



# Rubrik Security Cloud: Google SecOps SOAR Integration

User Guide

Version: 1.0

# Table of Contents

---

Table of Contents.....	1
Overview.....	1
Google SecOps SOAR Platform.....	2
Rubrik Security Cloud Platform.....	2
Rubrik Security Cloud for SecOps SOAR.....	2
Release Notes.....	3
v1.0.....	3
Actions:.....	3
Installation & Configuration.....	4
Prerequisites.....	4
Installing the Integration.....	6
Configuring the Integration.....	7
Parameters.....	9
Actions.....	10
Invoking an Action in SOAR.....	10
Invoke Action Manually (from Case).....	10
Invoke Action Automatically (from Playbook/Block).....	10
Actions provided in the Integration.....	12
Action 1: Ping.....	12
Action 2: List Events.....	13
Action 3: Get Sonar Sensitive Hits.....	16
Action 4: Get CDM Cluster Connection State.....	24
Action 5: Get CDM Cluster Location.....	25
Action 6: List Object-Snapshots.....	26
Action 7: List Sonar File Contexts.....	29
Action 8: Turbo IOC Scan.....	34
Action 9: Advanced IOC Scan.....	36
Action 10: IOC Scan Results.....	40
Playbooks.....	42
Uninstalling the Integration.....	43
Known Issues.....	44
Troubleshooting.....	45
1. PythonProcess Has timed out.....	45
2. Unknown error running Action.....	47
References.....	48

# Overview

---

## Google SecOps SOAR Platform

Google SecOps SOAR platform integrates seamlessly with existing security infrastructure, leveraging advanced analytics and machine learning to prioritize alerts and streamline the detection, investigation, and remediation of threats. It facilitates collaboration among security teams through a centralized platform, accelerating response times and improving overall organizational resilience against cyber threats. By automating routine tasks and coordinating actions across different security tools it enables security teams to focus on more strategic initiatives while effectively managing and mitigating cybersecurity risks.

## Rubrik Security Cloud Platform

Rubrik Security Cloud is a cloud-native SaaS platform that provides a unified control plane for data management and protection across hybrid and multi-cloud environments. It centralizes visibility, policy enforcement, compliance, and threat detection through a single, GraphQL driven interface.

## Rubrik Security Cloud for SecOps SOAR

The Rubrik Security Cloud Integration for Google SecOps SOAR strengthens your data security and resilience by enabling automated data protection workflows and faster incident investigation through rich contextual insights from your Rubrik environment.

# Release Notes

---

## v1.0

- This integration implements investigative and generic actions for the Rubrik Security Cloud platform on the Google SecOps SOAR Platform. It enables end-users to implement comprehensive network security use cases through a combination of the following actions:

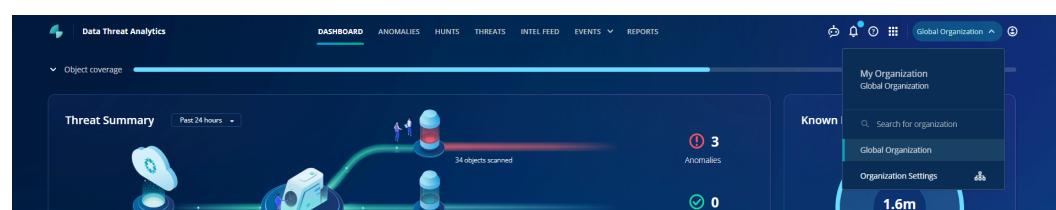
### Actions:

- **Ping:** Tests the connectivity of the Google SecOps SOAR server to the Rubrik Security Cloud platform.
- **List Events:** Retrieves a list of events from Rubrik Security Cloud.
- **Get Sonar Sensitive Hits:** Finds data classification hits on a specified object.
- **Get CDM Cluster Connection State:** Retrieves the connection state of a specified CDM cluster.
- **Get CDM Cluster Location:** Retrieves the geographic location of a specified CDM cluster.
- **List Object Snapshots:** Retrieves Rubrik snapshot(s) of an object.
- **List Sonar File Contexts:** Retrieves the context of files, folders, or file shares for a specified object and snapshot.
- **Turbo IOC Scan:** Starts a new Turbo Threat Hunt to scan for indicators of compromise (IOCs).
- **Advanced IOC Scan:** Starts a new Advanced Threat Hunt with granular control over scan parameters to scan for indicators of compromise (IOCs).
- **IOC Scan Results:** Retrieves detailed results of Turbo or Advanced Threat Hunts.

# Installation & Configuration

## Prerequisites

- A Google SecOps SOAR Instance with an Admin role user.
- Rubrik Security Cloud Credentials (Service Account JSON, Rubrik account domain)
- Licensed Rubrik Security Cloud portal to support required data
- Rubrik Security Cloud Credentials with a user role that can generate Service Account JSON.
  - To obtain a Service Account, go to Rubrik Security Cloud **Global Organization > Organization Settings** towards the top right corner.



Rubrik Security Cloud - Dashboard

- Search for **Service Account** in the search bar on the top left corner.



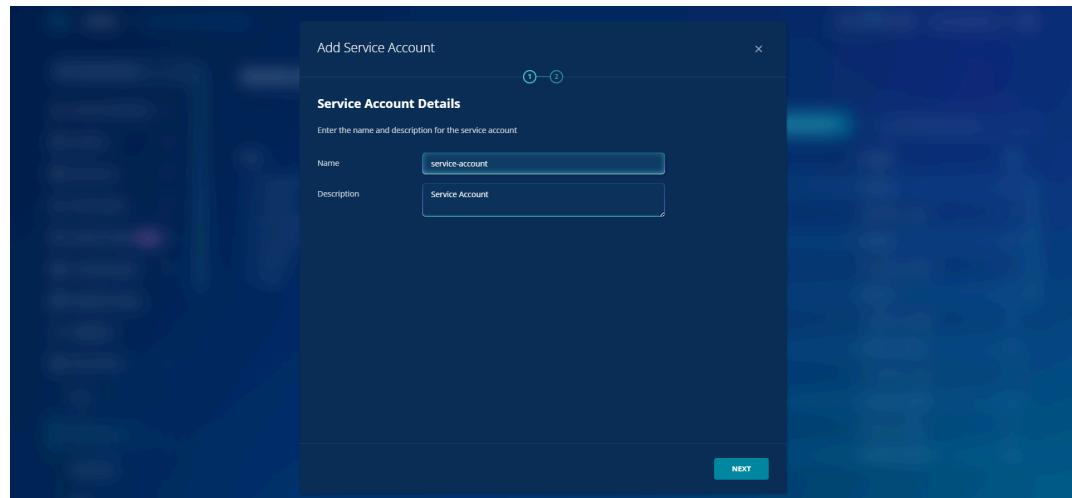
Rubrik Security Cloud - Organization Settings Page

- Click on **Add Service Account**



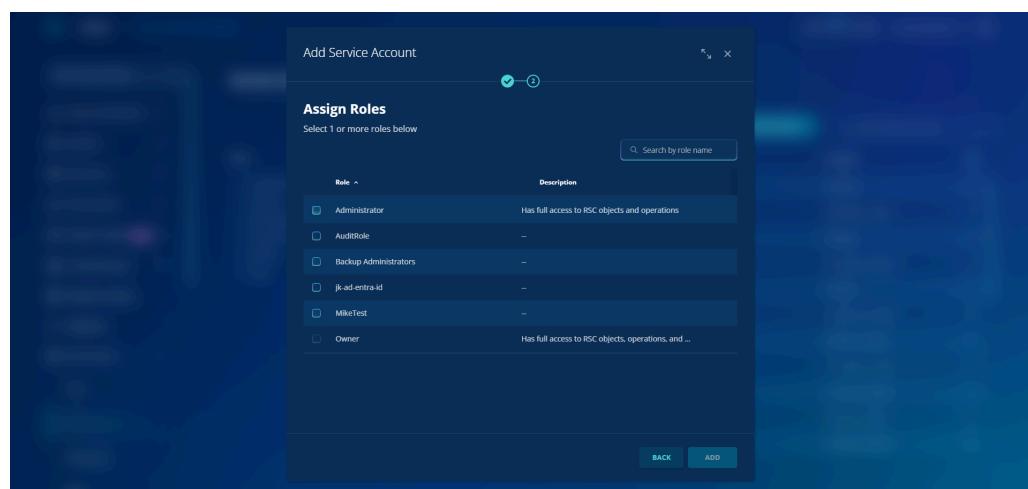
Rubrik Security Cloud - Service Accounts Page

- Add the relevant name and description for the service account json and click on **NEXT**



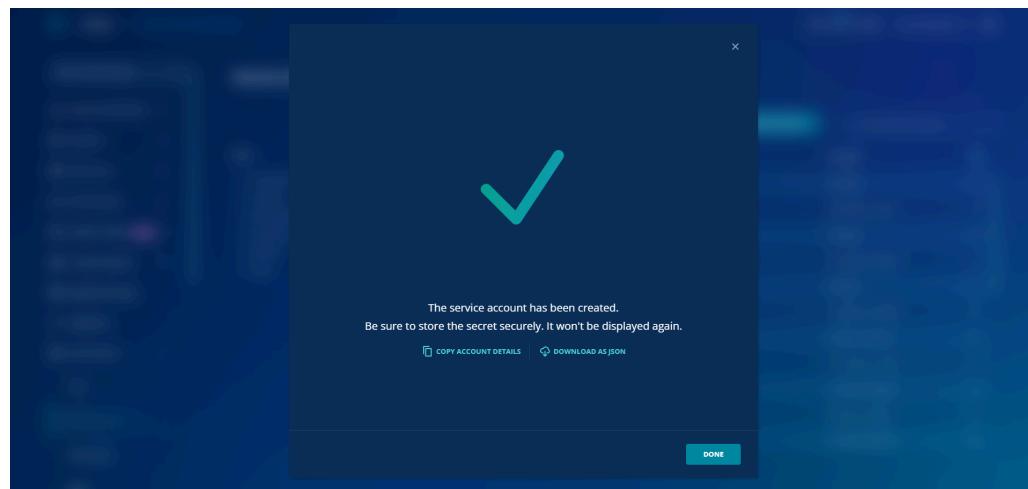
Rubrik Security Cloud - Create Service Account (Name and Description)

- Select the user role as **Administrator** and click on **ADD**



Rubrik Security Cloud - Create Service Account (User Role)

- The below page will appear after the service account is created successfully. Click on **COPY ACCOUNT DETAILS** or **DOWNLOAD AS JSON** to get the Service Account JSON.

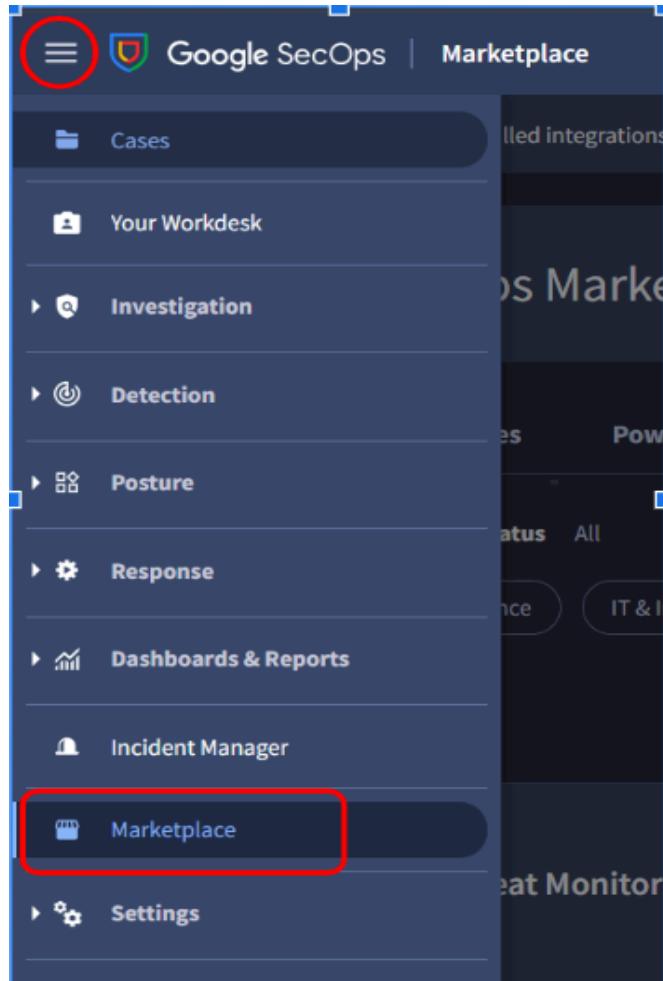


Rubrik Security Cloud - Service Account Created

## Installing the Integration

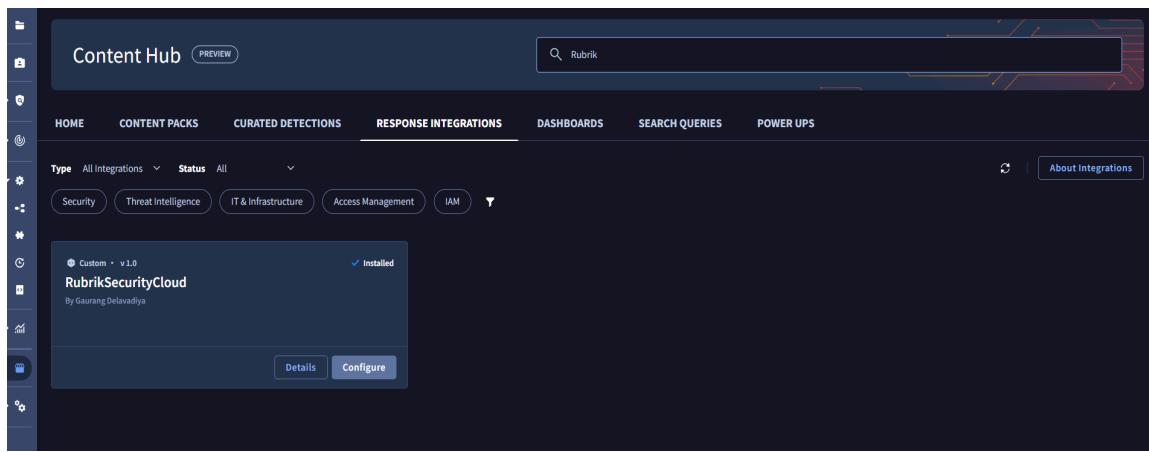
---

1. Log in to the Google SecOps SOAR Platform.
2. From the Sidebar, click on the **Marketplace** section.



*Google SecOps sidebar - Click on Marketplace*

3. From the Response Integrations tab, search for the term **Rubrik Security Cloud**.



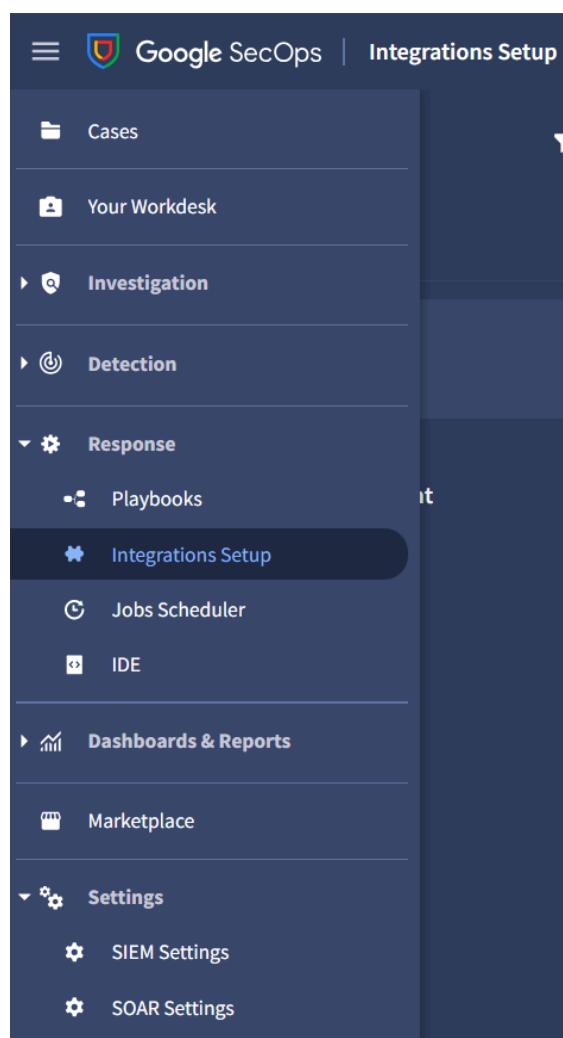
*Google SecOps Marketplace - Search the Integration*

4. On the integration named **Rubrik Security Cloud**, click **Install**.

# Configuring the Integration

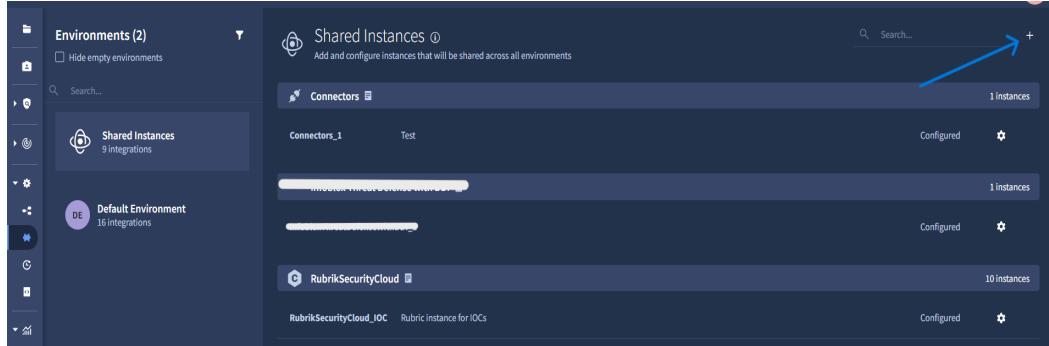
---

1. Once the integration has been installed successfully, the user needs to configure it to use the actions provided by the integration. These actions can be run manually from a case or can be used in playbooks.
2. To configure the integration, users can navigate to **Response > Integrations Setup**.
3. The integration can be configured in any of the desired environments. The integration actions can be used for playbooks and cases belonging to the environment in which the integration is configured.



*Google SecOps sidebar - Integrations Setup*

4. Users must click on the Plus (+) button to configure the integration for the desired environment.



*Google SecOps - Configure integration in the environment*

5. Search for **Rubrik Security Cloud** integration and select it. Click **Save**.
6. The instance of integration will be saved. However, in the next pop-up, users must add the necessary configuration parameters to use the actions.

**RubrikSecurityCloud - Configure Instance**  
Configure all the necessary fields and parameters for this instance

Environment	SI Shared Instances
Instance Name	RubrikSecurityCloud
Description	(Empty text area)
<b>Parameters</b>	
Service Account JSON *	<input type="text"/>
Verify SSL	<input type="checkbox"/>

**Test** **Cancel** **Save**

*Google SecOps - Integration Configuration*

## Parameters

Field name	Description	Default value	Required	Type
Service Account JSON	Service account JSON	-	True	String
Verify SSL	Controls SSL certificate verification when making HTTPS requests to the Rubrik Security Cloud GraphQL endpoint.	Unchecked	False	Checkbox

7. After adding the valid configuration parameters, click on the **Save** button to save the configurations. This is required to access the Rubrik Security Cloud GraphQL endpoint used in the actions.
8. After saving the configurations, the user can validate them using the **Test** button.
  - A green tick mark appears if the credentials provided are valid.



*Google SecOps Marketplace - Configurations Test successful*

- If invalid credentials are provided or any internal issue is faced, a red cross mark on the right side of the Test button will appear. The full error message can be displayed by clicking the red cross button.



*Google SecOps Marketplace - Configurations Test Unsuccessful*

```
----- Main - Param Init -----
-- Reading configuration from Server
Reading configuration from Server
Reading configuration from Server -----
----- Main - Started ----- Body:
{'client_id': 'client|1384ee2e-b2aa-4932-a5d0-159c8989d2ac', 'client_secret':
'yfUuDhUvuS7geSxVL8exFSCER6lT0xc7K4
wgTybiK7x4y6tCsGHZdbnWTemTHdb4'}
Data: None Connection to API failed,
performing action Rubrik Security Cloud -
Ping NOT_FOUND: no such client exists
(Original error: 404 Client Error: Not
Found for url: https://rubrik-tme-
rdp.my.rubrik.com/api/client_token)
Traceback (most recent call last): File
"/opt/siemplify/siemplify_server/bin/Scri
```

*Google SecOps Marketplace - Configuration failure message*

### NOTE:

- After making any changes in the configuration parameters, the user needs to save them before testing again using the Test button.

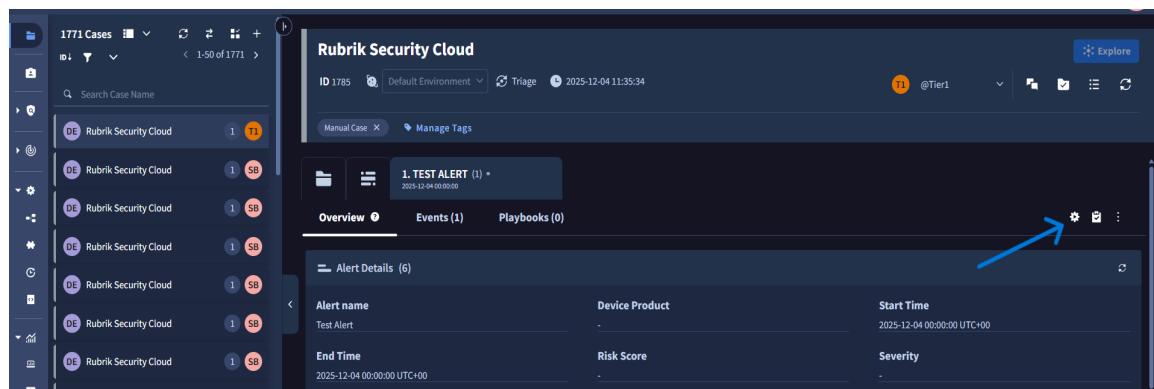
More information about configuring integrations in SecOps can be found [here](#).

# Actions

## Invoking an Action in SOAR

### Invoke Action Manually (from Case)

1. Navigate to the Case Overview tab of the case on which the action needs to be performed.
2. In the selected case, click Manual Action ('gear' icon) located on the right side under the Case Top Bar. The Manual Action dialog box appears.



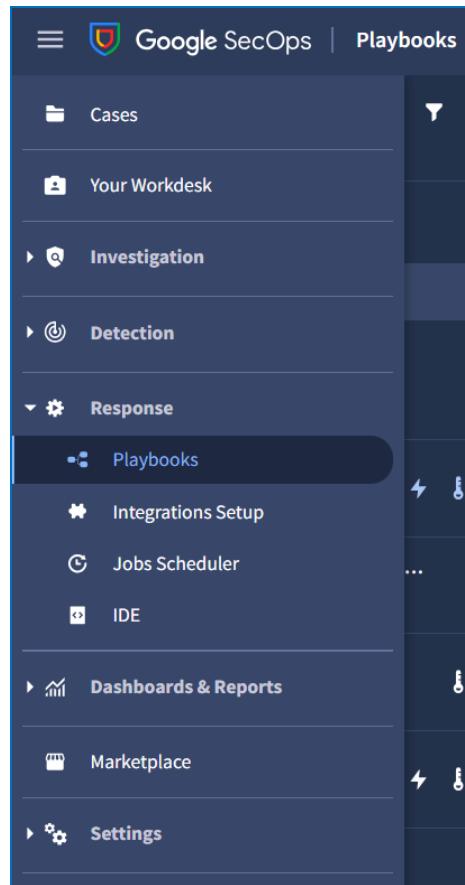
Google SecOps Case - Click on the gear icon

3. Select the required action: > [Action Name]. Make sure to fill in the required information.
4. Once the information is added, click on the Execute button.
5. Once the action is successfully executed, the result (success or failure) will be displayed on the Case wall.
6. The result contains different JSON output and data tables based on different actions.

More information on invoking an action manually can be found [here](#).

### Invoke Action Automatically (from Playbook/Block)

- Actions can be added as a step in a playbook. This action will be run when the playbook is executed. Playbooks, in turn, can be triggered on cases and alerts based on the conditions determined by the user.
- To add an action as a part of the playbook, follow these steps:
  1. Navigate to **Response > Playbooks**



*Google SecOps Sidebar - Playbooks*

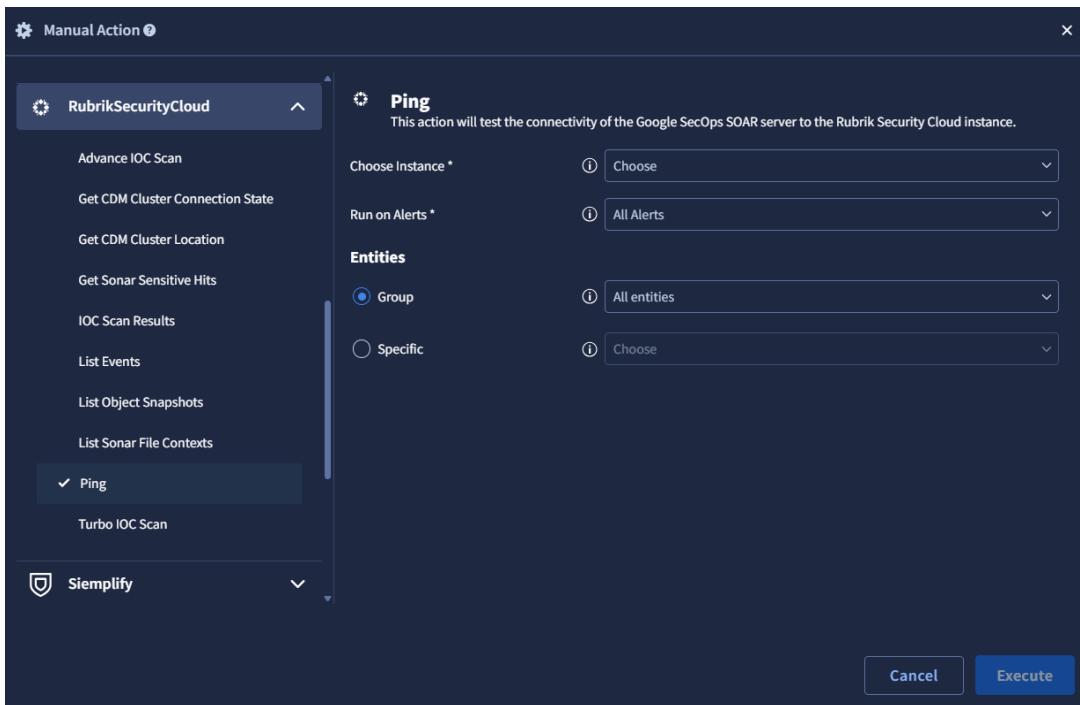
2. Select any existing playbook or create a new one.
3. Click on the **+ Open Step Selection** button, and navigate to the Actions tab.
4. Under Rubrik Security Cloud integration, all the actions available in the integration would be visible. Simply, drag and drop the action required to the playbook step.
5. The action should now be added to the playbook. Make sure to configure the input parameters (if applicable) for the action.

More information on invoking an action using a playbook can be found [here](#).

# Actions provided in the Integration

## Action 1: Ping

- When [configuring the Rubrik Security Cloud integration](#), the configured inputs can be tested. This validation of the inputs is done by Ping Action. Hence, Ping Action is responsible for the validation of the configuration parameters when the Integration is configured.



*Google SecOps Cases - Ping Action dialog box*

## Action 2: List Events

- Retrieves a list of events from Rubrik Security Cloud based on specified filters. Events include backup activities, anomalies, storage operations, and other system activities.
- Parameters:**

Argument Name	Type	Required (Yes / No)	Default Value	Description
Activity Status	String	No	N/A	Filter by activity status. Supports comma-separated values. Examples: "Failure", "Running", "Queued", "Success"
Activity Type	String	No	N/A	Filter by activity type. Supports comma-separated values. Examples: "Sync", "Anomaly", "Storage", "Backup"
Severity	String	No	N/A	Filter by severity level. Supports comma-separated values. Examples: "Critical", "Warning", "Info"
Object Name	String	No	N/A	Filter events by object name
Object Type	String	No	N/A	Filter by object type. Supports comma-separated values. Examples: "ShareFileset", "WindowsFileset", "VmwareVm"
Cluster ID	String	No	N/A	Filter by cluster ID. Supports comma-separated values
Start Date	String	No	N/A	Start date to fetch events from.

				Format: yyyy-mm-dd or yyyy-mm-ddTHH:MM: SSZ
--	--	--	--	--

- **Action Output:**

The screenshot shows a user interface for listing events. At the top, there's a header with a list icon, a success message ("Successfully retrieved 1 event(s) Showing up to 20 records in table... More results available. Next page Token: Y3Vyc29yOmliudDow View Less"), and a shared RubrikSecurityCloud\_IOC icon. Below the header is a section titled "Output message" which displays the same success message. Under "Scope", it says "All entities". The "Parameters" section lists NAME, Sort Order, Limit, Activity Type, Object Name, and Cluster ID. The "Return Values" section shows a "Script Result" with "ScriptResult" set to "true". The main area is a JSON tree viewer showing the structure of the returned data. The tree starts with "data [1]", which contains "activitySeriesConnection [2]". Each "activitySeriesConnection" node has an "edges [1]" child, which in turn has an "edge [1]" child, and finally a "node [15]" child. There is also a "pageInfo [3]" child under "activitySeriesConnection".

*Google SecOps Cases - List Events Output*

- **Output JSON:**

```
{
  "data": {
    "activitySeriesConnection": [
      {
        "edges": [
          {
            "node": {
              "id": 23229375,
              "fid": "7c9ba229-2caa-5746-a9ac-3cc61fe4d900",
              "activitySeriesId": "46448d2c-b100-5587-8f27-735354667e56",
              "startTime": "2025-10-17T17:01:25.589Z",
              "lastUpdated": "2025-10-17T17:11:00.637Z",
              "lastActivityType": "Anomaly",
              "lastActivityStatus": "Success",
              "location": "vcsa.rubrik.us",
              "objectName": "DEMO-RADAR",
              "objectId": "VirtualMachine:::2b260d66-29f9-4a57-bdbf-326cd3e6e162-vm-206",
              "objectType": "VmwareVm",
              "severity": "Critical",
              "progress": "100%",
              "cluster": {
                "id": "8b4fe6f6-cc87-4354-a125-b65e23cf8c90",
                "name": "Cluster_B"
              }
            },
            "activityConnection": {
              "nodes": [
                {
                  "id": "8b4fe6f6-cc87-4354-a125-b65e23cf8c90"
                }
              ]
            }
          }
        ]
      }
    ]
  }
}
```

```
        "id": "85d83e08-c44f-47f5-aedc-786f1af1ea5b",
        "message": "Detected anomalous filesystem activity with high confidence
and high levels of encryption (File Change: 4474 Added, 244 Modified, 4475
Removed)",
        "severity": "Critical",
        "time": "2025-10-17T17:11:00.637Z"
    }
]
}
}
}
],
"pageInfo": {
    "endCursor": "Y3Vyc29yOmludDow",
    "hasNextPage": true,
    "hasPreviousPage": false
}
}
}
}
```

## Action 3: Get Sonar Sensitive Hits

- Find data classification hits on an object.
- Parameters:**

Argument Name	Type	Required (Yes / No)	Default Value	Description
Object Name	String	Yes	N/A	The name of the Rubrik object to check for sensitive hits.
Lookback Days	Integer	No	7	Number of days in the past to retrieve scan results from. For example, a value of 7 will return results as of 7 days ago.

- Action Output:**

2026-01-27 00:18:28  
 RubrikSecurityCloud\_Get Sonar Sensitive Hits | Successfully retrieved Sonar Sensitive Hits for Object: DEMO-RADARShowing up to 20 records in table. View Less  
 Shared\_RubrikSecurityCloud\_1  
 Output message  
 Successfully retrieved Sonar Sensitive Hits for Object: DEMO-RADARShowing up to 20 records in table.  
 Scope  
 All entities  
 Parameters  
 NAME VALUE  
 Object Name DEMO-RADAR  
 Lookback Days 45  
 Return Values  
 Script Result  
 ScriptResult true  
 JSON Result  
 data [1]  
 policyObj [4]  
 id f29abec6-312e-597f-a877-b45f94da2aba  
 > rootFileResult [9]  
 > snappable [2]  
 snapshotId 928cd4c4-2cde-5360-bb11-452d46bcabbb

Google SecOps Cases - Get Sonar Sensitive Hits Output

- Output JSON:**

```
{
  "data": {
    "policyObj": {
      "id": "f29abec6-312e-597f-a877-b45f94da2aba",
      "snapshotId": "f37844d1-a440-56fa-91dd-4d8d707c1c54",
      "snappable": {
        "id": "f29abec6-312e-597f-a877-b45f94da2aba",
        "name": "DEMO-RADAR"
      },
      "rootFileResult": {
        "hits": { "totalHits": 178698 },
        "analyzerGroupResults": [
          {
            "analyzerGroup": { "name": "GLBA" },
            "analyzerResults": [
              {
                "analyzerResult": { "name": "GLBA" }
              }
            ]
          }
        ]
      }
    }
  }
}
```

```

    "hits": { "totalHits": 1130 },
    "analyzer": { "name": "Credit Card" }
},
{
    "hits": { "totalHits": 5 },
    "analyzer": { "name": "Bank Account Number" }
},
{
    "hits": { "totalHits": 11868 },
    "analyzer": { "name": "Social Security Number (SSN)" }
}
],
"hits": { "totalHits": 13003 }
},
{
    "analyzerGroup": { "name": "Financial" },
    "analyzerResults": [
        {
            "hits": { "totalHits": 10462 },
            "analyzer": { "name": "Synthetic Credit Card" }
        },
        {
            "hits": { "totalHits": 33 },
            "analyzer": { "name": "Salary Details" }
        },
        {
            "hits": { "totalHits": 1130 },
            "analyzer": { "name": "Credit Card" }
        },
        {
            "hits": { "totalHits": 5 },
            "analyzer": { "name": "Bank Account Number" }
        }
],
"hits": { "totalHits": 11630 }
},
{
    "analyzerGroup": { "name": "Business" },
    "analyzerResults": [
        {
            "hits": { "totalHits": 39441 },
            "analyzer": { "name": "test data type" }
        }
],
"hits": { "totalHits": 39441 }
},
{
    "analyzerGroup": { "name": "CCPA" },

```

```

"analyzerResults": [
  {
    "hits": { "totalHits": 19 },
    "analyzer": { "name": "Passport Number" }
  },
  {
    "hits": { "totalHits": 5 },
    "analyzer": { "name": "Bank Account Number" }
  },
  {
    "hits": { "totalHits": 11868 },
    "analyzer": { "name": "Social Security Number (SSN)" }
  }
],
"hits": { "totalHits": 11892 }
},
{
  "analyzerGroup": { "name": "Geographical" },
  "analyzerResults": [
    {
      "hits": { "totalHits": 9394 },
      "analyzer": { "name": "Country" }
    },
    {
      "hits": { "totalHits": 3416 },
      "analyzer": { "name": "County" }
    },
    {
      "hits": { "totalHits": 2 },
      "analyzer": { "name": "Street" }
    },
    {
      "hits": { "totalHits": 62 },
      "analyzer": { "name": "Country Code" }
    },
    {
      "hits": { "totalHits": 337 },
      "analyzer": { "name": "EU Country" }
    },
    {
      "hits": { "totalHits": 16379 },
      "analyzer": { "name": "City" }
    },
    {
      "hits": { "totalHits": 14900 },
      "analyzer": { "name": "US State" }
    },
    {
      "hits": { "totalHits": 548 },
      "analyzer": { "name": "ZIP Code" }
    }
  ]
}

```

```
{  
    "hits": { "totalHits": 12 },  
    "analyzer": { "name": "California ZIP Code" }  
},  
],  
    "hits": { "totalHits": 45050 }  
},  
{  
    "analyzerGroup": { "name": "Personal" },  
    "analyzerResults": [  
        {  
            "hits": { "totalHits": 37 },  
            "analyzer": { "name": "Driver's License" }  
        },  
        {  
            "hits": { "totalHits": 60 },  
            "analyzer": { "name": "Birth Date" }  
        },  
        {  
            "hits": { "totalHits": 120 },  
            "analyzer": { "name": "Synthetic SSN" }  
        },  
        {  
            "hits": { "totalHits": 13108 },  
            "analyzer": { "name": "Gender" }  
        },  
        {  
            "hits": { "totalHits": 4 },  
            "analyzer": { "name": "EU Phone Number" }  
        },  
        {  
            "hits": { "totalHits": 7 },  
            "analyzer": { "name": "Relationship info" }  
        },  
        {  
            "hits": { "totalHits": 28742 },  
            "analyzer": { "name": "Last Name" }  
        },  
        {  
            "hits": { "totalHits": 608 },  
            "analyzer": { "name": "Phone Number" }  
        },  
        {  
            "hits": { "totalHits": 16625 },  
            "analyzer": { "name": "First Name" }  
        },  
        {  
            "hits": { "totalHits": 3 },  
        }  
    ]  
}
```

```

    "analyzer": { "name": "EU Email Address" }
},
{
  "hits": { "totalHits": 6418 },
  "analyzer": { "name": "Full Name" }
},
{
  "hits": { "totalHits": 19 },
  "analyzer": { "name": "Passport Number" }
},
{
  "hits": { "totalHits": 14 },
  "analyzer": { "name": "US Phone Number" }
},
{
  "hits": { "totalHits": 11868 },
  "analyzer": { "name": "Social Security Number (SSN)" }
},
{
  "hits": { "totalHits": 4533 },
  "analyzer": { "name": "Email Address" }
}
],
"hits": { "totalHits": 82166 }
},
{
  "analyzerGroup": { "name": "PCI Scanner" },
  "analyzerResults": [
    {
      "hits": { "totalHits": 1130 },
      "analyzer": { "name": "Credit Card" }
    }
  ],
  "hits": { "totalHits": 1130 }
},
{
  "analyzerGroup": { "name": "United Kingdom PII" },
  "analyzerResults": [
    {
      "hits": { "totalHits": 19 },
      "analyzer": { "name": "Passport Number" }
    }
  ],
  "hits": { "totalHits": 19 }
},
{
  "analyzerGroup": { "name": "U.S. PII" },
  "analyzerResults": [

```

```
{
  "hits": { "totalHits": 19 },
  "analyzer": { "name": "Passport Number" }
},
{
  "hits": { "totalHits": 11868 },
  "analyzer": { "name": "Social Security Number (SSN)" }
}
],
"hits": { "totalHits": 11887 }
},
{
  "analyzerGroup": { "name": "HIPAA" },
  "analyzerResults": [
    {
      "hits": { "totalHits": 19 },
      "analyzer": { "name": "Passport Number" }
    },
    {
      "hits": { "totalHits": 11868 },
      "analyzer": { "name": "Social Security Number (SSN)" }
    }
],
"hits": { "totalHits": 11887 }
},
{
  "analyzerGroup": { "name": "Digital" },
  "analyzerResults": [
    {
      "hits": { "totalHits": 1 },
      "analyzer": { "name": "AWS Access Key ID" }
    },
    {
      "hits": { "totalHits": 7 },
      "analyzer": { "name": "Device ID" }
    },
    {
      "hits": { "totalHits": 125 },
      "analyzer": { "name": "Username" }
    },
    {
      "hits": { "totalHits": 261 },
      "analyzer": { "name": "Password" }
    },
    {
      "hits": { "totalHits": 1 },
      "analyzer": { "name": "AWS Connection String" }
    }
],
"hits": { "totalHits": 11887 }
}
]
```

```
{
  "hits": { "totalHits": 2 },
  "analyzer": { "name": "Azure Connection String" }
},
{
  "hits": { "totalHits": 8 },
  "analyzer": { "name": "Digital Certificate" }
}
],
"hits": { "totalHits": 405 }
},
{
  "analyzerGroup": { "name": "Medical" },
  "analyzerResults": [
    {
      "hits": { "totalHits": 6 },
      "analyzer": { "name": "Patient Number" }
    },
    "hits": { "totalHits": 6 }
  ],
  "analyzerGroup": { "name": "UK PII" },
  "analyzerResults": [
    {
      "hits": { "totalHits": 19 },
      "analyzer": { "name": "Passport Number" }
    },
    "hits": { "totalHits": 19 }
  ],
  "analyzerGroup": { "name": "PCI DSS" },
  "analyzerResults": [
    {
      "hits": { "totalHits": 1130 },
      "analyzer": { "name": "Credit Card" }
    },
    "hits": { "totalHits": 1130 }
  ],
  "analyzerGroup": { "name": "U.S. Financials" },
  "analyzerResults": [
    {
      "hits": { "totalHits": 1130 },
      "analyzer": { "name": "Credit Card" }
    },
  ]
}
```

```
{  
    "hits": { "totalHits": 5 },  
    "analyzer": { "name": "Bank Account Number" }  
}  
,  
    "hits": { "totalHits": 1135 }  
}  
],  
"filesWithHits": { "totalHits": 4708 },  
"openAccessFiles": { "totalHits": 0 },  
"openAccessFolders": { "totalHits": 0 },  
"openAccessFilesWithHits": { "totalHits": 1 },  
"staleFiles": { "totalHits": 0 },  
"staleFilesWithHits": { "totalHits": 4691 },  
"openAccessStaleFiles": { "totalHits": 0 }  
}  
}  
}  
}
```

## Action 4: Get CDM Cluster Connection State

- The goal of this action is to find the CDM Connection State of a CDM Cluster.
- Parameters:**

Argument Name	Type	Required (Yes / No)	Default Value	Description
Cluster ID	String	Yes	N/A	The ID of the CDM cluster.

- Action Output:**

Get CDM Cluster Connection State Successfully retrieved CDM Cluster Connection State for Cluster ID: 997d1797-2cc4-49b7-aad8-c97f8138c061 View Less

Shared\_RubrikSecurityCloud\_IOC

**Output message**

Successfully retrieved CDM Cluster Connection State for Cluster ID: 997d1797-2cc4-49b7-aad8-c97f8138c061

**Scope**

All entities

**Parameters**

NAME	VALUE
Cluster ID	997d1797-2cc4-49b7-aad8-c97f8138c061

**Return Values**

**Script Result**

ScriptResult true

**JSON Result**

```
[{"data": [{"clusterConnection": [{"nodes": [{"state": [{"connectedState": "Connected"}]}]}]}]}
```

Google SecOps Cases - Get CDM Cluster Connection State Output

- Output JSON:**

```
{  
  "data": {  
    "clusterConnection": {  
      "nodes": [  
        {  
          "state": {  
            "connectedState": "Connected"  
          }  
        }  
      ]  
    }  
  }  
}
```

## Action 5: Get CDM Cluster Location

- The goal of this action is to find the CDM GeoLocation of a CDM Cluster.
- Parameters:**

Argument Name	Type	Required (Yes / No)	Default Value	Description
Cluster ID	String	Yes	N/A	The ID of the CDM cluster.

- Action Output:**

Get CDM Cluster Location | Successfully retrieved CDM Cluster Location for Cluster ID: 997d1797-2cc4-49b7-aad8-c97f8138c061. [View Less](#)

Shared\_RubrikSecurityCloud\_IOC

**Output message**  
Successfully retrieved CDM Cluster Location for Cluster ID: 997d1797-2cc4-49b7-aad8-c97f8138c061

**Scope**  
All entities

**Parameters**

NAME	VALUE
Cluster ID	997d1797-2cc4-49b7-aad8-c97f8138c061

**Return Values**

**Script Result**  
ScriptResult: true

**JSON Result**

```
data [1]
  clusterConnection [1]
    nodes [1]
      0 [1]
        geoLocation [1]
          address: Palo Alto, CA, USA
```

Google SecOps Cases - Get CDM Cluster Location Output

- Output JSON:**

```
{
  "data": {
    "clusterConnection": {
      "nodes": [
        {
          "geoLocation": {
            "address": "Santa Clara, CA, USA"
          }
        }
      ]
    }
  }
}
```

## Action 6: List Object-Snapshots

- Retrieve Rubrik snapshot(s) of an object, based on the provided object ID.

- **Parameters:**

Argument Name	Type	Required (Yes / No)	Default Value	Description
Object ID	String	Yes	N/A	The object ID for which the snapshots are to be searched.
Start Date	String	No	N/A	The start date to get snapshots from. Format supported: yyyy-mm-dd, yyyy-mm-ddTHH:MM:SSZ
End Date	String	No	N/A	The end date to get snapshots until. Format supported: yyyy-mm-dd, yyyy-mm-ddTHH:MM:SSZ
Snapshot Type	String	No	N/A	List of snapshot types to filter snapshots. Supports comma separated values.
Limit	Integer	No	50	Number of results to retrieve in the response. Maximum size allowed is 1000.
Next Page Token	String	No	N/A	The next page cursor to retrieve the next set of results.
Sort Order	Dropdown	No	Asc	Specify the order to sort the data in.  Possible values are: "Asc", "Desc".

- **Action Output:**

The screenshot shows a user interface for viewing the output of a 'List Object-Snapshots' action. At the top, there's a message indicating success: 'Successfully retrieved 1 snapshot(s) for Object ID: f29abec6-312e-597f-a877-b45f94da2aba Showing up to 20 records in table.. More results available. Next page token... View Less'. Below this, there are sections for 'Output message', 'Scope', 'All entities', 'Parameters', and 'Return Values'. The 'Return Values' section is expanded, showing a hierarchical tree structure under 'JSON Result': 'data [1] > snapshotsListConnection [2] > edges [1] > edges [1] > pageInfo [2]'. The 'edges [1]' node is highlighted.

*Google SecOps Cases - List Object-Snapshots Output*

- **Output JSON:**

```
{
  "data": {
    "snapshotsListConnection": {
      "edges": [
        {
          "node": {
            "id": "5cdad0bf-b8e6-5a63-aba4-d2049c4a34e0",
            "date": "2022-04-04T07:00:01.000Z",
            "expirationDate": null,
            "isOnDemandSnapshot": false,
            "cdmVersion": "",
            "isDownloadedSnapshot": false,
            "cluster": {
              "id": "40fdb2a5-3591-40ee-a37a-50bce5240d62",
              "name": "Cluster_A",
              "version": "9.1.3-p8-28434",
              "status": "Connected"
            },
            "pendingSnapshotDeletion": null,
            "slaDomain": {
              "name": "DO_NOT_PROTECT",
              "id": "DO_NOT_PROTECT"
            },
            "pendingSla": null,
            "snapshotRetentionInfo": {
              "archivalInfos": [],
              "localInfo": {
                "name": "Cluster_A",
                "isExpirationDateCalculated": true,
                "expirationTime": null
              },
              "replicationInfos": []
            }
          }
        }
      ]
    }
  }
}
```

```
        "sapHanaAppMetadata": null,  
        "legalHoldInfo": null  
    }  
}  
],  
"pageInfo": {  
    "endCursor": "Y3Vyc29yOmludDow",  
    "hasNextPage": true  
}  
}  
}  
}  
}
```

## Action 7: List Sonar File Contexts

- Retrieve the context of the file, folder, or file share for the provided object and the file details.
- **Parameters:**

Argument Name	Type	Required (Yes / No)	Default Value	Description
Object ID	String	Yes	N/A	The Object ID or the Snappable ID.
Snapshot ID	String	Yes	N/A	The Snapshot ID of the object.
File Name	String	No	N/A	Specify the name of the file, folder, or file share object.
File Path	String	No	N/A	Specify the standard file path to filter with.
User ID	String	No	N/A	Specify the user ID to filter with.
Include Whitelisted Results	Dropdown	No	N/A	The boolean indicates to include the whitelisted results. Possible values are: "True", "False".
Limit	Integer	No	50	Number of results to retrieve in the response.
Next Page Token	String	No	N/A	The next page cursor to retrieve the next set of results.
Sort By	Dropdown	No	N/A	Specify the field to use for sorting the response.  Supported values are: HITS, NAME, DAILY_CHANGE, LAST_ACCESS_TIME, OPEN_ACCESS_TYPE, FILES_WITH_HITS, FILES_WITH_OPEN_ACCES_S_HITS, STALE_FILES_WITH_HITS, CLUSTER, OBJECT_NAME, OBJECT_LOCATION, SNAPSHOT_TIME, NUM_ACTIVITIES, NUM_ACTIVITIES_DELTA, NATIVE_PATH, HITS_BY_SENSITIVITY, LAST_MODIFIED,

				CREATION_TIME, LAST_SCAN_TIME, DATA_CATEGORY, DATA_TYPE, TOTAL_SENSITIVE_HITS, EXPOSED_FILES, DOCUMENT_TYPE
Sort Order	Dropdown	No	DESC	Specify the order to sort the data. Possible values are: "ASC", "DESC".

- **Action Output:**

RubrikSecurityCloud\_List Sonar File Contexts | Successfully retrieved 1 file context(s) for Object ID: f29abec6-312e-597f-a877-b45f94da2abaShowing up to 20 records in table. [View Less](#)

**Output message**  
Successfully retrieved 1 file context(s) for Object ID: f29abec6-312e-597f-a877-b45f94da2abaShowing up to 20 records in table.

**Scope**  
All entities

**Parameters**

NAME	VALUE
Object ID	f29abec6-312e-597f-a877-b45f94da2aba
Snapshot ID	537dd02c-39f7-5168-b7c7-088176d6d420
File Name	DATA3.csv
File Path	/C:/restore/File Shares/Public Share/Dave
User ID	5-1-9-21-2904300122-994430833-3950688663-1439
Limit	1
Sort By	HITS
Sort Order	Desc

**Return Values**

Script Result	JSON Result
ScriptResult true	JSON Result

This field contains large amounts of data. [Download File](#) to see its content.

Google SecOps Cases - List Sonar File Contexts Output

- **Output JSON:**

```
{
  "data": {
    "policyObj": {
      "id": "39e378c2-fb50-40ac-af77-06ce08277caf",
      "fileResultConnection": {
        "edges": [
          {
            "cursor": "Y3Vyc29yOmlkOnsia2V5ljoiTDBZNkwxTm9ZWEpsY3k5TVpXZGhiQ0JFWlhCaGNuUnRaVzUwTDBKdmlydE5ZWfj5YVhndVQyWm1hV05sTURNdWVHeHoiLCjb3J0S2V5lpbljQ2II19",
            "node": {
              "nativePath": "/F:/Shares/Legal Department/BookMatrix.Office03.xls",
              "stdPath": "/F:/Shares/Legal Department/BookMatrix.Office03.xls",
              "filename": "BookMatrix.Office03.xls",
              "mode": "FILE",
              "size": 4097024,
              "lastAccessTime": 1761588027,
              "lastModifiedTime": 1686679305,
              "directory": "/F:/Shares/Legal Department",
              "numDescendantFiles": 0,
              "numDescendantErrorFiles": 0,
              "numDescendantSkippedExtFiles": 0,
              "numDescendantSkippedSizeFiles": 0,
            }
          }
        ]
      }
    }
  }
}
```

```

"errorCode": "NOERROR",
"hits": {
    "totalHits": 0,
    "violations": 46,
    "violationsDelta": 0,
    "totalHitsDelta": 0,
    "__typename": "Hits"
},
"filesWithHits": {
    "totalHits": 0,
    "violations": 1,
    "__typename": "Hits"
},
"openAccessFilesWithHits": {
    "totalHits": 0,
    "violations": 0,
    "__typename": "Hits"
},
"staleFilesWithHits": {
    "totalHits": 0,
    "violations": 0,
    "__typename": "Hits"
},
"analyzerGroupResults": [
{
    "analyzerGroup": {
        "groupType": "CUSTOM",
        "id": "4e4687b9-a8a1-4e5b-9fc0-0ad9999af3c1",
        "name": "U.S. PII",
        "__typename": "AnalyzerGroup"
    },
    "analyzerResults": [
{
        "hits": {
            "totalHits": 0,
            "violations": 0,
            "__typename": "Hits"
        },
        "analyzer": {
            "id": "03b3dc9e-81c1-561c-8235-17cf2fc1c729",
            "name": "ITIN",
            "analyzerType": "US_ITIN",
            "__typename": "Analyzer"
        },
        "__typename": "AnalyzerResult"
    }
],
"hits": {

```

```

        "totalHits": 0,
        "violations": 46,
        "violationsDelta": 0,
        "totalHitsDelta": 0,
        "__typename": "Hits"
    },
    "__typename": "AnalyzerGroupResult"
]
],
"sensitiveFiles": {
    "highRiskFileCount": {
        "totalCount": 0,
        "violatedCount": 0,
        "__typename": "SummaryCount"
    },
    "mediumRiskFileCount": {
        "totalCount": 0,
        "violatedCount": 1,
        "__typename": "SummaryCount"
    },
    "lowRiskFileCount": {
        "totalCount": 0,
        "violatedCount": 0,
        "__typename": "SummaryCount"
    },
    "__typename": "SensitiveFiles"
},
"openAccessType": "UNKNOWN_ACCESS",
"stalenessType": "NOT_STALE",
"numActivities": 0,
"numActivitiesDelta": 0,
 "__typename": "FileResult"
},
 "__typename": "FileResultEdge"
}
],
"pageInfo": {
    "endCursor": "Y3Vyc29yOmlkOnsia2V5IjoiTDBZNkwxTm9ZWEpsY3k5TVpXZGhiQ0JFWlhCaGNuUnRaVzUwTDBKdmlydE5ZWfj5YVhndVQyWm1hV05sTURNdWVHeHoiLCjb3J0S2V5IjpbljQ2II19",
    "hasNextPage": false,
    "__typename": "PageInfo"
},
 "__typename": "FileResultConnection"
},
 "__typename": "PolicyObj"
}
}

```

```
 }  
 }
```

## Action 8: Turbo IOC Scan

- Start a new turbo threat hunt.
- Parameters:**

Argument Name	Type	Required (Yes / No)	Default Value	Description
IOC	String	Yes	N/A	Indicator value to scan for (MD5, SHA1, or SHA256 hash). Supports comma-separated values
Scan Name	String	No	SecOps-{DATE}-{TIME}	Name for the threat hunt scan
Cluster ID	String	No	N/A	ID of cluster(s) to scan. Supports comma-separated values.
Start Time	String	No	N/A	Filter snapshots from this date. Format: yyyy-mm-dd or yyyy-mm-ddTHH:MM:SSZ
End Time	String	No	N/A	Filter snapshots until this date. Format: yyyy-mm-dd or yyyy-mm-ddTHH:MM:SSZ
Max Snapshots Per Object	Integer	No	N/A	Maximum number of snapshots to scan per object

- Action Output:**

The screenshot shows the "Turbo IOC Scan" action output. It includes a success message, parameters, and return values. The "Return Values" section displays a JSON object with a single entry: "startTurboThreatHunt [2]" containing the hunt ID "019b2be9-3cd2-7a6f-8e41-7a8b8e865b56".

```

{
  "startTurboThreatHunt": [
    {
      "huntId": "019b2be9-3cd2-7a6f-8e41-7a8b8e865b56"
    }
  ]
}

```

Google SecOps Cases - Turbo IOC Scan Output

- Output JSON:**

```
{  
  "data": {  
    "startTurboThreatHunt": {  
      "huntId": "019a2f27-ed1e-7ba5-950f-c1ba8dac3472",  
      "__typename": "StartTurboThreatHuntReply"  
    }  
  }  
}
```

## Action 9: Advanced IOC Scan

- Start a new advance threat hunt.
- Parameters:**

Argument Name	Type	Required (Yes / No)	Default Value	Description
Object ID	String	Yes	N/A	Object ID(s) to scan. Supports comma-separated values
IOC Type	Dropdown	No	N/A	<p>Type of indicator. Values: "INDICATOR_OF_COMPROMISE_TYPE_PATH_OR_FILENAME", "INDICATOR_OF_COMPROMISE_TYPE_HASH", "INDICATOR_OF_COMPROMISE_TYPE_YARA_RULE"</p> <p>Example:</p> <ul style="list-style-type: none"> <li>File Path: "C:\Users\"</li> <li>IOC Hash: "44d886111ea111f36de82e1118abb02f"</li> <li>Yara L Rule: "rule match_everything {condition:true}"</li> </ul>
IOC Value	String	No	N/A	Value of the indicator to scan for
Scan Name	String	No	SecOps-{DATE}-{TIME}	Name for the advanced threat hunt scan
Advanced IOC	String	No	N/A	JSON-encoded IOCs. Json keys signify the type of IOC and the corresponding list of

				<p>values are the values of the IOC's.</p> <p>If provided, IOC Type and IOC Value are ignored.</p> <p>Format:</p> <pre>{"&lt;ioc_type1&gt;": "&lt;ioc_value1&gt;", "&lt;ioc_type2&gt;": "&lt;ioc_value2&gt;"}</pre> <p>Example:</p> <pre>{"IOC_HASH": ["1116bceb c0191110f9111b1111354 27e", "11191262b3111c88 41b54169511197f7"], "IOC_YARA": ["rule Generic_Hello_World { strings: \$test_string = \\"Hello World YARA Test\\" ascii wide condition: \$test_string }"], "IOC_FILE_PATTERN": ["C:\\ Users\\Test"] }</pre>
Max Matches Per Snapshot	Integer	No	N/A	Scan terminates after this many matches are found
Start Date	String	No	N/A	Filter snapshots from this date. Format: yyyy-mm-dd or yyyy-mm-ddTHH:MM:SSZ
End Date	String	No	N/A	Filter snapshots until this date. Format: yyyy-mm-dd or yyyy-mm-ddTHH:MM:SSZ
Max Snapshots Per Object	Integer	No	N/A	Maximum number of snapshots to scan per object

Min File Size	Integer	No	N/A	Minimum file size in bytes to include in scan
Max File Size	Integer	No	N/A	Maximum file size in bytes to include in scan
Paths To Include	String	No	N/A	Paths to include in scan. Supports comma-separated values
Paths To Exclude	String	No	N/A	Paths to exclude from scan. Supports comma-separated values
Paths To Exempt	String	No	N/A	Paths to exempt from exclusion. Supports comma-separated values

- **Action Output:**

2026-01-27 00:15:20

RubrikSecurityCloud\_Advanced IOC Scan | Successfully started Advance IOC Scan with 1 hunt(s)Showing up to 20 records in table. [View Less](#)

Shared\_RubrikSecurityCloud\_1

Output message

Successfully started Advance IOC Scan with 1 hunt(s)Showing up to 20 records in table.

Scope

All entities

Parameters

NAME	VALUE
Object ID	f29abec5-313e-597f-a877-b45f94d2aba
Scan Name	Advanced IOC
Advanced IOC	{"IOC_PATH_OR_FILENAME":"C:\Shares\eiarc.com","IOC_HASH":"44d88612fa8a8f36de82e1278abb02f"}

Return Values

Script Result

JSON Result

```

data [1]
  startBulkThreatHunt [2]
    _typename StartBulkThreatHuntReply
      hunts [1]
        0 [9]
  
```

Google SecOps Cases - Advanced IOC Scan Output

- **Output JSON**

```
{
  "data": {
    "startBulkThreatHunt": {
      "hunts": [
        {
          "huntId": "019a2f30-66d8-7559-b1dc-b4508ae34afd",
          "huntName": "testadvance",
          "config": {
            "huntType": "THREAT_HUNT_V2",
            "clusterUuids": [
              "997d1797-2cc4-49b7-aad8-c97f8138c061"
            ],
            "objectFids": [
  
```

```
"78a36a80-0a2e-5ebf-af92-2962ddc3e7e7"
],
  "__typename": "HuntConfig"
},
"status": "HUNT_TRIGGER_SUCCEEDED",
  "__typename": "HuntResponse"
}
],
  "__typename": "StartBulkThreatHuntReply"
}
}
}
```

## Action 10: IOC Scan Results

- Retrieve details of the Turbo and Advance Threat Hunt.
- **Parameters:**

Argument Name	Type	Required (Yes / No)	Default Value	Description
Hunt ID	String	Yes	N/A	The ID of the threat hunt.

- **Action Output:**

The screenshot shows the 'IOC Scan Results' output page. It includes sections for 'Output message', 'Scope', 'Parameters' (with Hunt ID set to 019b2b8c-c349-7dd0-b2ad-2dc02766cf8), 'Return Values' (Script Result: true), and a 'JSON Result' pane. The JSON Result pane displays a hierarchical tree view of the scan results, with the 'data [2]' node expanded to show 'threatHuntDetailV2 [10]' and 'threatHuntObjectMetrics [7]'.

*Google SecOps Cases - IOC Scan Results Output*

- **Output JSON:**

```
{  
  "data": {  
    "threatHuntObjectMetrics": {  
      "totalObjectsScanned": 87,  
      "totalAffectedObjects": 0,  
      "totalUnaffectedObjects": 87,  
      "totalObjectsUnscannable": 0,  
      "unaffectedObjectsFromDb": 87,  
      "cleanRecoverableObjectLimit": 500,  
      "__typename": "ThreatHuntObjectMetricsReply"  
    },  
    "threatHuntDetailV2": {  
      "totalObjectFids": 87,  
      "startTime": "2025-10-29T08:48:57.000Z",  
      "endTime": "2025-10-29T08:48:58.000Z",  
      "status": "SUCCEEDED",  
      "totalMatchedSnapshots": 0,  
      "totalScannedSnapshots": 816,  
      "totalUniqueFileMatches": 0,  
      "clusters": [  
        {  
          "id": "997d1797-2cc4-49b7-aad8-c97f8138c061",  
          "name": "Cluster_C",  
          "type": "OnPrem",  
        }  
      ]  
    }  
  }  
}
```

```
        "__typename": "Cluster"
    }
],
"baseConfig": {
    "name": "iocturboscan",
    "notes": "",
    "maxMatchesPerSnapshot": 0,
    "threatHuntType": "TURBO_THREAT_HUNT",
    "ioc": {
        "iocList": {
            "indicatorsOfCompromise": [
                {
                    "iocKind": "IOC_HASH",
                    "iocValue": "5156becbc019e3f0f9520b143435427e",
                    "__typename": "IndicatorOfCompromise"
                }
            ],
            "__typename": "IndicatorOfCompromiseInputOutputListType"
        },
        "__typename": "Loc"
    },
    "snapshotScanLimit": {
        "scanLimit": {
            "scanConfig": {
                "maxSnapshotsPerObject": 10,
                "startTime": "2024-11-03T06:30:00.000Z",
                "endTime": "2025-10-12T06:30:00.000Z",
                "__typename": "SnapshotScanConfig"
            },
            "objectSnapshotConfig": null,
            "__typename": "ScanLimit"
        },
        "__typename": "HuntScanSnapshotLimit"
    },
    "fileScanCriteria": null,
    "__typename": "ThreatHuntBaseConfig"
},
 "__typename": "ThreatHuntDetailsV2"
}
}
```

# Playbooks

---

Playbooks are a powerful feature in Google Security Operations (SecOps) used to automate responses to alerts or cases. When certain conditions are met or triggers occur, playbooks can automatically execute predefined actions. They help streamline incident response, reduce manual effort, and ensure consistent handling of security events.

As part of the Rubrik Security Cloud Integration, we created **four** playbooks to help you get started. Users can use and refer to the sample playbook provided in this [GitHub repository](#).

# Uninstalling the Integration

---

To uninstall the integration, the user must perform the following steps:

1. From the SecOps SOAR platform, navigate to the **Marketplace** section.
2. Search for the **Rubrik Security Cloud** Integration.
3. In the bottom left of the Rubrik Security Cloud Integration, click on the **Bin** icon to uninstall the integration.
4. Confirmation will be requested from the user to uninstall the integration.

## Known Issues

---

- The script timeout might not work as expected. It has been observed that when specifying the timeout to 10 seconds, the action script would timeout after around 39 seconds. The platform adds ~29 seconds of operation. This behavior differs for every SecOps SOAR instance.

**Reference:** [Solved: Facing inconsistencies in Script Timeout for Action... - Google Cloud Community](#)

# Troubleshooting

---

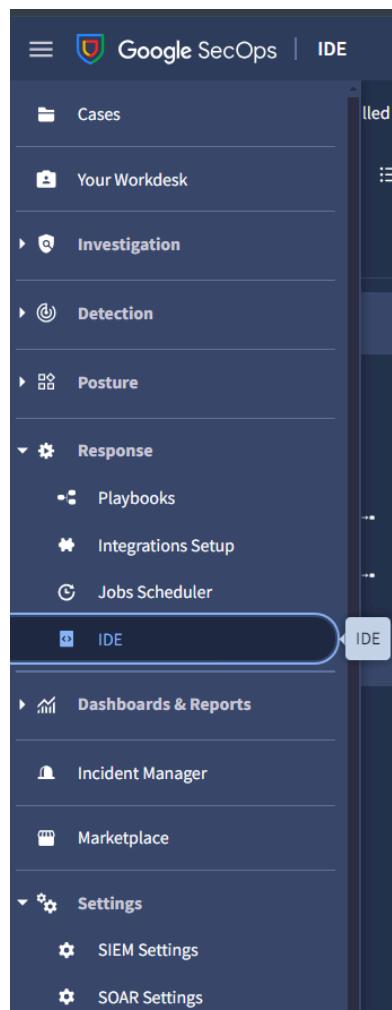
## 1. PythonProcess Has timed out.

The screenshot shows a search result for 'PythonProcess Has timed out. (Max 39 seconds)'. It includes a 'Default Environment' section, an 'Output message' section with the error message, a 'Scope' section set to 'All entities', and a note stating 'The step did not return any results.'

*Google SecOps Cases - Action Timeout error on the case wall*

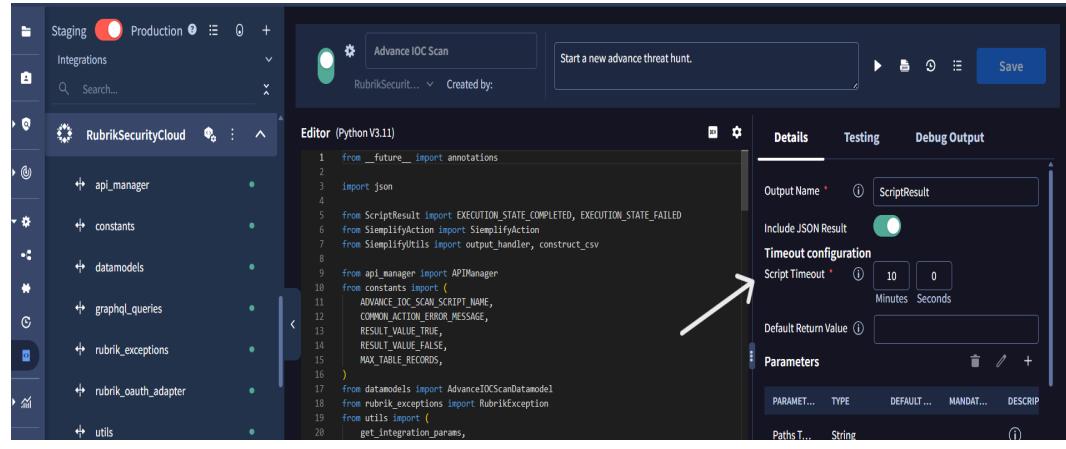
### Solution:

1. Increase the script timeout from the Timeout Configuration of an action
  - a. From the Sidebar, navigate to **Response > IDE**



*Google SecOps Sidebar - From the Response dropdown, click on IDE.*

- b. Search for the action script and select it. You will be able to see the codebase of the action, and on the right side, there should be an input field named **Timeout Configuration** under the details tab. Update the value of **Script Timeout** based on your requirement, and **Save** the action.



The screenshot shows the Google SecOps IDE - Action Editor interface. On the left, there's a sidebar with 'Staging' and 'Production' status, and a search bar. The main area has a tree view of 'RubrikSecurityCloud' with several sub-folders like 'api\_manager', 'constants', etc. A central window titled 'Advance IOC Scan' shows a button to 'Start a new advance threat hunt.' Below it is the 'Editor (Python V3.11)' pane containing Python code. To the right is the 'Details' tab of the configuration pane, which includes fields for 'Output Name' (set to 'ScriptResult'), 'Include JSON Result' (checked), 'Timeout configuration' (with 'Script Timeout' set to 10 Minutes and 0 Seconds), and 'Default Return Value'. A white arrow points from the text above to the 'Script Timeout' field.

```

from __future__ import annotations
import json
from ScriptResult import EXECUTION_STATE_COMPLETED, EXECUTION_STATE_FAILED
from SiemplyAction import SiemplyAction
from SiemplyUtils import output_handler, construct_csv
from api_manager import APIManager
from constants import (
    ADVANCE_IOC_SCAN_SCRIPT_NAME,
    COMMON_ACTION_ERROR_MESSAGE,
    RESULT_VALUE_TRUE,
    RESULT_VALUE_FALSE,
    MAX_TABLE_RECORDS,
)
from datamodels import AdvanceIOCScanDataModel
from rubrik_exceptions import RubrikException
from utils import get_integration_params,

```

*Google SecOps IDE - Action Editor*

2. Another way to increase the execution speed of the action is to tweak the query parameters of the GraphQL call by reducing the time frame to search and retrieve only filtered subsets instead of all results.

## 2. Unknown error running Action.

```
Script Result
is_success

Output message
Unknown error running ActiveDirectory_Ping. Details:
Status(StatusCode="Unavailable", Detail="no healthy
upstream")
```

*Google SecOps IDE - Running Action*

### Solution:

- The "**no healthy upstream**" error indicates an internal system issue. The most common cause is that all backend servers are currently unavailable or unresponsive. To resolve this problem, you should contact your system administrator for assistance. [OBJ]

# References

---

- Documentation for Google SecOps SOAR - [Documentation](#)