Detecting Google Cloud Platform (GCP) cross-account activity

Applicability

- Product: Splunk Cloud Platform or Splunk Enterprise
- Feature: Monitoring
- Technology: Splunk Add-on for Google Cloud Platform
- Data: Google Cloud Platform

Scenario

You are a Google Cloud Platform (GCP) admin who manages access to GCP resources and services across your organization using GCP Identity and Access Management (IAM) functionality. As part of your role, you need to be able to track when a user assumes an IAM role in another GCP account to obtain cross-account access to services and resources in that account. Accessing new roles could be an indication of malicious activity that you need to monitor closely.

IAM provides the ability to create and manage GCP users, groups, and roles-each with their own unique set of privileges and defined access to specific resources (such as Compute instances, the GCP Management Console, API, or the command-line interface). Unlike conventional (human) users, IAM roles are potentially assumable by anyone in the organization. They provide users with dynamically created temporary security credentials that expire within a set time period.

However, problems can occur in between the time when the temporary credentials are issued and when they expire. This gap represents a window of opportunity for a malicious actor to leverage the temporary credentials to spin up or remove instances, create new users, elevate privileges, and perform other malicious activities throughout the environment.

These searches are designed to help you monitor your GCP Audit logs logs for evidence of suspicious cross-account activity. For example, while accessing multiple GCP accounts and roles may be perfectly valid behavior, it may be suspicious when an account requests privileges of an account it has not accessed in the past.

- To run these searches, install the Splunk Add-on for Google Cloud Platform. These searches work with gcp:pubsub:message logs.
- Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.
Detection searches

► GCP accounts with high risk roles by project

This search provides detection of accounts with high risk roles by projects. Compromised accounts with high risk roles can move laterally or escalate privileges at different projects, depending on your organization’s schema.

This search may result in some false positives. Accounts with high risk roles should be reduced to the minimum number needed. However, specific tasks and setups may be expected behavior within your organization.

| search (sourcetype="google:gcp:pubsub:message" ("data.protoPayload.request.policy.bindings{}.role"=roles/owner OR roles/composer.admin OR roles/dataflow.admin OR roles/dataflow.developer OR roles/dataproc.admin OR roles/dataproc.editor OR roles/editor OR roles/iam.serviceAccountAdmin OR roles/iam.serviceAccountTokenCreator OR roles/iam.serviceAccountUser)) | table "data.resource.type", "data.protoPayload.authenticationInfo.principalEmail", "data.protoPayload.authorizationInfo{}.permission", "data.protoPayload.authorizationInfo{}.resource", "data.protoPayload.response.bindings{}.role", "data.protoPayload.response.bindings{}.members{}"

► GCPloit exploitation framework

This search provides detection of the GCPloit exploitation framework. This framework can be used to escalate privileges and move laterally from compromised high privilege accounts.

This search may result in some false positives since the Payload.request.function.timeout value can possibly be matched with other functions or requests. However, the source user and target request account may indicate an attempt to move laterally across accounts or projects.

| search ("data.protoPayload.request.function.timeout"=539s sourcetype="google:gcp:pubsub:message") | table src, src_user, "data.resource.labels.project_id", "data.protoPayload.request.function.serviceAccountEmail", "data.protoPayload.authorizationInfo{}.permission", "data.protoPayload.request.location", http_user_agent

► High risk GCP permissions by resource and account

This search provides detection of high risk permissions by resource and accounts. These are permissions that can allow attackers with compromised accounts to move laterally and escalate privileges.

This search may result in some false positives since high risk permissions are part of any GCP environment. However, it is important to track resource and accounts usage.

| search (sourcetype="google:gcp:pubsub:message" ("data.protoPayload.authorizationInfo{}.permission"=iam.serviceAccounts.getaccesstoken OR composer.environments.create OR dataflow.jobs.create OR dataproc.clusters.create OR iam.serviceAccounts.actas OR iam.serviceAccounts.setiamPolicy)) | table "data.protoPayload.requestMetadatta.callerIp", "data.protoPayload.authenticationInfo.principalEmail", "data.protoPayload.authorizationInfo{}.permission", "data.protoPayload.response.bindings{}.members{}", "data.resource.labels.project_id"
GCP Oauth token abuse

This search provides detection of possible GCP Oauth token abuse. GCP Oauth tokens without time limits can be exfiltrated and reused to keep access sessions alive without further control of authentication, allowing attackers to access and move laterally.

```bash
```

Additional resources

This use case is included within Splunk Enterprise Security, a Splunk app that provides prebuilt content and searches to help answer root-cause questions in real-time about malicious and anomalous events in your IT infrastructure. In addition, Splunk Enterprise Security provides a number of other searches to help reinforce your Cloud Security posture, including:

- Detecting AWS cross-account activity
- Detecting AWS network ACL activity
- Detecting AWS suspicious provisioning activities
- Monitoring user activity spikes in AWS
- Monitoring AWS EC2 for suspicious login activities
- Monitoring AWS S3 for suspicious activities
- Monitoring AWS for suspicious traffic
- Monitoring AWS EC2 for unusual modifications

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.