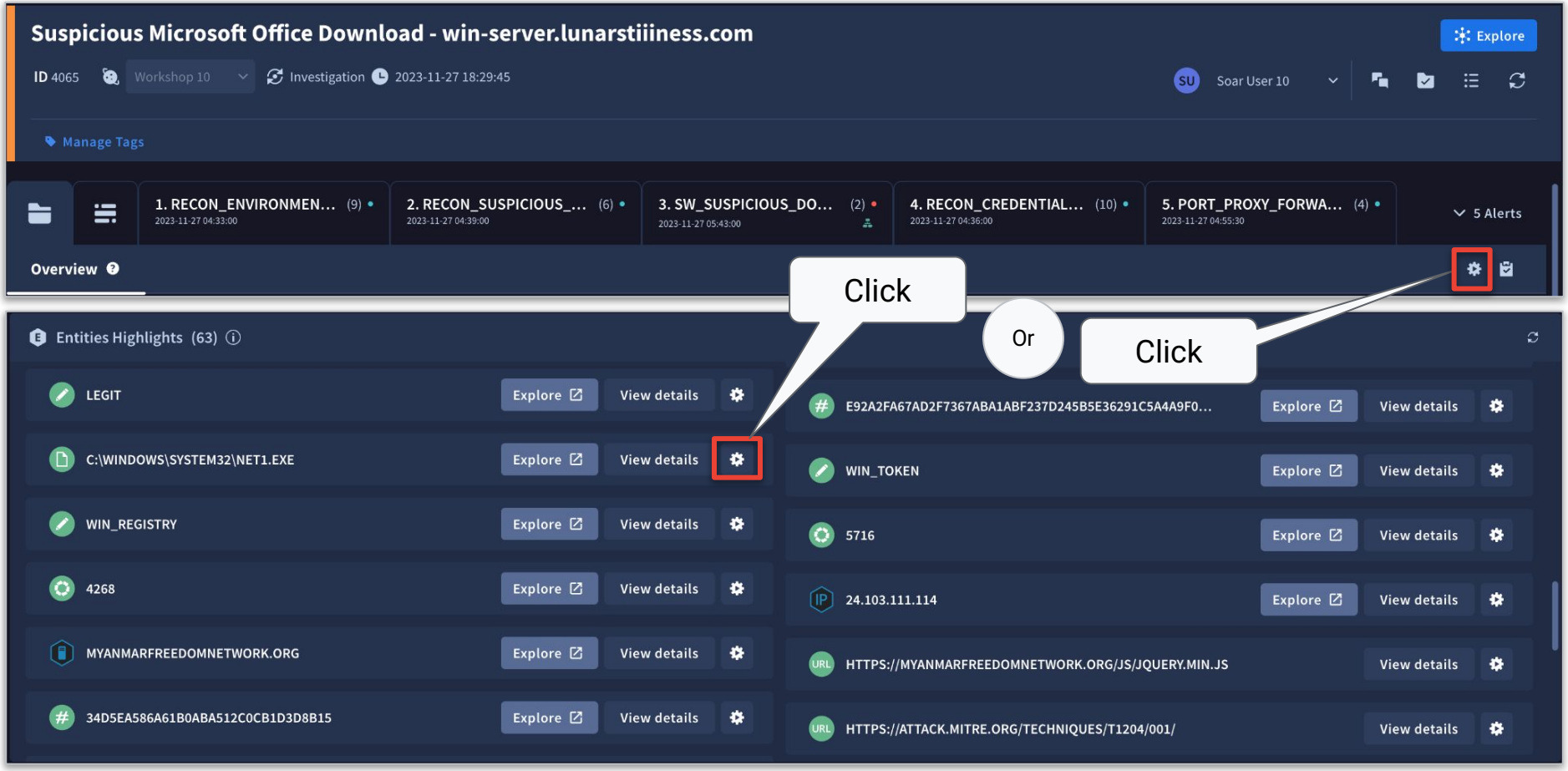
Cases & Alerts Review

Google SecOps



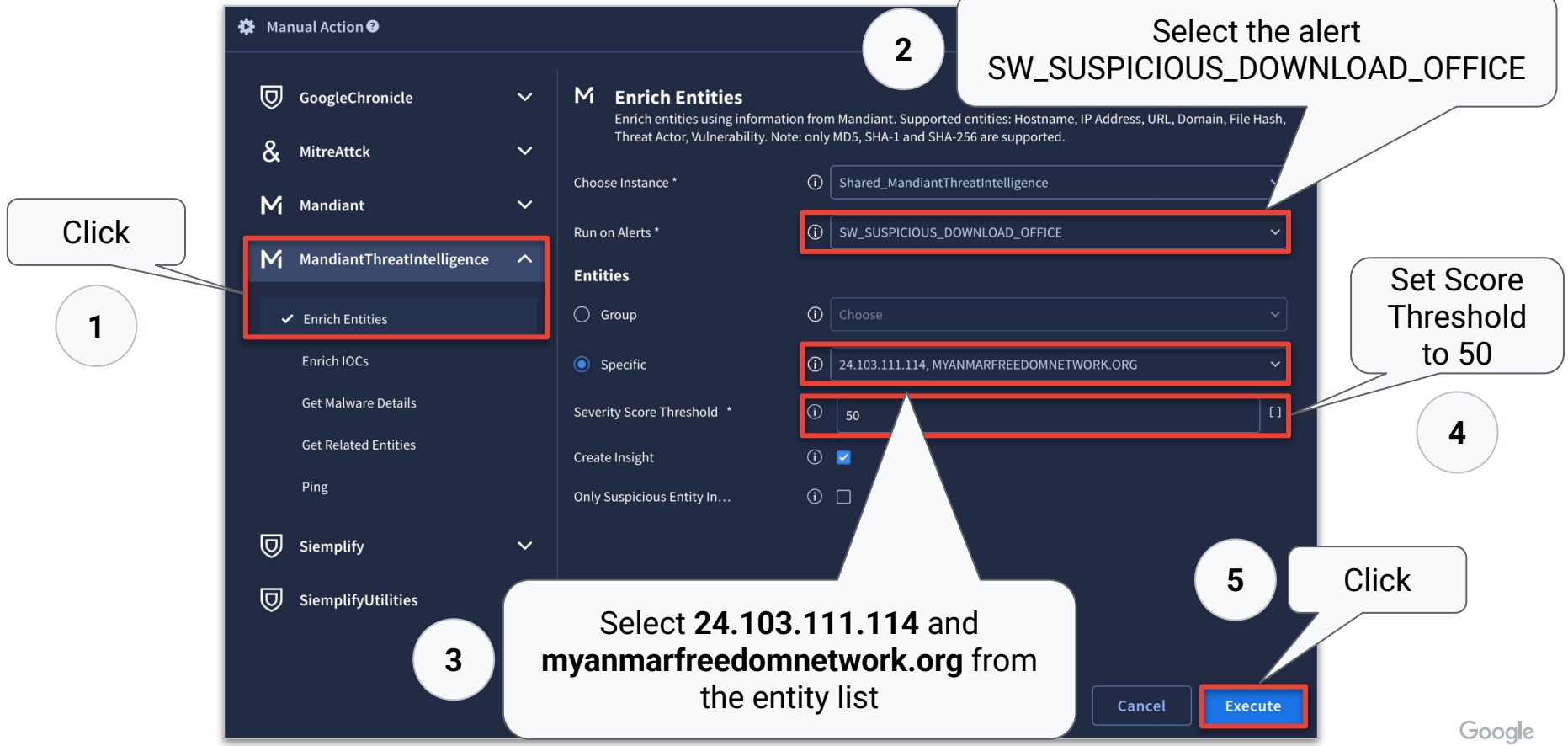
Manual Actions - Case View

Google SecOps



Manual Action - Mandiant Enrich Entities

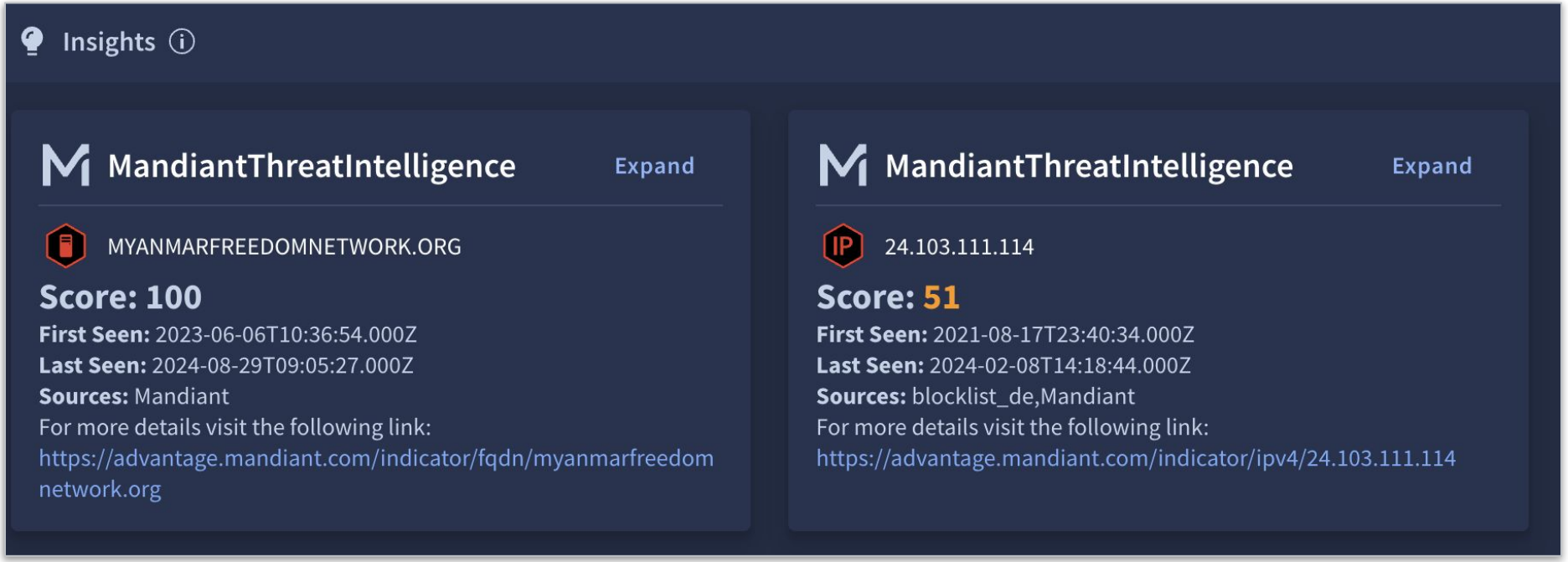
Google SecOps



Google

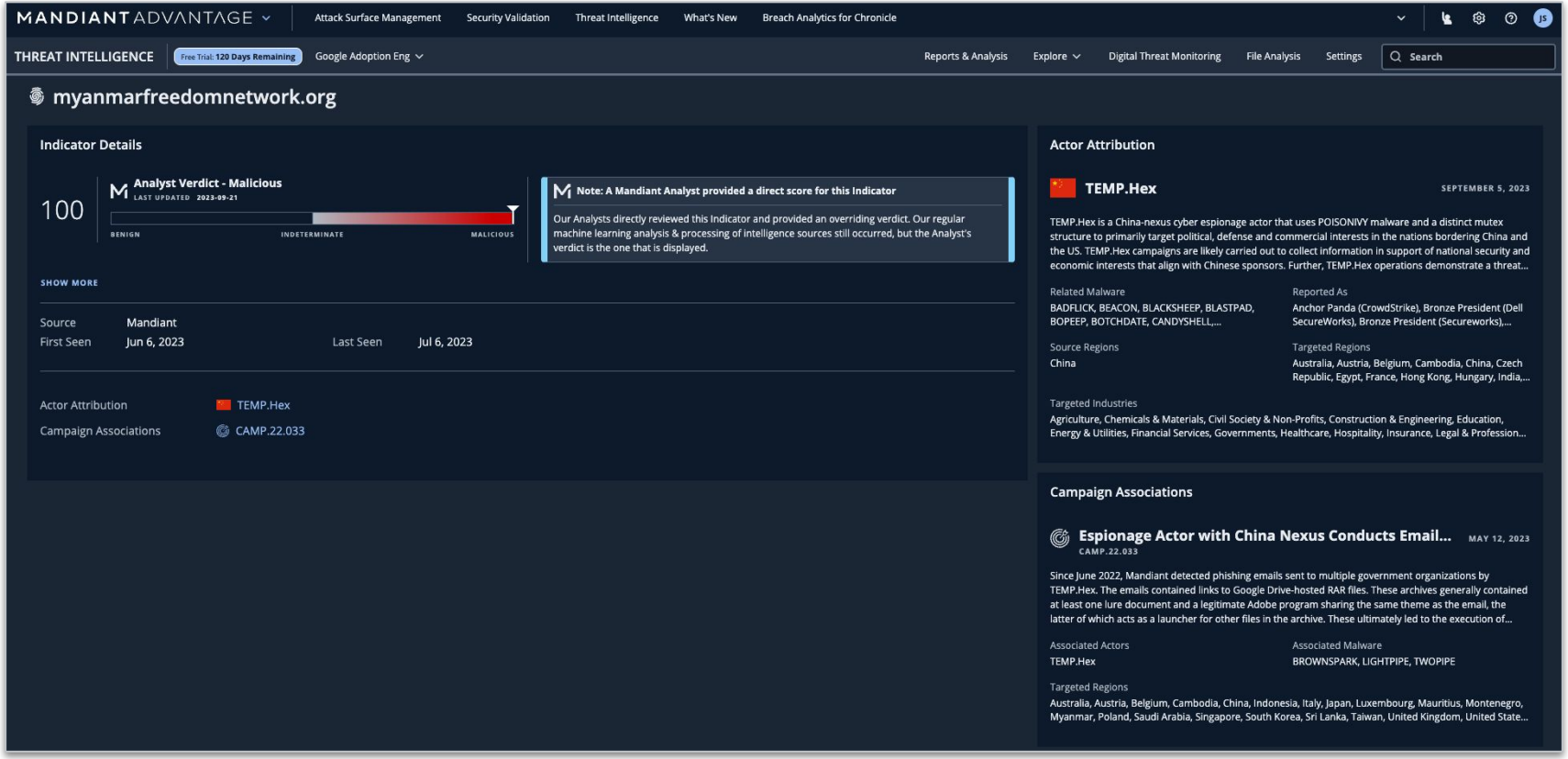
Insights

Google SecOps



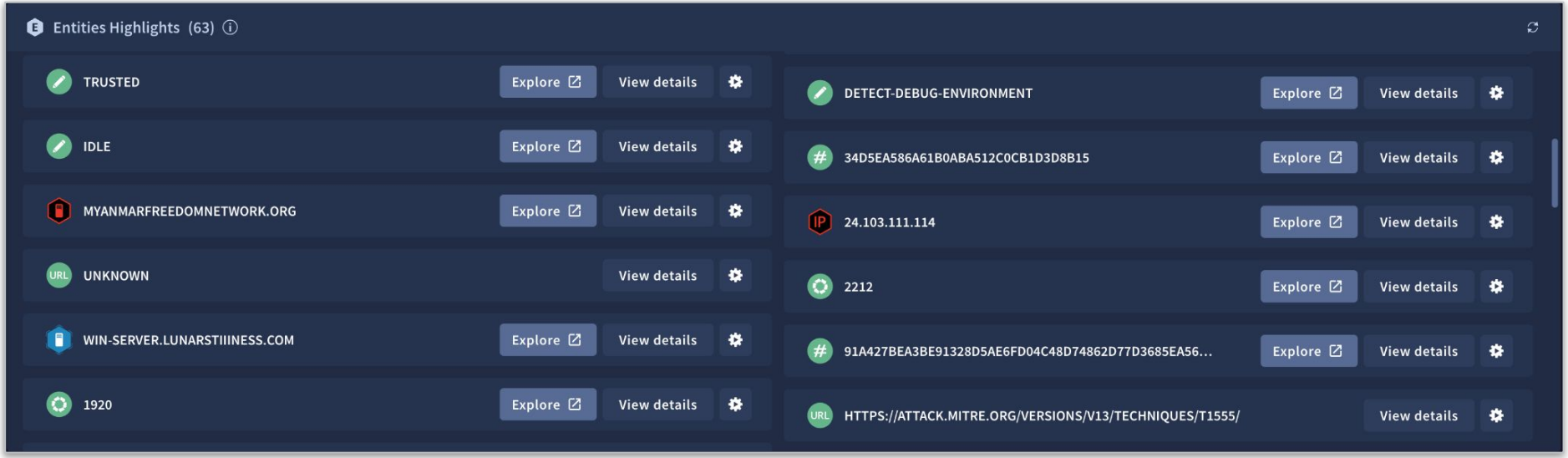
Mandiant Threat Intel Detail

Google SecOps



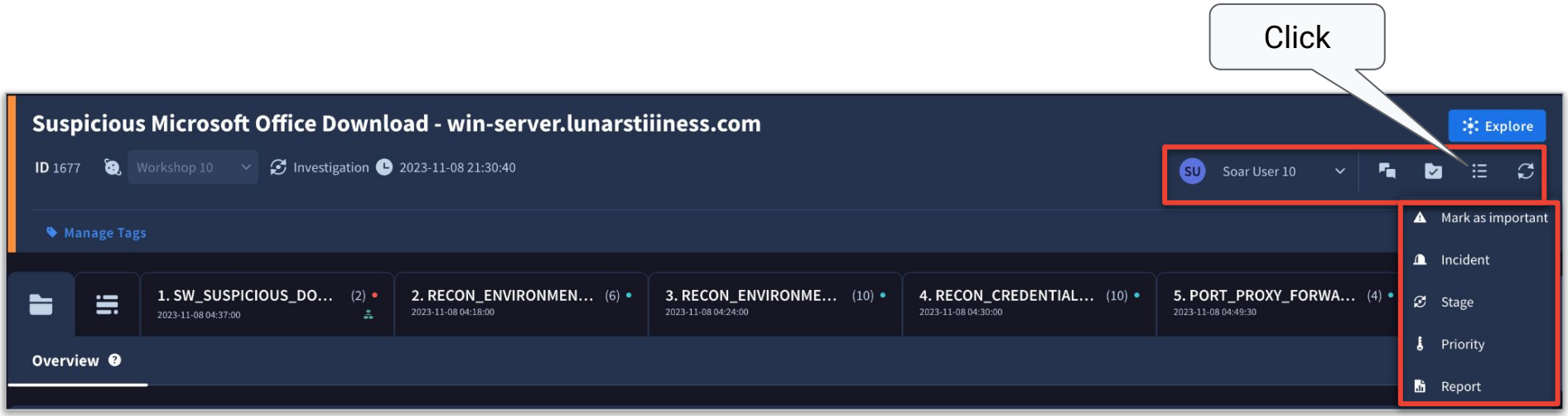
Entities Highlights - Suspicious Entities

Google SecOps



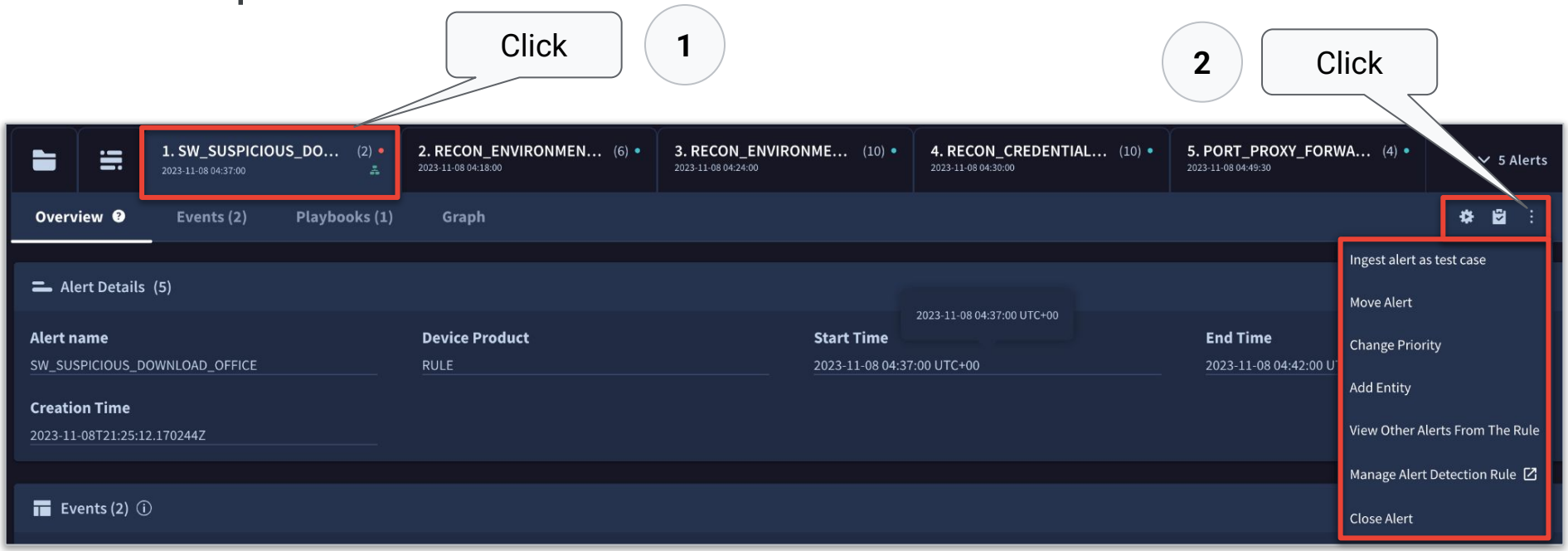
Case Options

Google SecOps



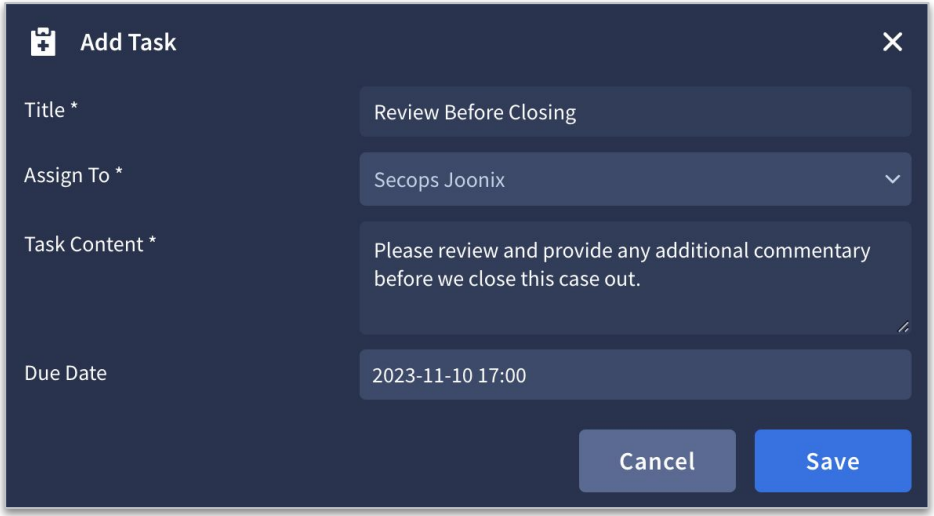
Alert Options

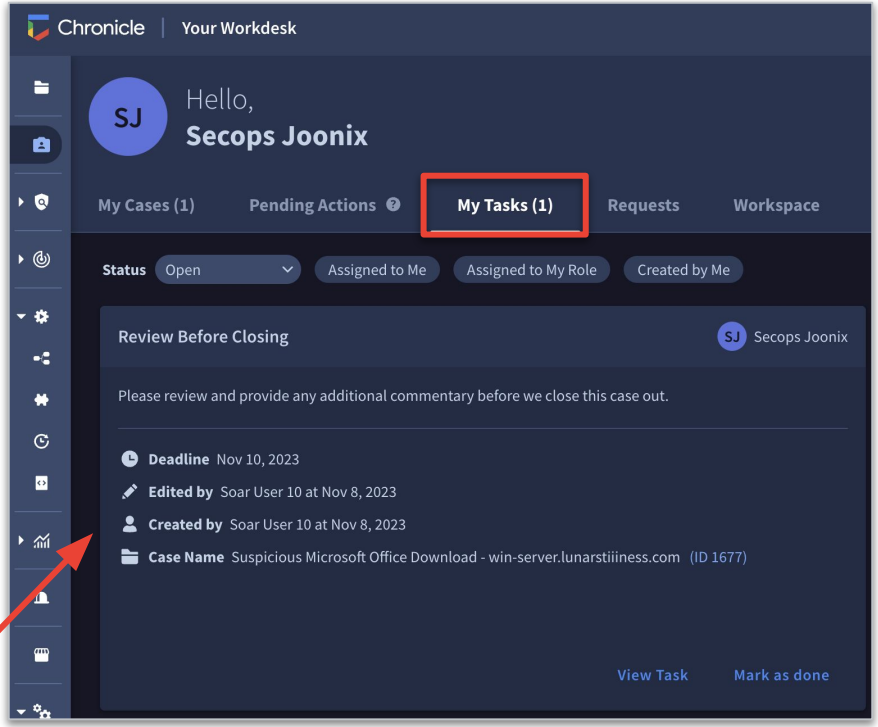
Google SecOps



Case Tasks

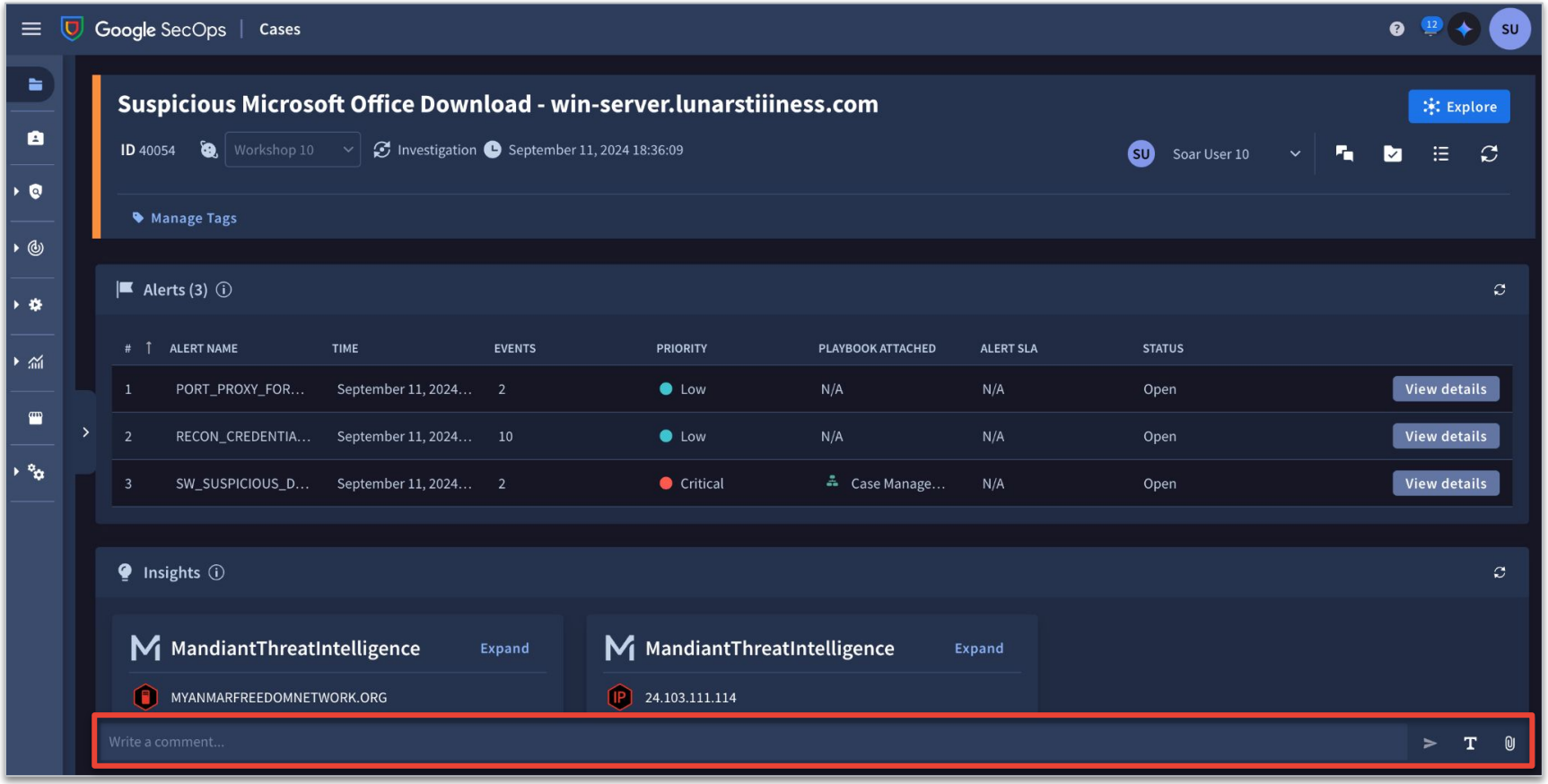
Google SecOps





Adding Files or Commentary to a Case

Google SecOps



Google

Exercise - Working in a Case

Google SecOps

Use the manual action to get related entities with a minimum score of 50 for the URL from the **Mandiant Threat Intelligence** integration for the URL: **https://myanmarfreedomnetwork.org/Js/jQuery.min.js**

- Find the results on the Case Wall and export the json output (if allowed)
- How many additional IOCs are there?
  - IP addresses? Domains? Email Addresses? File Hashes? URLs?
- Add the json attachment and a comment to the case - Validate that it was uploaded by reviewing the Case Wall

Use the manual action to get related IP addresses from VirusTotal for the domain **myanmarfreedomnetwork.org**

- What are those IP addresses?

Use the Case Tasks/Options and Alert Options to further tweak the case and alerts

- Go ahead and explore and let us know what else you find
- Note the changes on the case wall when different options are used

Exercise - Working in a Case

Google SecOps

Use the manual action to get related entities with a minimum score of 50 for the URL from the **Mandiant Threat Intelligence** integration for the URL: **https://myanmarfreedomnetwork.org/Js/jQuery.min.js**

- Find the results on the Case Wall and export the json output (if allowed)
- How many additional IOCs are there?
  - IP addresses? Domains? Email Addresses? File Hashes? URLs?
- Add the json attachment and a comment to the case - Validate that it was uploaded by reviewing the Case Wall

Use the manual action to get related IP addresses from VirusTotal for the domain **myanmarfreedomnetwork.org**

- What are those IP addresses?

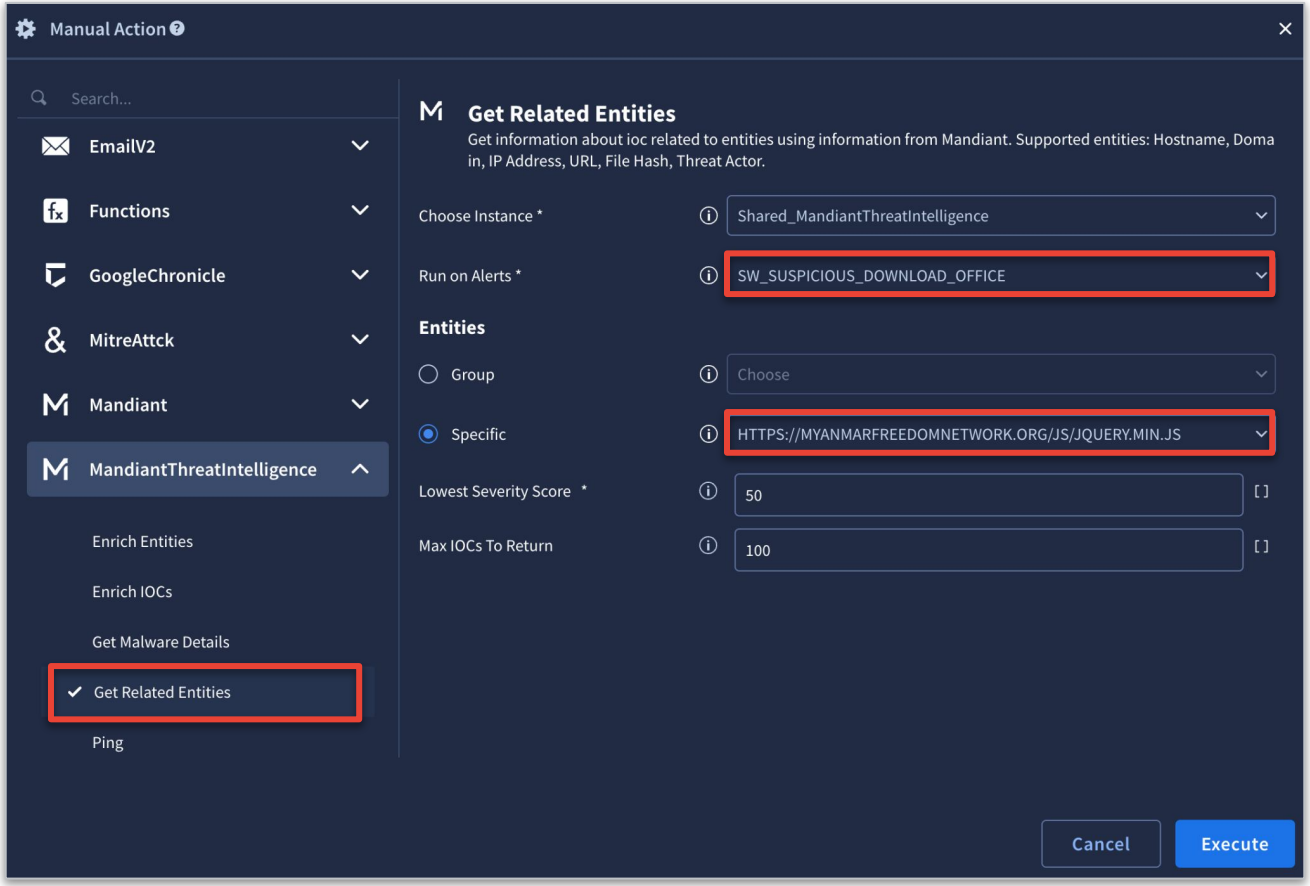
In the Entities Highlights, there should be an entity with the name **c:\program files\7-zip\7z.exe**. Our organization does not use 7-zip. Pivot and execute a search to determine which user, on what system and what processes are associated with 7-zip.

Use the Case Tasks/Options and Alert Options to further tweak the case and alerts

- Go ahead and explore and let us know what else you find
- Note the changes on the case wall when different options are used

Manual Action - Related Entities - URL

Google SecOps



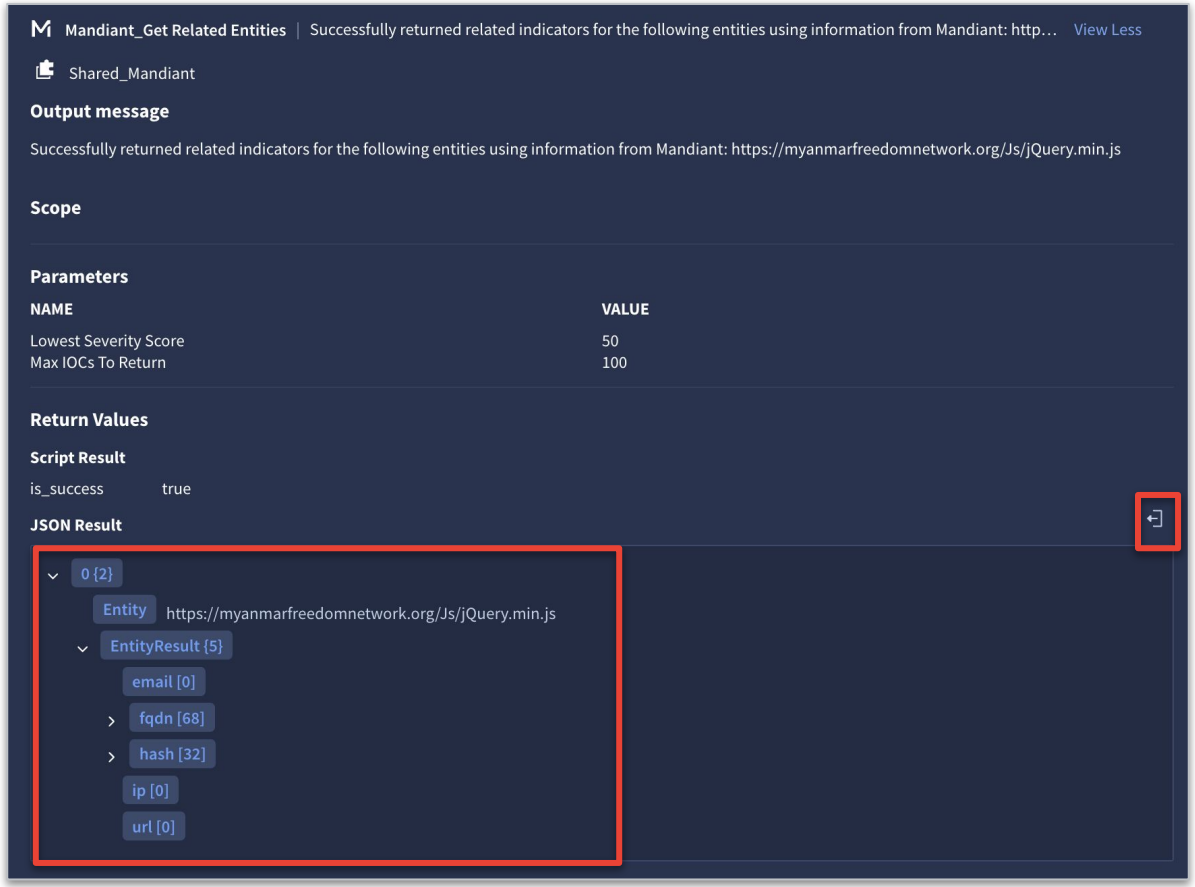
Google

Validating Actions

Google SecOps

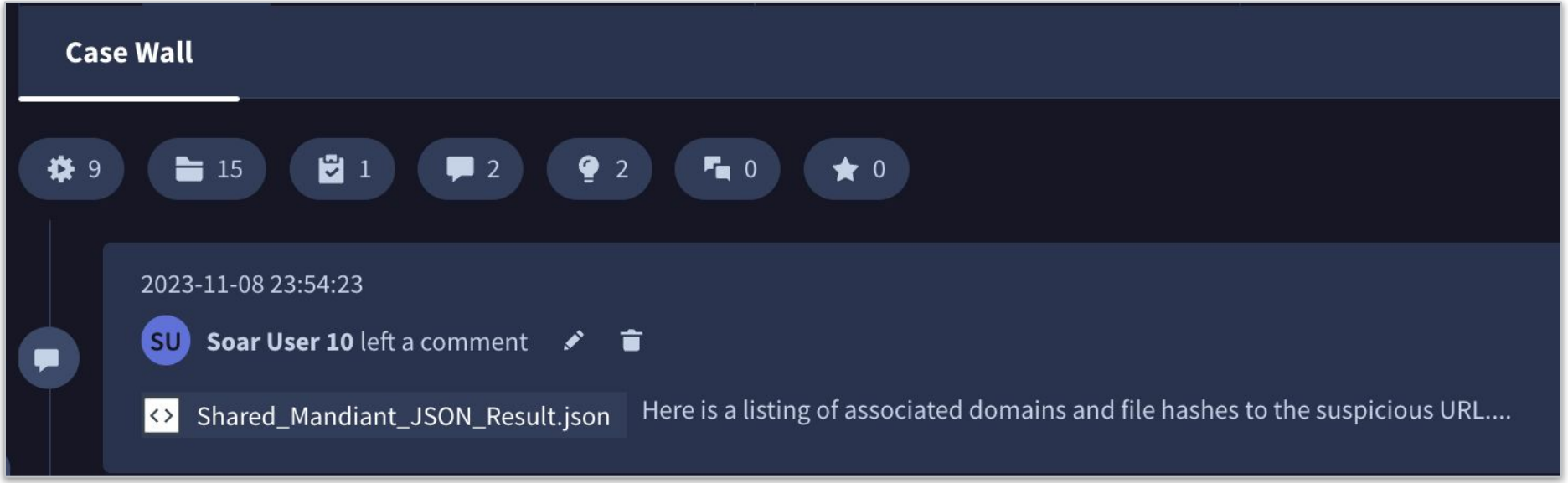
Get Related Entity Details

Google SecOps



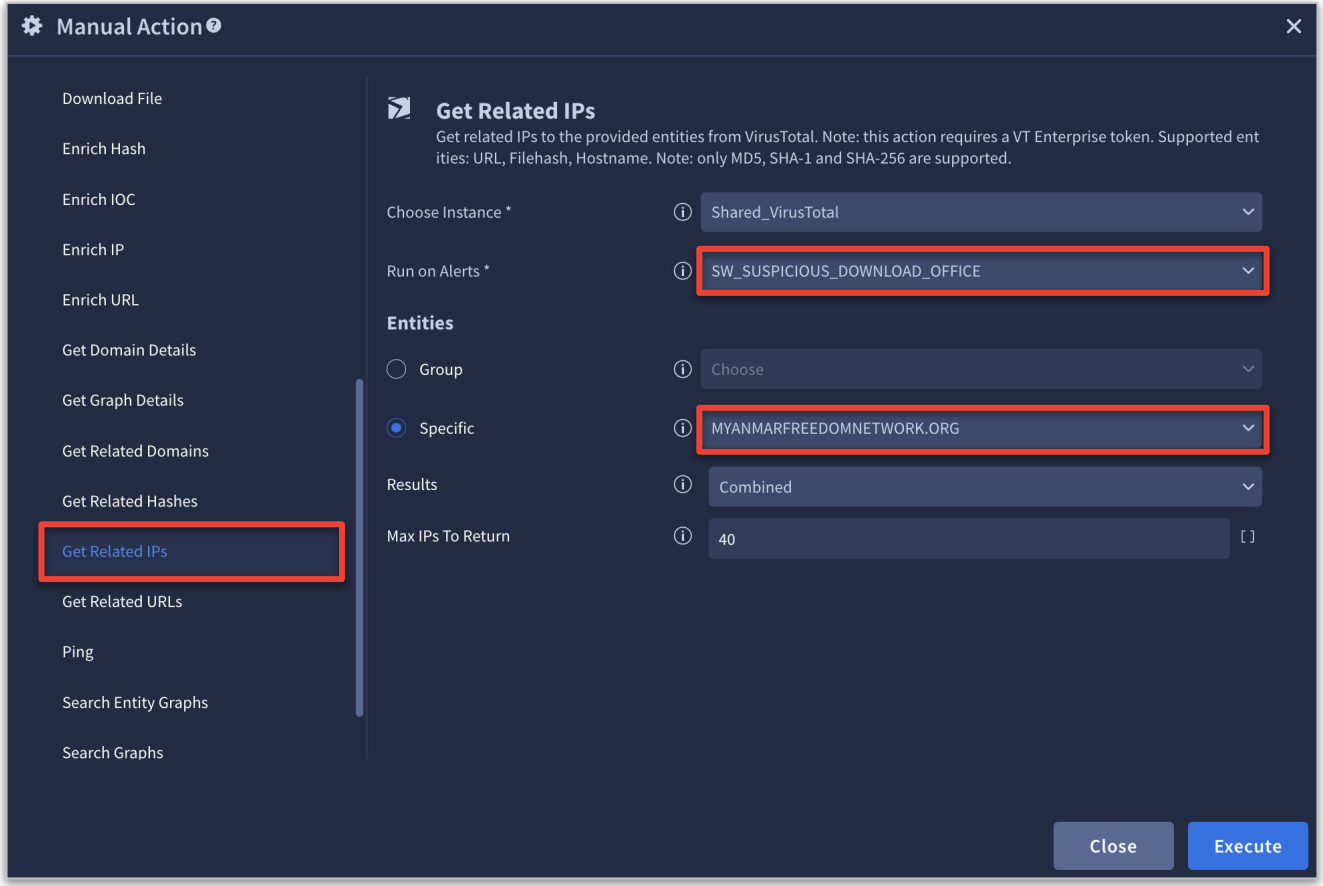
Adding Commentary to a Case

Google SecOps



Action - Related IPs from VirusTotal - Domain

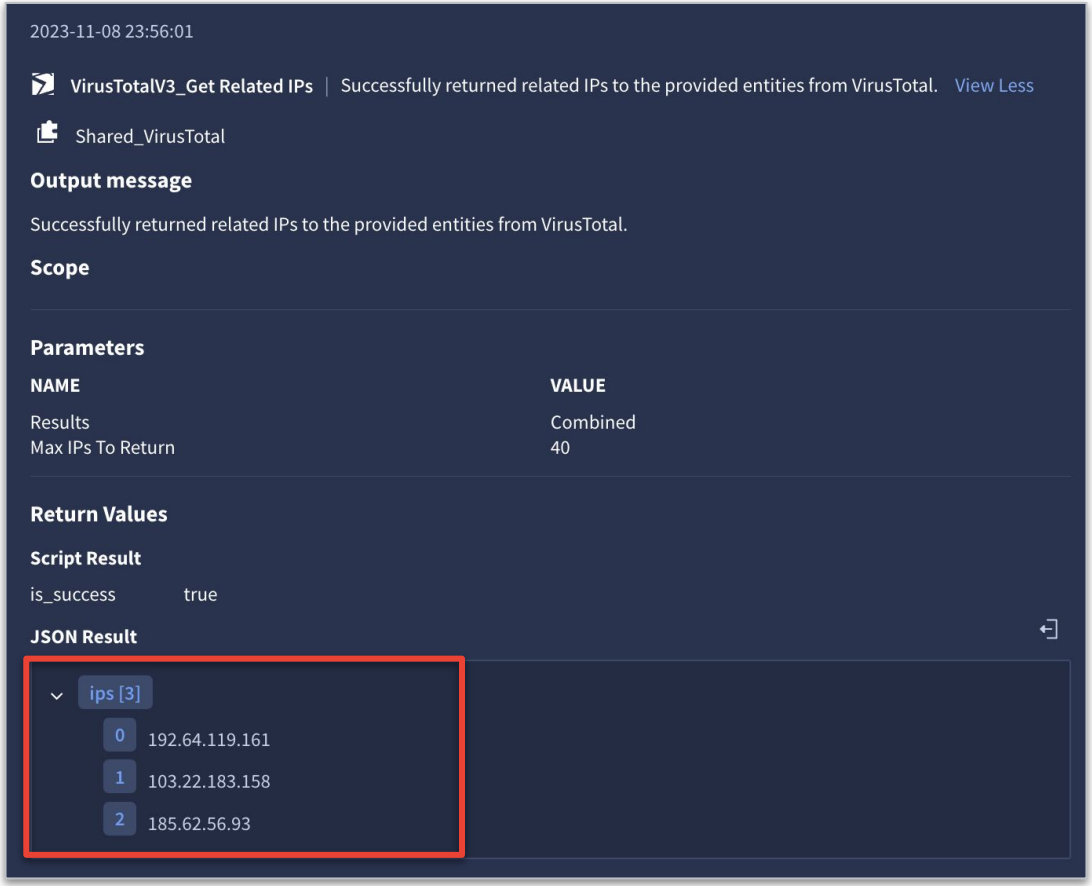
Google SecOps



Google

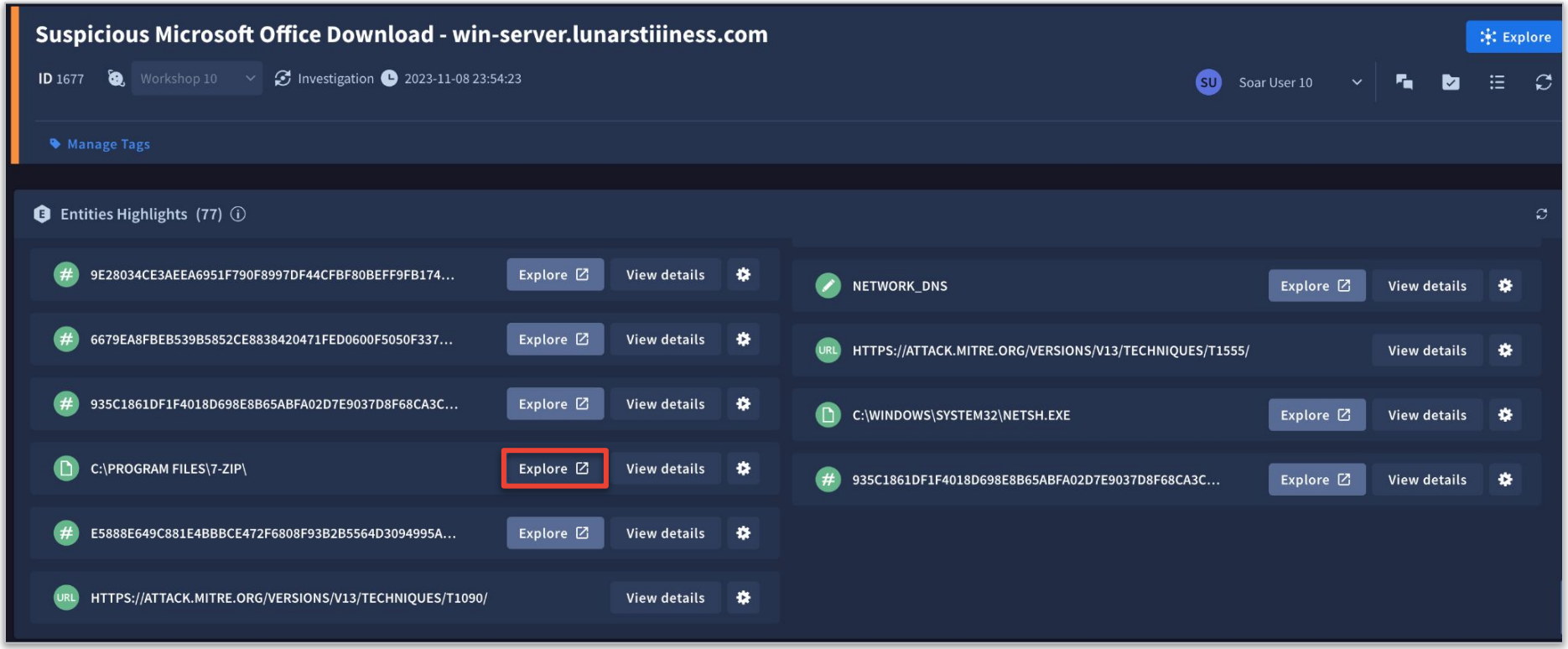
Get Related IPs

Google SecOps



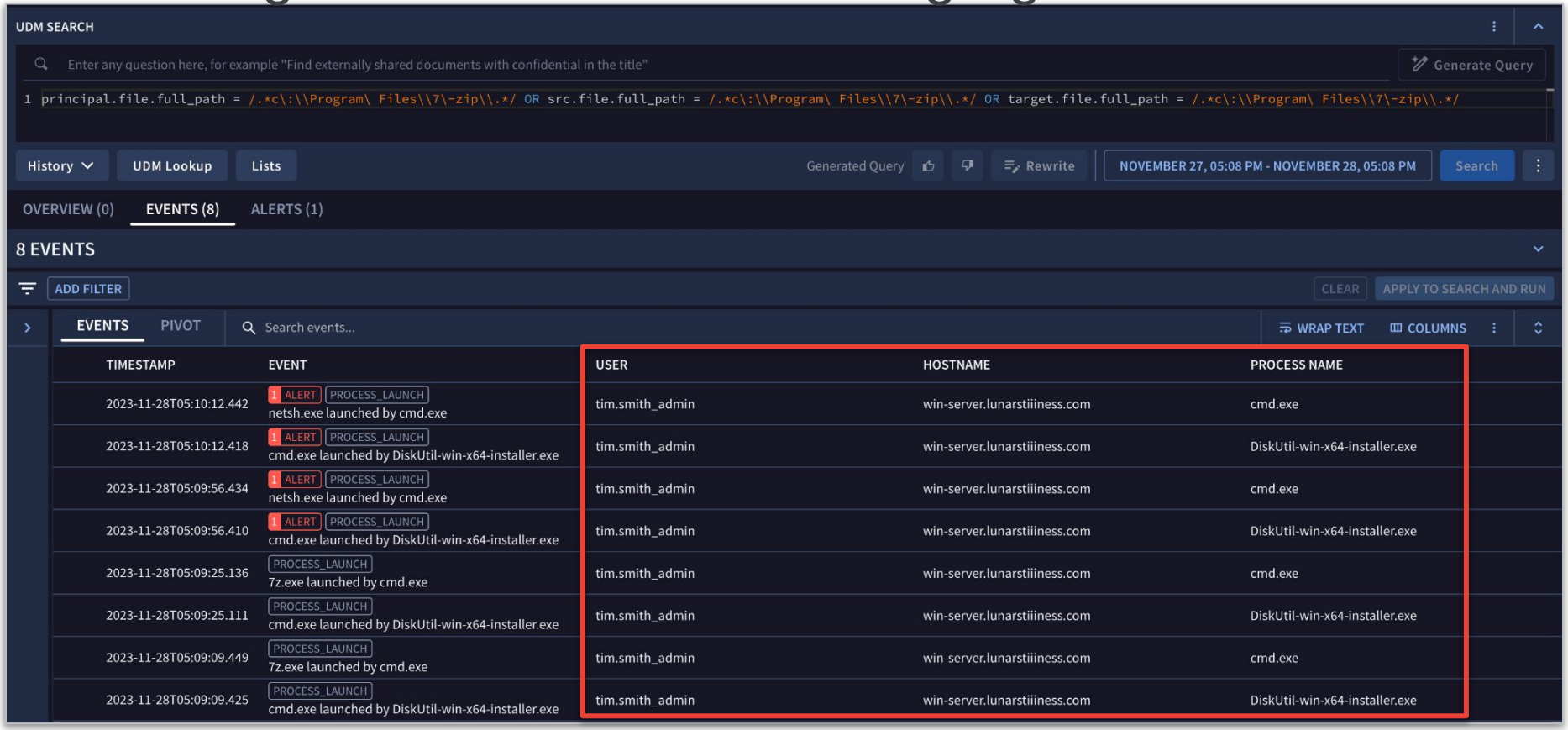
Search on a Specific Entity

Google SecOps



Searching for Values from Entities Highlights

Google SecOps



What Did We Learn About This Case?

Google SecOps

Uncovered a suspicious domain, IP and URL

- These in turn helped uncover related IPs, domains and file hashes

Did you find it easy to gather this information using actions?

Does anyone want to share other actions they performed or anything they identified?

Would you prefer to have some of this gathered automatically for you before you start diving into a case?

What Did We Learn About This Case?

Google SecOps

Uncovered a suspicious domain, IP and URL

- These in turn helped uncover related IPs, domains and file hashes

7-zip appears to be running on one system in our environment and is being used by an admin

- Is there more we can learn about diskutil-win-x64-installer.exe?

Did you find it easy to gather this information using actions?

Does anyone want to share other actions they performed or anything they identified?

Would you prefer to have some of this gathered automatically for you before you start diving into a case?

Summary

Google SecOps

Events are used to generate detections via the rules engine

Alerts are organized into Cases

Cases provide a top level view with one or more alerts in each one

Playbooks are run on alerts

Manual actions can be run on entities at a case or alert level

The workdesk provides a user specific interface for cases, alerts and tasks assigned to them

A common case queue is available as well

Handy Links

Google SecOps

Case Overview:
https://cloud.google.com/chronicle/docs/soar/investigate/working-with-cases/cases-overview

Alert Overview:
https://cloud.google.com/chronicle/docs/soar/investigate/working-with-alerts/whats-on-the-alert-overview-tab

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

SecOps Community: https://secopscommunity.com

Thank You