>

Security Command Center findings model the potential security risks of an organization's assets. A finding always relates to a specific asset in Security Command Center.

This guide shows you how to use Security Command Center client libraries to access an organization's findings. Each finding belongs to a source. Most detectors or finding providers will produce findings within the same source.

Before you set up a source, you'll need to complete the following:

- Set up a service account and SDK (/security-command-center/docs/how-to-programmatic-access)

All Security Command Center list APIs are paginated. Each response returns a page of results and a token to return the next page. The page size is configurable. The default pageSize is 10, it can be set to a minimum of 1, and maximum of 1000.

An organization might have a lot of Findings. The example above doesn't use a filter, so all finding records are returned. Security Command Center enables you to use finding filters to get information about only the findings you want, and limit the parent to a specific source.

Finding filters are like "where" clauses in SQL statements, except instead of columns, they apply to the objects returned by the API.

Below is an example of only listing findings that have a category "`MEDIUM_RISK_ONE`". Specific categories might change and you should consult the documentation of a finding provider to determine the categories they use.

Security Command Center also supports full JSON arrays and objects as potential property types. You can filter on:

- Array elements
- Full JSON objects with partial string match within the object
- JSON object sub-fields

Sub-fields must be numbers, strings, or booleans and they must use the following operators:

- Strings:
  - Full equality `=`
  - Partial string matching `:`
- Numbers:
  - Inequalities `<`, `>`, `<=`, `>=`
  - Equality `=`
- Booleans:
  - Equality `=`

The examples later on this page assume the following JSON object is a source property on a finding:

In this example, the previous JSON object is a source property named `my_property` on a finding. The following example includes queries for findings that have the object as a property. You can also use these filters with other filters using `AND` and `OR` in your query.

You can sort findings by strict sub-fields that are primitive types—strings, numbers, and booleans. In this example, the previous JSON object is a source property named `my_property` on a finding. The following example includes queries to sort the finding fields:

Security Command Center allows you to list findings as of a particular snapshot time:

Following are some other useful finding filters.

These example filters match findings that most recently occurred after Wednesday, June 5, 2019 10:12:05 PM GMT. With the `event_time` filter, you can express time using the following formats and types:

- Unix time (in milliseconds) as an integer literal

- RFC 3339 as a string literal