>

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

This guide describes how to enable Security Health Analytics to write security findings from Google Cloud native scanners to Security Command Center. Findings from Security Health Analytics scanners are searchable in the Security Command Center dashboard and using the Security Command Center API. When Security Health Analytics is enabled, scans automatically run twice each day, 12 hours apart.

- To enable Security Health Analytics, you must have the **Security Center Admin** Cloud Identity and Access Management role.
- To access the Security Command Center dashboard, you must have the **Security Center Admin Viewer** Cloud IAM role.
- To make changes to Security Command Center, like adding marks, you must have an appropriate editor role, like **Security Center Admin Editor**.

Learn more about Security Command Center roles (/security-command-center/docs/access-control).

To view Security Health Analytics findings in Security Command Center, you enable it as a security source. This step requires the **Security Center Admin** Cloud IAM role.

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

   Go to the Security Sources page (https://console.cloud.google.com/security/settings/source-management)

2. Under **Enabled**, click to enable **Security Health Analytics**.

After you enable Security Health Analytics, you can view vulnerabilities in Security Command Center. Security Health Analytics scans automatically run twice a day, 12 hours apart.

The DISK_CSEK_DISABLED (/security-command-center/docs/concepts-security-health-analytics-findings#compute-instance-findings) scanner doesn't apply to all users. To use this scanner, you must mark the assets for which you want to use self-managed encryption keys.

To enable the DISK_CSEK_DISABLED scanner for specific assets, apply the security mark (/security-command-center/docs/how-to-security-marks) 'enforce_customer_supplied_disk_encryption_keys' to the asset with a value of 'true'.

- Learn about available scanners and how to use Security Health Analytics (/security-command-center/docs/how-to-manage-security-health-analytics).
- Read recommendations for Security Health Analytics findings remediation (/security-command-center/docs/how-to-remediate-security-health-analytics).
- Learn how to use Security Command Center security marks (/security-command-center/docs/how-to-security-marks).
- Learn more about Using Assets (/security-command-center/docs/how-to-assets-display) or Using Findings (/security-command-center/docs/how-to-findings).
- Learn more about Viewing vulnerabilities and threats (/security-command-center/docs/how-to-view-vulnerabilities-threats#security-health-analytics).