

Cloud NGFW and Security Command Center Enterprise Integration Guide





Streamline your detection and response with Cloud NGFW and Security Command Center Enterprise

Cloud NGFW

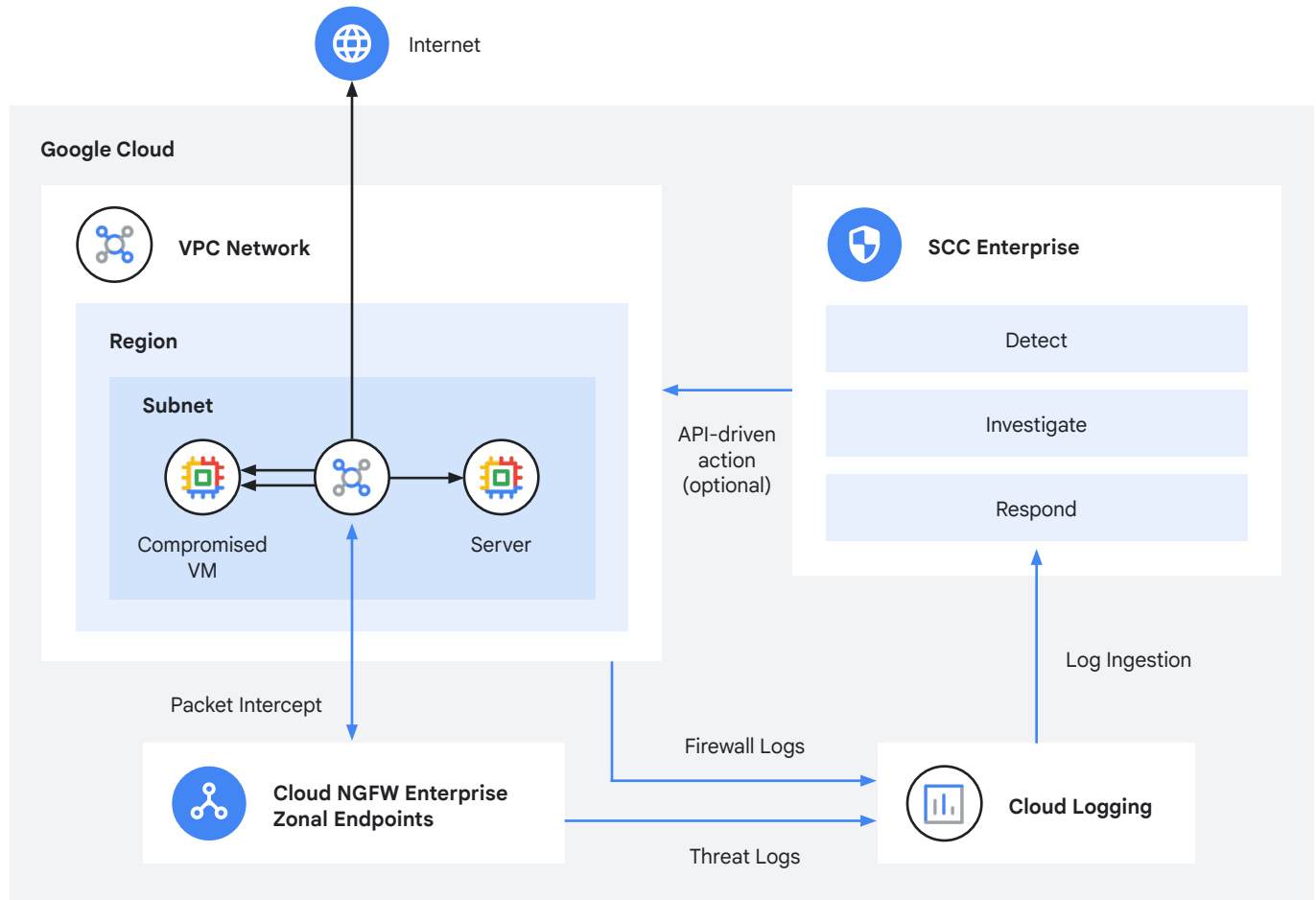
Cloud Next Generation Firewall (NGFW) Enterprise is a fully distributed, cloud-native firewall service that provides stateful advanced threat protection. Its micro-segmentation capabilities allow for granular control over network traffic, enhancing your ability to isolate and protect critical workloads. NGFW Enterprise provides advanced Intrusion Detection and Prevention Service (IDPS) capabilities, powered by Palo Alto Networks technology, and includes [vulnerability, anti-spyware and antivirus signatures](#) capabilities.

Security Command Center

[Security Command Center Enterprise](#) is Google's flagship cloud security and risk management solution, offering native Google Cloud log ingestion, including the ability to seamlessly ingest Cloud NGFW firewall and threat logs. Security Command Center Enterprise includes built-in parsers that automatically map these logs to the unified data model, simplifying analysis and correlation.

Topology

Integrating Cloud NGFW Enterprise with Security Command Center Enterprise helps you to streamline cloud security operations by combining the network threat detection in NGFW Enterprise with the security automation and response capabilities in Security Command Center. Here's how it works:



Network Threat Detection:

Cloud NGFW Enterprise identifies a potential threat, and [logs an event](#) in Cloud Logging which is [exported to Security Command Center Enterprise](#).

Unified view:

Security Command Center Enterprise automatically ingests this log entry. The [built-in parser](#) maps the log fields to the [Unified Data Model](#) structure, ensuring consistency and ease of analysis.

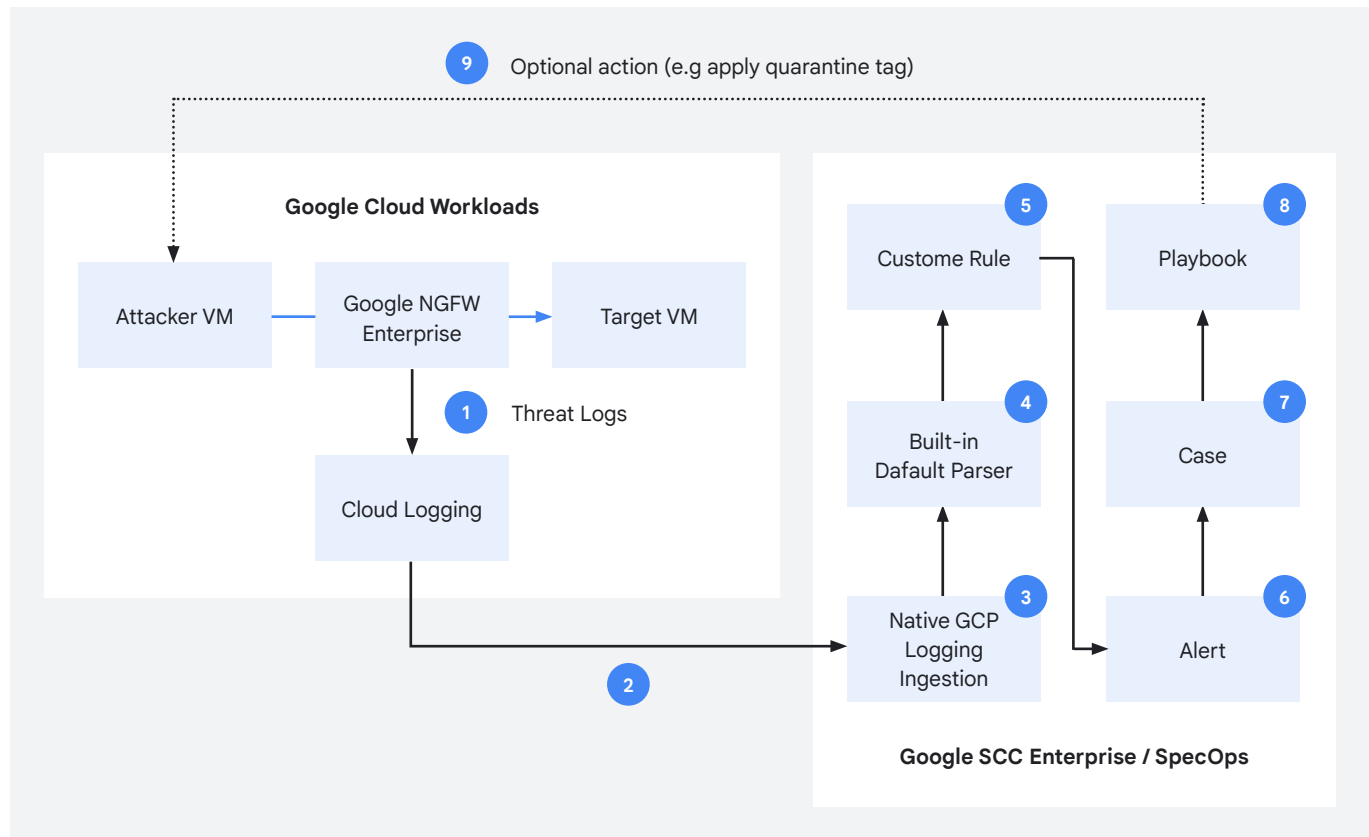
Prioritized findings:

You can create custom [detection rules](#) within Security Command Center Enterprise to identify specific events of interest. These rules generate alerts, which are aggregated into actionable [cases](#).

Automated response:

[Playbooks](#) can be attached to cases for automated response. For instance, a custom playbook might automatically add an [IAM-governed tag](#) to a compromised workload, isolating it for further investigation or remediation.

Sample Integration Workflow



Google Cloud's NGFW Enterprise and Security Command Center Enterprise can be seamlessly integrated in your environment without any additional agents or software. As outlined in the workflow diagram above, once Cloud NGFW Enterprise identifies a threat, it creates an event in Cloud Logging [1], the log entry is automatically forwarded to Security Command Center Enterprise [2] which natively ingests the threat finding [3] and has a default parser [4] that maps the fields using the [Unified Data Model](#) structure.

A [custom rule using the YARA-L 2.0 language](#) [5] is created to identify the relevant events and generate alerts [6] that are aggregated to raise a Case [7]. A playbook [8] can be attached to the case to be run automatically and, optionally, take an action such as adding a secure tag to a potentially compromised workload [9].

Cloud NGFW Enterprise Configuration Steps

If needed, follow the [Cloud NGFW Enterprise IPS codelab](#) to set up an environment and generate the sample threats. Make sure the threats show up in the Threats Logs and/or Cloud Logging as follows:

Threats												
Filter												
Alert severity	Alert time ↓	Threat name	Threat type	Threat ID	Source IP address	Source port	Destination IP address	Destination port	Protocol	Network	Action	Security profile group
HIGH	Nov 7, 2024, 9:44:31 AM	Microsoft Windows winrm Access Attempt Detected	VULNERABILITY	30851		1058		80	tcp	cloudingfw-vpc	RESET_SERVER	cloudingfw-spg
LOW	Nov 7, 2024, 9:44:31 AM	Possible HTTP Malicious Payload Detection	VULNERABILITY	58098		1059		80	tcp	cloudingfw-vpc	ALERT	cloudingfw-spg
MEDIUM	Nov 7, 2024, 9:44:31 AM	HTTP Directory Traversal Request Attempt	VULNERABILITY	30844		1058		80	tcp	cloudingfw-vpc	ALERT	cloudingfw-spg
LOW	Nov 7, 2024, 9:44:31 AM	Suspicious File Downloading Detection	VULNERABILITY	54469		1059		80	tcp	cloudingfw-vpc	ALERT	cloudingfw-spg
HIGH	Nov 7, 2024, 9:44:27 AM	HTTP /etc/passwd Access Attempt	VULNERABILITY	35107		1057		80	tcp	cloudingfw-vpc	RESET_SERVER	cloudingfw-spg
CRITICAL	Nov 7, 2024, 9:44:26 AM	Bash Remote Code Execution Vulnerability	VULNERABILITY	36729		1056		80	tcp	cloudingfw-vpc	RESET_BOTH	cloudingfw-spg
HIGH	Nov 7, 2024, 9:44:26 AM	Microsoft Windows winrm Access Attempt Detected	VULNERABILITY	30851	10.0.0.3	47802	10.0.0.2	80	tcp	cloudingfw-vpc	RESET_SERVER	cloudingfw-spg
MEDIUM	Nov 7, 2024, 9:44:26 AM	HTTP Directory Traversal Request Attempt	VULNERABILITY	30844	10.0.0.3	47802	10.0.0.2	80	tcp	cloudingfw-vpc	ALERT	cloudingfw-spg
LOW	Nov 7, 2024, 9:44:25 AM	Suspicious File Downloading Detection	VULNERABILITY	54469	10.0.0.3	47812	10.0.0.2	80	tcp	cloudingfw-vpc	ALERT	cloudingfw-spg
LOW	Nov 7, 2024, 9:44:25 AM	Possible HTTP Malicious Payload Detection	VULNERABILITY	58098	10.0.0.3	47812	10.0.0.2	80	tcp	cloudingfw-vpc	ALERT	cloudingfw-spg
HIGH	Nov 7, 2024, 9:44:20 AM	HTTP /etc/passwd Access Attempt	VULNERABILITY	35107	10.0.0.3	55586	10.0.0.2	80	tcp	cloudingfw-vpc	RESET_SERVER	cloudingfw-spg
CRITICAL	Nov 7, 2024, 9:44:20 AM	Bash Remote Code Execution Vulnerability	VULNERABILITY	36729	10.0.0.3	55574	10.0.0.2	80	tcp	cloudingfw-vpc	RESET_BOTH	cloudingfw-spg

Create a new quarantine tag key and value (required because two tag values from the same tag key cannot be assigned to the same instance):



```
gcloud resource-manager tags keys create $prefix-vpc-quarantine-key \
--parent projects/$project_id \
--purpose GCE_FIREWALL \
--purpose-data network=$project_id/$prefix-vpc
```



```
gcloud resource-manager tags values create $prefix-vpc-quarantine-value \  
--parent=$project_id/$prefix-vpc-quarantine-key
```

Create new firewall rules to block all traffic to and from instances
with the quarantine tag value:



```
gcloud compute network-firewall-policies rules create 10 \  
--description="block egress traffic from quarantined workloads" \  
--action=deny \  
--firewall-policy=$prefix-fwpolicy \  
--global-firewall-policy \  
--layer4-configs=all \  
--direction=EGRESS \  
--target-secure-tags $project_id/$prefix-vpc-quarantine-key/$pre-  
fix-vpc-quarantine-value \  
--dest-ip-ranges=0.0.0.0/0  
  
gcloud compute network-firewall-policies rules create 20 \  
--description="block ingress traffic to quarantined workloads" \  
--action=deny \  
--firewall-policy=$prefix-fwpolicy \  
--global-firewall-policy \  
--layer4-configs=all \  
--direction=INGRESS \  
--target-secure-tags $project_id/$prefix-vpc-quarantine-key/$pre-  
fix-vpc-quarantine-value \  
--src-ip-ranges=0.0.0.0/0
```

Security Command Center Enterprise Configuration

The following steps assume that Security Command Center Enterprise is already [activated](#) and ready to be configured.

Log Export Filters

Configure [custom log export filters](#) to include the threat logs, and, optionally, firewall logs (note the [required permissions](#)).



In the Google Cloud console, select the [management project](#) you used to activate Security Command Center Enterprise.



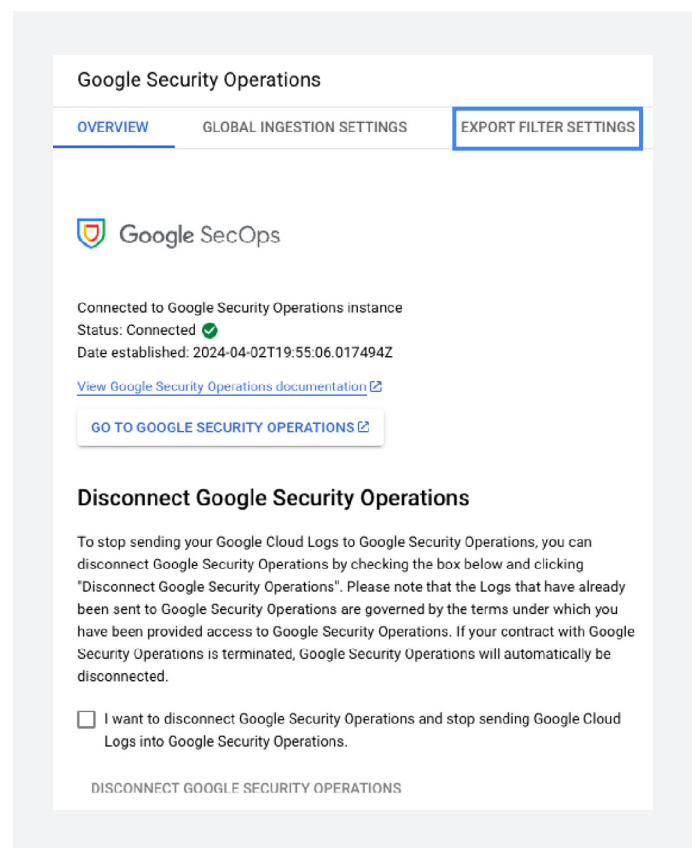
Navigate to **Security > Detections and Controls > Google SecOps**.



Click **Manage Organization Ingestion Settings** (you may need to select your organization).



Select the **Export Filter Settings** tab.



Edit the export filter settings to include the desired logs as shown in the following example (replacing [PROJECT_ID] with your own project):



```
log_id("dns.googleapis.com/dns_queries") OR  
log_id("clouddaudit.googleapis.com/activity") OR  
log_id("clouddaudit.googleapis.com/system_event") OR  
logName = "projects/[PROJECT_ID]/logs/networksecurity.googleapis.com%2Ffire  
wall_threat"
```

If desired, firewall logs can also be exported by [adding the following filter](#):



```
log_id("compute.googleapis.com/firewall")
```

Cloud NGFW [firewall](#) and [threat logs](#) are automatically parsed using [built-in default parsers](#).

Custom Rules

Once the logs are mapped to fields using the [Unified Data Model](#) structure, a custom rule needs to be created to identify the relevant events and generate alerts that are combined to raise a Case.



In the Google Cloud console, switch back to the Google SecOps **Overview** tab and then click **Go to Google Security Operations** to open the [Security Operations console](#) in a new tab.



Click **Menu** and navigate to **Detection > Rules & Detections**. Select the **Rules Editor** tab and [create a new rule](#) using the [YARA-L rules language](#) to raise alerts and detections based on the chosen criteria (in the following example, all events with log_type = "GCP_NGFW_ENTERPRISE").



```
rule gcp_ngfw_enterprise_threats {
  // This rule matches single events. Rules can also match multiple events with
  in
  // some time window. For details about how to write a multi-event rule, see
  // https://cloud.google.com/chronicle/docs/detection/yara-1-2-0-overview#single-event-versus-multi-event

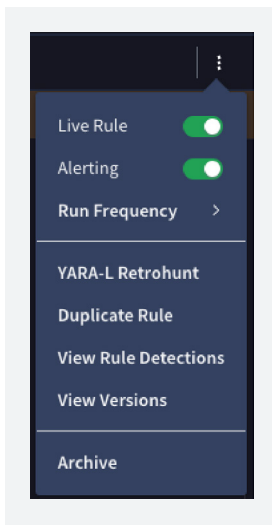
  meta:
    // Allows for storage of arbitrary key-value pairs of rule details - who
    // wrote it, what it detects on, version control, etc.
    // The "author" and "severity" fields are special, as they are used as
    // columns on the rules dashboard. If you'd like to be able to sort based on
    // these fields on the dashboard, make sure to add them here.
    // Severity value, by convention, should be "Low", "Medium" or "High"
    author = "Google Cloud Network Security"
    description = "Network threats detected by Google Cloud NGFW Enterprise"
    type = "alert"
    severity = "Medium"
    priority = "Medium"

  events:
    $network.metadata.event_type = "NETWORK_CONNECTION"
    $network.metadata.log_type = "GCP_NGFW_ENTERPRISE"

  outcome:
    // For a multi-event rule an aggregation function is required
    // e.g., risk_score = max(0)
    // See https://cloud.google.com/chronicle/docs/detection/yara-1-2-0-overview#outcome-conditionals-example_rule
    $risk_score = max(75)
    $event_count = count_distinct($network.security_result.severity)
    //added to populate alert graph with additional context
    $principal_ip = array_distinct($network.principal.ip)
    $target_ip = array_distinct($network.target.ip)
    $severity = array_distinct($network.security_result.severity)
    $action = array_distinct($network.security_result.action_details)


  condition:
    $network
}
```

After saving the new rule, click : associated with the rule. Click the **Live Rule** toggle to the on position. Then, Security Command Center Enterprise automatically raises alerts that are aggregated into cases.

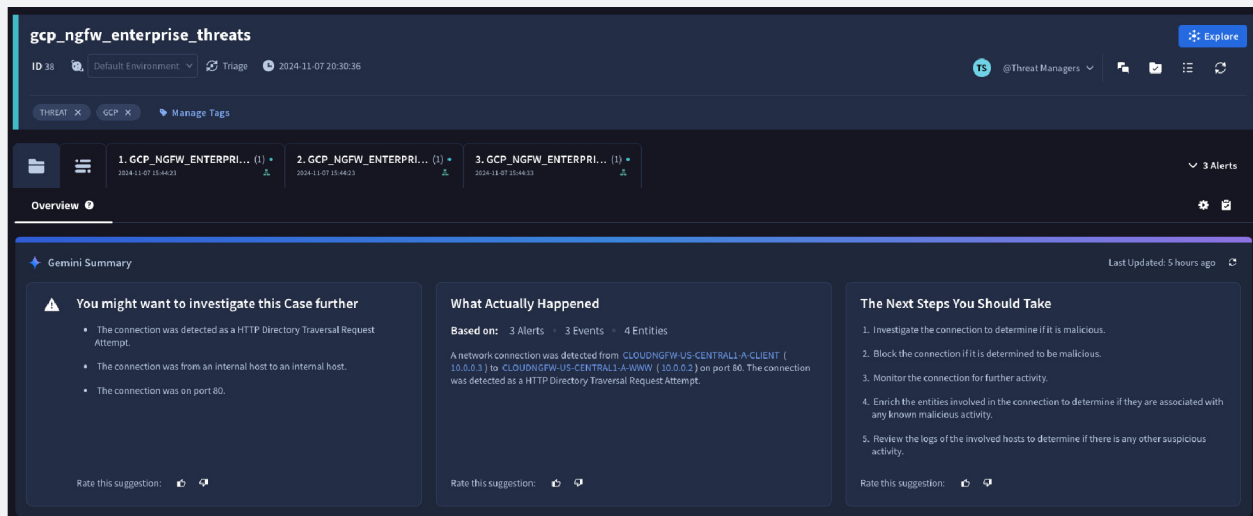


Follow the [Cloud NGFW Enterprise IPS codelab](#) to generate more sample threats, and confirm that they are showing up in the Threats Dashboard and/or Cloud Logging.

Cases and Events

In the Security Operations console, click ☰ Menu and select [Cases](#). You can switch the [view](#) by clicking  **Cases view selection**. Filter by name and date, if needed, to find the latest cases (it might take a few minutes for the log ingestion, rules detection, and case creation to be completed).

Select one of the cases. Then, select one of the alerts to further explore by going through the different tabs.



Overview tab

1. GCP_NGFW_ENTERPRI... (1) 2024-11-07 15:46:23

2. GCP_NGFW_ENTERPRI... (1) 2024-11-07 15:46:23

3. GCP_NGFW_ENTERPRI... (1) 2024-11-07 15:46:33


Overview

Events (1)

Playbooks (1)

Graph

Alert Overview



Rule ID: gcp.ngfw.enterprise.threats

Network threats detected by Google Cloud NGFW Enterprise

Event Details

Event Type

Principal IP

Target Hostname

NETWORK_CONNECTION

10.0.0.3

cloudngfw-us-central1-a-www

Principal Hostname

Principal Port

Target IP

cloudngfw-us-central1-a-client

55586

10.0.0.2

1

Events tab

1. GCP_NGFW_ENTERPRI... (1) 2024-11-07 15:46:23

2. GCP_NGFW_ENTERPRI... (1) 2024-11-07 15:46:23

3. GCP_NGFW_ENTERPRI... (1) 2024-11-07 15:46:33

Overview

Events (1)

Playbooks (1)

Graph

NAME	TYPE	SOURCE / PRODUCT	ARTIFACTS	PORT	OUTCOME	TIME
HTTP/etc/pass...	NETWORK_CON...	RULE		80		2024-11-07 15:4...

HTTP /etc/passwd Access Attempt

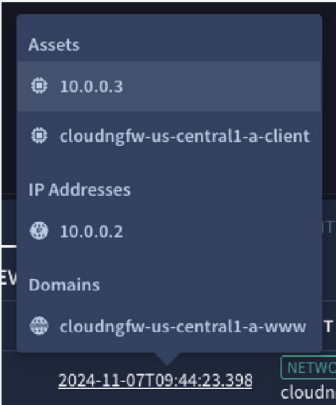
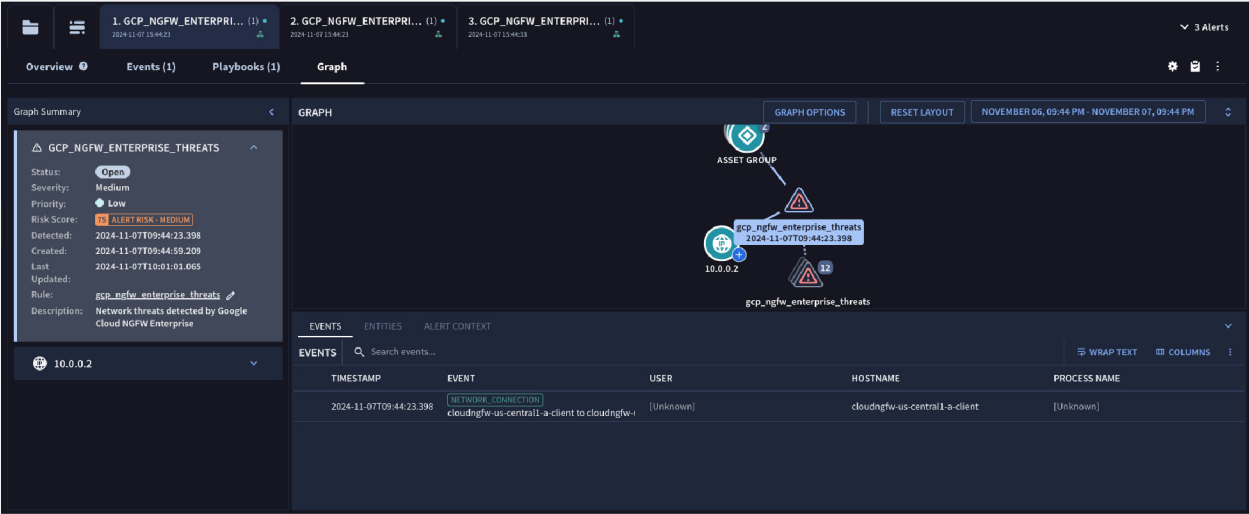
Search...

Default

Field Name	Value
event_metadata_productLogId	ky9f53in1e
event_metadata_eventTimestamp	2024-11-07T15:44:23.398117468Z
event_metadata_collectedTimestamp	2024-11-07T15:44:23.398117468Z
event_metadata_eventType	NETWORK_CONNECTION
event_metadata_vendorName	Google Cloud Platform
event_metadata_productName	GCP Firewall
event_metadata_productEventType	projects/admin-scc-nexus-manual-dev18/...
event_metadata_ingestedTimestamp	2024-11-07T15:44:31.013428Z
event_metadata_id	AAAAAJW/9yPvuj1MWGHEMG8oPUcAAAAA...
event_metadata_logType	GCP_NGFW_ENTERPRISE
event_metadata_baseLabels_logTypes_1	GCP_NGFW_ENTERPRISE
event_metadata_baseLabels_allowSco...	True
event_metadata_enrichmentLabels_log...	GCP_COMPUTE_CONTEXT
event_metadata_enrichmentLabels_all...	True

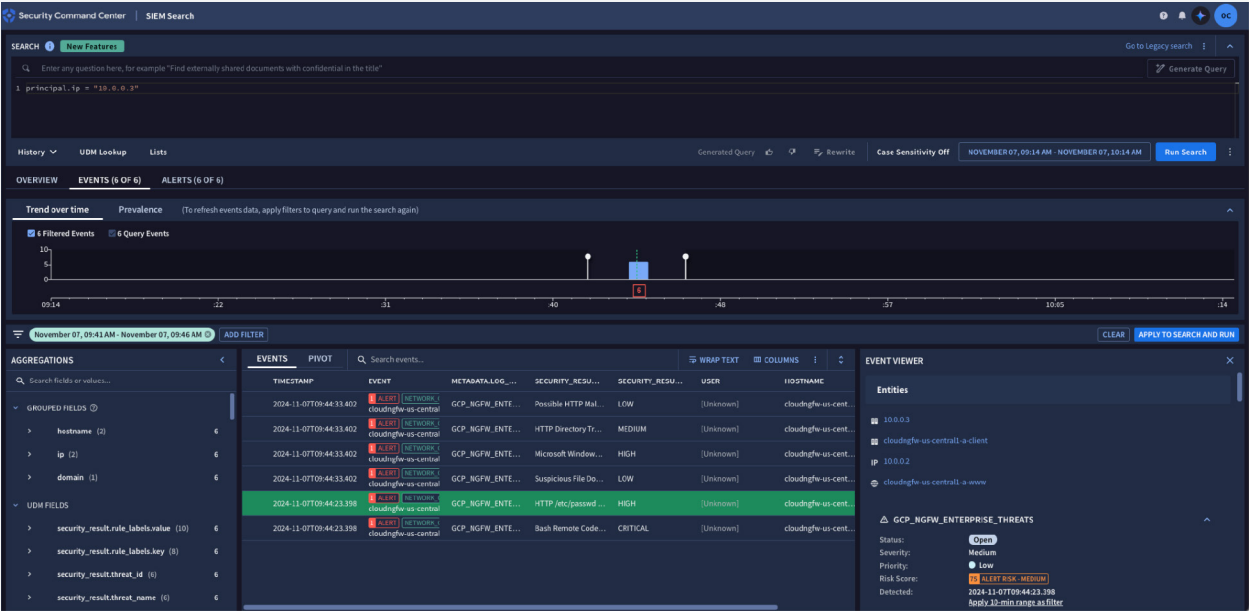
Graph and SIEM Search

On the Graph tab for a Case, select an Alert to see more detailed information about the Alert.



Click the timestamp and select one of the Assets.

The SIEM Search will open to display all events found filtered by the selected criteria (principal.ip in the following example). Click through the different logs and the Event Viewer to see all fields and the UDM mappings that can also be used to search.

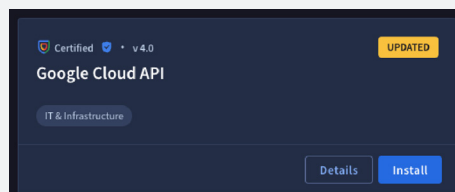


Google Cloud API Integration

Upon completion of the previous steps, Cloud NGFW Enterprise logs are ingested and parsed into Security Command Center Enterprise, and alerts and cases are generated automatically. You must configure the [Google Cloud API integration](#) to allow a response by assigning a quarantine tag to the attacker VM, but first you need to configure the integration.



In the Security Operations console, click **Menu** and select **Marketplace**. Click the **Integrations** tab and install the **Google Cloud API** integration (use the search box if needed).



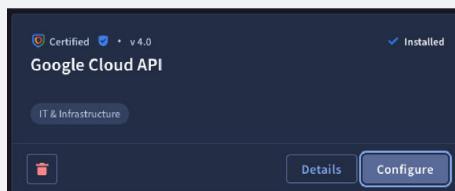
The authentication can be done using [Service Account](#) or [Workload Identity Federation](#). Configure the chosen option accordingly before proceeding.



Tip: Use [Service Account impersonation](#) for a specific gcloud command to make sure that the required permissions were granted to the Service Account being used.



After the installation is complete, click **Configure**.



[Configure](#) the details and click **Save**. Run a test to verify that the integration is working as expected (make sure to enter the Test URL according to the assigned permissions).

Google Cloud API - Configure Instance

Configure all the necessary fields and parameters for this instance

Environment

DE Default Environment

For Environments configuration, visit Settings screen

Instance Name

System Default Instance

Description

Parameters

For more information on configuration and integration details, click here

Test URL

https://compute.googleapis.com/compute/v1/...

Service Account Json File Content

.....

Organization ID

Project ID

Quota Project ID

Workload Identity Email

OAuth Scopes

https://www.googleapis.com/auth/cloud-platf...

Verify SSL

☒

Test

Cancel

Save



Tip: You may need to enable and configure the [Google Cloud Compute](#) integration similarly to the Google Cloud API steps above. This allows enriching entities to provide Google Cloud context that are used by the Playbook.

Custom Playbook Block

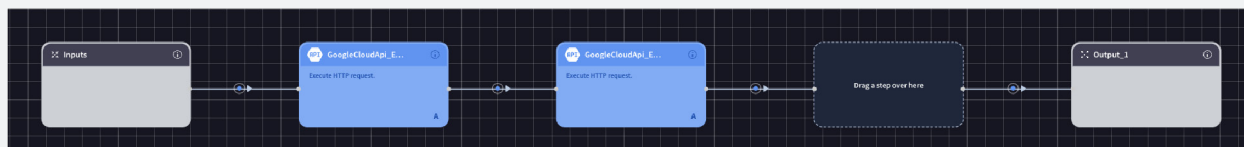
[Blocks](#) are mini playbooks that users can create and reuse in other playbooks. Blocks are being used in this guide because it's possible to manually trigger Blocks on a per alert basis.

You can create a custom Playbook Block that can be attached to alerts to add the quarantine tag to the attacker instance. All instances with this tag will have new connections automatically blocked.

To create a Block, in the Security Operations console, click **Menu** and navigate to **Response > Playbooks**. Click **+ (Add New Playbook or Block)** and create a new Block.

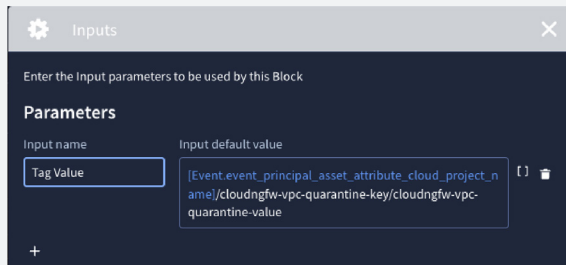
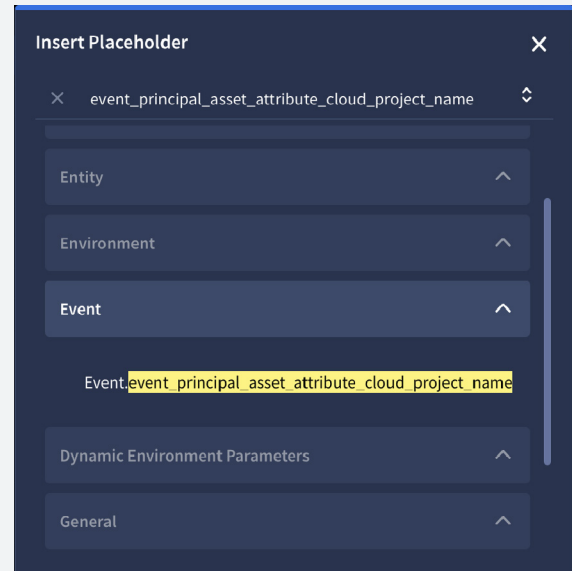


In the **Actions** list, expand the **GoogleCloudApi** option and drag two **Execute HTTP Request** actions as shown in the following example:





Double click the Inputs box and click + to add a new parameter. Enter the Input name. Click [], search for event_principal_asset_attribute_cloud_project_name and click to select.



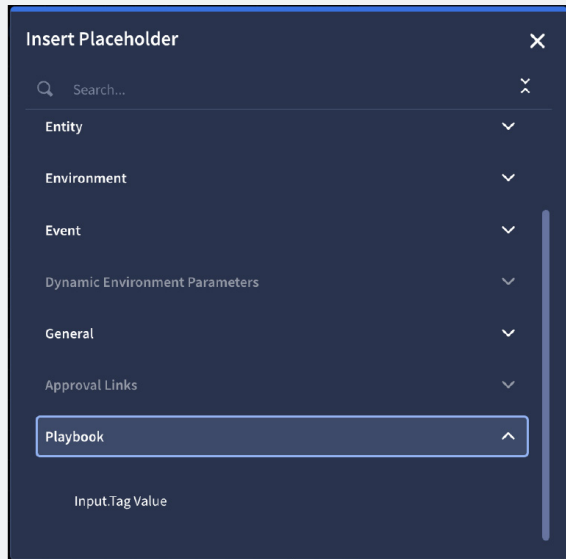
Click + again and add the quarantine tag key and value that were created when configuring [Cloud NGFW Enterprise](#). Click **Save**.



To configure an action that uses the tag value to retrieve the corresponding tag ID, double click the next GoogleCloudApi action box and configure the fields as follows:



Method: GET
URL Path:
`https://cloudresource
manager.googleapis.com/
v3/tagValues/name
spaced?name=`



Position your cursor at the end of the URL Path field and click []. Select **Playbook > Input.TagValue** (you may need to scroll down).

Delete the contents of the following fields:



URL Params

Headers

Cookie

Body Payload

Expected Response Values

Optionally, click the name of the action, enter a different name, and click enter to save the new name of the action. In the following example, this action is titled Get Tag ID.

Confirm that the action is configured as follows before saving:



To configure the action that will use the inputs to assign the quarantine tag to the malicious VM, double click the next GoogleCloudApi action box and configure the fields as follows:

Similarly to the previous step, click [] to populate the variables highlighted in blue.



Method: POST

URL Path: `https://[Event.event_principal_asset_attribute_cloud_availabilityZone]-cloudresourcemanager.googleapis.com/v3/tagBindings`

Body Payload:

```
{
  "parent": "//compute.googleapis.com/projects/[Event.event_principal_asset_attribute_cloud_project_name]/zones/[Event.event_principal_asset_attribute_cloud_availabilityZone]/instances/[Event.event_principal_asset_productObjectId]",
  "tagValue": "[Get Tag ID.JsonResult| \"response_data.name\"]"
}
```



Tip: Use Google Cloud API Explorer to build the URL request (see [tagBindings.create](#) as shown in the example above).

Delete the contents of the following fields:

URL Params

Headers

Cookie

Expected Response Values

Optionally, click the name of the action, enter a different name, and click enter to save the new name of the action. In the following example, this action is titled Set Secure Tag.

Confirm that the action is configured as follows before saving:

The screenshot shows a configuration window titled 'Set Secure Tag' with a 'Simulate' toggle. It contains several input fields for configuring an HTTP request:

- Choose Instance:** Default Environment_System Default Instance
- Entities:** All entities
- Method:** POST
- URL Path:** https://[Event.event_principal_asset_attribute_cloud_availabilityZone]-cloudresourcemanager.googleapis.com/v3/tagBindings
- URL Params:** (empty)
- Headers:** (empty)
- Cookie:** (empty)
- Body Payload:** { "parent": "[//compute.googleapis.com/projects/[Event.event_principal_asset_attribute_cloud_project_name]/zones/[Event.event_principal_asset_attribute_cloud_availabilityZone]/instances/[Event.event_principal_asset_productObjectId]", "tagValue": "[Get Tag ID.JsonResult]", "response_data.name": "" }

[Simulate the playbook](#) to make sure it's working as expected. This requires selecting one of the alerts as a test case.

Navigate to **Cases** and select an alert that has a Google Cloud VM as an attacker (in this example, principal hostname cloudngfw-us-central1-a-client and principal IP 10.0.0.3). Click : **(Alert Options)** and select **Ingest alert as test case**. Click **Simulate**.

The screenshot shows a 'Simulate Alert' dialog box with the following elements:

- Environment:** Default Environment
- Buttons:** Cancel and Simulate



Open the Google Cloud Console in a new window and access the attacker VM in Compute Engine. Make sure that the attacker VM does **not** have the quarantine tag applied.

Tags for cloudngfw-us-central1-a-client

Tags provides a way to conditionally allow or deny policies based on whether a resource has a specific tag. You can use tags and conditional enforcement of policies for fine-grained control across your resource hierarchy. [Learn more](#)

Inherited tags

The selected resources do not have any inherited tags.

Direct tags

Edit tags for the selected resource. Removing a tag may revert to an inherited value. Changing a tag will first remove a tag, before adding the new selection.

admin-scc-nexus-manual-dev18

Key 1 * cloudngfw-vpc-tags Value 1 * cloudngfw-vpc-client

+ ADD TAG

SELECT SCOPE

SAVE DISCARD CHANGES CLOSE

Simulator



Switch back to the Security Operations console window, open the Playbook Block and enable the Simulator.



Click **Run** and wait for all of the actions to complete.

Choose Case 45# gcp_ngfw_enterprise_threats - 2024-11-21 19:16:56 Run Entities

Output_1 2024-11-22 19:52:48 View Results

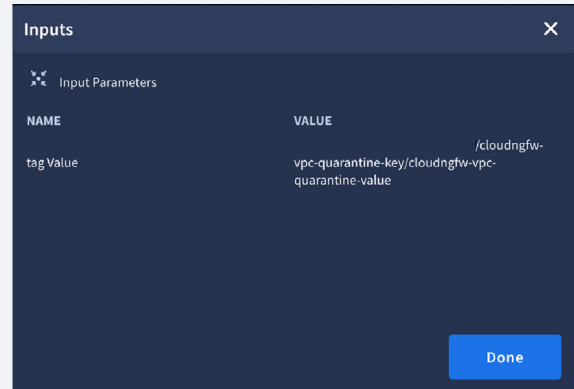
Set Secure Tag 2024-11-22 19:52:46 Pin Results View Results

Get Tag ID 2024-11-22 19:52:44 Pin Results View Results

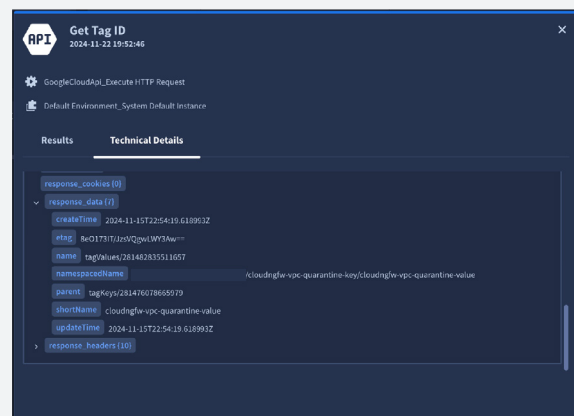
Input 2024-11-22 19:52:43 Inputs View Results



Click **View Results** for each block to check the output **Inputs** results:



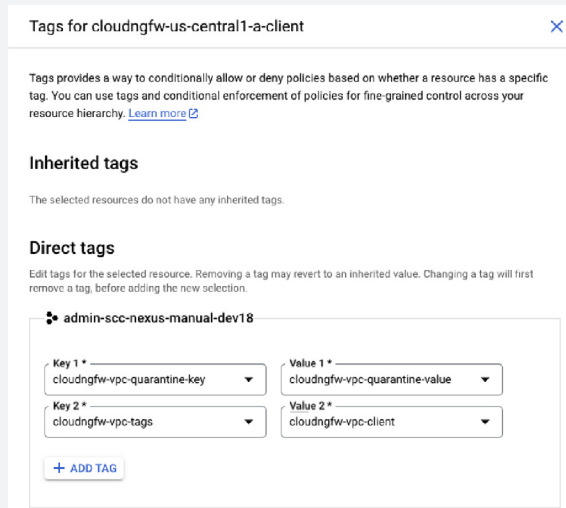
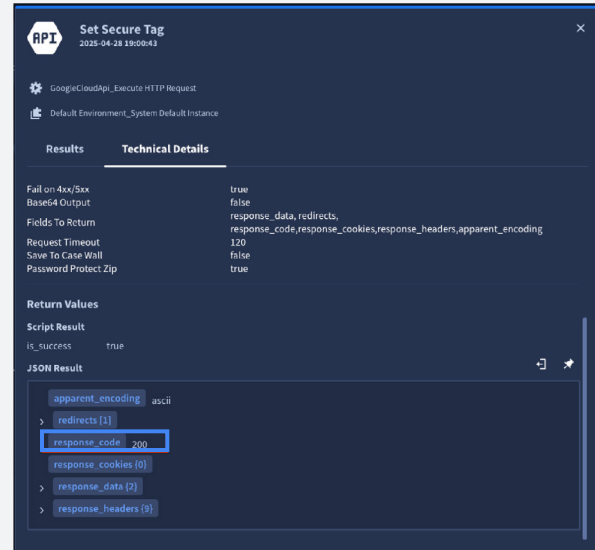
Get Tag Id results, **Technical Details** tab:
(You should check these parameters, both the API request and JSON result, to confirm that the returned tag value ID is correct.)





Set Secure Tag results, Technical Details tab:

(You should check these parameters, both the API request and JSON result, to confirm that the returned tag value ID is correct and that the response code is 200. You may need to scroll down to display the **JSON Result**.)



After confirming that the test was successful, switch back to the Google Cloud Console to confirm that the quarantine tag was successfully added to the attacker VM (you may need to refresh the screen).

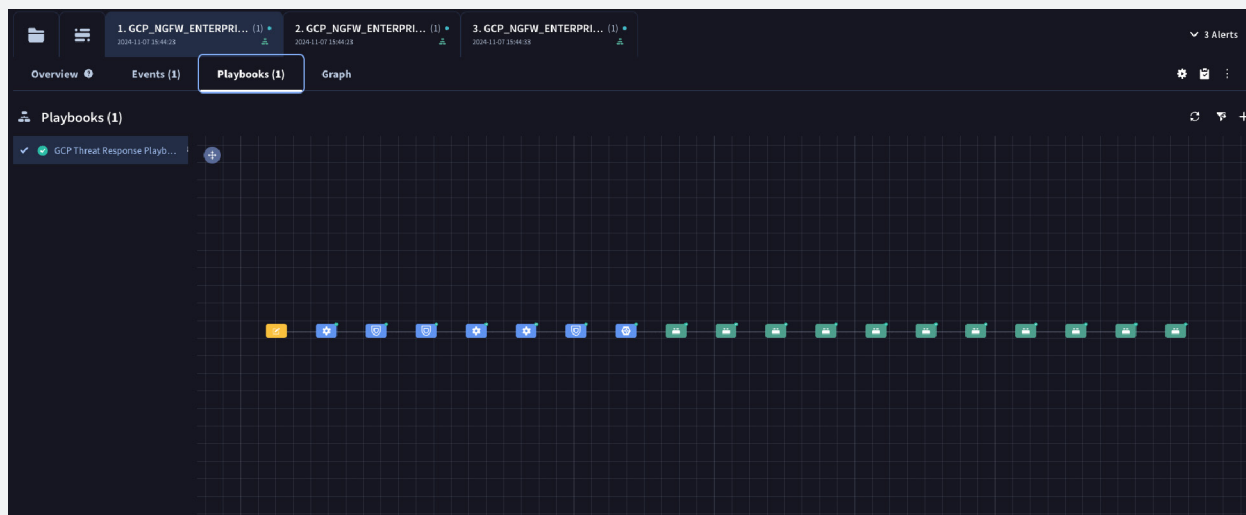
The playbook block can now be added to an alert and run on-demand to assign the quarantine tag to the attacker VM (or be called by another playbook, if the desire is to automate the action).

When you change the enforcement state of a firewall rule, or when you create a new rule that is enforced, the change applies to new connections only. [Existing connections are not affected by the change.](#)

Optionally, you can disable the Playbook Block Simulator. Make sure to manually remove the quarantine tag from the VM before proceeding.

Case Playbooks

Navigate to the **Cases** screen, select one of the alerts that has a Google Cloud VM as an attacker (in this example, principal hostname cloudngfw-us-central1-a-client and principal IP 10.0.0.3) and click the **Playbooks** tab.



The GCP Threat Response Playbook is automatically run, and will enrich the logs and associate tags among other actions. Click through the different blocks to explore further.

gcp_ngfw_enterprise_threats

ID 38

Default Environment

Triage

2024-11-07 20:30:36

THREAT

GCP

Manage Tags

1. GCP_NGFW_ENTERPRI... (1)

2. GCP_NGFW_ENTERPRI... (1)

3. GCP_NGFW_ENTERPRI... (1)

Overview

Events (1)

Playbooks (1)

Graph

Playbooks (1)

✓ GCP Threat Response Playb...

Write a comment...

THREAT TAG

Shared_Simplify_1

2024-11-07 15:58:20

Target Entities

CLOUDNGFW-US-CENTRAL1-A-WWW

CLOUDNGFW-US-CENTRAL1-A-CLIENT

IP 10.0.0.3

IP 10.0.0.2

Action Parameters

Action: Result

NAME	VALUE
Tag	THREAT

Outcome

The tag [THREAT] was added to the case

View Result

Add a Playbook

×

Playbooks

Show

All Playbooks

▼

×

ngfw

NGFW GCP Set Secure Tag

Playbook Description

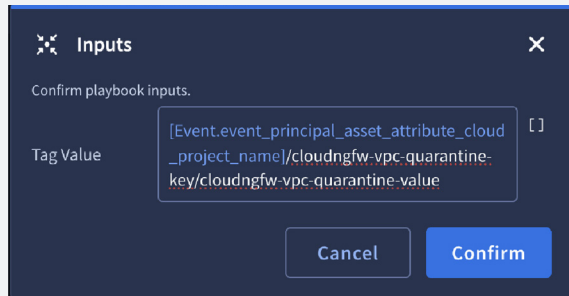
A playbook block that will add a project-level secure tag to the principal VM.

Cancel

Add

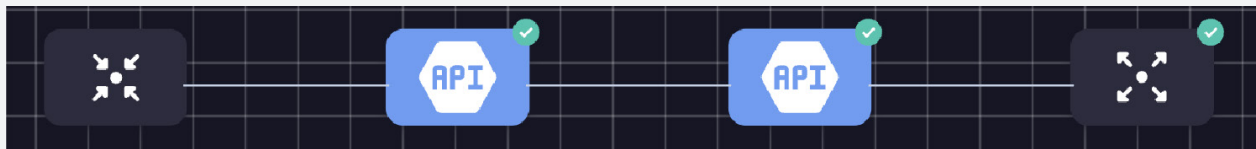
Click +, search for the Playbook Block you created, and click **Add**.

25



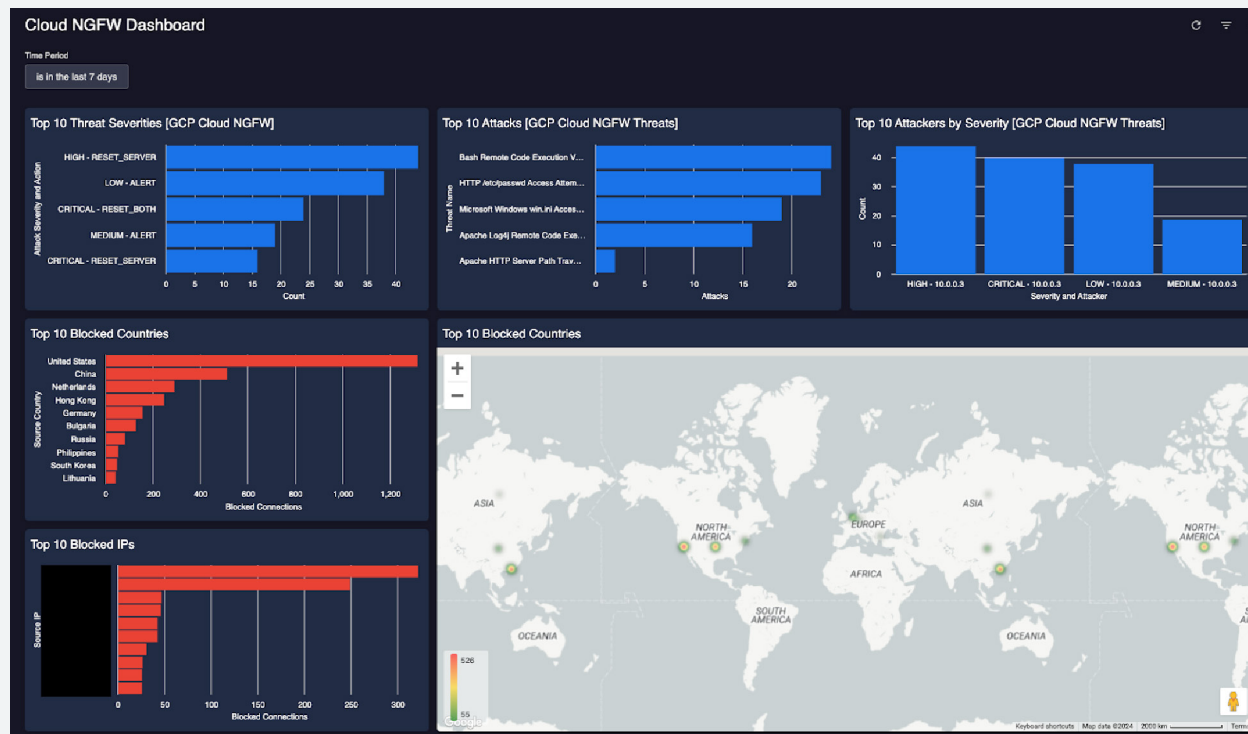
A new window will open.
Do **not** change the tag value.
Click **Confirm**.

The playbook block should successfully run (check that green checkboxes are shown) and add the quarantine tag to the VM. Click through the blocks to view the results.



Custom Dashboards

[Custom dashboards](#) can be created to provide specific insights into the data (as shown in the following example). You should generate sample traffic to make sure logs are being successfully ingested before creating dashboards. [UDM fields](#) can be used to specify the data to be filtered.



Top 10 Threat Severities widget (example)

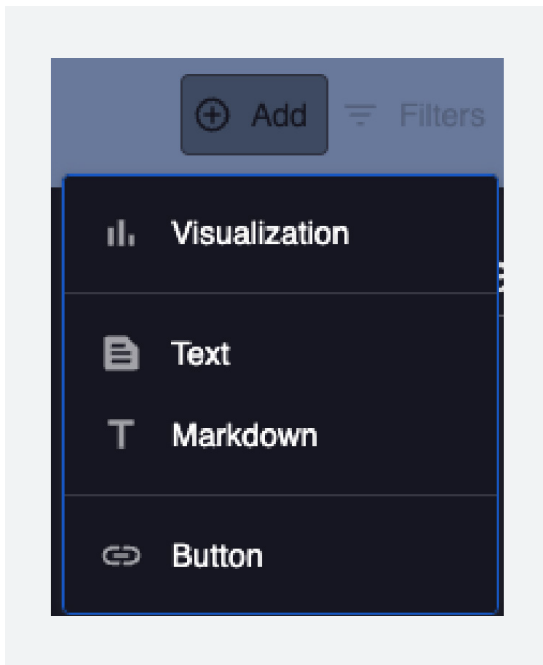
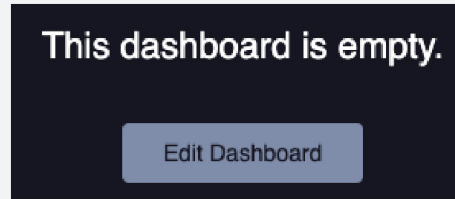
This section outlines how to create a dashboard with a widget that contains data related to the top 10 threat severities.



To create a [custom dashboard](#), in the [Security Operations console](#), navigate to **Dashboards & Reports > SIEM Dashboards**. For **Personal Dashboards** or **Shared Dashboards**, click **Add > Create New**.



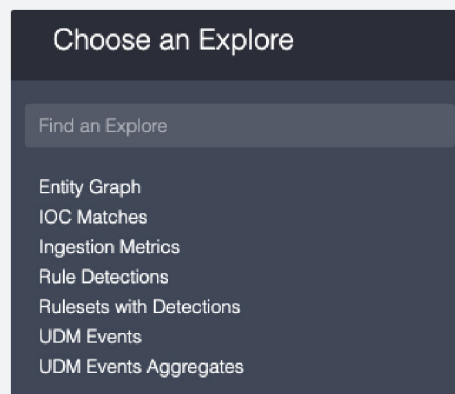
To add a widget to this new dashboard, click **Edit Dashboard**.



Click **Add > Visualization** to add a new widget.

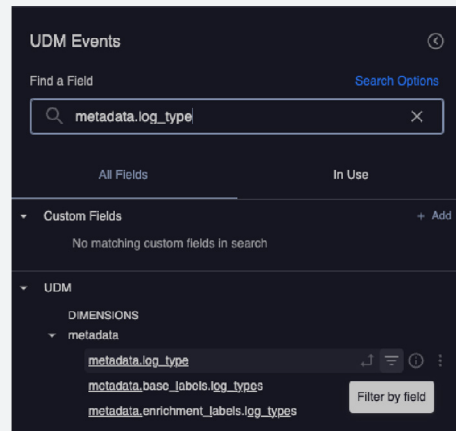


Select **UDM Events**.

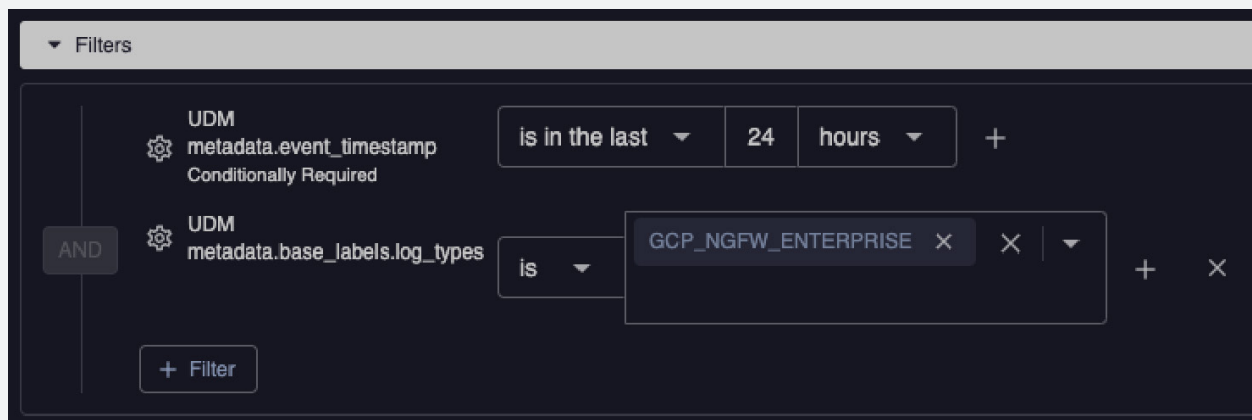




Search for the `metadata.log_type` field.
Hold your cursor over the result and
≡ select **Filter by field**.

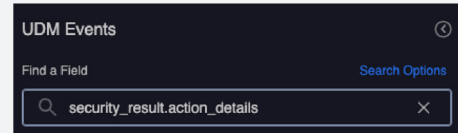


Type or select `GCP_NGFW_ENTERPRISE` as the value for this field.



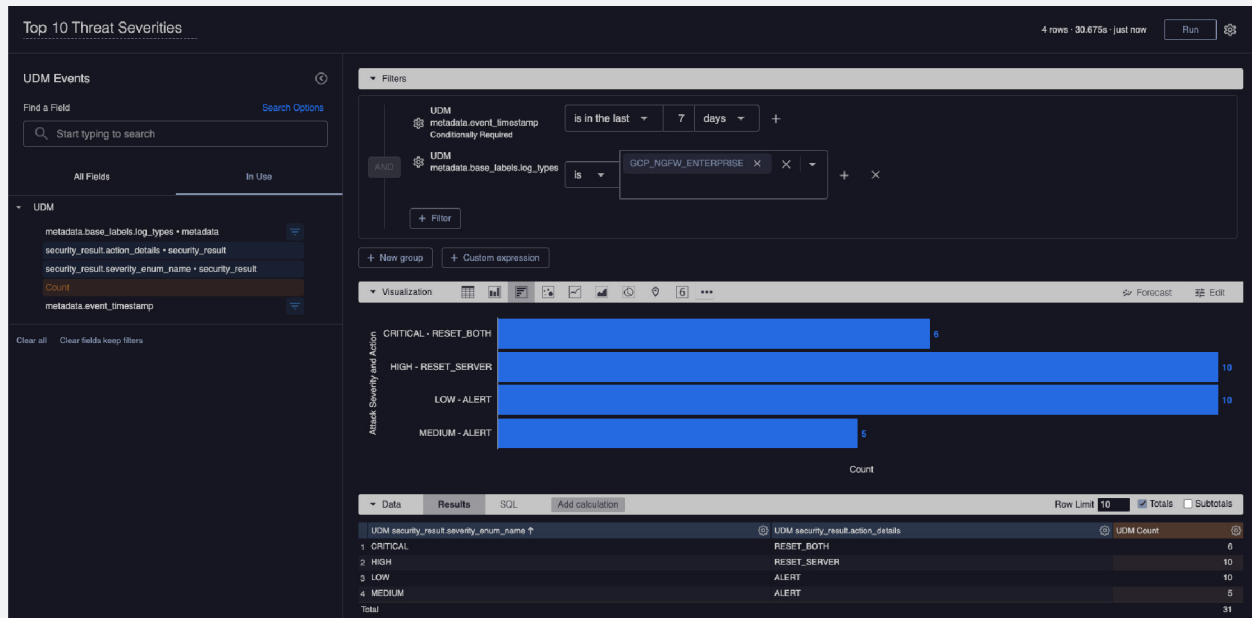


Search for the `security_result.action_details` field and click to select it. This field is added under **Data** on the right side.



Repeat this step to add both `security_result.severity_enum_name` and Count (under the **Measures** category).

Under the **Filters** category, adjust the timestamp, as needed. For the Data category, set the row limit to 10 and select the **Totals** checkbox. Then, click **Run** to verify that the data was populated.



Once you are happy with the result, retitle the widget and click **Save**.

Add additional widgets and customize your dashboard to suit your needs. Then, retitle and save the dashboard.



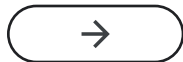
Tip: Click Duplicate Tile to create a copy of an existing widget.

The following sections outline the filters and fields you can use to create additional widgets, as shown in the earlier dashboard example

Cloud NGFW Enterprise Sample Widgets

This section outlines how to create a dashboard with a widget that contains data related to the top 10 threat severities.

Top 10 Threat Severities



Filters:

`metadata.log_type=GCP_NGFW_ENTERPRISE`

Fields:

`security_result.action_details`

`security_result.severity_enum_name [count]`

Top 10 Attacks



Filters:

`metadata.log_type=GCP_NGFW_ENTERPRISE`

Fields:

`security_result.threat_name`

`security_result.severity_enum_name [count]`

Top 10 Attackers by Severity



Filters:
metadata.log_type=GCP_NGFW_ENTERPRISE
Fields [count]:
principal.ip
security_result.severity_enum_name [count]

Cloud NGFW Sample Widgets

Top 10 Blocked Countries [Ingress]



Filters:
metadata.log_type=GCP_FIREWALL
security_result.action_details=DENIED
Fields:
principal.ip_geo_artifact.location.country_or_region

Top 10 Blocked Countries Map [Ingress]



Filters:
metadata.log_type=GCP_FIREWALL
security_result.action_details=DENIED
Fields:
principal.ip_geo_artifact.location.country_or_region
principal.ip_geo_artifact.location.location

Top 10 Blocked IPs [Ingress]



Filters:

`metadata.log_type=GCP_FIREWALL`

`security_result.action_details=DENIED`

Fields:

`principal.ip`

Google Cloud

