>

eature is in a pre-release state and might change or have limited support. For more information, see the product launc
s (/products/#product-launch-stages).

This page provides a list of reference guides and techniques for managing Security Health Analytics findings using Security Command Center.

A large organization might have many vulnerability findings across their deployment to review, triage, and track. By using Security Command Center with the available filters, you can focus on the highest severity vulnerabilities across your organization, and review vulnerabilities by asset type, security mark, and more.

To view a complete list of Security Health Analytics scanners and findings, see the Security Health Analytics findings (/security-command-center/docs/concepts-security-health-analytics-findings) page.

To view Security Health Analytics findings by project:

1. Go to the Security Command Center (https://console.cloud.google.com/security/command-center) in the Cloud Console.

   Go to the Security Command Center (https://console.cloud.google.com/security/command-center)

2. To display Security Health Analytics findings, click the **Vulnerabilities** tab.
3. In the **Projects Filter** box, click **Add a Project to the projects filter**, and then select the project that you want to display findings for.

The **Vulnerabilities** tab displays a list of findings for the project that you selected.

To view Security Health Analytics findings by category:

1. Go to the Security Command Center (https://console.cloud.google.com/security/command-center) in the Cloud Console.

   Go to the Security Command Center (https://console.cloud.google.com/security/command-center)

2. To display Security Health Analytics findings, click the **Vulnerabilities** tab.

3. In the **Finding Type** column, select the finding type that you want to display findings for.

The **Findings** tab loads and displays a list of findings that match the type you selected.

To view Security Health Analytics findings for a specific asset type:

1. Go to the Security Command Center Assets (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. Next to **View by**, click **Source Type**, and then select **Security Health Analytics**.

3. In the **Filter** box, enter `resourceName: asset-type`. For example, to display Security Health Analytics findings for all projects, enter `resourceName: projects`.

The list of findings updates to display all findings for the asset type that you specified.

To view Security Health Analytics findings by severity:

1. Go to the Security Command Center (https://console.cloud.google.com/security/command-center) in the Cloud Console.

   Go to the Security Command Center (https://console.cloud.google.com/security/command-center)

2. To display Security Health Analytics findings, click the **Vulnerabilities** tab.

3. Click the **Severity** column header to sort findings by the following values: `HIGH`, `MEDIUM`, `LOW`.

For more information about finding types, see Viewing vulnerabilities and threats (/security-command-center/docs/how-to-view-vulnerabilities-threats#security-health-analytics). Security Command Center also provides many built-in properties, including custom properties like security marks (/security-command-center/docs/how-to-security-marks).

After you filter by the vulnerabilities that are important to you, you can view detailed information about the finding by selecting the vulnerability in Security Command Center. This includes a description of the vulnerability and the risk, and recommendations for remediation.

You can add custom properties to findings and assets in Security Command Center by using security marks. Security marks enable you to identify high-priority areas of interest like production projects, tag findings with bug and incident tracking numbers, and more.

You can whitelist assets in Security Health Analytics so that a scanner doesn't create a security finding for the asset. When you whitelist an asset, the finding is marked as resolved when the next scan runs. This can be helpful when you don't want to review security findings for projects that are isolated or fall within acceptable business parameters.

To whitelist an asset, add a security mark `allow_`*`finding-type`* for a specific finding type. For example, for the finding type `SSL_NOT_ENFORCED`, use the security mark `allow_ssl_not_enforced:true`.

For a complete list of finding types, see the Security Health Analytics scanner list (#security-health-analytics-scanners) included earlier on this page. To learn more about security marks and techniques for using them, see Using Security Command Center security marks (/security-command-center/docs/how-to-security-marks).

You can use the Cloud Console or `gcloud` command-line tool commands to view active finding counts by finding type.

Using the `gcloud` command-line tool with the Security Command Center SDK enables you to automate anything you can do in the Security Command Center dashboard. You can also remediate many findings using the `gcloud` tool. For more information, review the documentation for the resource types described in each finding:

- Listing assets (/security-command-center/docs/how-to-api-list-assets)
- Listing security findings (/security-command-center/docs/how-to-api-list-findings)
- Creating, modifying, and querying security marks (/security-command-center/docs/how-to-api-add-manage-security-marks)
- Creating and updating security findings (/security-command-center/docs/how-to-api-create-manage-findings)
- Creating, updating, and listing finding sources (/security-command-center/docs/how-to-api-create-manage-security-sources)
- Configuring organization settings (/security-command-center/docs/how-to-api-configure-asset-discovery)

- Learn about Security Health Analytics scanners and findings (/security-command-center/docs/concepts-security-health-analytics-findings).
- Read recommendations for Security Health Analytics findings remediation (/security-command-center/docs/how-to-remediate-security-health-analytics).