Overview

Recorded Future has developed a new integration into Google SecOps SOAR to enhance the automation of threat intelligence in client's incident response workflows. This new integration contains several breaking changes from the previous, Google built version.

A note on Playbook alerts

Playbook alerts in Recorded Future are frequently updated with new information like updated DNS records, changing vulnerability lifecycles, and new infrastructure exposures. Unfortunately, Google SOAR case events cannot be updated after creation, making it difficult to synchronize these changes. The app has two different workarounds that you can implement to pull updated playbook alert data into Google SecOps SOAR

1. A "tracking" connector that will generate new alerts/cases in Google SecOps from **updates** in existing playbook alerts. The Connector would be enabled in addition to the Connector that imports newly created playbook alerts
2. A series of playbooks that will refresh the HTML views on the imported playbook alert "alert view" in a Google SecOps case. These playbooks would not change the raw events of a case, but would update the view so the analyst has the most up to date information. Note that a playbook can only be run on a case up to 10 times, so you can only refresh that case 10 times

It's recommended to use at least one of these workarounds

Installation

Install package from store

Install the package "RecordedFutureIntelligence" from the Google SecOps store. It will be listed as a community edition integration. Do **not** install the certified "Recorded Future" integration

Add the alert view widget

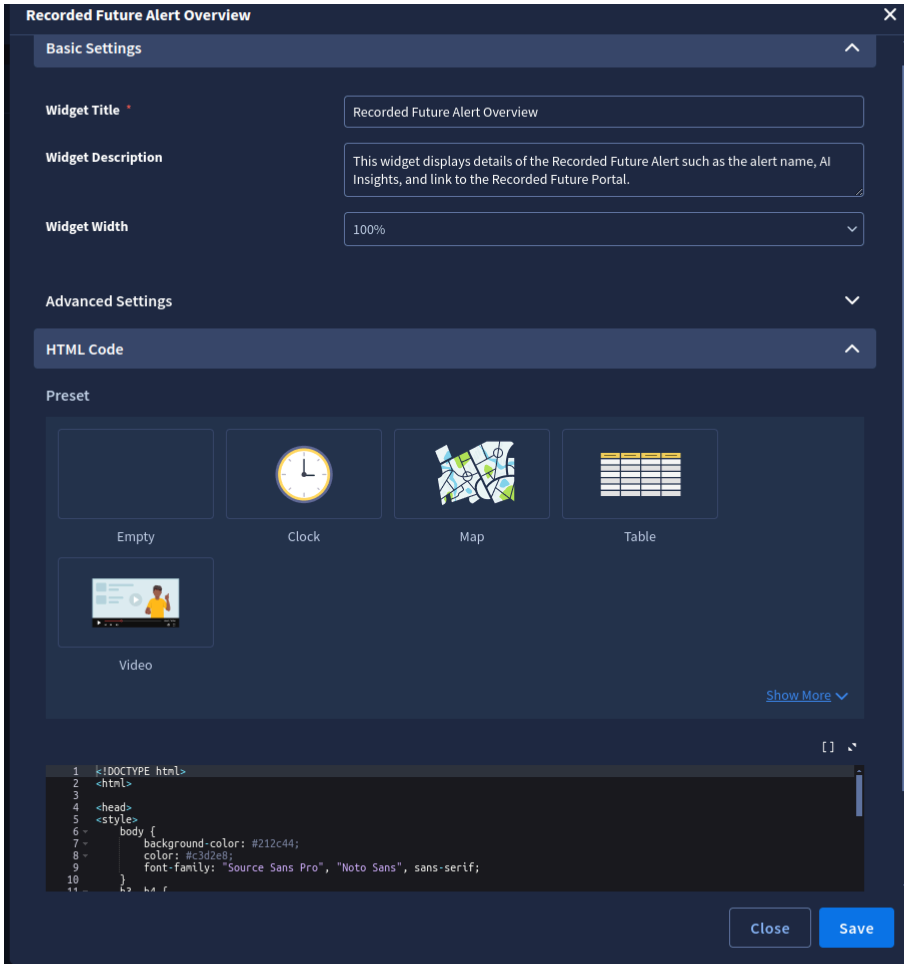
We highly recommend you add a classic alert widget to the default alert view. This will enable analysts triaging Recorded Future alerts to get a quick overview, as well as leverage AI insights.

Navigate to Settings->SOAR Settings->Case Data->Views->Default Alert View. In the "General" tab, drag an HTML widget into the Default Alert View. We recommend you put this widget at the top of the view

Unfortunately, widget settings cannot be automatically imported, so you will have to manually copy and paste the following fields

- **Widget Title**: Recorded Future Alert Overview
- **Widget Description:** This widget displays details of the Recorded Future Alert such as the alert name, AI Insights, and link to the Recorded Future Portal.
- **Widget Width**: 100%
- **Widget Height:**325 px

Paste the HTML from `recorded_future_classic_alert.html` into the box under "HTML Code". You can find the HTML in the appendix of this document



Widget Title * Recorded Future Alert Overview

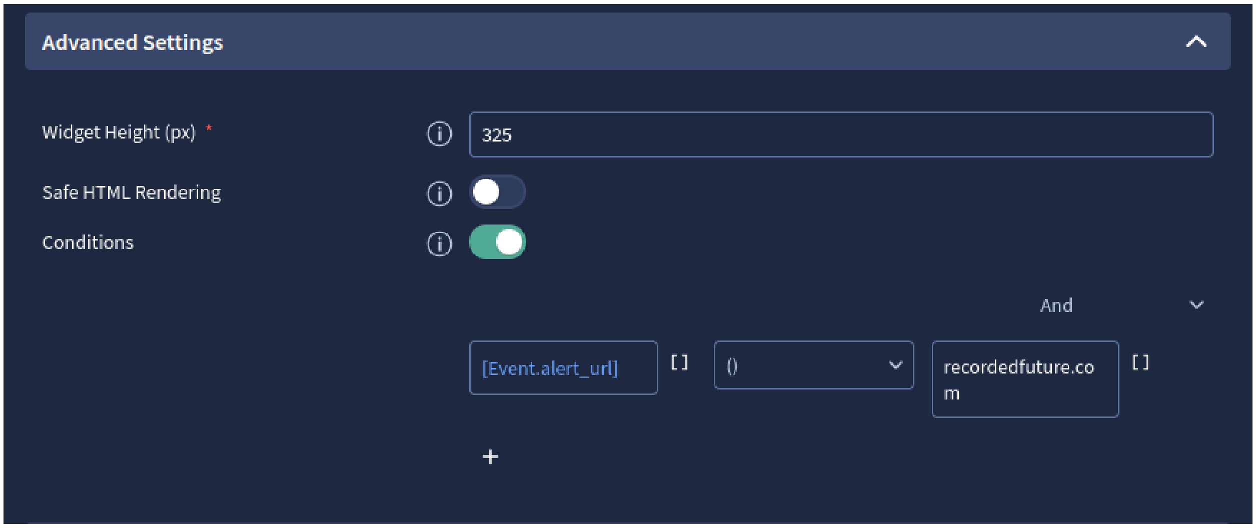
Widget Description This widget displays details of the Recorded Future Alert such as the alert name, AI Insights, and link to the Recorded Future Portal.

Widget Width 100%

```
<!DOCTYPE html>
<html>

<head>
<style>
    body {
        background-color: #212c44;
        color: #c3d2e8;
        font-family: "Source Sans Pro", "Noto Sans", sans-serif;
    }
    h3, h4 {
```

Next, add a condition to make this widget visible **only** for Recorded Future alerts, and not clutter the view for other Google SOAR alerts. Under Advanced settings, check “Conditions.” Set a condition of `[Event.alert_url] contains recordedfuture.com`.



Advanced Settings

Widget Height (px) * 325

Safe HTML Rendering ○

Conditions ●

And

[Event.alert_url] [ ] () recordedfuture.com [ ]

+

Install Use Case

This is currently not available until Google certifies the use case. Contact your Recorded Future account team if you want advanced access to these playbooks

Install the Use Case “Recorded Future Playbook Alerts” from the Google SecOps marketplace. Enable all 5 playbooks that accompany that make up the use case

Configuration

Configure the integration

Add an instance of the integration under Response->Integrations Setup. Click the plus sign and add the integration in your chosen environment

Parameters

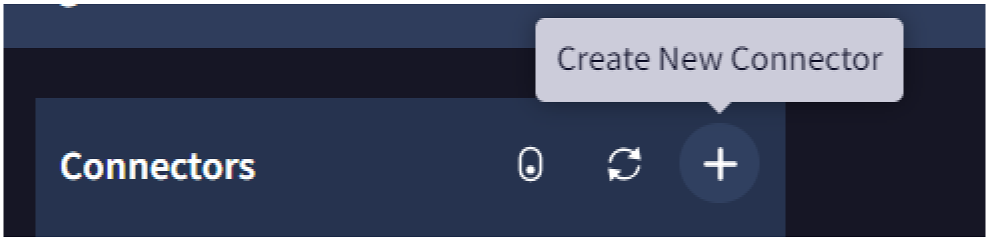
Name	Default Value	Description	Type
API URL	https://api.recordedfuture.com	URL of Recorded Future API. Do not change unless instructed to do so	string
API Key		Recorded Future API Key	string
Verify SSL	True	Verify SSL connection to the Recorded Future API	bool
Collective Insights	True	Enroll this integration in the Collective Insights program	bool

Please contact support@recordedfuture.com to get access to an API token. for accessing We recommend that **Collective Insights** is checked to true.

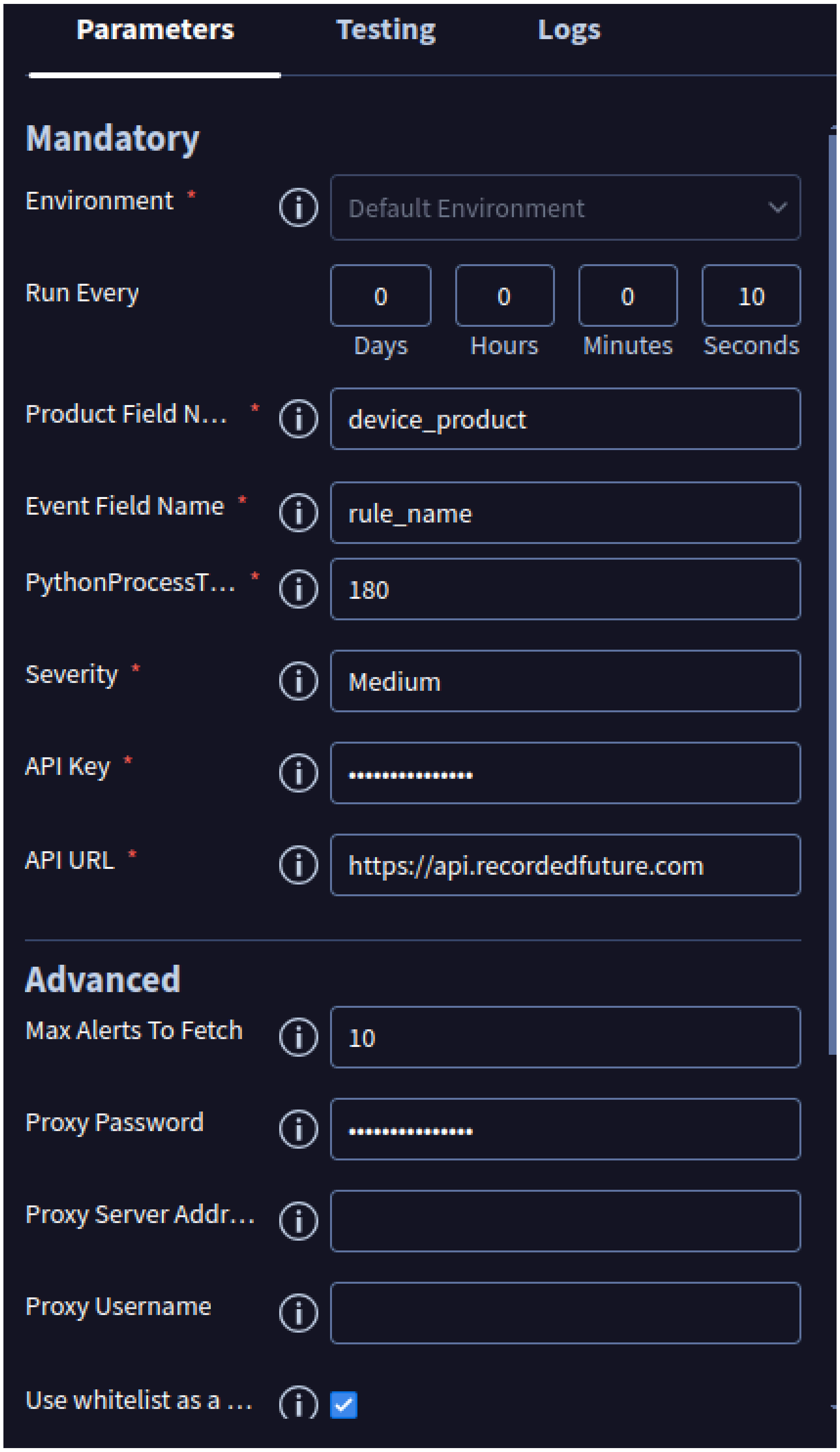
Connectors

Our integration comes with a trio of connectors that automatically imports Recorded Future classic alerts and playbooks alerts as alerts/cases in Google SecOps SOAR. You can add connectors by navigating to Settings->SOAR

Settings->Ingestion->Connectors. Click the plus sign, Create New Connector, and add one of the connectors that begins with “Recorded Future.”



Classic Alerts Connector



Mandatory

Environment *	Default Environment
Run Every	0 Days, 0 Hours, 0 Minutes, 10 Seconds
Product Field N... *	device_product
Event Field Name *	rule_name
PythonProcessT... *	180
Severity *	Medium
API Key *	•••••••••••••••
API URL *	https://api.recordedfuture.com

Advanced

Max Alerts To Fetch	10
Proxy Password	•••••••••••••••
Proxy Server Addr...	
Proxy Username	
Use whitelist as a ...	☑

This connector imports classic alerts Google SecOps cases. You can specify what alert rules you want to import by adding a dynamic list, one for each alert rule (as the name appears in the Recorded Future platform). Checking the option “Use whitelist as a blacklist” will pull all alerts except the ones specified in the dynamic list. If you want to pull all alerts, check that option and leave the dynamic list empty.

Parameters

Name	Default Value	Description	Type
Run Every	10 seconds	How frequently the Recorded Future API is polled for new alerts	timestamp
API Key		Recorded Future API Key. Contact Recorded Future support if you need access	string
Product Field Name	device_product	Which field in the alert structure populates the Product of the GSOAR alert	string
Event Field Name	rule_name	Which field in the alert structure populates the Event of the GSOAR alert	string

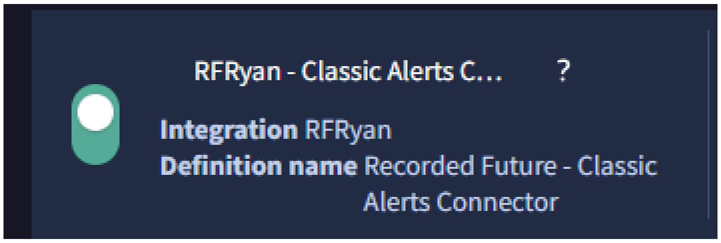
Name	Default Value	Description	Type
PythonProcessTimeout	180	How long the connector will run before timing out	int
Severity	medium	The severity of the alerts created by the connector	string
API Key		Recorded Future API Key	string
API URL	https://api.recordedfuture.com	URL of Recorded Future API. Do not change unless instructed to do so	string
Max Alerts to Fetch	100	Maximum alerts are fetched during a single run	int
Fetch Max Hours Backwards	1	How many hours back to query for alerts in the Recorded Future API	int

Name	Default Value	Description	Type
Use Whitelist as a Blacklist	False	Whether to fetch all alerts in the dynamic lists, or all alerts except those in the dynamic list	bool
Extract All Entities	False	If this option is unchecked, only the “primary” entities of an alert will be extracted and added as an entity. If this option is checked, all entities will be extracted	bool
Enable Overflow	False	Whether alerts will be deduped using Google’s “overflow” logic. For more details, contact your Google representative	bool

Name	Default Value	Description	Type
Proxy Password		Password if using a proxy	string
Proxy Username		Username if using a proxy	string
Proxy Server Address		Domain or IP if using a proxy	string

Changing the default values for `device_product` or `rule_name` will result in the built-in entity mapper failing. Do not modify these fields unless you know what you're doing

Enable the connector by clicking the toggle and then "Save".



RFRyan - Classic Alerts C... ?

Integration RFRyan
Definition name Recorded Future - Classic Alerts Connector

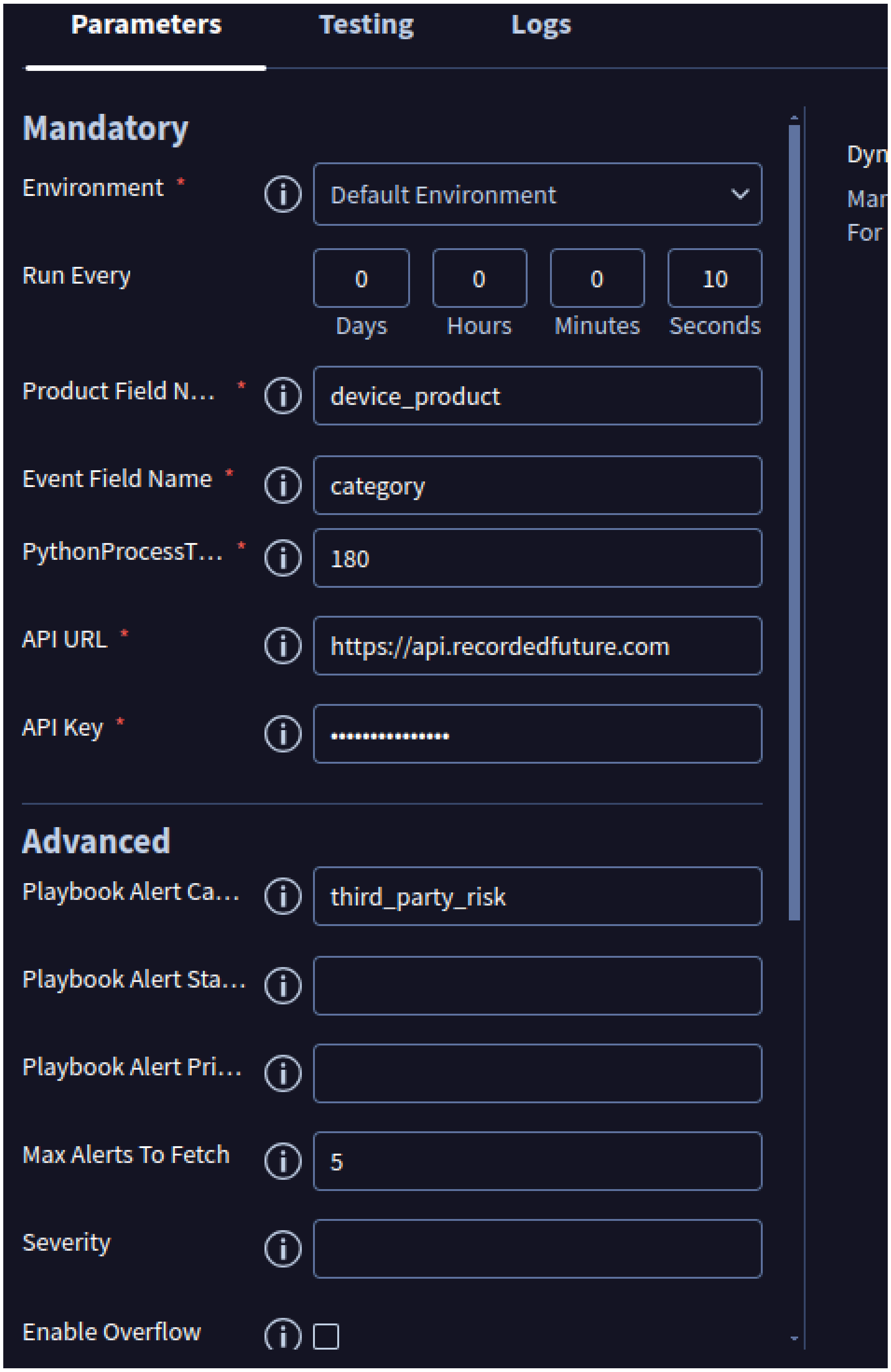
Enable Connector by clicking the toggle button

You can also test the connector under the "Testing" tab and click "Run connector once".

Configure the Playbook Alerts Connector

Playbook Alerts Connector

This Connector imports newly created Playbook Alerts as alerts/cases in Google SecOps SOAR



Mandatory

Environment *	Default Environment
Run Every	0 Days 0 Hours 0 Minutes 10 Seconds
Product Field N… *	device_product
Event Field Name *	category
PythonProcessT… *	180
API URL *	https://api.recordedfuture.com
API Key *	•••••••••••••••

Advanced

Playbook Alert Ca…	third_party_risk
Playbook Alert Sta…	
Playbook Alert Pri…	
Max Alerts To Fetch	5
Severity	
Enable Overflow	□

Parameters

Name	Default Value	Description	Type
Run Every	10 seconds	How frequently the Recorded Future API is polled for new alerts	timestamp
Product Field Name	device_product	Which field in the alert structure populates the Product of the GSOAR alert	string
Event Field Name	category	Which field in the alert structure populates the Event of the GSOAR alert	string
PythonProcessTimeout	180	How long the connector will run before timing out	int
API Key		Recorded Future API Key. Contact Recorded Future	string

Name	Default Value	Description	Type
		support if you need access	
API URL	https://api.recordedfuture.com	URL of Recorded Future API. Do not change unless instructed to do so	string
Playbook Alert Categories	domain_abuse, cyber_vulnerability, code_repo_leakage, third_party_risk, identity_novel_exposures, geopolitics_facility	Which playbook alert rules to import. Must be one of the default values in a comma separated list	string
Playbook Alert Statues		Filter playbook alerts to ones with certain statuses. Must be one or more of 'New', 'InProgress', 'Resolved', 'Dismissed' in a	string

Name	Default Value	Description	Type
		comma separated list.	
Playbook Alert Priorities		Filter playbook alerts to ones with certain priority values. Must be one or more of 'Informational', 'Moderate', 'High' in a comma separated list	string
Max Alerts to Fetch	100	Maximum alerts are fetched during a single run	int
Severity		Set if you want to override the Recorded Future determined severity with a hardcoded severity. Must be one of ‘Low’,	string

Name	Default Value	Description	Type
		‘Medium’, ‘Critical’, ‘High’	
Fetch Max Hours Backwards	1	How many hours back to query for alerts in the Recorded Future API	int
Enable Overflow	False	Whether alerts will be deduped using Google’s “overflow” logic. For more details, contact your Google representative	bool
Proxy Password		Password if using a proxy	string
Proxy Username		Username if using a proxy	string
Proxy Server Address		Domain or IP if using a proxy	string

Playbook Alerts tracking connector

This Connector imports updates to Playbook Alerts as new alerts/cases in Google SecOps SOAR. It is meant to be run **in addition to** the “normal” Playbook Alerts Connector, not as a replacement for it.

At least one of these options must be checked in order for the connector to create any cases.

- New Assessment Added
- Playbook Alert Reopened
- Priority Increased
- Entity Added or removed

Parameters

Name	Default Value	Description	Type
Run Every	10 seconds	How frequently the Recorded Future API is polled for new alerts	timestamp
API Key		Recorded Future API Key. Contact Recorded Future support if you need access	string

Name	Default Value	Description	Type
Product Field Name	device_product	Which field in the alert structure populates the Product of the GSOAR alert	string
Event Field Name	category	Which field in the alert structure populates the Event of the GSOAR alert	string
PythonProcessTimeout	180	How long the connector will run before timing out	int
API Key		Recorded Future API Key. Contact Recorded Future support if you need access	string
API URL	https://api.recordedfuture.com	URL of Recorded Future API. Do not change unless instructed to do so	string

Name	Default Value	Description	Type
Playbook Alert Categories	domain_abuse, cyber_vulnerability, code_repo_leakage, third_party_risk, identity_novel_exposures, geopolitics_facility	Which playbook alert rules to import. Must be one of the default values in a comma separated list	string
Playbook Alert Statues		Filter playbook alerts to ones with certain statuses. Must be one or more of 'New', 'In Progress', 'Resolved', 'Dismissed' in a comma separated list.	string
New Assessment Added	false	Create a new Google SecOps alert/case if a new assessment is added to the playbook alert	bool

Name	Default Value	Description	Type
Playbook Alert Reopened	false	Create a new Google SecOps alert/case if the playbook alert is reopened	bool
Priority Increased	false	Create a new Google SecOps alert/case if the priority of the playbook alert increases	bool
Entity Added	false	Create a new Google SecOps alert/case if an entity (e.g. DNS record) is added to the playbook alert	bool
Playbook Alert Priorities		Filter playbook alerts to ones with certain priority values. Must be one or more of	string

Name	Default Value	Description	Type
		'Informational', 'Moderate', 'High' in a comma separated list	
Max Alerts to Fetch	100	Maximum alerts are fetched during a single run	int
Severity		Set if you want to override the Recorded Future determined severity with a hardcoded severity. Must be one of ‘Low’, ‘Medium’, ‘Critical’, ‘High’	string
Fetch Max Hours Backwards	1	How many hours back to query for alerts in the Recorded Future API	int

Name	Default Value	Description	Type
Enable Overflow	False	Whether alerts will be deduped using Google's "overflow" logic. For more details, contact your Google representative	bool
Proxy Password		Password if using a proxy	string
Proxy Username		Username if using a proxy	string
Proxy Server Address		Domain or IP if using a proxy	string

Action documentation

Enrich Actions - common

The Enrich IOC, Enrich CVE, Enrich Hash, Enrich Host, Enrich IP, and Enrich URL actions share most of the same parameters, outputs, and enrichment fields. Any field specific to an action will be listed in that section of the documentation

Parameters

Name	Default Value	Description	Type
Risk Score Threshold	25	The risk score threshold for an entity to be marked as "malicious" in Google SecOps	int
Include Links	False	Determines if links are include in the JSON response	bool
Enable Collective Insights	True	Determines if the indicator being enriched is sent to Collective Insights	bool

Sample Output

Script Result Name	Value Options	Example
is_risky	True/False	is_risky:False

JSON

Unset

```
{
        "Entity": "47.104.169.49",
        "EntityResult":
        [
            {
                "entity":
                {
                    "id": "ip:47.104.169.49",
                    "name": "47.104.169.49",
                    "type": "IpAddress"
                },
                "intelCard":
"https://app.recordedfuture.com/live/sc/entity/ip%3A47.104.169.49
",
                "risk":
                {
                    "criticalityLabel": "Suspicious",
                    "riskString": "2/79",
                    "rules": 2,
                    "criticality": 2,
                    "riskSummary": "2 of 79 Risk Rules currently
observed.",
                    "score": 25,
                    "evidenceDetails":
                    [
                        {
                            "mitigationString": "",
                            "evidenceString": "10 sightings on 1
source: Recorded Future Network Intelligence. Multiple
communications observed between 47.104.169.49 on port 44694 and
207.174.3.213 (Platypus C2 Server) on port 13337 on 2024-09-08 at
01:07 UTC.  ",
                            "rule": "Recently Communicating With
Reported C&C Server",
                            "criticality": 1,
                            "timestamp":
"2024-09-08T00:00:00.000Z",
                            "criticalityLabel": "Unusual"
                        },
                        {
                            "mitigationString": "",
                            "evidenceString": "2 sightings on 1
source: Recorded Future Network Intelligence. Multiple
communications observed between 47.104.169.49 on port 37656 and
207.174.3.213 (validated Platypus C2 Server) on port 13337 on
2024-09-10 at 12:01 UTC.  ",
                            "rule": "Recently Communicating With
Validated C&C Server",
                            "criticality": 2,
                            "timestamp":
"2024-09-10T00:00:00.000Z",
                            "criticalityLabel": "Suspicious"
                        }
                    ]
                },
                "timestamps":
                {
                    "lastSeen": "2024-09-11T23:59:59.000Z",
                    "firstSeen": "2024-09-11T00:00:00.000Z"
                },
                "links":
                {
                    "Indicators & Detection Rules":
                    [
                        {
                            "id": "ip:207.174.3.213",
                            "name": "207.174.3.213",
                            "type": "IpAddress"
                    }
                ],
                "Victims & Exploit Targets":
                [
                    {
                        "id": "CBfUP",
                        "name": "Alibaba",
                        "type": "Company"
                    }
                ],
                "Actors, Tools & TTPs":
                [
                    {
                        "id": "mitre:T1071",
                        "name": "T1071",
                        "type": "MitreAttackIdentifier"
                    },
                    {
                        "id": "mitre:TA0011",
                        "name": "TA0011",
                        "type": "MitreAttackIdentifier"
                    },
                    {
                        "id": "qNa4Aj",
                        "name": "Platypus",
                        "type": "Malware"
                    }
                ]
            }
        }
    ]
}
```

Enrichment Fields

Enrichment Field Name	Example value
RF_asn	AS37963
RF_org	Hangzhou Alibaba Advertising Co.,Ltd.
RF_city	Qingdao
RF_country	China
RF_intel_card	https://app.recordedfuture.com/live/sc/entity/ip%3A47.104.169.49
RF_risk_rules	Recently Communicating With Reported C&C Server,Recently Communicating With Validated C&C Server
RF_risk_score	25
RF_risk_string	2/79

Enrich IOC

Enrich any CVE, IP Address, URL, File Hash, Host, or Domain entities attached to an alert

Enrich Host

Enrich any Host or Domain entities attached to an alert

Enrich URL

Enrich any URL entities attached to an alert

Enrich IP

Output

JSON

This shows only the net new fields

Unset

```
{
    "EntityResult":
    [
        {
            "location":
            {
                "organization": "Hangzhou Alibaba Advertising
Co.,Ltd.",
                "cidr":
```

```
                {
                    "id": "ip:47.104.0.0/16",
                    "name": "47.104.0.0/16",
                    "type": "IpAddress"
                },
                "location":
                {
                    "continent": "Asia",
                    "country": "China",
                    "city": "Qingdao"
                },
                "asn": "AS37963"
            }
        }
    ]
}
```

Enrichment Fields

Enrichment Field Name	Example value
RF_asn	AS37963
RF_org	Hangzhou Alibaba Advertising Co.,Ltd.
RF_city	Qingdao
RF_country	China

Enrich Hash

Output

JSON

This shows only the net new fields

Unset

```
{
    "Entity":
"e187f969939b4de4340c942a0f50171ae9ca446566d562744d2447aa5d99c151
",
    "EntityResult":
    [
        {
            "hashAlgorithm": "SHA-256"
        }
    ]
}
```

Get Alert Details

Parameters

Name	Default Value	Description	Type
Alert ID		The ID of the Recorded Future Alert to fetch	string

Sample Output

JSON

Unset

```
{
    "id": "adfebg",
    "title": "Malicious Infrastructure on Monitored IP Addresses
- 19 references",
    "triggered": "2024-07-29T05:04:21.166Z",
    "url":
"https://app.recordedfuture.com/live/sc/notification/?id=adfebg",
    "type": "EVENT",
    "hits":
    [
        {
            "entities":
            [
                {
                    "id": "hHQyM6",
                    "name": "Automated Verification",
                    "type": "Category"
                },
                {
                    "id": "m343cq",
                    "name": "5555",
                    "type": "NetworkPort"
                },
                {
                    "id": "un2fMJ",
                    "name": "Malware Staging Server",
                    "type": "Category"
                },
                {
                    "id": "gf7N84",
                    "name": "6",
                    "type": "NetworkProtocol"
                },
                {
                    "id": "KDxJDS",
                    "name": "Ramnit",
                    "type": "Malware"
                },
                {
                    "id": "ip:47.104.139.94",
                    "name": "47.104.139.94",
                    "type": "IpAddress"
                },
                {
                    "id": "uCr290",
                    "name": "Validated IOC",
                    "type": "Category"
                },
                {
                    "id": "mitre:T1608",
                    "name": "T1608",
                    "type": "MitreAttackIdentifier"
                }
            ],
            "noteId": null,
            "fragment": "Recorded Future validated 47.104.139.94
as high confidence Malware Staging Server on July 28, 2024",
            "noteLink": null,
            "id": "HFAZwAAcRkE",
            "language": "eng",
            "source":
            {
                "id": "source:un26Ie",
                "name": "Insikt Group Malware Staging Server
Validation",
                "type": "Source"
            },
            "title": "Recorded Future validated 47.104.139.94 as
high confidence Malware Staging Server on July 28, 2024",
            "triggered_by":
            [
                {
                    "id": "ip:47.104.139.94",
                    "name": "47.104.139.94",
                    "type": "IpAddress",
                    "relationship": "InfrastructureAnalysis.host"
                },
                {
                    "id": "ip:47.104.0.0/16",
                    "name": "47.104.0.0/16",
```

```json
                    "type": "IpAddress",
                    "relationship": "IpAddress.cidr"
                },
                {
                    "id": "report:mfLASp",
                    "name": "IP Watch List",
                    "type": "EntityList",
                    "relationship": "Entity.lists"
                }
            ]
        },
        {
            "entities":
            [
                {
                    "id": "hHQyM6",
                    "name": "Automated Verification",
                    "type": "Category"
                },
                {
                    "id": "m3zYAl",
                    "name": "2027",
                    "type": "NetworkPort"
                },
                {
                    "id": "un2fMJ",
                    "name": "Malware Staging Server",
                    "type": "Category"
                },
                {
                    "id": "gf7N84",
                    "name": "6",
                    "type": "NetworkProtocol"
                },
                {
                    "id": "KDxJDS",
                    "name": "Ramnit",
                    "type": "Malware"
                },
                {
                    "id": "ip:47.104.139.94",
                    "name": "47.104.139.94",
                    "type": "IpAddress"
                },
                {
                    "id": "uCr290",
                    "name": "Validated IOC",
                    "type": "Category"
                },
                {
                    "id": "mitre:T1608",
                    "name": "T1608",
                    "type": "MitreAttackIdentifier"
                }
            ],
            "noteId": null,
            "fragment": "Recorded Future validated 47.104.139.94
as high confidence Malware Staging Server on July 28, 2024",
            "noteLink": null,
            "id": "HFAZwAArtWg",
            "language": "eng",
            "source":
            {
                "id": "source:un26Ie",
                "name": "Insikt Group Malware Staging Server
Validation",
                "type": "Source"
            },
            "title": "Recorded Future validated 47.104.139.94 as
high confidence Malware Staging Server on July 28, 2024",
            "triggered_by":
            [
                {
                    "id": "ip:47.104.139.94",
                    "name": "47.104.139.94",
                    "type": "IpAddress",
                    "relationship": "InfrastructureAnalysis.host"
                },
                {
                    "id": "ip:47.104.0.0/16",
                    "name": "47.104.0.0/16",
                    "type": "IpAddress",
                    "relationship": "IpAddress.cidr"
                },
                {
                    "id": "report:mfLASp",
                    "name": "IP Watch List",
                    "type": "EntityList",
                    "relationship": "Entity.lists"
                }
            ]
        }
    ],
    "rule":
    {
        "name": "Malicious Infrastructure on Monitored IP
Addresses",
        "use_case_deprecation": null,
        "url":
"https://app.recordedfuture.com/live/sc/ViewIdkobra_view_report_i
tem_alert_editor?view_opts=%7B%22reportId%22%3A%22vvfym1%22%2C%22
bTitle%22%3Atrue%2C%22title%22%3A%22Malicious+Infrastructure+on+M
onitored+IP+Addresses%22%7D",
        "owner_id": "uhash:69sKLfTGsS",
        "owner_name": "Professional Services Development",
        "id": "vvfym1",
        "organisation_name": "Professional Services Development",
        "organisation_id": "uhash:5zQaSyRpA1"
    },
    "counts":
    {
        "references": 2,
        "entities": 0,
        "documents": 1
    },
    "review":
    {
        "assignee": null,
        "statusDate": null,
        "statusInPortal": "New",
        "status": "no-action",
        "noteDate": null,
        "statusChangeBy": null,
        "noteAuthor": null,
        "note": null
    }
}
```

Update Alert

Parameters

Name	Default Value	Description	Type
Alert ID		The Recorded Future ID of the alert to update	string
Assign to		Specify to whom to assign the Recorded Future alert. You can provide id, username, user hash, or email	string
Note		Specify a note that should be updated on the alert	string
Status		Specify the new status for the alert	string

Get Playbook Alert Details

Gets full playbook alert from Recorded Future API and returns as JSON object

Parameters

Name	Default Value	Description	Type
Playbook Alert ID		The ID of the Recorded Future Playbook Alert to fetch	string
Category		The category of the Playbook Alert to fetch. Must be one of: domain_abuse, cyber_vulnerability, code_repo_leakage, third_party_risk, identity_novel_exposures, geopolitics_facility	string

Refresh Playbook Alert

- Gets full playbook alert from Recorded Future API and returns as JSON object.
- Extracts entities from the PBA and attaches them to the case
- Renders HTML panels for use by alert view widgets

Parameters

Name	Default Value	Description	Type
Playbook Alert ID		The ID of the Recorded Future Playbook Alert to fetch	string
Category		The category of the Playbook Alert to fetch. Must be one of: domain_abuse, cyber_vulnerability, code_repo_leakage, third_party_risk, identity_novel_exposures, geopolitics_facility	string

Update Playbook Alert

Updates the specified Playbook Alert in the Recorded Future platform

Parameters

Name	Default Value	Description	Type
Playbook Alert ID		The ID of the Recorded Future Playbook Alert to fetch	string
Assign To		Specify to whom to assign the alert. You can provide id, username, user hash, or email	string
Log Entry		Specify a comment to be added to the playbook alert	string
Status		Specify the new status for the alert. Must be one of 'New', 'InProgress',	string

		'Dismissed', 'Resolved'	
Priority		Specify the new priority for the alert. Must be one of 'High', 'Moderate', 'Informational'	string
Reopen Strategy		Specify the reopen strategy for the alert. Must be ‘Never’ or ‘SignificantUpdates’	string

Add Analyst Note

Parameters

Name	Default Value	Description	Type
Note Title		Title of the Analyst Note	string

Note Text		Text of the Analyst Note	string
Topic		Specify the relevant Note topic from the list, if needed	string

Ping

Parameters

N/A

Playbooks

This is currently not available until Google certifies the use case. Contact your Recorded Future account team if you want advanced access to these playbooks

Update RF Playbook alerts

There are 5 playbooks that update playbook alerts

- Refresh RF Domain Abuse
- Refresh RF Code Repo Leakage
- Refresh RF Cyber Vulnerability
- Refresh RF Identity Exposures
- Refresh RF Third Party Risk

To enable these playbooks, make sure they are toggled on after installing them from the use case. Each of these playbooks provides an alert view on cases imported by the Playbook Alerts connectors. Rerunning the playbook will update the case view with new information.

Changelog

Version 1.0

Enrichment

- Removed separate related entity commands, folded everything into the enrichment command
- Replaced Related Entities with links
- Improved display for entity insights
- Improved JSON and CSV reports attached to entities in playbooks
- Added new enrichment fields
- Added option to send enriched IOCs to collective insights

Classic Alerts

- Split alert references into multiple events. For each reference in an alert, an event is created
- Added support for the Why The Alert feature
  - In both the Alert Connector and the “Get Alert Details” action
- Added option to enable/disable Alert overflow in Google SOAR
- Added support for AI insights in alerts
- Automatically extract indicators from alerts and attach them to the alert/case
  - Option to extract only primary entities or all entities
- Name change “Recorded Future Security Alerts” → “Recorded Future Classic Alerts”
- Product for alerts changed from “Recorded Future” to “Recorded Future Classic Alerts”
- Remove the option for “Get Alert Details” in the connector, as all alerts now fetch details

Version 1.1

This is listed a Version “3.0” in the Google SecOps marketplace

Classic Alerts

- Fix bug where “triggered_by” fields had unexpected null values

Playbook Alerts

- Add actions to pull, refresh, and update Playbook Alerts for all 6 PBA types
- Add connector to import playbook alerts as cases
- Add tracking connector to import playbook alert updates as cases
- Adds use case “Recorded Future Playbook Alerts” containing playbooks to refresh Playbook Alert cases with new data in Recorded Future. This will not be

available until the “Recorded Future Playbooks” use case is certified in the Google SecOps marketplace

Version 1.2

- Fixed a bug that caused duplication of imported playbooks
- Fixed a bug that prevented statuses for Playbook Alerts from being updated correctly

Appendix

recorded_future_classic_alert.html

Unset

```
<!DOCTYPE html>
<html>

<head>
    <style>
        body {
            background-color: #212c44;
            color: #c3d2e8;
            font-family: "Source Sans Pro", "Noto Sans", sans-serif;
        }

        h3,
        h4 {
            font-weight: 500 !important;
        }

        h3 {
            border-bottom-width: 2px;
            border-bottom-style: solid;
            border-bottom-color: #3a4a6c;
        }

        h4 {
            margin-top: 10px;
            margin-bottom: 5px;
        }

        p {
            font-size: 14px;
            font-weight: 100;
            margin-top: 0;
        }

        button {
            background-color: #6275a3;
            color: #fff;
            border-radius: 4px;
            font-weight: 400;
            font-size: 14px;
            padding: 0 12px;
            line-height: 24px;
            letter-spacing: 0.5px;
            border: none;
            text-align: center;
            user-select: none;
            cursor: pointer;
        }

        a {
            width: 160px;
            display: flex;
            gap: 2px;
            text-decoration: none;
        }
    </style>
</head>

<body>
    <h3>[Event.alert_title]</h3>
    <div>
        <h4 style="display: inline;">Alert ID: </h4>
        <p style="display: inline;">[Event.alert_id]</p>
    </div>
    <div>
        <h4>AI Insights:</h4>
        <p>[Event.ai_insights_text]</p>
    </div>
    <a href=[Event.alert_url] target="_blank">
        <button>Open Alert in Portal</button>
    </a>
</body>
<script>
    //This script enables the widget theme to reflect the user's choice in the platform.
    //Removing this script will result in your HTML widget permanently displayed in the light theme.
    onmessage = evt => {
        for (const [key, value] of Object.entries(evt.data)) {
            document.body.style[key] = value;
        }
    }
</script>

</html>
```

About Recorded Future

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com