Using Security Command Center security marks

This guide describes how to use security marks in Security Command Center. Security marks, or just "marks", enable you to annotate assets or findings in Security Command Center and then search, select, or filter using the mark. You can provide ACL annotations on assets and findings using security marks. Then you can group them by these annotations for management, policy application, or integration with workflow. You can also use marks to add priority, access level, or sensitivity classifications.

Before you begin

To add or change security marks, you must have a Cloud Identity and Access Management (Cloud IAM) role that includes permissions for the kind of mark that you want to use:

- Asset marks: **Asset Security Marks Writer**, `securitycenter.assetSecurityMarksWriter`
- Finding marks: **Finding Security Marks Writer**, `securitycenter.findingSecurityMarksWriter`

Security marks, labels, and tags

Security marks are unique to Security Command Center and only exist in the Security Command Center database. Cloud IAM permissions apply to security marks, and they are restricted to only users who have the appropriate Security Command Center roles. Reading and editing marks require the Security Center Asset Security Marks Writer and Security Center Finding Security Marks Writer roles. These roles don't include permissions to access the underlying resource.

Security marks enable you to add your business context for assets and findings. Labels and tags are similar kinds of metadata that are available through Security Command Center, but

they have a slightly different use and permissions model. Because Cloud IAM roles apply to security marks, they can be used to group and enforce policies on both assets and findings.

Labels (https://cloud.google.com/resource-manager/docs/creating-managing-labels) are user-level annotations that are applied to specific resources and are supported across multiple Google Cloud products. Labels are primarily used for billing accounting and attribution.

Tags (https://cloud.google.com/vpc/docs/add-remove-network-tags) are also a user-level annotation, specific to Compute Engine resources. Tags are primarily used to define security groups, network segmentation, and firewall rules.

Reading or updating labels and tags is tied to the permissions on the underlying resource. Labels and tags are ingested as part of the resource attributes in the Security Command Center assets display. You can search for specific label and tag presence, and specific keys and values, during post-processing of List API results.

Using security marks

You can use security marks to group, filter, define policy groups, or add business context to assets and findings in Security Command Center.

Security marks in the assets display

The following steps allow you to filter projects as assets that you group together under the same mark:

1. Go to the Security Command Center Assets (https://console.cloud.google.com/security/assets) page in the Cloud Console.
   GO TO THE ASSETS PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SECURITY/ASSETS)
2. Select the organization you want to review.
3. On the assets display that appears, under **resourceProperties.name**, select two or more projects that you want to mark.
4. On the **Info Panel**, under **Security Marks**, click **Add mark**.
   - If the info panel isn't displayed, click **Show Info Panel**.
5. Identify the projects by adding **Key** and **Value** items.

For example, if you want to mark projects that are in a production stage, add a key of "stage" and a value of "prod". Each project then has the new `mark.stage: prod`.

6. When you're finished adding marks, click **Save**.

The projects you selected are now associated with a mark. By default, marks display as a column in the assets display. To include or exclude specific marks in the assets display, select the mark name in the **Columns** drop-down list at the top of the displayed assets.

Security marks in the findings display

The following steps allow you to filter findings that you group under the same mark:

1. Go to the Security Command Center Findings (https://console.cloud.google.com/security/findings) page in the Cloud Console.

   GO TO THE FINDINGS PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SECURITY/FINDINGS)
2. Select the organization you want to review.
3. On the findings display that appears, under **Finding type**, select the type of finding you want to mark.
4. Under `category`, select two or more finding categories that you want to mark.
5. On the **Info Panel**, under **Security Marks**, click **Add mark**.
   - If the info panel isn't displayed, click **Show Info Panel**.
6. Identify the finding categories by adding **Key** and **Value** items.

   For example, if you want to mark findings that are part of the same incident, add a key of "incident-number" and a value of "1234". Each finding then has the new `mark.incident-number: 1234`.
7. When you're finished adding marks, click **Save**.

Managing policies

You can set marks on assets to explicitly include or exclude those resources from specific policies. For example, each Security Health Analytics detector has a dedicated mark type that enables you to exclude marked resources from the detection policy. This mark type provides granularity of control for each resource and detector.

What's next

- Learn more about using the assets display (https://cloud.google.com/security-command-center/docs/how-to-assets-display).
- Learn more about using findings (https://cloud.google.com/security-command-center/docs/how-to-findings).

Last updated January 7, 2020.