# Viewing vulnerabilities and threats in Security Command Center

This page provides information about the Google Cloud native *security sources* available in Security Command Center. When enabled, a security source provides vulnerability and threat data in the Security Command Center dashboard.

Security Command Center enables you to filter and view vulnerability and threat findings in many different ways, like filtering on a specific finding type, resource type, or for a specific asset. Each security source might provide more filters to help you organize your organization's findings.

For more information about how to use the Security Command Center dashboard, see using the assets display (https://cloud.google.com/security-command-center/docs/how-to-assets-display) and using findings (https://cloud.google.com/security-command-center/docs/how-to-findings).

## Vulnerabilities

Vulnerability scanners can help you find potential weaknesses.

### Security Health Analytics vulnerability types

**Beta**

This feature is in a pre-release state and might change or have limited support. For more information, see the product launch stages (https://cloud.google.com/products/#product-launch-stages).

Security Health Analytics (https://cloud.google.com/security-command-center/docs/how-to-enable-security-health-analytics) managed vulnerability assessment scanning for Google Cloud can automatically detect common vulnerabilities and misconfigurations across:

- Stackdriver Monitoring and Stackdriver Logging
- Compute Engine
- Google Kubernetes Engine containers and networks
- Cloud Storage
- Cloud SQL
- Cloud Identity and Access Management (Cloud IAM)
- Cloud Key Management Service (Cloud KMS)
- Cloud DNS

To get started with Security Health Analytics, follow the guide to Enable Security Health Analytics (https://cloud.google.com/security-command-center/docs/quickstart-security-health-analytics). When Security Health Analytics is enabled, scans automatically run twice a day, 12-hours apart.

Security Health Analytics scans for many vulnerability types. You can group findings by scanner type. Use Security Health Analytics scanner names to filter findings by the resource type the finding is for.

To view a complete list of Security Health Analytics scanners and findings, see the Security Health Analytics findings (https://cloud.google.com/security-command-center/docs/concepts-security-health-analytics-findings) page, or expand the following section.

### Security Health Analytics scanners

The following tables describe the scanner types and specific vulnerability finding types that Security Health Analytics can generate. You can filter findings by scanner name and finding type using the Security Command Center Vulnerabilities tab in the Google Cloud Console. Available finding categories include:

- 2-Step verification vulnerability findings (#two-sv-findings)
- API key vulnerability findings (#api-findings)
- Compute image vulnerability findings (#compute-image-findings)
- Compute instance vulnerability findings (#compute-instance-findings)
- Container vulnerability findings (#container-findings)

- Dataset vulnerability findings (#dataset-findings)
- DNS vulnerability findings (#dns-findings)
- Firewall vulnerability findings (#firewall-findings)
- IAM vulnerability findings (#iam-findings)
- KMS vulnerability findings (#kms-findings)
- Logging vulnerability findings (#logging-findings)
- Monitoring vulnerability findings (#monitoring-findings)
- Network vulnerability findings (#network-findings)
- SSH password vulnerability findings (#ssh-findings)
- SQL vulnerability findings (#sql-findings)
- Storage vulnerability findings (#storage-findings)
- Subnetwork vulnerability findings (#subnetwork-findings)

#### 2-Step verification findings

The `2SV_SCANNER` detects vulnerabilities related to 2-step verification for users.

**Table 1.** 2-Step verification scanner

| Category | Finding description |
|---|---|
| `2SV_NOT_ENFORCED` | Indicates that there are users who aren't using 2-step verification. |

#### API key vulnerability findings

The `API_KEY_SCANNER` scanner detects vulnerabilities related to API keys used in your cloud deployment.

**Table 2.** API key scanner

| Category | Finding description |
|---|---|
| `API_KEY_APIS_UNRESTRICTED` | Indicates that there are API keys being used too broadly, and should be limited to allow only the APIs needed by the application. |

| | |
|---|---|
| `API_KEY_APPS_UNRESTRICTED` | Indicates that there are API keys being used in an unrestricted way, allowing use by any untrusted app. |
| `API_KEY_EXISTS` | Indicates that a project is using API keys instead of standard authentication. |
| `API_KEY_NOT_ROTATED` | Indicates that the API key hasn't been rotated for more than 90 days. |

#### Compute image vulnerability findings

The `COMPUTE_IMAGE_SCANNER` scanner detects vulnerabilities related to Google Cloud image configurations.

**Table 3. Compute image scanner**

| Category | Finding description |
|---|---|
| `PUBLIC_COMPUTE_IMAGE` | Indicates that a Compute Engine instance is using a public image. |

#### Compute instance vulnerability findings

The `COMPUTE_INSTANCE_SCANNER` scanner detects vulnerabilities related to Google Cloud instance configurations.

**Table 4. Compute instance scanner**

| Category | Finding description |
|---|---|
| `COMPUTE_PROJECT_WIDE_SSH_KEYS_ALLOWED` | Indicates that project-wide SSH keys are used, allowing login to all instances in the project. |
| `COMPUTE_SERIAL_PORTS_ENABLED` | Indicates that serial ports are enabled for an instance, allowing connections to the instance's serial console. |
| `DISK_CSEK_DISABLED` | Indicates that disks on this VM are not encrypted with Customer Supplied Encryption Keys (CSEK). This scanner requires additional configuration to enable. To enable this detector, apply the security mark (https://cloud.google.com/security-command-center/docs/how-to-security-marks) **`enforce_customer_supplied_disk_encryption_keys`** with a value of **`true`** to the assets you want to monitor. |

| | |
|---|---|
| FULL_API_ACCESS | Indicates that an instance is configured to use the default service account with full access to all Google Cloud APIs. |
| IP_FORWARDING_ENABLED | Indicates that IP forwarding is enabled on Instances. |
| OS_LOGIN_DISABLED | Indicates that OS Login is disabled on this instance. |
| PUBLIC_IP_ADDRESS | Indicates that an instance has a public IP address. |
| WEAK_SSL_POLICY | Indicates that an instance has a weak SSL policy. |

#### Container vulnerability findings

These finding types all relate to GKE container configurations, and belong to the `CONTAINER_SCANNER` scanner type.

**Table 5. Container scanner**

| Category | Finding description |
|---|---|
| AUTO_REPAIR_DISABLED | Indicates that the GKE clusters auto repair feature, which keeps nodes in a healthy, running state, is disabled. |
| AUTO_UPGRADE_DISABLED | Indicates that GKE clusters auto upgrade feature, which keeps clusters and node pools on the latest stable version of Kubernetes, is disabled. |
| CLUSTER_LOGGING_DISABLED | Indicates that logging is not enabled for a GKE cluster. |
| CLUSTER_MONITORING_DISABLED | Indicates that Stackdriver Monitoring is disabled on GKE clusters. |
| CLUSTER_PRIVATE_GOOGLE_ACCESS_DISABLED | Indicates that cluster hosts are not configured to use only private, internal IP addresses to access Google APIs. |
| COS_NOT_USED | Indicates that Compute Engine VMs are not using the Container-Optimized OS designed for running Docker containers on Google Cloud securely. |
| IP_ALIAS_DISABLED | Indicates that a GKE cluster was created with Alias IP ranges enabled. |
| LEGACY_AUTHORIZATION_ENABLED | Indicates that Legacy Authorization is enabled on GKE clusters. |

| | |
|---|---|
| `LEGACY_METADATA_ENABLED` | Indicates that legacy metadata is enabled on GKE clusters. |
| `MASTER_AUTHORIZED_NETWORKS_DISABLED` | Indicates that **Master authorized networks** is not enabled on GKE clusters. |
| `NETWORK_POLICY_DISABLED` | Indicates that Network policy is disabled on GKE clusters. |
| `OVER_PRIVILEGED_ACCOUNT` | Indicates that a service account has overly broad project access in a cluster. |
| `OVER_PRIVILEGED_SCOPES` | Indicates that a node service account has broad access scopes. |
| `POD_SECURITY_POLICY_DISABLED` | Indicates that **`PodSecurityPolicy`** is disabled on a GKE cluster. |
| `PRIVATE_CLUSTER_DISABLED` | Indicates that a GKE cluster has a Private cluster disabled. |
| `WEB_UI_ENABLED` | Indicates that the GKE web UI (dashboard) is enabled. |
| `WORKLOAD_IDENTITY_DISABLED` | Indicates that Workload Identity is disabled on a GKE cluster. |

#### Dataset vulnerability findings

Vulnerabilities of this scanner type all relate to BigQuery Dataset configurations, and belong to the `DATASET_SCANNER` scanner type.

**Table 6. Dataset scanner**

| Category | Finding description |
|---|---|
| `PUBLIC_DATASET` | Indicates that a dataset is configured to be open to public access. |

#### DNS vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud DNS configurations, and belong to the `DNS_SCANNER` scanner type.

**Table 7. DNS scanner**

| Category | Finding description |
|---|---|

| | |
|---|---|
| `DNSSEC_DISABLED` | Indicates that DNSSEC is disabled for Cloud DNS zones. |
| `RSASHA1_FOR_SIGNING` | Indicates that RSASHA1 is used for key signing in Cloud DNS zones. |

#### Firewall vulnerability findings

Vulnerabilities of this scanner type all relate to firewall configurations, and belong to the `FIREWALL_SCANNER` scanner type.

**Table 8. Firewall scanner**

| Category | Finding description |
|---|---|
| `OPEN_FIREWALL` | Indicates that a firewall is configured to be open to public access. |
| `OPEN_RDP_PORT` | Indicates that a firewall is configured to have an open RDP port that allows generic access. |
| `OPEN_SSH_PORT` | Indicates that a firewall is configured to have an open SSH port that allows generic access. |

#### IAM vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud Identity and Access Management (Cloud IAM) configuration, and belong to the `IAM_SCANNER` scanner type.

**Table 9. IAM Scanner**

| Category | Finding description |
|---|---|
| `ADMIN_SERVICE_ACCOUNT` | Indicates that there is a service account configured with administrator roles. |
| `KMS_ROLE_SEPARATION` | Indicates that separation of duties is not enforced, and a user exists who has any of the: Cloud Key Management Service (Cloud KMS) CryptoKey Encrypter/Decrypter, Encrypter, or Decrypter roles at the same time. |
| `NON_ORG_IAM_MEMBER` | Indicates that there is a user who isn't using organizational credentials. |
| `OVER_PRIVILEGED_SERVICE_ACCOUNT_USER` | Indicates that a user has the Service Account User role at the project level, instead of for a specific service account. |

| | |
|---|---|
| `SERVICE_ACCOUNT_ROLE_SEPARATION` | Indicates that a user has been assigned the Service Account Admin and Service Account User roles. This violates the "Separation of Duties" principle. |

#### KMS vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud KMS configurations, and belong to the `KMS_SCANNER` scanner type.

**Table 10. KMS scanner**

| Category | Finding description |
|---|---|
| `KMS_KEY_NOT_ROTATED` | Indicates that rotation isn't configured on a Cloud KMS encryption key. |

#### Logging vulnerability findings

Vulnerabilities of this scanner type all relate to logging configurations, and belong to the `LOGGING_SCANNER` scanner type.

**Table 11. Logging scanner**

| Category | Finding description |
|---|---|
| `AUDIT_LOGGING_DISABLED` | Indicates that audit logging has been disabled for this resource. |
| `BUCKET_LOGGING_DISABLED` | Indicates that there is a storage bucket without logging enabled. |
| `LOG_NOT_EXPORTED` | Indicates there is a resource that does not have an appropriate log sink configured. |
| `OBJECT_VERSIONING_DISABLED` | Indicates that object versioning isn't enabled on a storage bucket where sinks are configured. |

#### Monitoring vulnerability findings

Vulnerabilities of this scanner type all relate to monitoring configurations, and belong to the `MONITORING_SCANNER` type. All Monitoring scanner finding properties will include:

- The `RecommendedLogFilter` to use in creating the log metrics.

- The `QualifiedLogMetricNames` that cover the conditions listed in the recommended log filter.
- The `AlertPolicyFailureReasons` that indicate if the project does not have alert policies created for any of the qualified log metrics or the existing alert policies do not have the recommended settings.

**Table 12. Monitoring scanner**

| Category | Finding description |
|---|---|
| `AUDIT_CONFIG_NOT_MONITORED` | Indicates that log metrics and alerts aren't configured to monitor Audit Configuration Changes. |
| `BUCKET_IAM_NOT_MONITORED` | Indicates that log metrics and alerts aren't configured to monitor Cloud Storage Cloud IAM permission changes. |
| `CUSTOM_ROLE_NOT_MONITORED` | Indicates that log metrics and alerts aren't configured to monitor Custom Role changes. |
| `FIREWALL_NOT_MONITORED` | Indicates that log metrics and alerts aren't configured to monitor VPC Network Firewall rule changes. |
| `NETWORK_NOT_MONITORED` | Indicates that log metrics and alerts aren't configured to monitor VPC network changes. |
| `OWNER_NOT_MONITORED` | Indicates that log metrics and alerts aren't configured to monitor Project Ownership assignments or changes. |
| `ROUTE_NOT_MONITORED` | Indicates that log metrics and alerts aren't configured to monitor VPC network route changes. |
| `SQL_INSTANCE_NOT_MONITORED` | Indicates that log metrics and alerts aren't configured to monitor Cloud SQL instance configuration changes. |

#### Network vulnerability findings

Vulnerabilities of this scanner type all relate to an organization's network configurations, and belong to the `NETWORK_SCANNER` type.

**Table 13. Network scanner**

| Category | Finding description |
|---|---|

| | |
|---|---|
| DEFAULT_NETWORK | Indicates that the default network exists in a project. |
| LEGACY_NETWORK | Indicates that a legacy network exists in a project. |

#### SSH password vulnerability findings

Vulnerabilities of this scanner type all relate to passwords, and belong to the `SSH_PASSWORD` type.

**Table 14.** SSH password scanner

| Category | Finding description |
|---|---|
| WEAK_SSH_PASSWORD | Indicates that a resource has a weak SSH password. |

#### SQL vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud SQL configurations, and belong to the `SQL_SCANNER` type.

**Table 15.** SQL scanner

| Category | Finding description |
|---|---|
| AUTO_BACKUP_DISABLED | Indicates that a Cloud SQL database doesn't have automatic backups enabled. |
| PUBLIC_SQL_INSTANCE | Indicates that a Cloud SQL database instance accepts connections from all IP addresses. |
| SSL_NOT_ENFORCED | Indicates that a Cloud SQL database instance doesn't require all incoming connections to use SSL. |
| SQL_NO_ROOT_PASSWORD | Indicates that a Cloud SQL database doesn't have a password configured for the root account. |
| SQL_WEAK_ROOT_PASSWORD | Indicates that a Cloud SQL database has a weak password configured for the root account. |

#### Storage vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud Storage Buckets configurations, and belong to the `STORAGE_SCANNER` type.

**Table 16. Storage scanner**

| Category | Finding description |
|---|---|
| `BUCKET_POLICY_ONLY_DISABLED` | Indicates that **`uniform bucket-level access`**, previously called **`Bucket Policy Only`**, isn't configured. |
| `LOGGING_DISABLED` | Indicates that logging is disabled for a Cloud Storage bucket. |
| `PUBLIC_BUCKET_ACL` | Indicates that a Cloud Storage bucket is publicly accessible. |

#### Subnetwork vulnerability findings

Vulnerabilities of this scanner type all relate to an organization's subnetwork configurations, and belong to the `SUBNETWORK_SCANNER` type.

**Table 17. Subnetwork scanner**

| Category | Finding description |
|---|---|
| `FLOW_LOGS_DISABLED` | Indicates there is a VPC subnetwork that has flow logs disabled. |
| `PRIVATE_GOOGLE_ACCESS_DISABLED` | Indicates private subnets without access to Google public APIs. |

### Web Security Scanner

Web Security Scanner (https://cloud.google.com/security-scanner/) provides managed web vulnerability scanning for public App Engine, GKE, and Compute Engine serviced web applications. Web Security Scanner displays granular information about application vulnerability findings, like outdated libraries, cross-site scripting, or use of mixed content. Web Security Scanner findings are available in Security Command Center if you've completed the Web Security Scanner quickstart (https://cloud.google.com/security-scanner/docs/quickstart).

**Table A. Web Security Scanner finding types**

| Vulnerability | Description |
|---|---|

| | |
|---|---|
| Mixed Content | A page that was served over HTTPS also serves resources over HTTP. A man-in-the-middle attacker could tamper with the HTTP resource and gain full access to the website that loads the resource or monitor users' actions. |
| Outdated Library | The version of an included library is known to contain a security issue. The scanner checks the version of library in use against a known list of vulnerable libraries. False positives are possible if the version detection fails or if the library has been manually patched.<br><br>Web Security Scanner identifies some vulnerable versions of the following popular libraries:<br><br>• jQuery, for example: CVE-2011-4969 (https://nvd.nist.gov/vuln/detail/CVE-2011-4969)<br>• jQuery Mobile, for example: known XSS vulnerability (https://github.com/jquery/jquery-mobile/issues/4787)<br>• AngularJS, for example: XSS via SVG vulnerability (https://vulnerabledoma.in/ngSanitize1.6.8_bypass.html)<br><br>This list is updated periodically with new libraries and updated vulnerabilities as applicable. |
| Rosetta Flash | This type of vulnerability occurs when the value of a request parameter is reflected at the beginning of the response. For example, the format of JSONP requests can allow this type of exploit. An attacker can supply an alphanumeric-only Flash file in the vulnerable parameter, and then the browser executes it as if the file originated on the vulnerable server. |
| XSS Callback | A cross-site scripting (XSS) bug is found via JavaScript callback. For detailed explanations on XSS, see Cross-site scripting (https://www.google.com/about/appsecurity/learning/xss/). |
| XSS Error | A potential cross-site scripting (XSS) bug due to JavaScript breakage. In some circumstances, the application under test might modify the test string before the browser parses it. When the browser attempts to run this modified test string, it is likely to break and throw a JavaScript execution error, causing an injection issue. However, it might not be exploitable. To determine if the issue is an XSS vulnerability, you must manually verify that the test string modifications can be evaded. For detailed explanations on XSS, see Cross-site scripting (https://www.google.com/about/appsecurity/learning/xss/). |
| XSS Angular Callback | An application appears to be transmitting a password field in clear text. An attacker can eavesdrop network traffic and sniff the password field. |
| Clear Text Password | An application returns sensitive content with an invalid content type, or without an `X-Content-Type-Options: nosniff` header. |
| Invalid Content Type | A cross-site scripting (XSS) vulnerability in AngularJS module that occurs when Angular interpolates a user-provided string. |
| Invalid Header | A malformed or invalid valued header. |
| Misspelled | Misspelled security header name. |

| | |
|---|---|
| Security Header Name | |
| Mismatching Security Header Values | Mismatching values in a duplicate security header. |
| Accessible GIT Repository | The scan found an accessible git repository. |
| Accessible SVN Repository | The scan found an accessible SVN repository. |

To display Web Security Scanner results in Security Command Center, you need to run the security scan in the project that contains the public-facing candidate App Engine, Compute Engine, or GKE application. Any application vulnerabilities that are detected are automatically displayed in Security Command Center.

- To explore details about a specific finding, click the finding under **Finding**.
- To display details about all Web Security Scanner findings, click **View all security findings**.

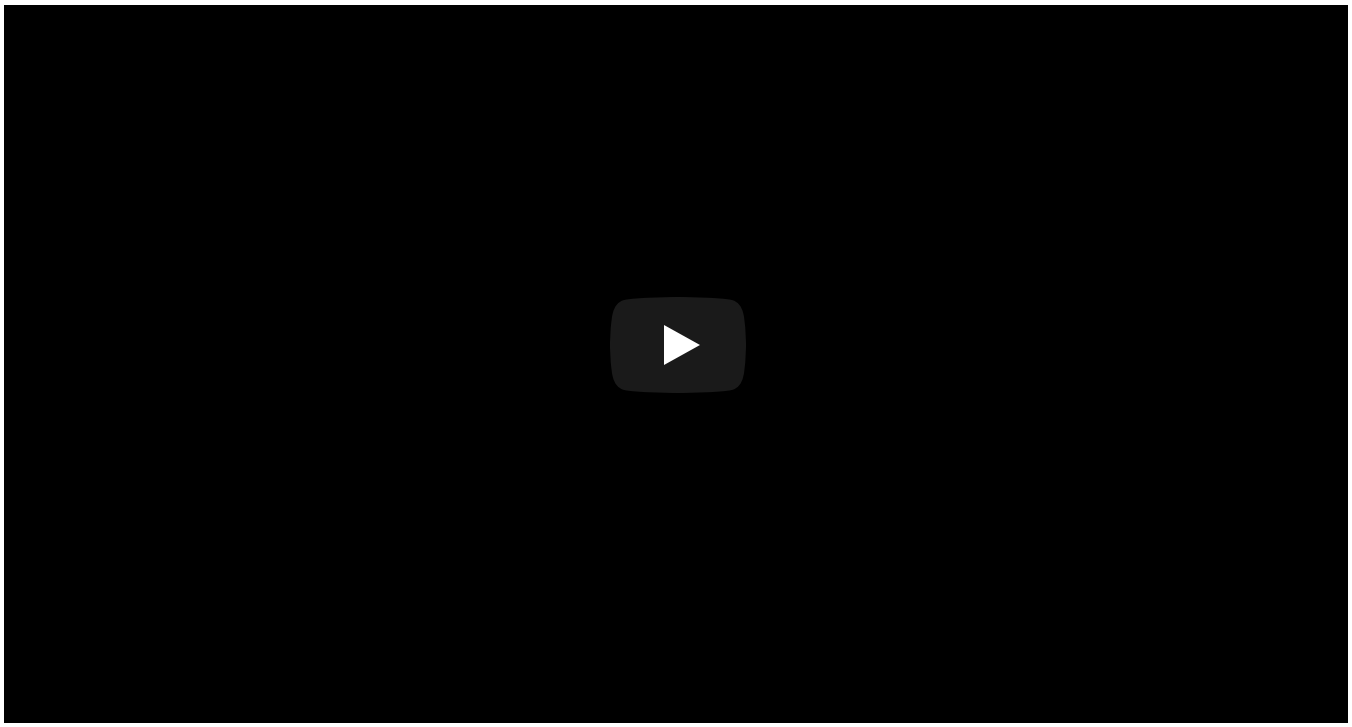
## Threats

Threat detectors can help you find potentially harmful events.

### Anomaly Detection

**Anomaly Detection** is a built-in service that uses behavior signals from *outside* your system. It displays granular information about security anomalies detected for your projects and Virtual Machine (VM) instances, like potential leaked credentials, unusual activity, and coin mining. Anomaly Detection findings are automatically available in Security Command Center and are displayed when you enable it as a security source (https://cloud.google.com/security-command-center/docs/quickstart-scc#add-security-sources).

The following video shows you how to enable Anomaly Detection and then review and remediate a finding. Example finding types are also described in Table B later on this page.



Example Anomaly Detection findings include the following:

**Table B. Anomaly Detection finding types**

| Potential for Compromise | Description |
|---|---|
| Leaked Service Account Credentials | Google Cloud service account credentials that are accidentally leaked online or compromised. |
| Potential Compromised Machine | Potential compromise of a resource in your organization. |
| **Abuse Scenarios** | **Description** |
| Resource used for cryptomining | Behavioral signals around a VM in your organization indicate that it might have been compromised and could be getting used for cryptomining. |
| Resource used for outbound intrusion | Intrusion attempts and Port scans: One of the resources or Google Cloud services in your organization is being used for intrusion activities, like an attempt to break in or compromise a target system. These include SSH brute force attacks, Port scans, and FTP brute force attacks. |
| Resource used for | One of the resources or Google Cloud services in your organization is being used for |

| | |
|---|---|
| phishing | phishing. |

| Anomalies | Description |
|---|---|
| Unusual Activity/Connection | Unusual activity from a resource in your organization. |

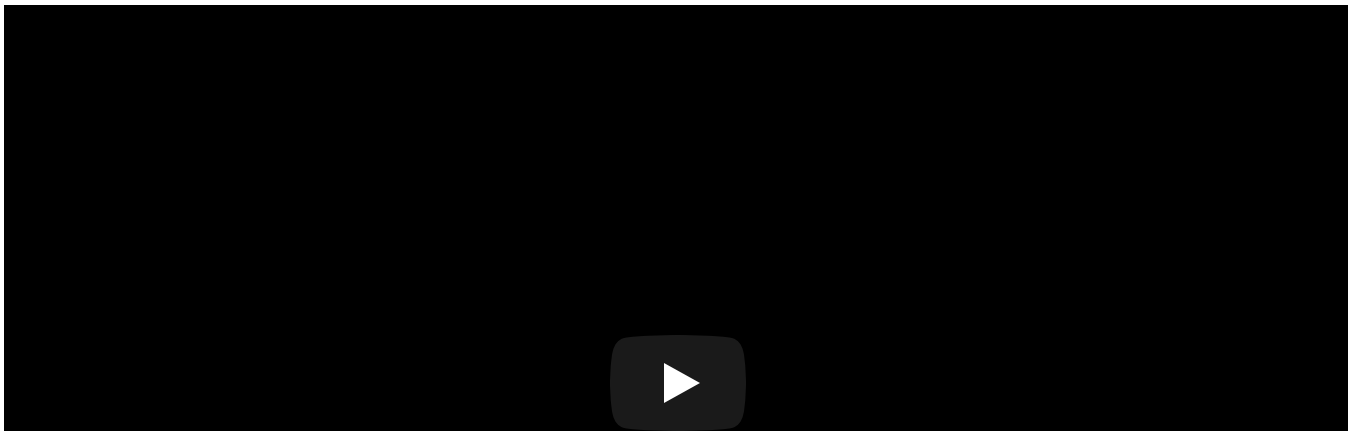
## Cloud Data Loss Prevention

**Cloud DLP Data Discovery** enables you to surface the results of Cloud Data Loss Prevention (Cloud DLP) scans directly in the Security Command Center dashboard and Findings inventory. Cloud DLP can help you to better understand and manage sensitive data and Personally Identifiable Information (PII) like the following:

- Credit card numbers
- Names
- Social security numbers
- US and selected international identifying numbers
- Phone numbers
- Google Cloud credentials

Each Cloud DLP Data Discovery finding **only includes the category type** of the identified PII data and the resource it was found in. It doesn't include any of the specific underlying data.

The following video shows you how to set up Cloud DLP to send scan results to Security Command Center. The setup steps are also described in the guide to send DLP API results to Security Command Center (https://cloud.google.com/dlp/docs/sending-results-to-cscc).



After you complete the guide, Cloud DLP scan results will display in Security Command Center:

- To display details about a specific category of findings, click the finding under **Finding**.
- To display details about all Cloud DLP scanner findings, click **More**.

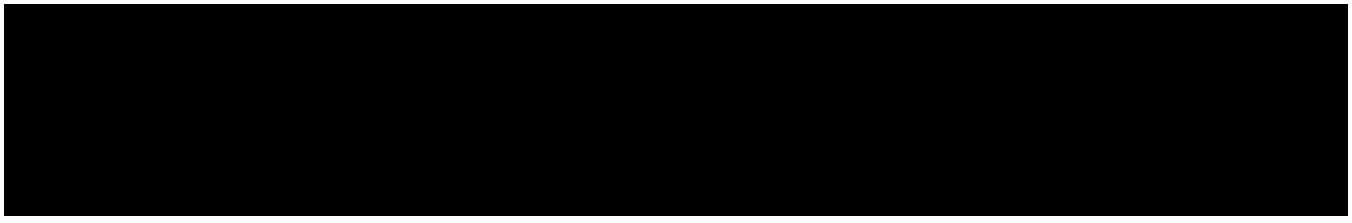
For more information:

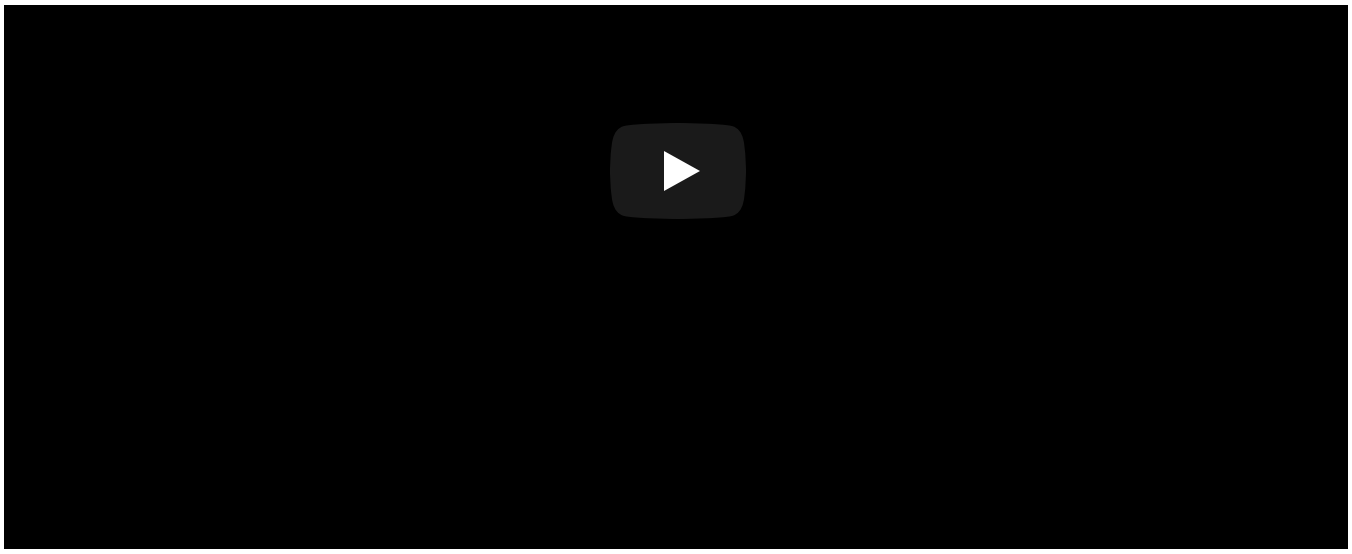
- Learn more about the `publishSummaryToCscc` action (https://cloud.google.com/dlp/docs/reference/rpc/google.privacy.dlp.v2#google.privacy.dlp.v2.Action.PublishSummaryToCscc) in Cloud DLP.
- Learn more about scanning storage repositories for sensitive data (https://cloud.google.com/dlp/docs/inspecting-storage) using Cloud DLP.

## Event Threat Detection

Event Threat Detection uses log data from *inside* your systems. It watches your organization's Stackdriver Logging stream for one or more projects, and consumes logs as they become available. When a threat is detected, Event Threat Detection writes a Finding to Security Command Center and to a Logging project. Event Threat Detection findings are available in Security Command Center after you set up Event Threat Detection (https://cloud.google.com/event-threat-detection).

The following video describes some of the threat types that Event Threat Detection detects, and how to review them in the Security Command Center dashboard. The threat types are also described in Table C later on this page.





Example Event Threat Detection findings include the following:

**Table C. Event Threat Detection finding types**

| Monitoring & Logging | Description |
|---|---|
| Brute force SSH | Event Threat Detection detects brute force of SSH by examining SSH logs for repeated failures followed by success. |
| Cryptomining | Event Threat Detection detects coin mining malware by examining VPC logs for connections to known bad domains for mining pools and other log data. |
| Cloud IAM abuse | Malicious grants - Event Threat Detection detects the addition of accounts from outside of your organization's domain that have the Owner or Editor permission at the organization or project level. The malicious grants finding helps you to identify:<br>• Which accounts have which permissions<br>• The resource the permission applies to<br>• The user inside your organization that granted the permissions |
| Malware | Event Threat Detection detects Malware by examining VPC logs for connections to known bad domains and other log data. |
| Phishing | Event Threat Detection detects Phishing by examining VPC logs for connections and other log data. |

Get started with Event Threat Detection (https://cloud.google.com/event-threat-detection).

### Forseti Security

Forseti Security gives you tools to understand all the resources you have in Google Cloud. The core Forseti modules work together to provide complete information so you can secure resources and minimize security risks.

To display Forseti violation notifications in Security Command Center, follow the Forseti Security Command Center notification guide (https://forsetisecurity.org/docs/latest/configure/notifier/#cloud-scc-notification).

For more information:

- Learn about Forseti (https://forsetisecurity.org/about/).
- Get help with Forseti (https://forsetisecurity.org/docs/latest/use/get-help.html).

### Phishing Protection

Phishing Protection helps prevent users from accessing phishing sites by classifying malicious content that uses your brand and reporting the unsafe URLs to Google Safe Browsing (https://safebrowsing.google.com/). After a site is propagated to Safe Browsing, users will see warnings across more than three billion devices.

To get started with Phishing Protection, follow the guide to Enable Phishing Protection (https://cloud.google.com/phishing-protection/docs/quickstart-console). After you enable Phishing Protection, results are displayed in Security Command Center in the **Phishing Protection** card under **Findings**.

## What's next

- Learn about Security Command Center and example use cases in the Security Command Center overview (https://cloud.google.com/security-command-center/docs/concepts-overview).
- Learn how to add security sources to Security Command Center (https://cloud.google.com/security-command-center/docs/how-to-security-sources).

*Last updated January 7, 2020.*