Google Cloud

Guide to event threat detection

You've learned about how cloud security analysts monitor activity in their environments using tools and alerts. In this reading, you'll dive deeper into Security Command Center (SCC) features by exploring one of its log-based monitoring services, Event Threat Detection. You'll also learn how to trigger an Identity and Access Management (IAM) alert finding, and use Logs Explorer to query the logs associated with the triggered alert.

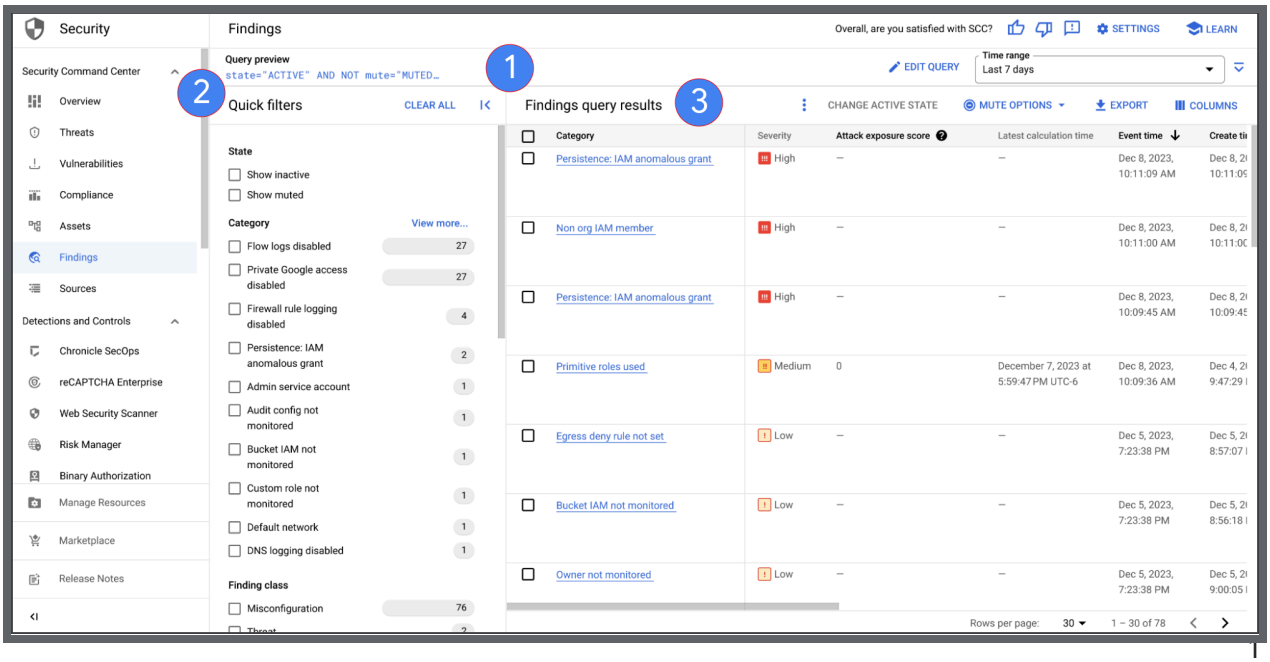
Event Threat Detection

As a quick reminder, SCC is Google Cloud's centralized vulnerability and threat reporting service. SCC uses *services* which scan Google Cloud resources to detect security issues, like vulnerabilities and misconfigurations. One of SCC's built-in services includes Event Threat Detection. The Event Threat Detection service provides log-based threat analysis that continuously monitors Google Cloud logs to scan for potential threats. When Event Threat Detection finds a threat, it displays the finding in SCC.

Note: Security Command Center has two service tiers: Standard and Premium. The tier type determines which built-in services and their features are available to use. In this program, the labs provide you with access to the Premium tier.

Findings

SCC's Findings page displays findings that Event Threat Detection generates.



When you create a query, you must specify the required settings and set any optional settings that define what the query does. These settings include the following:

1. **Query editor**: Add and edit filters to your queries, and search for findings based on their property or attribute values. Common filters include the presence of values, the absence of values, or the matching of a partial string. For example, this query, state="ACTIVE" AND NOT mute="MUTED" displays all active findings that are not muted. You can also adjust the query's time range using the time range field.
2. **Quick filters**: Select and add one or more predefined attribute filters to a query.
3. **Finding query results**: Displays the findings. Click a finding to access its details. Findings can have the following properties:
    - **Category**: Provides the name of the finding type. For example, **Persistence: IAM anomalous grant** relates to the category of Identity and Access Management (IAM).
    - **Severity**: Relates the severity of the finding: **critical, high, medium, low,** or **unspecified.**
    - **Attack exposure score**: Marks the attack exposure score of the finding. This score tells you how much the security issue in the finding exposes critical resources to potential threats.
    - **Event time**: Tells the timestamp of when the finding was first detected or when it was last updated.
    - **Create time**: Tells the timestamp of when the finding was created in SCC.
    - **Resource display name**: Provides the display name of the resource in which the issue was detected.
    - **Resource full name**: Provides the full name of the resource in which the issue was detected.
    - **Resource path**: Identifies the path to the resource in which the issue was detected.
    - **Resource type**: Relates the type of resource in which the issue was detected.
    - **Security marks**: Assigns any security marks that are added to the finding.
    - **Finding class**: Relates the class to the finding: **threat, vulnerability, misconfiguration, observation, SCC error,** or **finding class unspecified.**

Trigger an IAM detector

Event Threat Detection identifies threats and generates findings using detection rules also known as *detectors*. These rules define the specific type of threat and logs that Event Threat Detection uses to identify threats. In the upcoming lab, you'll intentionally generate activity to trigger the **Persistence: IAM anomalous grant** detector to record a finding in SCC. This

finding will indicate that an anomalous IAM grant was detected, which can be a potential indication of a malicious actor attempting to gain unauthorized access to a cloud environment. An example of an anomalous grant is inviting an external user, with a gmail.com email account, to a Google Cloud project as a project owner.

To trigger this finding in this lab, you'll assign a project *owner* role to the external user bad.actor.demo@gmail.com. The external user is a one that exists outside of the qwiklabs.net organization.

Note: In the lab, two student user accounts are configured for the qwiklabs.net organization: username 1 and username 2. Information about these two user accounts are in the **Lab Details** panel. These two users have owner roles to the lab project, which will trigger an alert finding. Username 2 will trigger a benign **Persistence: IAM anomalous grant** finding automatically in the background as part of the lab provisioning process. You operate with username 1, which will trigger a genuine **Persistence: IAM anomalous** grant finding by granting access to **bad.actor.demo@gmail.com**.

Analyze the findings in SCC

After you trigger the IAM detector, you can access the details in the SCC's Findings page. Click a finding to access a detailed view, which includes the following tabs that you can select to learn more about a finding and take action:

- **Summary** tab: This is the default view and highlights key information and attributes about the finding.
- **Source properties** tab: This displays the finding's **sourceProperties object** attributes JSON. In the lab, you'll use this tab to examine the **properties** field details, which lists information about the user's action, user's assigned role, and the user's email address.
- **JSON** tab: This is where you can see the full JSON format of the finding.

Query logs using Logs Explorer

Recall that you can use Logs Explorer to filter logs. In the lab, you'll run the following query:

```
Unset
protoPayload.authorizationInfo.permission="resourcemanager.projects.setIamPolicy"
protoPayload.methodName="InsertProjectOwnershipInvite"
```

- protoPayload.authorizationInfo.permission="resourcemanager.projects.setIamPolicy"

This line filters for logs with attempts to set the IAM policy for a project. This permission grants the ability to modify the roles and permissions assigned to users, groups, and service accounts for a specific project.

- protoPayload.methodName="InsertProjectOwnershipInvite"

This line filters for logs related to InsertProjectOwnershipInvite, with attempts to invite users or groups to become owners of a project.

Combined, this query searches for logs related to attempts to grant ownership of a project, which can be useful for to investigate events where a user tried to invite new owners to a project.

Key takeaways

Knowing how to investigate security events and potential security incidents using log details will help you add context to findings to help you understand what happened during a potential attack.

Resources for more information

- For more information about the Event Threat Detection service, visit Overview of Event Threat Detection.
- To learn more about how to create and edit queries in SCC, check out Query findings in the Google Cloud console.