Detecting unusual GCP service account usage

Scenario: You started off using just a few components in your GCP system, but over time that usage expanded across a wider variety of services and use cases. This makes it important for you to monitor how usage changes over time and to set up alerting mechanisms that will notify the security team when unexpected access occurs.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Threat hunter
- Technologies:
  - Splunk Enterprise
  - Splunk SOAR
  - Playbook: Azure new user census
- Data: Azure Active Directory

How to use Splunk software for this use case

The playbook checks whether there is a service account and a Compute VM or just a service account. Metadata about the keys owned by that service account are gathered using the GCP IAM app, and if there is a Compute VM instance, the playbook gathers metadata about that as well. After gathering this data, format blocks are used to compile it into a prompt, and the analyst is asked whether to delete the associated service account keys and stop the Compute instance, if applicable. To use the playbook:

1. Ensure that your Splunk Enterprise deployment is ingesting GCP logs.
2. Ensure that Splunk Enterprise is configured to send alerts to Splunk SOAR.
3. In Splunk Enterprise, set up a detection to trigger this use case. For example, you might trigger on potentially destructive API methods executed using the Compute service, such as “stop,” “setMetadata,” or “delete”.

   `sourcetype="google:gcp:pubsub:message" tag=compute "data.protoPayload.methodName" IN ("*stop", "*setMetadata", "*delete") | rex field="data.resource.parentDisplayName" ".*/(?<KeyName>.*)$" | rename "data.protoPayload.authenticationInfo.principalEmail" AS KeyName | transaction KeyName`

   The transaction command is used to group together events with the same key name to prevent the playbook from running multiple times for the same account. To reduce false positives, you could also introduce a lookup file that would exclude specific accounts that are allowed to use these API methods.
4. Use the “Send to Phantom” action or an event forwarding search to automatically forward events to Splunk SOAR.

5. Set up the Google Cloud IAM and Google Cloud Compute Engine apps on Splunk SOAR:
   2. Give the asset a name such as “google_cloud_iam”.
   3. On the Asset Settings page, provide the service account JSON and project ID.
   4. Save and test connectivity to make sure the asset is functional.
   5. Follow similar steps for the Google Cloud Compute Engine app.

6. Synchronize the playbook list with the community repository, then find and activate the GCP Unusual Service Account Usage playbook using the label created for Splunk Enterprise alerts.

Results

After your GCP are streamed to Splunk Enterprise, the security team can start to detect usage of service accounts that does not fit into expected patterns. This could be an API method that should not be executed from a certain account, an instance created in a new region that should not be used, or any other behavior that can be defined based on metadata in the GCP audit log. As expected usage changes over time, one or more searches can be updated to reduce the false positive rate or continue to enforce the principle of least privilege across user accounts and services. By leveraging Splunk SOAR to automatically monitor new accounts and detect malicious conduct within cloud platforms like GCP, you can add another line of defense to prevent threat actors from exfiltrating sensitive information.

Aside from the particular API methods listed in the SPL search for this detection, there is nothing limiting this detection and response pattern to just the Compute service in GCP. Detections from Google Security Command Center could also be used to trigger Splunk SOAR.

On the response side, the options for expansion include a wide range of options both within GCP and elsewhere in the organization. The main areas to focus on in GCP tend to be service accounts, compute instances, and object storage. Elsewhere in the organization there are opportunities to add threat intelligence integrations, ticket creation, endpoint detection and response workflows, and correlation with identity systems such as Okta or Active Directory.

Additional resources

These additional Splunk resources might help you understand and implement this use case:

- Blog: Splunk SOAR Playbooks: GCP Unusual Service Account Usage
- Docs: Use the Splunk Phantom App for Splunk to forward events
- Tech Talk: GCP unusual service account usage

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.