Google Kubernetes Engine

Detection Strategy Guide

July 2025

Product Overview

Google Kubernetes Engine (GKE) is a managed Kubernetes service that allows for the deployment and operation of containerized applications on Google's infrastructure. Drawing on Google's experience with its internal cluster manager, Borg, GKE automates cluster lifecycle management, including auto-scaling, auto-upgrades, and node auto-repair to enhance reliability and reduce operational burden. GKE offers two modes of operation: Autopilot, which provides a fully managed, hands-off experience by managing the underlying nodes, and Standard, for users who require more granular control over their node configurations. The platform is designed for production workloads, integrating with Google Cloud's security and observability tools to provide a secure and scalable environment for applications ranging from simple web services to complex AI/ML workloads.

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.

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.

What We Support for Google Kubernetes Engine

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 Kubernetes Engine, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported platforms	■ Google Cloud Platform
Supported event log sources	■ Kubernetes Audit Events via Cloud Logging
Google Kubernetes Engine detection rules support	Yes.
Detection rules written by Expel	Yes.
Auto remediations	No.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events: ■ DescribeCluster - Get details about the provided GKE cluster ■ DescribePod - Get details about the provided pod in a GKE cluster ■ DescribeRole - Get details about the provided Role in a GKE cluster ■ DescribeRoleBinding - Get details about the provided RoleBinding in a GKE cluster ■ DescribeClusterRole - Get details about the provided ClusterRole in a GKE cluster ■ DescribeClusterRoleBinding - Get details about the provided ClusterRoleBinding in a GKE cluster
Hunting support	No. Hunting is not currently available for this integration.

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.