

Google SecOps App for Jira On-Prem

v3.2.0

Release Documentation and User Guide

Contents

Release Notes	3
v3.1.0	3
v3.2.0	3
Installation Instructions	3
Login Page	4
Landing Page	4
Goto Manage Apps	4
Manage Apps Page	5
Upload App OBR/JAR file	6
Google SecOps App Upload Process	6
Google SecOps App Confirmation	7
Listing of Google SecOps App	7
Google SecOps App Config Page Confirmation	8
Installing the app from the marketplace	8
Upgrade	9
Un-installation Instructions	9
Login Page	9
Goto Manage Apps	10
Password for the Administrator Access	10
Manage Apps Page	11
Search Google SecOps for Jira (On-Prem)	12
Uninstallation Confirmation	12
Uninstallation Successful	12
Confirm the Uninstallation	13
Project Creation from the Google SecOps Template	14
App Configuration Page with Default Values and Fields usage	17
Authentication Information and Proxy Configuration	21
Proxy Details: Default	22
Proxy Details: When the checkbox is checked	22
Proxy Details: Proxy configuration	22

Scheduler Daily	23
Scheduler Weekly	23
Scheduler Monthly	23
Scheduler Periodically	23
Data Polling: Default	23
Data Polling: Stream Detections	25
Project & Users: Default	26
Project & Users: When the project is selected	26
User Assignment Criteria	27
User Assignment Criteria: Creation	27
Ticket Creation Criteria	29
Ticket Creation Criteria: Creation	30
Detection Criteria List	31
Detection Criteria List: Creation	32
Curated Detection Criteria List: Creation	34
Button Event Action	37
Retrohunt	38
Start Retrohunt	38
Cancel Retrohunt	40
Ticket Created by the App	41
IoC Domain Match	41
User Alert Ticket	42
Asset Alert Ticket	43
Detection Ticket	44
Curated Detection Ticket	45
Enrichments	46
IoC Details	46
List Assets Impacted	48
List Asset Aliases	49
List User Aliases	50
List Events Discovered	51
UDM Search	51
Update Detection Rule State	53
Development Assumptions	54
Troubleshooting	56
Additional Information	59
Application Dependencies	59
App - Jira Version Compatible Matrix	60

Release Notes

v3.1.0

- Added support for Curated Detections:
 - Fetch Curated detections and create Jira issues.
 - New issue type for Curated Detections with certain custom fields.
- Added support to fetch Detections via Streaming:
 - Users would have an option to fetch both Detections and Curated Detections via Streaming APIs.
- Added a Reset button on the configuration page, which would allow users to reset the configurations to default.
- Added functionality where the app checks and retries to do project customization for custom issue types, custom fields and schema mappings if they have been updated or do not exist when clicking on the save button.
- Various Minor Bug Fixes and Improvements.

v3.2.0

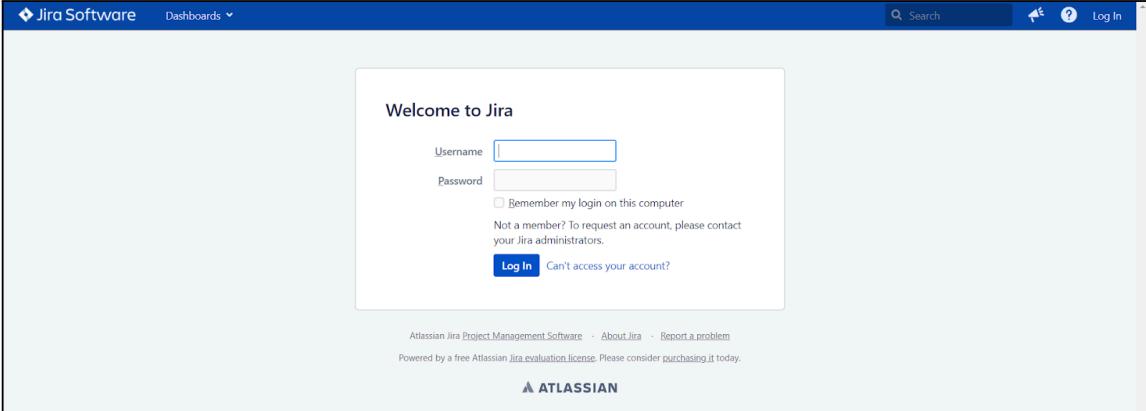
- Rebranding
 - Google Google SecOps is now rebranded to Google SecOps.
 - Updated app configuration title, field descriptions, logs, and logos as per the new name across the app.
- UDM Search
 - The app also provides the ability to search UDM events based on provided query and time interval.
 - This action is provided as issue enrichment in all the Jira issues created by the app and would add the results to the Jira Issue comment.
- Added support for Jira Server (Data Center) v10.

Installation Instructions

This section will cover the installation procedure of the Google SecOps App for Jira(On-Prem). For installation of the app, the Jira admin user will need the Google SecOps App(OBR/JAR) file.

Login Page

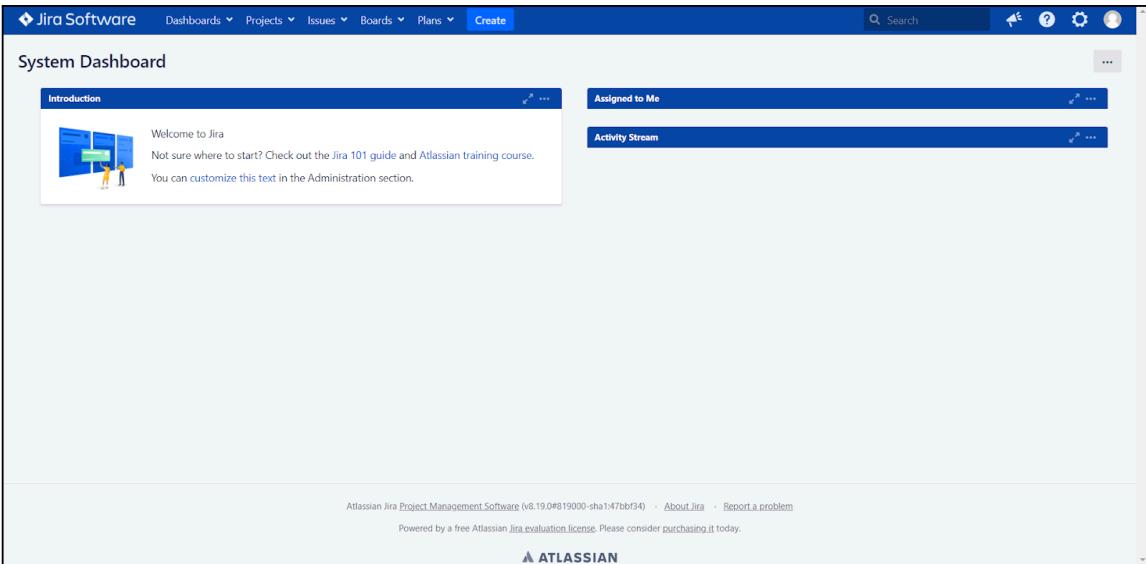
Enter the Jira Admin credentials, to start the installation process for the Google SecOps App.



The screenshot shows the Jira Software login interface. At the top, there's a navigation bar with the Jira logo, a search bar, and a 'Log In' button. Below the navigation bar is a large white box titled 'Welcome to Jira'. It contains fields for 'Username' and 'Password', a checkbox for 'Remember my login on this computer', and a link for 'Not a member? To request an account, please contact your Jira administrators.' At the bottom of this box are two buttons: 'Log In' and 'Can't access your account?'. At the very bottom of the page, there are links for 'Atlassian Jira Project Management Software', 'About Jira', 'Report a problem', and a note about a free evaluation license.

Landing Page

Upon Login with the admin credentials, the below-displayed landing page should be visible.



The screenshot shows the Jira Software System Dashboard. The top navigation bar includes the Jira logo, a search bar, and various menu options like 'Dashboards', 'Projects', 'Issues', 'Boards', 'Plans', and a prominent 'Create' button. Below the navigation is a section titled 'System Dashboard' containing three cards: 'Introduction' (with a welcome message and a small icon), 'Assigned to Me' (empty), and 'Activity Stream' (empty). At the bottom of the dashboard, there are links for 'Atlassian Jira Project Management Software', 'About Jira', 'Report a problem', and a note about a free evaluation license.

Goto Manage Apps

Click on the **Gear** Icon in the top right corner of the screen and click on the **Manage Apps** option.

The screenshot shows the Jira Software System Dashboard. On the left, there's a 'System Dashboard' panel with sections like 'Introduction' and 'Assigned to Me'. On the right, a vertical sidebar titled 'JIRA ADMINISTRATION' is open, showing options such as 'Applications', 'Projects', 'Issues', 'Manage apps', 'User management', 'Latest upgrade report', and 'System'. At the bottom of the dashboard, there's a footer with links to 'Atlassian Jira Project Management Software (v8.19.0#819000-sha147bbf34)', 'About Jira', 'Report a problem', and information about a free evaluation license.

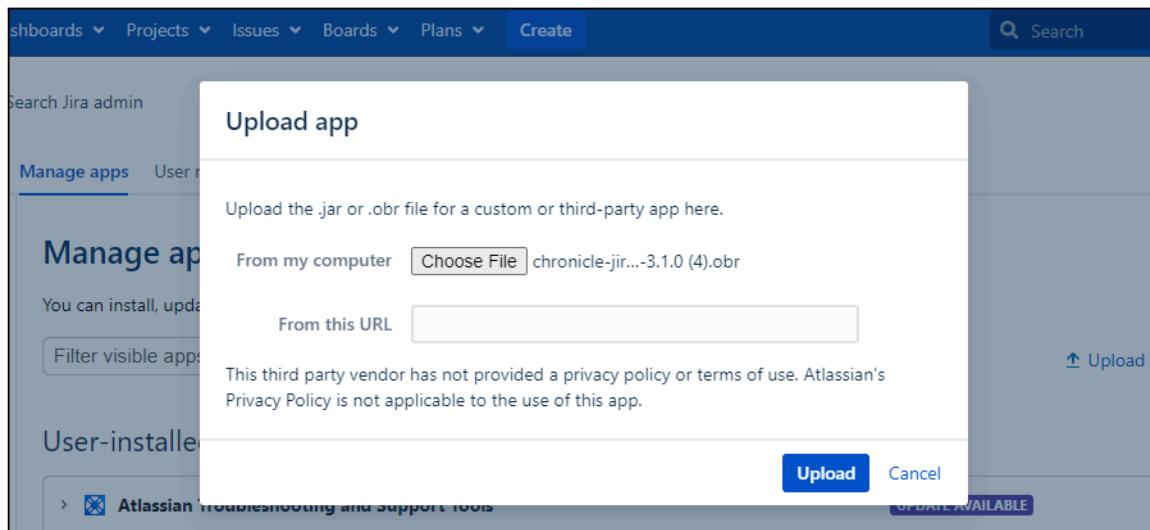
Manage Apps Page

Upon clicking on the **Manage Apps** option, the displayed page below will be visible listing all the apps that have been currently installed.

The screenshot shows the 'Administration' page with the 'Manage apps' tab selected. It displays a list of installed apps under the heading 'User-installed apps'. Each app entry includes a small icon, the app name, a 'UPDATE AVAILABLE' button, and an 'Update' button. The apps listed are: Atlassian Troubleshooting and Support Tools, Atlassian Universal Plugin Manager Plugin, JIRA iCalendar Plugin, JIRA Software Chinese (China) Language Pack, JIRA Software Czech (Czech Republic) Language Pack, and JIRA Software Danish (Denmark) Language Pack. There are also buttons for 'Skip this version' and 'Remind me later' at the top of the app list.

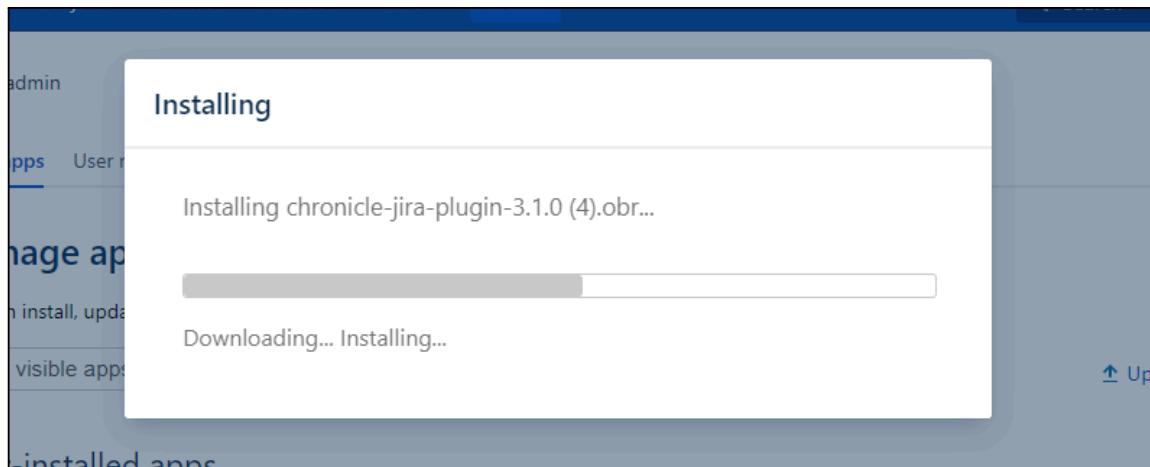
Upload App OBR/JAR file

Click on Upload all options from the previous screen, and a popup will appear as displayed below.



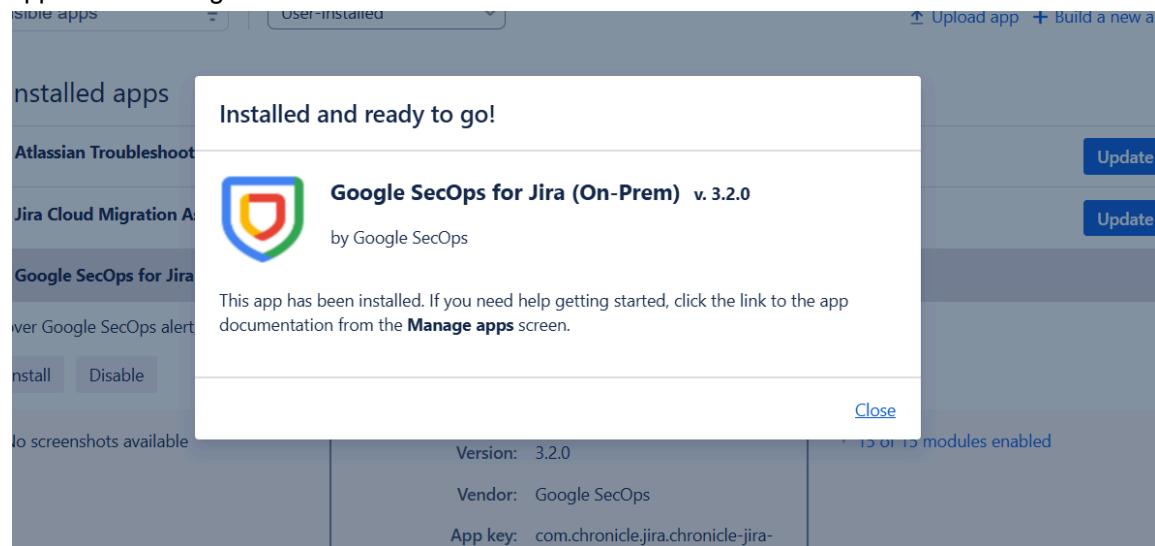
Google SecOps App Upload Process

Upon selection of the OBR/JAR file that will be provided by the customer to the end user, the below-displayed popup will appear showcasing the progress for the installation of the app.



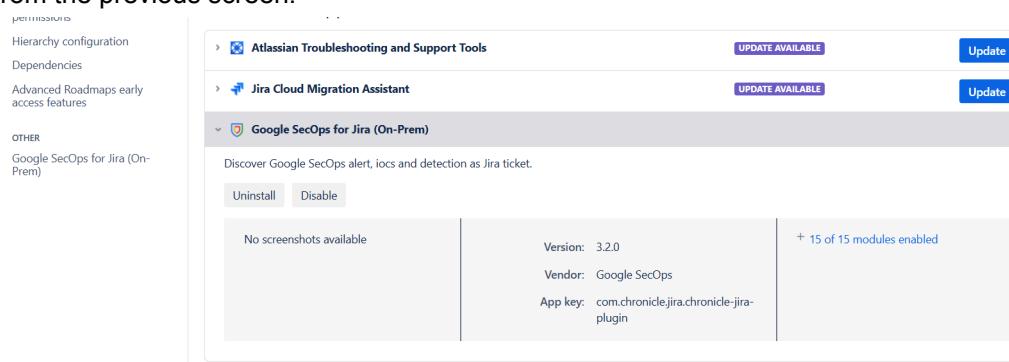
Google SecOps App Confirmation

Upon the successful installation of the Google SecOps app, the below-displayed popup will appear confirming the Installation was successful.



Listing of Google SecOps App

The Google SecOps app will be displayed in the list of apps installed, upon closing the popup from the previous screen.



Google SecOps App Config Page Confirmation

Once the installation process is completed, then the app with the name **Google SecOps App** will be displayed in the **Manage Apps** screen under the **OTHER** segment, which will present on the left side of the screen, as shown in the screenshot below.

The screenshot shows the Jira Software Administration interface. On the left sidebar, under the 'OTHER' section, 'Google SecOps for Jira (On-Prem)' is listed. The main content area is titled 'Configuration' and shows the 'Authentication Information and Proxy Configuration' section. It includes fields for 'Enable Proxy' (unchecked), 'Service Account Credential File' (with a 'Choose File' button and 'No file chosen' message), and 'Region' (with a placeholder 'Enter Region for API call to Google SecOps. Leave blank for General region. Ex: "europe-west2" for London region.' and a 'Reference' link). A 'Authenticate & Save' button is present. Below this is the 'Scheduler' section with 'Run:' set to 'Daily' and 'Time Hours(HH:mm):' set to '00:00'. There are 'Activate W' and 'Go to Settings' buttons on the right. The top navigation bar includes 'Dashboards', 'Projects', 'Issues', 'Boards', 'Plans', 'Create', and a search bar.

This marks the successful completion of the Installation of the Google SecOps App for **Jira(on-prem)**. The same steps need to be followed for the different flavours of Jira(**Software** and **Service Desk**).

Installing the app from the marketplace

- Users will have a provision to install the application from the marketplace. Click on the **Gear** Icon on the top right corner of the screen, and click on the **Manage Apps** option.
- In the **Find New Apps** screen, enter the name of the app **Google SecOps for Jira (On-Prem)** in the Search the Marketplace search bar and click Enter.
- **Google SecOps for Jira (On-Prem)** will be available in the marketplace based on the search from where the user would be able to install the app.

Upgrade

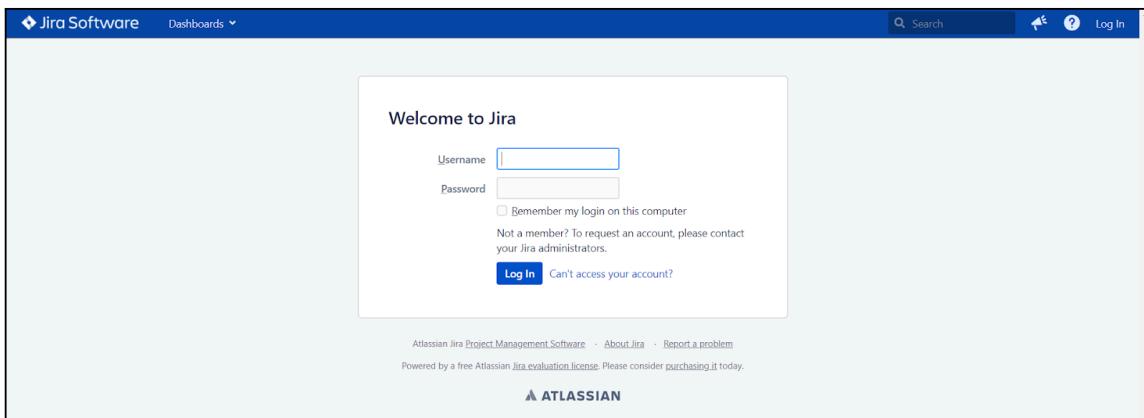
- If the user has already installed the previous version of the app and installed the new version/upgrades it to v3.2.0 from previous versions, they would not need to reconfigure the app.

Un-installation Instructions

Note: If you uninstall v3.2.0 of the app, existing schedulers will be deregistered and the saved app configurations will not be deleted from the Jira instance.

Login Page

Enter the Jira admin credentials and click on Log In



Goto Manage Apps

Click on the **Manage Apps** from the Settings gear that is located in the top right corner.

Jira Software

Dashboards ... Projects ... Issues ... Boards ... Plans ... Create

System Dashboard

Introduction

Welcome to Jira
Not sure where to start? Check out the [Jira 101 guide](#) and [Atlassian training course](#). You can customize this text in the Administration section.

Assigned to Me

Activity Stream

JIRA ADMINISTRATION

- Applications
- Projects
- Issues
- Manage apps
- User management
- Latest upgrade report
- System

Atlassian Jira Project Management Software (v8.19.0#819000-sha1:47bbf34) · [About Jira](#) · [Report a problem](#)

Powered by a free Atlassian [Jira evaluation license](#). Please consider [purchasing it](#) today.

Password for the Administrator Access

Enter the Jira Administrator Access credentials and click on Confirm.

Jira Software

Dashboards ... Projects ... Issues ... Boards ... Plans ... Create

Administrator Access

⚠️ If you were sent to this page from a link obtained from an untrusted source please proceed with caution or validate the link source before continuing.

You have requested access to an administrative function in Jira and are required to validate your credentials below.

Username **admin Not You?**

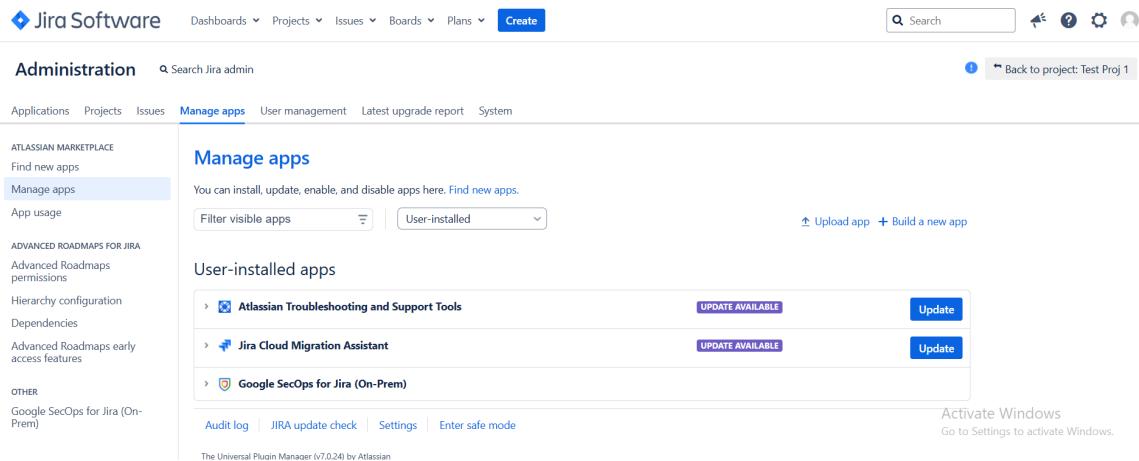
Password

Confirm Cancel

Atlassian Jira Project Management Software (v8.19.0#819000-sha1:47bbf34) · [About Jira](#) · [Report a problem](#)

Manage Apps Page

Click on Manage Apps which is located on the left side under the ATLASSIAN MARKETPLACE section.



The screenshot shows the Jira Software interface with the 'Manage Apps' section selected. The left sidebar includes links for ATLASSIAN MARKETPLACE, ADVANCED ROADMAPS FOR JIRA, and OTHER. The main content area displays a list of installed apps: 'Atlassian Troubleshooting and Support Tools' (Update Available), 'Jira Cloud Migration Assistant' (Update Available), and 'Google SecOps for Jira (On-Prem)'. Navigation links at the bottom include 'Audit log', 'JIRA update check', 'Settings', and 'Enter safe mode'.

Search Google SecOps for Jira (On-Prem)

Search and Expand the Google SecOps for Jira (On-Prem) and click Uninstall.

The screenshot shows the Atlassian Marketplace interface. On the left, there's a sidebar with sections like 'Hierarchy configuration', 'Dependencies', 'Advanced Roadmaps early access features', and 'OTHER' which includes 'Google SecOps for Jira (On-Prem)'. The main panel displays the 'Google SecOps for Jira (On-Prem)' plugin. It has a summary section with the description 'Discover Google SecOps alert, iocs and detection as Jira ticket.' Below this are two buttons: 'Uninstall' and 'Disable'. To the right, there's a detailed view of the plugin: 'Version: 3.2.0', 'Vendor: Google SecOps', and 'App key: com.chronicle.jira.chronicle-jira-plugin'. A note indicates '+ 15 of 15 modules enabled'.

Uninstallation Confirmation

Click on the Uninstall app button to uninstall the Google SecOps Plugin.

This screenshot shows the same marketplace interface as above, but with a modal dialog box centered over it. The dialog is titled 'Uninstall app?' and contains the message 'Uninstalling will permanently remove this version of the app from JIRA and your filesystem. Do you want to continue?'. At the bottom of the dialog are two buttons: 'Uninstall app' (highlighted in blue) and 'Cancel'. The background of the marketplace shows the same plugin details as the previous screenshot.

Uninstallation Successful

The below screenshot will be displayed upon successful uninstallation.

The screenshot shows the Jira Marketplace interface. At the top, there's a header with "Jira Cloud Migration Assistant" and "UPDATE AVAILABLE" with an "Update" button. Below it is a section for "Google SecOps for Jira (On-Prem)". A message box says "This app was successfully uninstalled." Below this, there's a note: "Discover Google SecOps alert, iocs and detection as Jira ticket." There are two buttons: "Uninstall" and "Disable". Underneath, there's a summary: "No screenshots available", "Version: 3.2.0", "Vendor: Google SecOps", and "App key: com.chronicle.jira.chronicle-jira-plugin". At the bottom, there are links for "Audit log", "JIRA update check", "Settings", and "Enter safe mode". On the right side, there's a "Activate V" button.

Confirm the Uninstallation

Click on Manage Apps and confirm that the Google SecOps App is no longer displayed in the list and also it is not listed in the left section of Atlassian Marketplace.

The screenshot shows the Jira Administration interface under the "Manage apps" tab. At the top, there's a message: "⚠ You have temporary access to administrative functions. [Drop access](#) if you no longer require it. For more information, refer to the [documentation](#)." Below this is a search bar and some navigation icons. The main area is titled "Manage apps" and contains the sub-instruction: "You can install, update, enable, and disable apps here. [Find new apps](#)". There are two dropdown filters: "Filter visible apps" and "User-installed". At the bottom, there are links for "Audit log", "JIRA update check", "Settings", and "Enter safe mode". The footer notes: "The Universal Plugin Manager (v4.0.0.bca9de41B9) by Atlassian".

User Manual

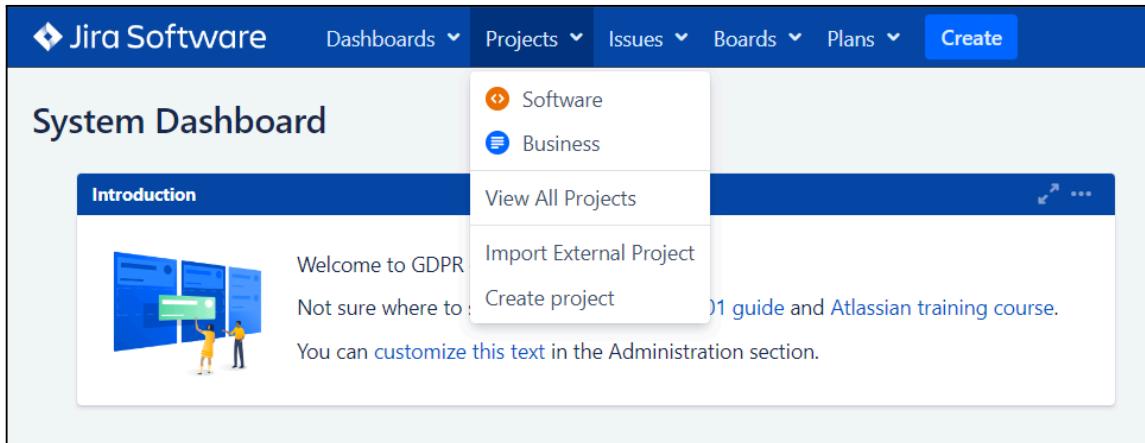
This section will cover the step-by-step process for configuring the Google SecOps App. The Google SecOps App offers the following functionality:

1. Types of scheduler settings, that enables users to select how frequently the data needs to be collected from the SecOps.
2. User Assignment Criteria, wherein the user can create the criteria based upon the filter condition, which scheduled job will assign the tickets directly to the user that has been mentioned in the criteria.
3. Ticket Creation Criteria, wherein the user can create the criteria based upon the filter condition, enabling the user to only create those tickets which match the criteria.
4. Detection Criteria, where the user can create criteria based on the filter condition, and a scheduled job will generate detection tickets as well as assign the tickets directly to the user that has been mentioned in the criteria.
5. Curated Detection Criteria, where the user can create criteria based on the filter condition, and a scheduled job will generate Curated Detection tickets as well as assign the tickets directly to the user that has been mentioned in the criteria.
6. Show the last job run date and time, which enables the user to understand when the last successful job was executed.
7. Custom Issue types, through which the tickets can be identified whether the tickets are of IoC, Alerts, Detections and Curated Detections.
8. Enrichment, 6 types of enrichment a user will be able to perform:
 - a. IoC Matches
 - b. List Assets Impacted
 - c. List Events
 - d. List Asset Aliases
 - e. List User Aliases
 - f. UDM Search
9. Update Rule State, wherein the user will be able to update the Detection Rule state associated with the Detection issue using the custom issue action “Update Detection Rule State”.
10. Retrohunt, wherein the users will be able to see a list of Retrohunts created earlier. Users will also be able to start/cancel the retrohunts.

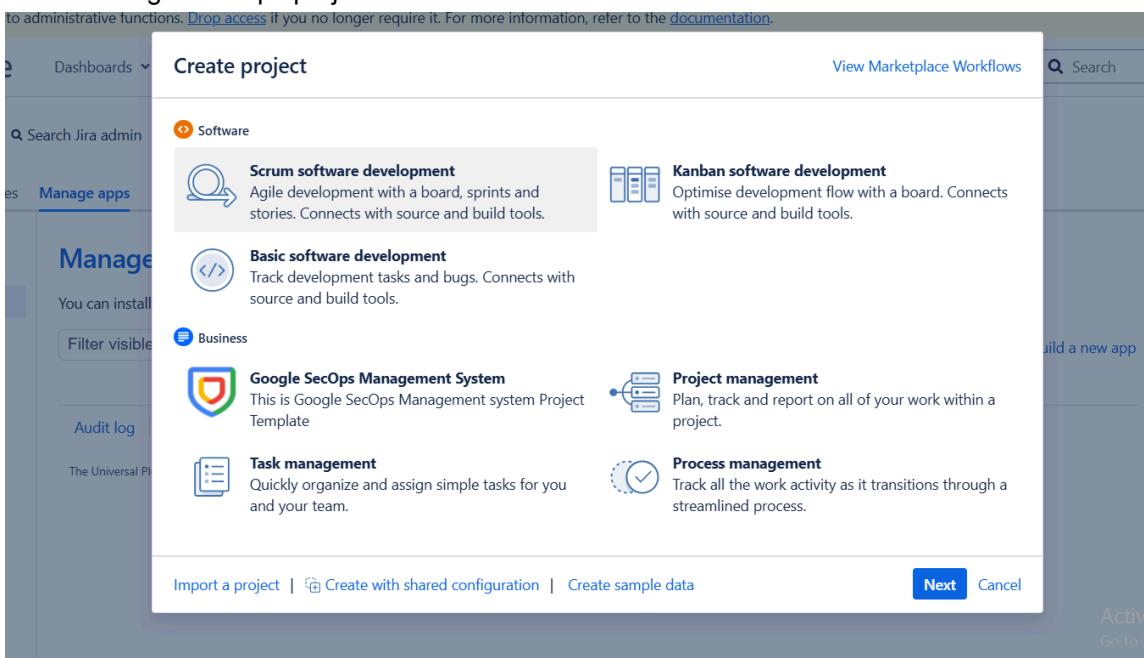
Project Creation from the Google SecOps Template

This section will go through the process of Project Creation with the Google SecOps template. It is important to do this, even before starting with the configuration of the app. As the Project that is created with the Google SecOps template will only be listed in the configuration screen, also this custom project will have all the custom fields, Issue types and labels that will be used when the ticket is created in order to map the response from Google SecOps to the jira fields

Hover / Click on the Projects section from the menu bar, and select Create Project as displayed below:



Select the **Google SecOps Management System** from the Create Project popup to create the custom Google SecOps project.



Fill in the Name, Key and Project Lead(will be used as the reporter of the ticket), and Click on the Submit button to create the project.

The screenshot shows a configuration dialog box titled "Google SecOps Management System". It contains fields for "Name" (with placeholder "Max. 80 characters."), "Key" (with placeholder "Max. 10 characters."), and "Project Lead" (with placeholder "Enter the username of the Project Lead."). To the right of these fields is a descriptive text block: "Google SecOps Management System. Create simple alerts, iocs and detections, organize them and get them resolved. You can use this project to manage your alerts, iocs and detections or assign them to someone else." At the bottom of the dialog are buttons for "Back", "Submit" (highlighted in blue), and "Cancel".

The below screen confirms that the custom Google SecOps Project has been created, and now the user is ready to configure the Google SecOps App.

The screenshot shows the "Open issues" page for the "Google Chronicle JIRA" project in Jira Software. The left sidebar includes links for "Summary", "Issues" (which is selected and highlighted in grey), and "Reports". A "PROJECT SHORTCUTS" section allows adding links to useful information. The main content area displays a search interface with a magnifying glass icon and the message "No issues were found to match your search. Try modifying your filter or creating a new issue below." At the bottom, there is a "What needs to be done?" dropdown menu with options like "New Detection", "Open in dialog", and "Cancel". The URL "10.50.5.184:8080/secure/MyJiraHome.jspa" is visible at the bottom left.

App Configuration

This section will cover the configuration of the Google SecOps App and its detailed usage.

App Configuration Page with Default Values and Fields usage

Manage apps User management Latest upgrade report System

Configuration Retrohunt

Authentication Information and Proxy Configuration

Enable Proxy:

Service Account Credential File: * No file chosen

Region:
Enter Region for API call to chronicle. Leave blank for General region.
Ex. "europe-west2" for London region. Reference

Scheduler

Run: * Daily

Time Hours(HH:mm): * 00 00

Number of days to fetch* 4
IoCs/Alerts/Detections initially:

Data Polling

Enable IoC Matches: Please select to pull IoCs

Enable Alerts: Please select to pull Alerts

Stream Detections: X Please enable to pull Stream Detections. Stream would auto pull both Detections and Curated Detections. If this is disabled, select below checkbox to fetch detections via list APIs.

Enable Detections: Enable Curated Rule Detection
Please select to pull Detections Please select to pull Curated Detections

Number of retries in case of Error: * 6
Value must be in range 1 to 10.

Limit of IOC tickets to create per Invocation: 10000
Value must be in range 1 to 10k.

Limit of Alert tickets to create per Invocation: 10000
Value must be in range 1 to 100k.

Limit of Detection tickets to create per Invocation:
Leave blank for no limit OR Value must be less than or equal to 1B.

Limit of Curated Detection tickets to create per Invocation:
Leave blank for no limit OR Value must be less than or equal to 1B.

Project & Users

Default Project: Project in which chronicle incidents will be created

Last Sync Details

Last Job Run Time for IoCs:	<input type="text"/>
Last Job Run Time for Alerts:	<input type="text"/>
Last Job Run Time for Detections:	<input type="text"/>
Last Job Run Time for Curated Detections:	<input type="text"/>
Scheduler Status:	<input type="text" value="Not Scheduled"/>

Below are the fields and their details:

Field Name	Description
Enable Proxy (<u>Checkbox</u>)	Upon checking, the proxy details will be visible to the user.
Proxy URL (<u>Textbox</u>)	URL of the proxy server.
Proxy Username (<u>Textbox</u>)	Username to access the proxy service.
Proxy Password (<u>Textbox</u>)	Password to authenticate the proxy service.
Service Account Credential File (<u>File picker</u>)	Service Account file provided by Google for Authorisation of API.
Region (<u>Textbox</u>)	Region to which the Google SecOps account belongs.
Run (<u>Dropdown</u>)	How often does the app need to fetch the data from the Google SecOps Instance? The total options that we get are Daily, Weekly, Monthly and Periodically.
Time Hours(HH:mm) (<u>HH field picker</u>) (<u>mm field picker</u>)	At what Time of the day the Google SecOps app should fetch the data from the Google SecOps instance. Time can be configured in Hours and Minutes. This field will only be visible for Daily, Weekly and Monthly.

Day (<u>Dropdown for Weekly</u>) (<u>Day field picker for Monthly</u>)	For the Weekly Run option, the Day dropdown list will have the day of the week value from Sunday to Saturday. Users can configure any day of the week as per their preference. For the Monthly Run option, the Day picker will have the day of the month values from 1 to 31. Users can configure any day of the month as per their preference.
Run Interval (<u>Minutes field picker</u>)	At what interval of time(in minutes) does the data from the Google SecOps app need to be fetched from the Google SecOps instance.
No of days to fetch IoCs/Alerts/Detections Initially (<u>Day field picker</u>)	Historical data that we need to fetch in days, the value entered in this field will fetch the data for those many days to the current date.
Default Project (<u>Dropdown</u>)	It will display the list of the projects that were created by the Google SecOps Project Creation Template.
Enable IoC Matches (<u>Checkbox</u>)	Upon checking, the app will create the Tickets for IoC Matches.
Enable Alerts (<u>Checkbox</u>)	Upon checking, the app will create the Tickets for User and Asset Alerts.
Stream Detections (<u>Toggle Button</u>)	Enable this toggle button to receive detections continuously. Once enabled, the checkbox for detection and curated detection would get disabled as they would be auto-pulled.
Enable Detections (<u>Checkbox</u>)	Upon checking, the app will create the Tickets for Detection. This checkbox will be deactivated if Stream Detections is enabled.
Enable Curated Detections(<u>Checkbox</u>)	Upon checking, the app will create the Tickets for Curated Detections. This checkbox will be deactivated if Stream Detections is enabled.
The number of retries in case of Error (<u>Number</u>)	How many times should the app retry Google SecOps API call in case of a rate limit error
Limit of IOC tickets to create per Invocation (<u>Number</u>)	How many IOC tickets to create per sync interval
Limit of Alert tickets to create per Invocation (<u>Number</u>)	How many Alert tickets to create per sync interval

Limit of Detection tickets to create per Invocation (<u>Number</u>)	How many Detection tickets to create per sync interval (This configuration is not applicable for stream detections.)
Limit of Curated Detection tickets to create per Invocation (<u>Number</u>)	How many Curated Detection tickets to create per sync interval (This configuration is not applicable for stream detections.)
Last Job Run Time for IoCs (<u>Read-only text box</u>)	Last successful job run time for fetching the IoCs from the Google SecOps instance.
Last Job Run Time for Alerts (<u>Read-only text box</u>)	Last successful job run time for fetching the Alerts from the Google SecOps instance.
Last Job Run Time for Detections (<u>Read-only text box</u>)	Last successful job run time for fetching the Detections from the Google SecOps instance.
Last Job Run Time for Curated Detections (<u>Read-only text box</u>)	Last successful job run time for fetching the Curated Detections from the Google SecOps instance.
Scheduler Status (<u>Read-only text box</u>)	This field displays the Status of the Job: <ul style="list-style-type: none">• Scheduled: This means the Job is currently scheduled and it will run based on the configuration saved• Not Scheduled: This means the Job is currently not scheduled and no API calls will be made to SecOps
Next Job Run Time (<u>Read-only text box</u>)	When will the next call be made to SecOps? Note that this status is not applicable for stream detections.
Save (<u>Button</u>)	Save the configuration and Sync will be initiated, with the confirmation box.
Stop Sync (<u>Button</u>)	Stop pulling the data from the SecOps.
Reset (<u>Button</u>)	Reset the configuration to default and stop the existing sync, with the confirmation box.
Start Retrohunt (<u>Button</u>)	Open dialogue box to take user inputs to start retrohunt
Rule ID or Version ID (<u>Textbox</u>)	Rule ID or Version ID for which Retrohunt needs to be started.
Start DateTime (<u>Datetime picker</u>)	Start time for the time range of retrohunt
End DateTime (<u>Datetime picker</u>)	The end time for the time range of retrohunt

Refresh List (Button)	Refresh the list of retrohunts in the table
Cancel (Button)	Cancel the particular “RUNNING” retrohunt

Authentication Information and Proxy Configuration

Users need to upload the valid Service Account file that will be provided by the Google SecOps team for the Authentication of the Google SecOps API and provide the region to which the Google SecOps account belongs.

Once the “Authenticate & Save” button is clicked, it validates the provided service account file and region.

- On successful authentication, it would show a success message.

Authentication Information and Proxy Configuration

Enable Proxy:

Service Account Credential File: [Choose File](#) gc-jira.json
Valid Service Account file exists.

Region:
Enter Region for API call to chronicle. Leave blank for General region.
Ex. "europe-west2" for London region. [Reference](#)

[Authenticate & Save](#)

Successfully validated service account.

- On failure, it would show the appropriate failure message.

Authentication Information and Proxy Configuration

Enable Proxy:

Service Account Credential File: [Choose File](#) gc-jira-invalid.json

Region:
Enter Region for API call to chronicle. Leave blank for General region.
Ex. "europe-west2" for London region. [Reference](#)

[Authenticate & Save](#)

Authentication Failure: Either due to Invalid Service Account File / Invalid Proxy Detail (If proxy is enabled)

Proxy Details: Default

- An optional provision will be available to configure the proxy server details in case the user wants the Google SecOps API requests used for ticket creation, enrichment and detection to be routed via a proxy server
- There will be an Enable Proxy checkbox in the ‘Authentication Information and Proxy Configuration’ section. By default, it will be unchecked.

Authentication Information and Proxy Configuration
Enable Proxy: <input type="checkbox"/>

Proxy Details: When the checkbox is checked

If the checkbox is checked, the user will have the provision to configure the details of the proxy server like Proxy URL, Proxy Username and Proxy Password in case the user wants the Google SecOps API requests to be routed via a proxy server.

Note: Please ensure that the proxy URL should be entered as <Hostname/IP-Address>:<Port>. The hostname/IP address where the proxy server is installed and the port at which the proxy server is listening.

Proxy Details: Proxy configuration

Users can configure the proxy server details with proxy credentials and without proxy credentials. However, in both cases the proxy URL value is mandatory.

Authentication Information and Proxy Configuration
Enable Proxy: <input checked="" type="checkbox"/>
Proxy URL*: <input type="text"/>
Please enter Proxy URL without http or https
Proxy Username: <input type="text"/>
Proxy Password: <input type="password"/>

Authentication Information and Proxy Configuration
Enable Proxy: <input checked="" type="checkbox"/>
Proxy URL*: <input type="text"/>
Please enter Proxy URL without http or https
Proxy Username: <input type="text"/>
Proxy Password: <input type="password"/>

Scheduler Daily

Upon configuration, the job will run daily on the time(Hours: Minutes) defined by the user

Scheduler
Run: * <input type="button" value="Daily"/>
Time Hours(HH:mm): * <input type="text" value="00"/> 00

Scheduler Weekly

Upon configuration, the job will be scheduled on the selected day of the week and the time(Hours: Minutes) defined by the user

Scheduler
Run: * <input type="button" value="Weekly"/>
Day: * <input type="button" value="Sunday"/>
Time Hours(HH:mm): * <input type="text" value="00"/> 00

Scheduler Monthly

Upon configuration, the job will be scheduled on the selected date of the month and the time(Hours: Minutes) defined by the user

Scheduler
Run: * <input type="button" value="Monthly"/>
Day: * <input type="text" value="1"/>
Time Hours(HH:mm): * <input type="text" value="00"/> 00

Scheduler Periodically

Upon configuration, the job will be scheduled periodically based on the Run Interval(Minutes) defined by the user

Scheduler
Run: * <input type="button" value="Periodically"/>
Run Interval: * <input type="text" value="01"/> <small>Interval of scheduled job (in minutes)</small>

Note: In the case of Stream Detections the data is continuous, it will continually collect the detections from the Google SecOps and create JIRA tickets in the Google SecOps without relying on the scheduler configuration.

Data Polling: Default

- Enable IoC Matches, upon checking it will create the IoC tickets in the selected project.
- Enable Alerts, upon checking it will create the User Alerts and Asset Alerts tickets into the selected project.

- Stream Detections: To receive continuous detection alerts and create JIRA tickets in the selected project, please enable the 'Stream Detections' toggle button. This will activate the 'Stream Detection' feature, which provides both 'Detection' and 'Curated Detections' types of detection alerts. As a result, the 'Enable Detections' and 'Enable Curated Detections' checkboxes will be deactivated, as the 'Stream Detection' option covers both types of detections. Therefore, there is no need to select individual detection options.
 - Enable Detections, upon checking will create the Detection tickets for the selected project.
 - Enable Curated Detections, upon checking will create the Curated Detection tickets into the selected project.
- Provide the value of the field “Number of retries in case of Error” to restrict the maximum retries the app should do in case of Rate Limit error from Google SecOps API. The user can provide a maximum value of 10.
- Provide the value of the field “Limit of IOC tickets to create per Invocation” to restrict the maximum number of IOC tickets the app should create per sync interval. The user can provide a maximum value of 10k(10000).
- Provide the value of the field “Limit of Alert tickets to create per Invocation” to restrict the maximum number of Alert tickets the app should create per sync interval. The user can provide a maximum value of 100k(100000).
- Provide the value of the field “Limit of Detection tickets to create per Invocation” to restrict the maximum number of Detection tickets the app should create per sync interval. Leave this field blank for no limit in detection ticket creation or if the user wants to create a particular number of tickets for Detection criteria then the value must be less than or equal to 1B(1000000000). This configuration is not applicable for stream detections as it provides continuous data.
- Provide the value of the field “Limit of Curated Detection tickets to create per Invocation” to restrict the maximum number of Curated Detection tickets the app should create per sync interval. Leave this field blank for no limit in curated detection ticket creation or if the user wants to create a particular number of tickets for Curated Detection criteria then the value must be less than or equal to 1B(1000000000). This configuration is not applicable for stream detections as it provides continuous data.

Data Polling

Enable IoC Matches:	<input checked="" type="checkbox"/>	<i>Please select to pull IoCs</i>
Enable Alerts:	<input checked="" type="checkbox"/>	<i>Please select to pull Alerts</i>
Stream Detections:	<input checked="" type="checkbox"/>	<i>Please enable to pull Stream Detections. Stream would auto pull both Detections and Curated Detections. If this is disabled, select below checkbox to fetch detections via list APIs.</i>
<input checked="" type="checkbox"/> Enable Detections:	<input checked="" type="checkbox"/> Enable Curated Rule Detection	<i>Please select to pull Detections</i>
<i>Please select to pull Curated Detections</i>		
Number of retries in case of Error: [*]	<input type="text" value="6"/>	<i>Value must be in range 1 to 10.</i>
Limit of IOC tickets to create per [*] Invocation:	<input type="text" value="10000"/>	<i>Value must be in range 1 to 10k.</i>
Limit of Alert tickets to create per [*] Invocation:	<input type="text" value="10000"/>	<i>Value must be in range 1 to 100k.</i>
Limit of Detection tickets to create per Invocation:	<input type="text"/>	<i>Leave blank for no limit OR Value must be less than or equal to 1B.</i>
Limit of Curated Detection tickets to create per Invocation:	<input type="text"/>	<i>Leave blank for no limit OR Value must be less than or equal to 1B.</i>

Data Polling: Stream Detections

The Stream Detections provides real-time access to detections generated by both User-defined Rules and Google Security Operations Rules. For each detection fetched from the API, JIRA tickets are created with detection details.

- A single toggle button labelled "Stream Detections" is provided to enable continuous detections.
- Once the "Stream Detections" toggle is enabled, the "Enable Detections" and "Enable Curated Detections" checkboxes will be deactivated because "Stream Detections" provides both types of detections: "Detections" and "Curated Detections", rendering the individual checkboxes redundant.
- The "Number of days to fetch IoCs/Alerts/Detections initially" determines the continuation time parameter for API calls. However, if the user inputs a value exceeding the last 7 days, the app will automatically set the continuation time to 7 days from the current time.
- The "Limit of Detection tickets to create per Invocation" and "Limit of Curated Detection tickets to create per Invocation" field inputs are deactivated for Stream Detections, as it operates as a continuous stream connection.
- Based on the provided configuration create HTTP stream connection.
- Once the connection is established according to the configured data, it continuously receives Detection Engine results over an HTTP stream as the detections are discovered.
- All the detections created by rules whose alerting status was enabled at the time of detection should parse data according to the JIRA ticket.

- Upon successful parsing of data, the app will generate a JIRA ticket for each detection. These tickets will be created with the "Detection" or "Curated Detection" Issue Type.

Data Polling

Enable IoC Matches:	<input checked="" type="checkbox"/>	<i>Please select to pull IoCs</i>
Enable Alerts:	<input checked="" type="checkbox"/>	<i>Please select to pull Alerts</i>
Stream Detections:	<input checked="" type="checkbox"/>	<i>Please enable to pull Stream Detections. Stream would auto pull both Detections and Curated Detections. If this is disabled, select below checkbox to fetch detections via list APIs.</i>
<input type="checkbox"/> Enable Detections:	<input type="checkbox"/>	<i>Please select to pull Detections</i>
<i>Please select to pull Curated Detections</i>		
Number of retries in case of Error: [*]	<input type="text" value="6"/>	<i>Value must be in range 1 to 10.</i>
Limit of IOC tickets to create per [*] Invocation:	<input type="text" value="10000"/>	<i>Value must be in range 1 to 10k.</i>
Limit of Alert tickets to create per [*] Invocation:	<input type="text" value="10000"/>	<i>Value must be in range 1 to 100k.</i>
Limit of Detection tickets to create per Invocation:	<input type="text"/>	<i>Leave blank for no limit OR Value must be less than or equal to 1B.</i>
Limit of Curated Detection tickets to create per Invocation:	<input type="text"/>	<i>Leave blank for no limit OR Value must be less than or equal to 1B.</i>

Project & Users: Default

Users can select the project from the drop-down menu and can select a particular project under which the tickets will be created. Only those projects will be listed which are created from the Google SecOps Project creation template.

Project & Users

Default Project: [*]	<input type="button" value="<- Select Project -->"/>	<i>Project in which chronicle incidents will be created</i>
-------------------------------	--	---

Project & Users: When the project is selected

Once the project is selected then the User Assignment, Ticket Creation Criteria section, Detection Criteria and Curated Detection CriteriaList section will be displayed.

Assignment User Criteria List	Ticket Creation Criteria List	Detection Criteria List	Curated Detection Criteria List
<i>Ticket(s) will be assigned based on the Assignment criteria</i>			
Assignment User Criteria List[PROJECT:Google Chronicle JIRA Integration] NEW			
Assignment User	Condition	Order	Created By

User Assignment Criteria

Over here the criteria can be defined with the filter condition, which will enable the app to directly assign the tickets which will be created by the scheduler to the user as defined in the criteria.

Following are the steps by which a user can create the criteria:

- Click on the **NEW** Button in the Assignment User Criteria List tab

The screenshot shows a user interface for managing assignment user criteria. At the top, there are tabs: 'Assignment User Criteria List', 'Ticket Creation Criteria List', 'Detection Criteria List', and 'Curated Detection Criteria List'. Below the tabs, a message says 'Ticket(s) will be assigned based on the Assignment criteria'. The main area has a blue header bar with the text 'Assignment User Criteria List[PROJECT:Google Chronicle JIRA Integration]' and a 'NEW' button. Below the header is a table with columns: 'Assignment User', 'Condition', 'Order', 'Created By', and 'Created At'. The table is currently empty.

User Assignment Criteria: Creation

- Assignment User needs to be part of either of the mentioned User Groups depending upon the Jira(on-prem) flavour installed, along with the permission for the Google SecOps project that is created via the Google SecOps template.
 - Jira-administrators
 - Jira-software-users
 - Jira-service desk-users
- The assignment User Criteria List window will appear where the user will have the provision to configure the assignment user criteria for the tickets to be assigned to a specific user
- Tickets will be assigned to the selected user from the Assignment User dropdown list, by the scheduled job.
- Click on Add Filter Condition, and a criteria section will appear which will have the below criteria for configuration.

Assignment User Criteria List [PROJECT:Go...]

Assignment User* Order*

Conditions*

Conditions will be executed as AND Clause.

-- choose field -- [X]

Alert Product Id
Asset Host Name
Asset IP Address
Asset MAC
User Email
User Name
IoC Domain Name

- Prepare the filter condition as desired and then click on the Submit button to save the criteria.

Field Name	Description
Assignment User	List of users that are part of the User Groups
Add Filter Condition	Add the new filter condition, and all the filter conditions that the user defines, will work in conjunction with each other
Choose Field	Select the field on which the tickets need to be assigned to the user
Operator	Which condition the user wants to apply to filter out the data
Values	Enter the value that will satisfy the condition criteria
Order	The priority of the criteria, that will be used to filter the response in order to assign the tickets to the user. Lowest to Highest, where lowest will be preferred

Assignment User Criteria List [PROJECT:Go...]

Assignment User*	Administrator	Order*	100
Conditions*	Add Filter Condition Conditions will be executed as AND Clause.		
IoC Domain Name <input type="text"/> is <input type="text"/> Authentication Failure <input type="button" value="[X]"/>			
<input type="button" value="Submit"/> <input type="button" value="Close"/>			

- Once the assignment user criteria are saved, it will be displayed in the config screen as a list view as shown below:

Assignment User Criteria List				
Ticket Creation Criteria List				
Detection Criteria List				
Curated Detection Criteria List				
<i>Ticket(s) will be assigned based on the Assignment criteria</i>				
Assignment User Criteria List[PROJECT:Google Chronicle JIRA Integration]				<input type="button" value="NEW"/>
Assignment User	Condition	Order	Created By	Created At
Admin	CHRONICLE_ALERT_NAME	100	Admin	05/14/2024 05:21:43

- So, as per this configuration, the user alert or asset alert tickets will have the alert name “Authentication Failure” assigned to the admin user.

Ticket Creation Criteria

Over here the criteria can be defined with the filter condition, which will enable the app to create only those tickets that satisfy the ticket creation criteria as defined by the user.

Following are the steps by which a user can create the criteria:

- Click on the **New** button in the Ticket Creation Criteria List tab

Assignment User Criteria List			
Ticket Creation Criteria List			
Detection Criteria List			
Curated Detection Criteria List			
<i>Ticket(s) will be created based on the Ticket Creation criteria</i>			
Ticket Creation Criteria List[PROJECT:Google Chronicle JIRA Integration]			
<input type="button" value="NEW"/>			
Condition	Order	Created By	Created At

Ticket Creation Criteria: Creation

- Ticket Creation Criteria List window will appear where the user will have the provision to configure the ticket creation criteria in case any specific tickets need to be created in the selected project.
- Click on Add Filter condition, and a criteria section will appear which will have the below criteria for configuration.

Ticket Creation Criteria List [PROJECT:Goo...]

Order*	100	X
Conditions* Add Filter Condition Conditions will be executed as AND Clause. -- choose field -- <input type="button" value="-- operator --"/> <input type="text"/> [X] <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <input type="text"/> <input type="button" value="Search"/> <ul style="list-style-type: none"> Alert Product Id Asset Host Name Asset IP Address Asset MAC User Email User Name IoC Domain Name </div>		
Submit Close		

- Prepare the filter condition as desired and then click on the Submit button to save the criteria.

Field Name	Description
Add Filter Condition	Add the new filter condition and all the filter conditions that the user defines, all will work in conjunction with each other
Choose Field	Select the field on which the tickets need to be assigned to the user
Operator	Which condition the user wants to apply to filter out the data
Values	Enter the value that will satisfy the condition criteria
Order	The priority of the criteria, that will be used to filter the response in order to assign the tickets to the user. Lowest to Highest, where lowest will be preferred

Ticket Creation Criteria List [PROJECT:Goo...]

Order*

Conditions* [Add Filter Condition](#)

Conditions will be executed as AND Clause.

[\[X \]](#)

[Submit](#) [Close](#)

- Once the ticket creation criteria are saved, it will be displayed in the config screen as a list view as shown below:

Assignment User Criteria List Ticket Creation Criteria List Detection Criteria List Curated Detection Criteria List			
<i>Ticket(s) will be created based on the Ticket Creation criteria</i>			
Ticket Creation Criteria List[PROJECT:Google Chronicle JIRA Integration] NEW			
Condition	Order	Created By	Created At
CHRONICLE_ALERT_NAME	100	Admin	05/14/2024 05:25:53

- So, as per this configuration, tickets will be created for IoC Domain matches which contain the phrase “static” in the domain name.

Detection Criteria List

Over here the criteria can be defined with the filter condition, which will enable the app to create only those tickets that satisfy the detection criteria list as defined by the user.

Following are the steps by which a user can create the criteria:

- Click on the **New** button in the Detection Criteria List tab.

Assignment User Criteria List	Ticket Creation Criteria List	<u>Detection Criteria List</u>	Curated Detection Criteria List
Ticket(s) will be created based on the Detection criteria			
Detection Criteria List[PROJECT:Google Chronicle JIRA Integration]		Condition	Order
Detection Assign User	Condition	Order	Created By
			Created At

Detection Criteria List: Creation

- Detection Criteria List window will appear where the user will have the provision to configure the detection criteria in case any specific tickets need to be created in the selected project.
- Click on *Select Detection Rules*, and a multi-select dropdown with different rules will be displayed.
- Enter comma-separated version IDs of the selected rule in '*Fetch Detection for Specific Versions*' to create the detection ticket for the specific version of the rule
- Click on the checkbox '*Fetch detections for all versions*' to fetch the detection for all the versions of the selected rules.
- Click on the *Detection Alert State* to filter the detections by alert state.
- Click on the *Sort Detection By* dropdown to filter the detections by time.

Note: The Detection Criteria and Curated Detection Criteria List will be deactivated for Stream Detections since it does not provide responses based on Criteria.

Detection Criteria List

Assignment User*	<input type="text"/>	Order*	<input type="text" value="100"/>
Select Detection Rules	<input type="button" value="Please select rules if you want to fetch detections for only selected rules"/>		
Fetch Detection for Specific Versions	<input type="text"/> <small>Please enter specific version ids for rules to fetch detection</small>		
Fetch Detection for all versions	<input type="checkbox"/>		
Detection Alert State*	BOTH	<input type="button"/>	
Sort Detection By*	DETECTION_TIME	<input type="button"/>	
<input type="button" value="Submit"/> <input type="button" value="Close"/>			

Select Detection Rules

UserCreationThenDeletion (redacted)
rule_1676269733620 (redacted)
rule_1676005979907 (redacted)
rule_1675853701770 (redacted)
not_used (redacted)
rule_1675850587404 (redacted)
armis_demo (redacted)

DETECTION_TIME

Assignment User* Test Assignee **Order*** 100

Select Detection Rules

Fetch Detection for Specific Versions

Fetch Detection for all versions

Detection Alert State*

Sort Detection By* DETECTION_TIME

Submit **Close**

Field Name	Description
Assignment User	List of users that are part of the User Groups
Order	The priority of the criteria will be used to filter the response in order to assign the tickets to the user. Lowest to Highest, where the Highest will be preferred Default order: 100
Select Detection Rules	Select the rules needed to create the detection ticket
Fetch Detection for Specific Versions	Enter comma-separated version IDs of the selected rule to create the detection ticket for the specific version of the rule
Fetch Detection for all Versions	To fetch the detection for all the versions of the selected rules
Detection Alert State	Select the alert state for fetching the desired detection
Sort Detection By	Select the option to fetch the detection on the basis of time

- Once the detection criteria are saved they will be displayed in the config screen as listed below

Assignment User Criteria List	Ticket Creation Criteria List	<u>Detection Criteria List</u>	Curated Detection Criteria List
Ticket(s) will be created based on the Detection criteria			
Detection Criteria List[PROJECT:Google Chronicle JIRA Integration]		NEW	
Detection Assign User	Condition	Order	Created By
Admin	CHRONICLE_DETECTION_1	100	Admin
			05/14/2024 05:28:56

Curated Detection Criteria List: Creation

- A curated Detection Criteria List window will appear where the user will have the provision to configure the curated detection criteria in case any specific tickets need to be created in the selected project.
- Click on *Select Curated Detection Rules*, and a multi-select dropdown with different rules will be displayed.
- Click on the *Curated Detection Alert State* to filter the Curated Detections by alert state, the default value for alert state BOTH(ALERTING, NON_ALERTING)
- Click on the *Sort Curated Detection By* dropdown to filter the Curated Detections by time

Note: The Detection Criteria and Curated Detection Criteria List will be deactivated for Stream Detections since it does not provide responses based on Criteria.

Curated Detection Criteria List

Assignment User*	Admin	Order*	100
Select Curated Detection Rules	<div style="border: 1px solid #ccc; padding: 5px; width: 300px;"> <small>Please select rules if you want to fetch curated detections for only selected rules</small> </div>		
Curated Detection Alert State*	BOTH		
Sort Curated Detection By*	DETECTION_TIME		

Submit **Close**

Curated Detection Criteria List

Assignment User*	Admin	Order*	100
Select Curated Detection Rules	<input type="text"/> GCE Project SSH Keys (Redacted) GCP Service Account Editor or Owner (Redacted) GCP Service Account Key Creation (Redacted) Privileged Service Account Role at Project Level - TokenCreatorRole (Redacted) GCP Billing Disabled (Redacted) GCP Multi-Project Billing Disabled (Redacted) VPC Firewall Mass Rule Deletion (Redacted)		
Curated Detection Alert State*			
Sort Curated Detection By*			
<input type="button" value="Submit"/> <input type="button" value="Close"/>			

Field Name	Description
Assignment User	List of users that are part of the User Groups
Order	The priority of the criteria will be used to filter the response in order to assign the tickets to the user. Lowest to Highest, where the Highest will be preferred Default order: 100
Select Curated Detection Rules	Select the rules needed to create the Curated Detection ticket
Curated Detection Alert State	Select the alert state for fetching the desired Curated Detection
Sort Curated Detection By	Select the option to fetch the Curated Detection on the basis of time

- Once the Curated Detection criteria are saved they will be displayed in the config screen as listed below

Assignment User Criteria List	Ticket Creation Criteria List	Detection Criteria List	Curated Detection Criteria List
<i>Ticket(s) will be created based on the Curated Detection criteria</i>			
Curated Detection Criteria List[PROJECT:Google Chronicle JIRA Integration] NEW			
Curated Detection Assign User	Condition	Order	Created By
Admin	CHRONICLE_CURATED_DETECTION_1	100	Admin
			05/14/2024 05:47:11

Last Sync Details

- Upon Clicking Save, the scheduler will trigger the Job to fetch the data from Google SecOps in order to start creating the tickets.
- Once the Job has been executed successfully, wait for a few moments and then click on the Refresh icon beside the Last Sync Details label.
- Upon clicking the Refresh icon, it will update the Last Job Run Time for IoCs, Alerts, Detections and Curated Detections.
- Scheduler Status: Scheduled means that the job has been configured and scheduled successfully.
- Scheduler Status: Not Scheduled means that the Job is currently not scheduled and no API calls will be made to SecOps.
- Next Job Run Time: The Date and time for the next scheduled job run.

Last Sync Details	
Last Job Run Time for IoCs:	23-05-2024 11:13:49 UTC
Last Job Run Time for Alerts:	23-05-2024 11:13:53 UTC
Last Job Run Time for Detections:	23-05-2024 11:13:53 UTC
Last Job Run Time for Curated Detections:	23-05-2024 11:13:53 UTC
Scheduler Status:	Scheduled
Next Job Run Time:	23-05-2024 11:23:46 UTC
<input type="button" value="Save"/> <input type="button" value="Stop Sync"/> <input type="button" value="Reset"/>	

Button Event Action

- Save: This action will stop the current sync process and initiate the new sync process as per the new configuration provided.
- Stop Sync: This action will stop the current sync process and deregister the scheduler.
- Reset: This action will stop the current sync process, deregister the scheduler and set the configuration to the default one.

Existing sync would be completed in case of updates and changes would be applicable from the next invocation.

Last Sync Details ↴

Last Job Run Time for IoCs:	23-05-2024 11:13:49 UTC
Last Job Run Time for Alerts:	23-05-2024 11:13:53 UTC
Last Job Run Time for Detections:	23-05-2024 11:13:53 UTC
Last Job Run Time for Curated Detections:	23-05-2024 11:13:53 UTC
Scheduler Status:	Scheduled
Next Job Run Time:	23-05-2024 11:23:46 UTC

Retrohunt

Once the user opens the Retrohunt tab, it will check whether the user has done the Google SecOps authentication configuration or not.

If the user has not already done the Google SecOps authentication then the below message will be displayed



If the user has already done the SecOps authentication then the below screen would be displayed with options to start/cancel the retrohunt and see a list of retrohunts created earlier as the table view.

Start Retrohunt

In order to start the new retrohunt, click on the “Start Retrohunt” button, which will open a popup asking for the user input required to start the new retrohunt.

After entering all the required information click on the “Start Retrohunt” button to start the new retrohunt.

In case any error occurs while starting the new retrohunt, the Error message will be displayed as shown below.

Start Retrohunt

Rule ID or Version ID:*

Rule Id or Version Id for which Retrohunt would run.

Start DateTime:*

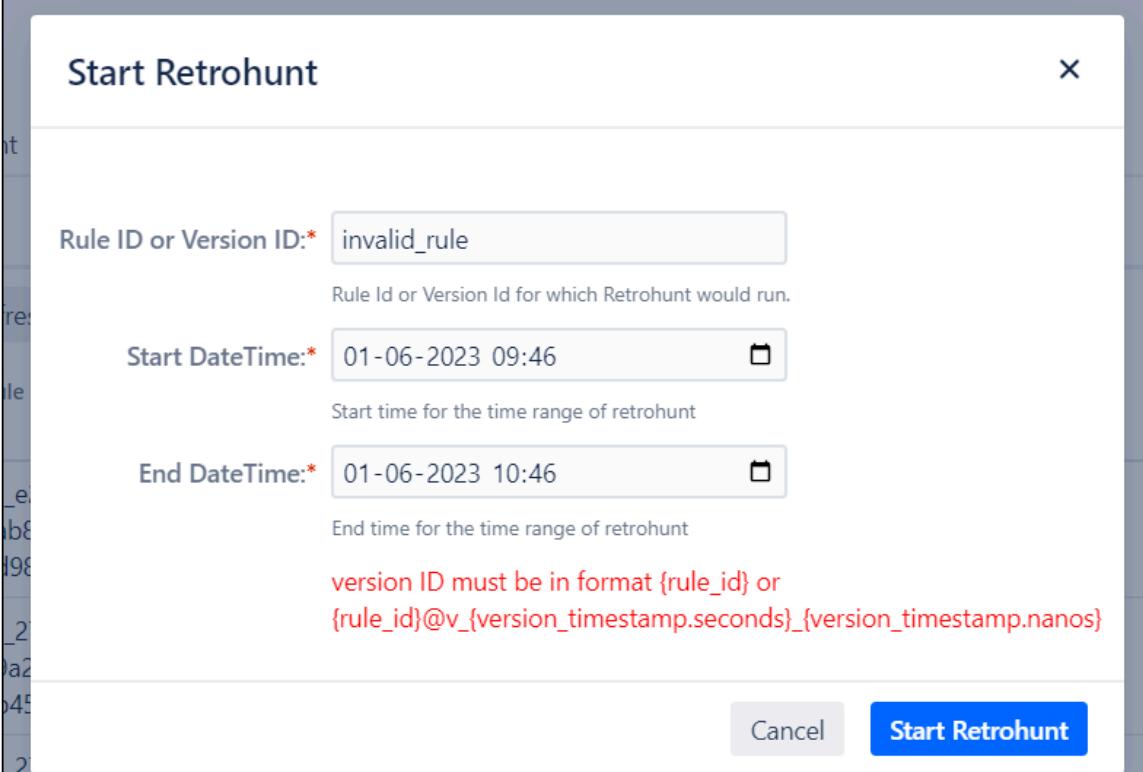
Start time for the time range of retrohunt

End DateTime:*

End time for the time range of retrohunt

version ID must be in format {rule_id} or
{rule_id}@v_{version_timestamp.seconds}_{version_timestamp.nanos}

[Cancel](#) [Start Retrohunt](#)



On success, the below message will be displayed to the user and the user can click on the "Refresh List" button to refresh the list of the retrohunts displayed in the table to see the details of the latest retrohunt.



Configuration	Retrohunt						
Start Retrohunt	Refresh List						
Retrohunt ID	Rule ID	Version ID	State	Progress Percentage	Start Time	End Time	Cancel Retrohunt
[REDACTED]	[REDACTED]	[REDACTED]	RUNNING	35.48	2023-06-01T05:22:14.173595Z	-	<button>Cancel</button>
[REDACTED]	[REDACTED]	[REDACTED]	CANCELLED	95.95	2023-05-30T10:55:35.469916Z	2023-05-30T11:03:21.274932Z	<button>Cancel</button>
[REDACTED]	[REDACTED]	[REDACTED]	CANCELLED	15	2023-05-30T10:00:19.647353Z	2023-05-30T10:00:54.035274Z	<button>Cancel</button>
[REDACTED]	[REDACTED]	[REDACTED]	DONE	100	2023-05-30T09:57:58.838074Z	2023-05-30T09:59:31.906040Z	<button>Cancel</button>

Cancel Retrohunt

In order to cancel the running retrohunt click on the “Cancel” button placed in the last column of that particular row of the retrohunt. The users would not be able to cancel the retrohunts which are cancelled or done.

On success, the below message will be displayed to the user.



A screenshot of the Jira Admin interface. At the top, there is a search bar with the text "Search Jira admin". Below the search bar, there are navigation links: "Manage apps", "User management", "Latest upgrade report", and "System". Under the "System" section, there are two tabs: "Configuration" and "Retrohunt", with "Retrohunt" being the active tab. Below the tabs are two buttons: "Start Retrohunt" and "Refresh List". A success message is displayed in a modal window: "Retrohunt cancelled successfully." with a checkmark icon.

Ticket Created by the App

The app can create a total of 4 different types of tickets, based on the configuration that the user chooses:

1. IoC Match
2. User Alert
3. Asset Alert
4. Detections
5. Curated Detections

IoC Domain Match

IoC(Indicators of Compromise) ticket, will help users to determine which domain has been compromised, catering all the information for that domain and will display in the ticket form as displayed below.

The deduplication criteria over here is the summary of Jira Issue which is built using Artifact, which means only a single ticket will be created for the artifact that is compromised until the ticket is in the Todo, In-Progress and In-Review stages.

The screenshot shows a Jira Software interface with the following details for an issue:

Issue Summary: Google Chronicle JIRA Integration / GCJI-7

Details:

- Type: IoC
- Priority: High
- Status: TO DO (View Workflow)
- Resolution: Unresolved
- Component/s: Malware Command and Control Server
- Labels: None
- IoC Ingest: 2019-07-09T08:00:00Z
- Int Raw Confidence: 0
- Last Seen: 2021-11-10T11:12:45.571Z
- Source: ET Intelligence Rep List
- Normalized Confidence: Low
- First Seen: 2021-03-30T11:21:04.892Z

People:

- Assignee: Unassigned
- Reporter: Administrator
- Votes: 0
- Watchers: 1 (Stop watching this issue)

Dates:

- Created: 14 minutes ago
- Updated: 14 minutes ago

Description:

URI: URL back to Chronicle

Attachments:

Drop files to attach, or browse.

Activity:

All Comments Work Log History Activity

There are no comments yet on this issue.

Add comment

User Alert Ticket

When any alert occurs for a particular user, then those data are captured and displayed in the form of a ticket as displayed below, helping the user to understand what could be the cause of the alert and to take appropriate action.

The deduplication criteria for the User Alert is the combination of the Email Address and Alert Name until the ticket is in the Todo, In-Progress and In-Review stage.

Note that here component names are case insensitive.

The screenshot shows a Jira Software issue page for ticket BCJ-17. The ticket is of type 'Alert' with priority 'Medium'. It has the component 'Office 365' and label 'User-Alert'. The time stamp is 2020-12-01T20:47:02Z. The 'Details' section contains JSON data under 'Udm Event' with sections for 'Metadata', 'Security Result', 'Principal', 'Target', 'Network', 'Extension', and 'About'. The 'People' section shows it is unassigned, created by 'admin', and updated 2 hours ago. The 'Dates' section shows creation and update times. The 'Hipchat discussions' section asks if you want to discuss the issue in Hipchat, with 'Connect' and 'Dismiss' buttons. The 'Attachments' section has a placeholder for file uploads. The 'Activity' section shows tabs for All, Comments, Work Log, History, and Activity, with a note that there are no comments yet. A 'Comment' button is at the bottom.

BCJ / BCJ-17

Type: Alert Status: Unresolved

Priority: Medium Resolution:

Component/s: Office 365

Labels: User-Alert

Time Stamp: 2020-12-01T20:47:02Z

URI: URI - 0

Udm Event

Metadata

```
{
  "eventTimestamp": "2020-12-01T20:47:02Z",
  "eventType": "EMAIL_TRANSACTION",
  "vendorName": "Microsoft",
  "productName": "Office 365",
  "productEventType": "SupervisoryReviewDAudit",
  "ingestedTimestamp": "2020-12-04T16:53:58.381236Z"
}
```

Security Result

```
[
  {
    "summary": "Threat Model Positive Score:74", "severity": "HIGH", "confidence": "HIGH_CONFIDENCE", "confidenceDetails": "74"
  }
]
```

Principal

```
[
  {
    "ip": [
      "10.169.83.60"
    ]
  }
]
```

Target

```
[
  {
    "user": {
      "emailAddresses": [
        "████████████████"
      ]
    },
    "application": "Exchange"
  }
]
```

Network

```
{
  "email": {
    "from": "████████████████@outlook.com",
    "to": [
      "████████████████@outlook.com"
    ],
    "subject": "Invoice for Goods"
  }
}
```

About

Attachments

Drop files to attach, or browse.

Activity

All Comments Work Log History Activity

There are no comments yet on this issue.

Comment

Asset Alert Ticket

When any alert occurs for a particular asset, then those data are captured and displayed in the form of a ticket as displayed below, helping the user to understand what could be the cause that would have impacted the asset and to take appropriate action.

The deduplication criteria for the Asset Alert is the combination of the Asset Name and Alert Name until the ticket is in the Todo, In-Progress and In-Review stage.

Note that here component names are case insensitive.

The screenshot shows a Jira Software interface for an issue titled "Suspicious Powershell Ancestry". The issue is categorized under "Alert" and has a priority of "Medium". It is currently "Unresolved". The "Details" section includes a "Description" field containing JSON data representing an "Udm Event". This event has fields like "Metadata", "Security Result", "Principal", "Target", "Network", "Extensions", and "About". The "Attachments" section shows a placeholder for file uploads. The "Activity" section indicates there are no comments yet. The sidebar on the left shows project navigation options like "Summary", "Issues", "Reports", and "Components".

Issue Details:

- Type: Alert
- Priority: Medium
- Status: Unresolved
- Resolution: (View Workflow)

Description:

```
URI URL back to Chronicle
```

Udm Event

Metadata	{ "eventTimestamp": "2021-03-25T11:00:00Z", "eventType": "GENERIC_EVENT", "productName": "Tanium EDR", "ingestedTimestamp": "2021-03-25T07:07:58.084169Z" }
Security Result	[{"summary": "Suspicious Powershell Ancestry"}]
Principal	-
Target	-
Network	-
Extensions	[{"hostname": "████████", "ip": ["████████"]}]
About	[{"hostname": "████████", "ip": ["████████"]}])

Attachments: Drop files to attach, or browse.

Activity:

All Comments Work Log History Activity

There are no comments yet on this issue.

Add comment

Detection Ticket

When any detection occurs for the particular rule, then those data are captured and are displayed in the form of a ticket as displayed below, helping the user to understand what could be the cause that would have impacted the rule and to take appropriate action.

The deduplication criteria for the Detection is the Detection ID until the ticket is in the Todo, In-Progress and In-Review stages.

There will not be any Enrichment feature for detections, instead, the data will be populated and a comment will be added to the corresponding detection ticket.

The screenshot shows a Jira Software interface for a ticket titled "Google Chronicle Jira Integration / GOOG-2".

Summary: Google Chronicle Jira Integration / GOOG-2

Details:

Type:	+ Detection	Resolution:	Unresolved
Priority:	= Medium		
Labels:	None		
Rule Type:	SINGLE_EVENT		
Alert State:	ALERTING		
Rule Author:	Nitin		
Rule Version:			
Rule ID:			

Description:

URI	URL back to Chronicle
Chronicle Detection ID	[REDACTED]
Chronicle Rule Description	-
Chronicle Detection Host Name	-
Chronicle Detection Source Host	-
Chronicle Detection Dest Host	-
Chronicle Detection Time	2024-05-23T12:33:36.672872300Z
Chronicle Detection Created Time	2024-05-23T12:34:16.166386Z
Chronicle Detection Window Start Time	2024-05-23T12:33:36.672872300Z
Chronicle Detection Window End Time	2024-05-23T12:33:36.672872300Z
Event Time-stamp	2024-05-23T12:33:36.672872300Z
Event Type	USER_LOGIN
Principal Asset Identifier	Host Name: [REDACTED]
Target Asset Identifier	IP Address: [REDACTED] Host Name: [REDACTED]

People:

- Assignee: Unassigned
- Reporter: Admin
- Votes: 0
- Watchers: 1 Stop watching this issue

Dates:

Created:	Just now
Updated:	Just now

Attachments:

Drop files to attach, or browse.

Activity:

All Comments Work Log History Activity

You can now pin up to five comments to highlight important information. Pinned comments will appear above all other comments, so they're easy to find.
Got it • Learn more about pinned comments

There are no comments yet on this issue.

Add a comment...

Pro tip: press m to comment

Curated Detection Ticket

When any Curated Detection occurs for the particular rule, then those data are captured and displayed in the form of a ticket as displayed below, helping the user to understand what could be the cause that would have impacted the rule and to take appropriate action.

The deduplication criteria for the Curated Detection is the Curated Detection ID until the ticket is in the Todo, In-Progress and In-Review stages.

There will not be any Enrichment feature for Curated Detections, instead, the data will be populated and a comment will be added to the corresponding Curated Detection ticket.

The screenshot shows a Jira Software interface for a ticket titled "Google Chronicle Jira Integration / GOOG-2". The ticket is categorized under "Issues".

Details:

- Type: Detection
- Priority: Medium
- Labels: None
- Rule Type: SINGLE_EVENT
- Alert State: ALERTING
- Rule Author: Nitin
- Rule Version: Rule ID: [REDACTED]

Description:

URI	URL back to Chronicle
Chronicle Detection ID	[REDACTED]
Chronicle Rule Description	-
Chronicle Detection Host Name	-
Chronicle Detection Source Host	-
Chronicle Detection Dest Host	-
Chronicle Detection Time	2024-05-23T12:33:36.672872300Z
Chronicle Detection Created Time	2024-05-23T12:34:16.166386Z
Chronicle Detection Window Start Time	2024-05-23T12:33:36.672872300Z
Chronicle Detection Window End Time	2024-05-23T12:33:36.672872300Z
Event Time-stamp	2024-05-23T12:33:36.672872300Z
Event Type	USER_LOGIN
Principal Asset Identifier	Host Name: [REDACTED]
Target Asset Identifier	IP Address: [REDACTED] Host Name: [REDACTED]

People:

- Assignee: Unassigned
- Reporter: Admin
- Votes: 0
- Watchers: 1 Stop watching this issue

Dates:

- Created: Just now
- Updated: Just now

Attachments:

Drop files to attach, or browse.

Activity:

All Comments Work Log History Activity

You can now pin up to five comments to highlight important information. Pinned comments will appear above all other comments, so they're easy to find.
Got it • Learn more about pinned comments

There are no comments yet on this issue.

Add a comment...
Pro tip: press **m** to comment

Enrichments

The enrichment process enables the user to select the time frame(number of days/date range) to determine which Assets were impacted and which Events were discovered related to a particular Domain or IP address.

This segment will take through the enrichment process that users can do on the created tickets. There are six different types of enrichment that the users can perform:

1. IoC Details
2. List Assets Impacted
3. List Events Discovered
4. List Asset Aliases
5. List User Aliases
6. UDM Search

IoC Details

- Click on the More Menu, and then click on the Google SecOps Enrichment option.

The screenshot shows a Jira Software interface for a project named 'proj2'. On the left, there's a sidebar with 'Issues' selected. The main area shows a ticket for 'PROJ2-24693' with the IP address '172.67.216.234'. In the top navigation bar, there's a 'More' button. A dropdown menu is open from this button, showing several enrichment options: 'Google SecOps Enrichment', 'UDM Search', 'Log work', 'Archive', 'Attach files', 'Attach Screenshot', 'Add vote', 'Voters', 'Stop watching', and 'Watchers'. The 'Google SecOps Enrichment' option is highlighted.

- Upon clicking on the Google SecOps Enrichment, the below-displayed popup will be displayed.
- Selected the Enrichment type as IOC Details, as we would like to perform enrichment for IoC.
- The Input dropdown list will have two values Domain Name and IP Address.
- Select For Input as Domain Name, which will determine on which domain we would like to perform the enrichment.
- Enter the Domain Name in For Value, and click on Submit.

Issues Boards Plans Create

Google SecOps Enrichment

Enrich Type: IOC Details

For Input: Domain Name

For Value: *

Submit Cancel

Priority: High
Component/s: Blocked
Labels: None
IoC Ingest: 2020-09-28T07:46:23.720Z

- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.

Jira Software Dashboards Projects Issues Boards Plans Create Search Help Admin

Google Chronicle JIRA Integration / GCJI-59

Issues

Details

Type:	loc	Status:	TO DO (View Workflow)	Assignee:	Unassigned
Priority:	High	Resolution:	Unresolved	Reporter:	Administrator
Component/s:	Malware Command and Control Server			Votes:	0
Labels:	None			Watchers:	1 Stop watching this issue
IoC Ingest:	2020-09-07T11:00:00Z				
Int Raw Confidence:	0				
Last Seen:	2021-04-14T13:18:11.207814Z				
Source:	ET Intelligence Rep List				
Normalized Confidence:	Medium				
First Seen:	2021-04-14T13:18:11.207814Z				

Description

URI URL back to Chronicle

Attachments

Drop files to attach, or browse.

Activity

All Comments Work Log History Activity

Administrator added a comment - Just now

Action: loc Details
Input: webwerks.in

Address	First Active Time	Last Active Time	Source Url
[port=[80], domain=[webwerks.in]]	2014-03-13T00:00:00Z	2022-03-21T00:00:00Z	https://tools.emergingthreats.net/docs/ET%20Intelligence%20Re

Edit · Delete · ⚙

Add comment

List Assets Impacted

- Upon clicking the More Menu and then Google SecOps Enrichment, the below-displayed popup will be displayed.
- Select the Enrichment type as List Assets Impacted, as we would like to perform enrichment for Asset Impacted.
- The input dropdown list will have multiple values like Domain Name, IP Address, HASH MD5, Hash SHA1 and Hash SHA256
- Select For Input as Domain Name, which will determine on which domain we would like to perform the enrichment.
- Enter the Domain Name in For Value.
- Then either enter the number of days or select the date range, and then click on Submit.

The screenshot shows a modal dialog box titled "Google SecOps Enrichment". The "Enrich Type:" dropdown is set to "List Assets Impacted(Max 5)". The "For Input:" dropdown is set to "Domain Name". The "For Value:" field is empty. Below these fields are two buttons: "Last Days" and "Date Range", with "Last Days" being selected. A "Day:" input field is also present. At the bottom of the dialog are "Submit" and "Cancel" buttons. In the background, there's a dark interface with some tabs like "Issues", "Boards", and "Plans", and a sidebar with "Admin" and "Unresolved" status indicators. Below the dialog, there's a table with two rows of data.

alx_high_severity	Int Raw Confidence:	0
alx_high_severity	Last Seen:	2025-04-10T04:52:10Z
alx_high_severity	Source:	ESET Threat Intelligence

- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.

All **Comments** Work Log History Activity Newest first ↓

 admin@local.com added a comment - Just now

Action: List Assets Impacted
Input Value: www.google.com
Start Time: 2023-05-02T17:59:56.245Z
End Time: 2023-06-01T17:59:56.245Z

Asset	First Seen	Last Seen
[REDACTED]	2023-05-23T19:57:56.965Z	2023-05-23T19:57:56.965Z
[REDACTED]	2023-05-07T22:36:45.837Z	2023-05-22T15:32:59.350Z
[REDACTED]	2023-05-09T11:54:37.939Z	2023-05-09T11:54:37.939Z
[REDACTED]	2023-04-07T10:57:38.068Z	2023-05-08T02:11:28.384Z
[REDACTED]	2022-05-29T06:00:06Z	2023-05-08T06:00:07Z

List Asset Aliases

- Upon clicking the More Menu and then Google SecOps Enrichment, a popup will be displayed.
- Select the Enrichment type as List Asset Aliases, as we would like to perform enrichment for Asset Aliases.
- For Input dropdown list will have multiple values like Host Name, IP Address, MAC Address and Product ID.
- Select For Input as Hostname, which will determine on which Hostname we would like to perform the enrichment.
- Enter the Hostname in For Value.
- Then either enter the number of days or select the date range, and then click on Submit.

Issues Boards Plans Create

Google SecOps Enrichment

Enrich Type: List Asset Aliases(Max 5)

For Input: Host Name

For Value:*

Last Days Date Range

Day:*

Submit Cancel

x_high_severity Int Raw Confidence: 0
Last Seen: 2025-04-10T04:52:10Z

- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.

Activity

All Comments Work Log History Activity Newest first ↓

admin added a comment - Just now

Action: List Assets Aliases
 Input Type: Host Name
 Input Value: [REDACTED]
 Start Time: 2023-05-16T09:30:40.379Z
 End Time: 2023-06-15T09:30:40.379Z

Hostname	IP Address	MAC Address	Product ID	Start Date	End Date
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	2023-05-16T09:30:40.379Z	2023-06-15T09:30:40.379Z

List User Aliases

- Upon clicking the More Menu and then Google SecOps Enrichment, the below-displayed popup will be displayed.
- Select the Enrichment type as List User Aliases, as we would like to perform enrichment for User Aliases.
- For Input dropdown list will have multiple values like Email, Username, Windows SID, Employee ID and Product Object ID.

- Select For Input as Username, which will determine on which username we would like to perform the enrichment.
- Enter the Username in For Value.
- Then either enter the number of days or select the date range, and then click on Submit.

The screenshot shows a Jira-like application interface. A modal dialog box titled "Google SecOps Enrichment" is open. Inside the dialog, there are dropdown menus for "Enrich Type" (set to "List User Aliases(Max 5)"), "For Input" (set to "Email"), and "For Value" (empty). Below these, there are tabs for "Last Days" and "Date Range", with a "Day:" input field next to it. At the bottom of the dialog are "Submit" and "Cancel" buttons. In the background, a list of issues is visible, and a comment card for issue #5 is shown with fields for "Int Raw Confidence: 0", "Last Seen: 2025-04-10T04:52:10Z", and "Source: ESET Threat Intelligence".

- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.

The screenshot shows a Jira-like application interface. A comment is posted under an issue, detailing the enrichment process: "Action: List User Aliases", "Input Type: Username", "Input Value: [REDACTED]", "Start Time: 2004-04-15T09:17:51.540Z", and "End Time: 2023-06-15T09:17:51.540Z". Below the comment is a table with columns "User ID", "User Display Name", "Title", "Company Name", "Start Date", and "End Date". Two rows of data are present, both with redacted values in the first four columns and specific dates in the last two columns: "2004-04-15T09:17:51.540Z" and "2022-12-08T06:47:56.197021Z" for the first row, and "2022-12-08T06:47:56.197021Z" and "2023-06-15T09:17:51.540Z" for the second row.

List Events Discovered

- Upon clicking the More Menu and then Google SecOps Enrichment, the below-displayed popup will be displayed.
- Select the Enrichment type as List Assets Impacted, as we would like to perform enrichment for Events Discovered.
- The Input dropdown list will have multiple values like Host Name, IP Address, MAC Address and Product ID.
- Select For Input as MAC Address, which will determine on which domain we would like to perform the enrichment.
- Enter the MAC Address in For Value.
- Then either enter the number of days or select the data range, and then click on Submit.

The screenshot shows a modal dialog box titled "Google SecOps Enrichment". The "Enrich Type:" dropdown is set to "List Events Discovered(Max 5)". The "For Input:" dropdown is set to "Host Name". The "For Value:" field is empty. Below these fields are two buttons: "Last Days" and "Date Range". Under "Last Days", there is a "Day:" input field which is also empty. At the bottom of the dialog are "Submit" and "Cancel" buttons. In the background, there is a dark interface with some text and a user profile icon.

- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.

UDM Search

- For searching UDM events, the user needs to click on the More button in the top of the issue details screen.
- Select the UDM Search option from the menu.

The screenshot shows a Jira interface for an issue titled "proj2 / PROJ2-24693 172.67.216.234". The sidebar on the left lists several other open issues. The main panel displays the issue details, including fields like Type (loc), Priority (High), Component/s (Blocked), Labels (None), IoC Ingest (2020-09-28T07:4), Int Raw Confidence (0), and Last Seen (2025-04-10T04:5). A sidebar on the right shows "People" information such as Assignee, Reporter, Votes, and Watchers. A vertical scrollbar is visible on the right side of the main content area.

- Users need to enter the UDM query, select Start DateTime and EndTime. Set the Limit field which represents the no. of results fetched from the UDM search API and then click on the Submit button which will start the query execution.
- The query execution will run in the background after the user clicks on the Submit button. Once the execution is completed, the search results will be added as Jira comments and can be seen in the Jira issue details screen. An appropriate error message will be added in Jira comment in case any error occurs in query execution or while adding Jira comments.
- The search results will be added in batches of 10 per comment. If there are more than 10 results, additional Jira comments will be created.

[Access](#) if you no longer require it. For more information, refer to the [documentation](#).

▼ Issues

Switch

UDM Search

UDM Query:

Limit:
Limit for number of events to be fetched from UDM query results. Range is 1 to 100.

Start Date Time (Local Time):

End Date Time (Local Time):

Admin

Submit Cancel

Note: Google SecOps has a limit of 120 UDM Search Query executions in an hour.

Int Raw Confidence:	0
Last Seen:	2025-04-10T04:52:10Z
Source:	ESET Threat Intelligence

Update Detection Rule State

This option enables the user to enable/disable the Alerting and Live Rule State of the detection rule associated with the detection ticket. Only Jira issues of detection issue type having a value of “Rule ID” custom field will have the option of “Update Detection Rule State”.

Click on the More Menu, and then click on the “Update Detection Rule State” option.

Upon clicking on the “Update Detection Rule State”, a popup will be displayed as below with the prefilled values of the Rule Name and Rule ID according to the Rule ID associated with the Detection ticket. Based on the current state of Alerting and Live for the given Rule ID, checkboxes would be selected/deselected by default.

Select/Deselect the Checkbox to enable/disable the Alerting or Live Rule State and click on “Submit” to update the Rule state.

Update Detection Rule State

Rule Name:	singleEventRule2
Rule ID:*	[REDACTED]
Alerting Rule State	<input checked="" type="checkbox"/> <i>Please select/deselect to activate/deactivate the Alerting Rule State</i>
Live Rule State	<input type="checkbox"/> <i>Please select/deselect to activate/deactivate the Live Rule State</i>
Submit Cancel	

The comment will be added to the Jira issue indicating whether the Update Rule State was successful or not.

Activity

All	Comments	Work Log	History	Activity	Newest first ↓
<p>admin@local.com added a comment - Just now Successfully enabled Alerting for Detection Rule [REDACTED]. Successfully disabled Live Rule State for Detection Rule [REDACTED].</p>					
<p>Edit · Delete · Pin · ⚙</p>					

Development Assumptions

1. Only those projects will be listed which would have been created via the [Google SecOps Project Creation Template](#)
2. For Daily, weekly and monthly the job won't trigger immediately. It will only fetch the data as the user configures it.

3. The deduplication criteria for the ticket creation are as follows:
 - IoC: Summary of Jira Issue which is built using artifacts (Domain Name, DestinationIP, SHA etc.)
 - Asset Alert: Combination of Asset and Alert Name.
 - User Alert: Combination of Email Address and Alert Name.
 - Detection: Detection Id.
 - Curated Detection: Detection Id.
4. If the severity is empty/NA and has not been sent as part of the Google SecOps API response then, in that case, the ticket severity will be set to the project default.
5. No Updation will take place once the tickets are created based on deduplication criteria.
6. The same tickets will be created based on the deduplication criteria when those tickets are closed by the user.
7. When the project is changed and the configuration is saved, the Last Job runtime for IoCs, Alerts, Detections and Curated Detections will be reset and the data will be fetched based on the No of days to fetch IoCs/Alerts/Detections/Curated Detections Initially.
 - If an app is configured with Project A, and it's currently synching the data, and then a user changes the Project to B and then clicks on Save. Then the Last Job Run time will Reset and the synching will start based on the days that would have been mentioned in **No of days to fetch IoCs/Alerts/Detections/Curated Detections Initially** for Project B.
8. The Stream Detection feature utilizes a separate scheduler that is invoked every 10 minutes. If a scheduled job is currently running, it will skip the new job and continue the ongoing stream collection. However, if the stream fails due to any reason, it will start the new job in the next 10-minute interval.
9. In the Stream Detection feature, when the user configures the new stream detection configuration and saves the new configuration, the stream detection will start using the new configuration after a maximum of 10-minute time range, at the next scheduled job invocation.
10. The "Number of days to fetch IoCs/Alerts/Detections/Curated Detections initially" determines the continuation time parameter for Stream API calls. However, if the user inputs a value exceeding the last 7 days, the app will automatically set the continuation time to 7 days from the current time.
11. On installation, if configurations are present then the scheduler will be registered and sync will start with the existing configuration.
12. When the invalid service account file is selected and authenticated, then it would consider the previously saved valid service account file for fetching the IOCs, alerts, Detections and Curated Detections and it won't interrupt the current scheduler.
13. When the incorrect proxy details are entered and authenticated, then it would consider the previously saved valid data when the configuration is saved, for fetching the IOCs, alerts, Detections, and Curated Detections and it won't interrupt the current scheduler.
14. The app sends the entered inputs to the Google SecOps API and validations are handled by the Google SecOps itself. Based on the API response, the following message will be displayed in the comment section based on the user input

- No Response / Empty Response / Null Response: Display the User-entered criteria with the message “No Data Found for the above Enrichment Criteria.”
 - Bad Response / Error Response: Display the User-entered criteria with the reason for failure.
15. For the Asset Aliases option in Google SecOps Enrichment, if the value of the selected input type parameter in the entity response is the same as the input value then that alias will not be added in the comment.
16. It is suggested that the user must first Reset the config before uninstallation.
17. If there is more data available for IOCs, Alerts, Detection or Curated Detection than the limit set on the configuration page then data beyond that limit will be lost.
Ex. Suppose the “*Limit of IOC tickets to create per invocation*” is set to 1000 and the Daily scheduler is configured. If there are 1200 IOCs present in the Google SecOps for an interval of 1 day then only 1000 IOCs will be created in Jira and the remaining 200 will be missed.
18. Jira admin users won’t be able to change the workflow(Todo, In-Progress, In-Review and Done), custom fields and the Issue types of the project which are created by the Google SecOps Management System template. The restriction in the customized templates is good, as that doesn’t allow any user to make changes stopping causing issues in the creation of the tickets
19. [The users should be part of either of the following groups:](#)
- Jira Software
 - Jira Service Desk
 - Jira Administrator

Troubleshooting

1. For any issues, please refer to the “atlassian-jira.log” log file.
(Location: \$JIRA_HOME/atlassian/application-data/jira/log/atlassian-jira.log)
2. Following are the log errors.

Messages	Responses	Location
Invalid service account file or Invalid region.	If the Invalid service account file is uploaded or the Invalid region value	Config Screen

	is entered	
Failed to authenticate the service account file.	If the existing service account is no longer valid	Config Screen
Internal Server error.	The Jira server is down	Config Screen
Successfully validated service account.	Valid service account file	Config Screen
Valid Service Account file exists.	The existing service account file is valid	Config Screen
Previously saved valid authentication data will be considered.	The previously saved valid service account file/ proxy detail is considered.	Config Screen
Failure: Either due to invalid region selection / Google SecOps instance is unreachable	When an invalid region is selected for a service account credential file.	Config Screen
Authentication Failure: Either due to Invalid Service Account File / Invalid Proxy Detail (If proxy is enabled)	The uploaded service account file is invalid or the proxy details entered are incorrect.	Config Screen
API call failed on path[%s] status:%s & reason-phrase:%s	For the Google SecOps API error	Logs
authenticate() Failed to authenticate message:	Authentication Failed	Logs
Failed to call API on the path:	API called failed	Logs
Failed to close Http-Client	Cannot establish Http client connection	Logs
pullIoCDetails() Failed	Failed to pull loc's Data	Logs
pullAssets() Failed	Failed to pull Asset Data	Logs
pullEvents() Failed	Failed to pull Events Data	Logs
pullDetections() Failed	Failed to pull Detections data	Logs
pullCuratedDetections() Failed	Failed to pull Curated Detections data	Logs
pullStreamDetection() Failed	Stream connection failed.	Logs
pullStreamDetections() Finish	Stream connection closed and data collection was stopped.	Logs
pullRules() Failed	Failed to pull Rules data	Logs
pullCuratedRules() Failed	Failed to pull Curated Rules data	Logs
pullloc() finish @ {}, IOC Match Count: {} & Ticket Count : {}	Display the counts of loc and how many tickets are created	Logs
iOcs() response: {}	Display the list of IoC under comments and in logs	Ticket comments and Logs
iocDetails() response: {}	Display the details of IoC under comments and in logs	Ticket comments and Logs

pullAlerts() finish @ {}, Alerts Count: {} & Ticket Count: {}	Display the counts of Alerts and how many tickets are created	Logs
assets() response: {}	Display the details of Asset under comments and in logs	Ticket comments and Logs
events() response: {}	Display the details of Events under comments and in logs	Ticket comments and Logs
pullDetection.detections() Finish @ {}, Last-Sync-Time {}, Detection Count : {}, Ticket Count : {} & Duplicate Ticket Count : {}	Display the counts of Detections and how many tickets are created	Logs
detections() response: {}	Display the details of Detections under comments and in logs	Ticket comments and Logs
pullCuratedDetection.curatedDetections() Finish @ {}, Last-Sync-Time {}, Curated Detection Count : {}, Ticket Count : {} & Duplicate Ticket Count : {}	Display the counts of Curated Detectors and how many tickets are created	Logs
streamDetection(), Finish @ {}, Last-Sync-Time {}, Detection Ticket Count : {} & Curated Detection Ticket Count : {}	Display the counts of Detection and Curated Detectors received and how many tickets are created.	Logs
curatedDetections() response: {}	Display the details of Curated Detections under comments and in logs	Ticket comments and Logs
getAccessToken() Failed: Access-token can not be null or empty.	Access Token not valid	Logs
iocTicket() duplicate ticket[{}]: {}	Duplicates IoC found	Logs
iocTicket() created ticket: {}	IoC Tickets Created	Logs
Can not find %s custom field	If the custom field is not found	Logs
Can not find %s issue type	If the Issue Types is not found	Logs
Failed job runner	If the job is failed	Logs
registerSchedule() with parameter	When the job is registered based on the configuration	Logs
Error waiting until next try for the backoff strategy. Error: {}	When 429 error received for calling API endpoint	Logs
Retry Failed: Total of attempts: {}. Total waited time {} ms.	When the number of retries exceeded the maximum limit	Logs
userAliases() Failed: {}	When Google SecOps Enrichment ["User Aliases"] fails	Logs
assetAliases() Failed: {}	When Google SecOps Enrichment ["Asset Aliases"] fails	Logs
enableAlerting Failed: {}	When "Update Detection Rule State" fails to enable alerting for given rule	Logs

disableAlerting Failed: {}	When “Update Detection Rule State” fails to disable alerting for given rule	Logs
enableLiveRule Failed: {}	When “Update Detection Rule State” fails to enable Live state for given rule	Logs
disableLiveRule Failed: {}	When “Update Detection Rule State” fails to disable Live state for given rule	Logs
runRetrohunt() Failed: {}	When Starting a new retrohunt fails	Logs
cancelRetrohunt() Failed: {}	When cancelling a retrohunt fails	Logs
pullRetrohunts() Failed: {}	When getting retrohunts fails	Logs
getRuleDetails() Failed: {}	When getting rule details for particular detection rule fails	Logs

Additional Information

The below segment covers some additional information about the Google SecOps App

Application Dependencies

Area	Version
Java	8 (1.8.x)

Atlassian SDK	8.2.7
Google SecOps API Version	v1, v2

App - Jira Version Compatible Matrix

Jira Software	9.0.x - 9.15.x, 10.0.x - 10.3.x
Jira Service Desk	5.0.x - 5.15.x

-----End of Document-----