Google Cloud Platform

Detection Strategy Guide

June 2025

Product Overview

Google Cloud Platform (GCP) is a major cloud infrastructure provider that provides many products and services that rival Amazon's AWS. The Expel overall strategy for GCP includes supporting the GCP native detection service, Event Threat Detection (ETD), while also providing monitoring coverage for areas, products, and services that the native detection service doesn't monitor. Expel Workbench consumes events from the Admin Activity audit logs through the GCP Pub/Sub service and uses detection rules to identify events which can present security risks to our customers.

Detection Strategy for Cloud Integrations

Detection

Our cloud security detection strategy focuses on two common signal types at the control plane and resource levels: authentication events and API events. In limited cases, we also ingest certain data plane events such as network activity. We do this by integrating directly with cloud providers as well as cloud security service providers to gain a complete view of your cloud footprint.

We consume these events through a mix of raw log analysis and security alert processing, which are then run through our detection engine to look for signs of post-exploitation activity. When a threat is detected, our automated response bot, Ruxie, takes action by enriching evidence fields with first- and third-party threat intelligence. Additional Ruxie actions query a wide span of technologies in order to directly arm analysts with key pieces of investigative information and related events.

Response

In addition to verbose evidence collection for cloud alerts, cloud technologies are useful for triaging SaaS and identity alerts as well. User activities within the cloud providers, along with related alerts for anomalous indicators, help analysts gain a full picture of the activity that occurred within a session.

To learn more about our overall approach to detection strategy, see About Detection Strategy in the Help Center.

What We Support for Google Cloud Platform

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for Google Cloud Platform, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ Event Threat Detection (includes Container Threat Detection) ■ Cloud IAM ■ Cloud Compute ■ Cloud Endpoint ■ Cloud Function ■ Cloud App Engine ■ Cloud Storage ■ Cloud SQL ■ Cloud VPC ■ KMS ■ BigQuery ■ Logging ■ Container Registry
Supported event log sources	■ Event Threat Detection (includes Container Threat Detection) ■ Cloud IAM ■ Cloud Compute ■ Cloud Endpoint ■ Cloud Function ■ Cloud App Engine ■ Cloud Storage

	■ Cloud SQL ■ Cloud VPC ■ KMS ■ BigQuery ■ Logging ■ Container Registry
Google Cloud Platform detection rules support	Yes.
Detection rules written by Expel	Yes.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query IP ■ Query user ■ Query raw logs ■ Query logs ■ Interacted Services: provides stats on GCP resources interacted with by the alerted user within the last 7 days. ■ API Authentication Trends: provides authentication trends (Source IP and UserAgent pairs) used by the alerted user in the last 7 days. ■ Interesting API Calls: shows any non-(Get|List|Describe|Head) API calls from Admin Activity audit log used by the alerted user in the last 7 days. ■ Service Account Delegations: shows information on the use of service accounts in the last 7 days by the alerted principal user. ■ Organization Resource Interactions: shows stats based on where the alerted principal user spends most of their time within the organization hierarchy. For example, what projects the user mostly interacts with.
Hunting support	Yes. Hunting is available for this integration to

	customers who purchase this option. Contact your Sales or Support rep for help understanding the hypotheses and objectives for each hunting technique. For a full list of techniques by integration, see Hunting Techniques in the Help Center.

Additional Details and Common Questions

Console Access

A vendor alert does not typically include all of the contextual timeline activity surrounding the event of interest. Because this integration does not allow us to get all necessary data via the API, we will ask you for a certain level of console access during onboarding.

The level of access that we require is meant to support essential triage and research activities, and to help us determine the vector and extent of attacker activity for an identified threat. At minimum, we will ask for visibility into alert data, timeline events recorded, and live response/real time response shell (if applicable).

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.

Use Cases Not Supported

Use Case	Description	Why it's not supported
Expel detections using Data Access audit logs	Data Access audit logs generate log events from the resource interaction plane of GCP. This tells	To generate these logs, GCP customers must pay $0.50 /GiB to enable these logs by GCP

	our SOC analysts who accessed or modified a resource. For example, who and when someone accessed data within a storage bucket.	service. These logs can be voluminous, sometimes generating upwards of a TB per day. Monitoring these logs is cost-prohibitive for most of our customers.
Arbitrary command execution through OS Config	GCP has a service named OS Config, which is an agent-based endpoint management tool. Its primary purpose is to enable easy patch management and endpoint configuration on Compute instances with the agent. An attacker using an account with proper permissions can arbitrarily execute commands across a fleet of Compute instances with the OS Config agent. An explicit example is an attacker mass-deploying backdoors and/or malware across systems managed by OS Config.	The OS Config service doesn't have sufficient logging to monitor its usage or what commands are executed through it.
Cloud Storage exfiltration to an attacker-owned Cloud Storage bucket.	The GCP Transfer Service allows for the mass transfer of data from one GCP Cloud Storage bucket to another. A threat actor can use this service to clone the entire contents of a Cloud Storage bucket to a Cloud Storage bucket in a GCP account they own.	The Transfer Service doesn't log when an overall transfer is committed nor what its destination is. All that's logged is the Transfer Service service account reading objects from the Cloud Storage bucket data is being exfiltrated from.