CADO//

GCP Cheat sheet

Introduction

With the rapid migration to the cloud, it's becoming increasingly difficult to keep track of all of the different data sources, commands, and tools available from each Cloud Service Provider (CSP). This cheat sheet is designed to provide an overview of key best practices, data sources and tools that you should have at your disposal when responding to an incident in a Google Cloud Platform (GCP) environment.

About Cado Security

Cado Security is the provider of the first cloud forensics and incident response platform. The platform leverages the scale and speed of the cloud to automate the end-to-end incident response process – from data capture and processing to investigation and response. Cado enables security teams to gain immediate access to forensic-level data in multi-cloud, container, and serverless environments to enable rapid response.

Open source tools

There are a number of community tools for responding to incidents in GCP:

- Cloud Forensic Utils - A Python-based toolkit for extracting evidence from virtual machines
- Prowler - Can be used for best practices assessments, audits, incident response, continuous monitoring, hardening and forensics readiness.
- SANS SIFT toolkit - Collection of free and open-source incident response and forensic tools
- Security monkey - Monitors cloud accounts for policy changes.
- Cartography - Creates maps of infrastructure

Useful Commands:

Authentication:

- gcloud auth login: Initiates the OAuth 2.0 authorization flow for authenticating the GCP CLI.
- gcloud config set project PROJECT_ID: Sets the default GCP project.

Cloud Storage:

- gsutil ls gs://bucket: Lists objects in a Cloud Storage bucket.
- gsutil cp local_file gs://bucket: Copies a file to Cloud Storage.
- gsutil rm gs://bucket/object: Deletes an object in Cloud Storage.

Compute Engine:

- gcloud compute instances list: Lists all Compute Engine instances.
- gcloud compute ssh instance_name: Connects to a Compute Engine instance via SSH.
- gcloud compute instances reset instance_name: Resets a Compute Engine instance.

Cloud Logging:

- gcloud logging logs list: Lists all logs in the current project.
- gcloud logging read "logName=projects/PROJECT_ID/logs/LOG_NAME" --limit=10: Reads recent log entries for a specific log.
- gcloud logging write "MESSAGE" --severity=LEVEL: Writes a log entry to Cloud Logging.

Cloud Monitoring:

- gcloud monitoring dashboards list: Lists all Cloud Monitoring dashboards.
- gcloud monitoring dashboards describe dashboard_id: Describes a specific Cloud Monitoring dashboard.
- gcloud monitoring metrics list --project=PROJECT_ID: Lists available metrics for a project.

Cloud IAM (Policy):

- gcloud projects get-iam-policy PROJECT_ID: Retrieves the IAM policy for a project.
- gcloud projects add-iam-policy-binding PROJECT_ID --member=MEMBER --role=ROLE: Adds a new IAM policy binding.

Cloud IAM:

- gcloud iam list-grantable-roles: Lists roles that can be granted in a resource hierarchy.
- gcloud iam roles describe ROLE_ID: Describes a specific IAM role.
- gcloud organizations get-iam-policy ORGANIZATION_ID: Retrieves the IAM policy for an organization.

VPC Networking:

- gcloud compute networks list: Lists all VPC networks in the current project.
- gcloud compute firewall-rules list: Lists all firewall rules in the current project.
- gcloud compute addresses list: Lists all IP addresses in the current project.

Cloud Functions:

- gcloud functions list: Lists all Cloud Functions in the current project.
- gcloud functions logs read FUNCTION_NAME: Reads logs for a specific Cloud Function.
- gcloud functions describe FUNCTION_NAME: Describes a specific Cloud Function.

Cloud DNS:

- gcloud dns managed-zones list: Lists all managed DNS zones.
- gcloud dns record-sets list --zone=ZONE_NAME: Lists DNS records in a managed zone.
- gcloud dns changes list --zone=ZONE_NAME: Lists recent changes to a managed zone.

Cloud Identity Platform:

- gcloud beta identity-platform users list: Lists users in Cloud Identity Platform.
- gcloud beta identity-platform providers list: Lists identity providers configured for Cloud Identity Platform.
- gcloud beta identity-platform policies describe POLICY_NAME: Describes an Identity Platform policy.

Cloud Security Command Center (Cloud SCC):

- gcloud scc assets list: Lists all assets in Security Command Center.
- gcloud scc sources list: Lists all Security Command Center sources.
- gcloud scc findings list: Lists findings from Security Command Center.

Logs

The best way to view logs is by using the Google Cloud Console Log Explorer page. However, you can also download the logs in CSV format by simply pulling them from the bucket they are stored in. Google's cloud audit logs are broken down into four categories:

Admin Activity Audit Logs

- Contains log entries for API calls or other administrative actions that modify the configuration or metadata of resources.
- Admin Activity audit logs are always written and you can't configure or disable them in any way.

System Event Audit Logs

- Contains log entries for administrative actions taken by Google Cloud that modify the configuration of resources.
- System Event audit logs are always written so you can't configure or disable them.
- There is no additional charge for your System Event audit logs.

Data Access Audit Logs

- Contains API calls that read the configuration or metadata of resources, including user-driven API calls that create, modify, or read user-provided resource data.
- You must explicitly enable Data Access audit logs to be written. They are disabled by default because they are large.

Policy Denied Audit Logs

- Contains logs when a Google Cloud service denies access to a user or service account triggered by a security policy violation.
- Policy Denied audit logs are generated by default. Your cloud project is charged for the logs storage.

If you'd like to learn more about what Cado Security is doing to help advance investigations and incident response in the cloud, request a demo today.

Further Reading and Resources:

How to conduct live network forensics in GCP

Google Cloud security best practices center

Google Cloud forensics best practices and tools

Getting started with Cloud Security Command Center

Google Cloud: Cloud Forensics 101

GCP Security Foundations Blueprint

Google Cloud Better Practices for Cloud IAM

Security Command Center Gcloud Commands

Google Cloud Architecture Framework: Security, privacy, and compliance