

## Cloud Security Command Center (Cloud SCC) finding.

A finding is a record of assessment data like security, risk, health, or privacy, that is ingested into Cloud SCC for presentation, notification, analysis, policy testing, and enforcement. For example, a cross-site scripting (XSS) vulnerability in an App Engine application is a finding.

### JSON representation

### Fields

<b>name</b>	<b>string</b>
	The relative resource name of this finding. See: <a href="https://cloud.google.com/apis/design/resource_names#relative_resource">https://cloud.google.com/apis/design/resource_names#relative_resource</a> ( <a href="https://cloud.google.com/apis/design/resource_names#relative_resource">https://cloud.google.com/apis/design/resource_names#relative_resource</a> ) Example: "organizations/{organization_id}/sources/{source_id}/findings/{findingId}"

Fields	
<b>parent</b>	<p><b>string</b></p> <p>The relative resource name of the source the finding belongs to. See: <a href="https://cloud.google.com/apis/design/resource_names#relative_resource_name">https://cloud.google.com/apis/design/resource_names#relative_resource_name</a> (<a href="https://cloud.google.com/apis/design/resource_names#relative_resource_name">https://cloud.google.com/apis/design/resource_names#relative_resource_name</a>) This field is immutable after creation time. For example: "organizations/{organization_id}/sources/{source_id}"</p>
<b>resourceName</b>	<p><b>string</b></p> <p>For findings on Google Cloud Platform (GCP) resources, the full resource name of the GCP resource this finding is for. See: <a href="https://cloud.google.com/apis/design/resource_names#full_resource_name">https://cloud.google.com/apis/design/resource_names#full_resource_name</a> (<a href="https://cloud.google.com/apis/design/resource_names#full_resource_name">https://cloud.google.com/apis/design/resource_names#full_resource_name</a>) When the finding is for a non-GCP resource, the resourceName can be a customer or partner defined string. This field is immutable after creation time.</p>
<b>state</b>	<p><b>enum (State)</b> (/security-command-center/docs/reference/rest/v1/organizations.sources.findings#State)</p> <p>)</p> <p>The state of the finding.</p>
<b>category</b>	<p><b>string</b></p> <p>The additional taxonomy group within findings from a given source. This field is immutable after creation time. Example: "XSS_FLASH_INJECTION"</p>
<b>externalUri</b>	<p><b>string</b></p> <p>The URI that, if available, points to a web page outside of Cloud SCC where additional information about the finding can be found. This field is guaranteed to be either empty or a well formed URL.</p>

Fields	
<b>sourceProperties</b>	<p><b>map (key: string, value: value (Value (https://developers.google.com/protocol-buffers/docs/reference/google.protobuf.Value) format))</b></p> <p>Source specific properties. These properties are managed by the source that generated the finding. The key names in the sourceProperties map must be between 1 and 255 characters, and must start with a letter and contain alphanumeric characters or underscores only.</p> <p>An object containing a list of "key": value pairs. Example: { "name": "wrench", "mass": "1.3kg", "count": "3" }.</p>
<b>securityMarks</b>	<p><b>object (SecurityMarks (/security-command-center/docs/reference/rest/v1/organizations.sources.findings#SecurityMarks))</b></p> <p>Output only. User specified security marks. These marks are entirely managed by the user and come from the SecurityMarks resource that belongs to the finding.</p>
<b>eventTime</b>	<p><b>string (Timestamp (https://developers.google.com/protocol-buffers/docs/reference/google.protobuf.Timestamp) format)</b></p> <p>The time at which the event took place. For example, if the finding represents an open firewall it would capture the time the detector believes the firewall became open. The accuracy is determined by the detector.</p> <p>A timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds. Example: "2014-10-02T15:01:23.045123456Z".</p>

## Fields

<b>createTime</b>	<p><b>string</b> (<b>Timestamp</b> (<a href="https://developers.google.com/protocol-buffers/docs/reference/google.protobuf#google.protobuf.Timestamp">https://developers.google.com/protocol-buffers/docs/reference/google.protobuf#google.protobuf.Timestamp</a>) format)</p> <p>The time at which the finding was created in Cloud SCC.</p> <p>A timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds. Example: "2014-10-02T15:01:23.045123456Z".</p>
-------------------	--

The state of the finding.

## Enums

<b>STATE_UNSPECIFIED</b>	Unspecified state.
<b>ACTIVE</b>	The finding requires attention and has not been addressed yet.
<b>INACTIVE</b>	The finding has been fixed, triaged as a non-issue or otherwise addressed and is no longer active.

User specified security marks that are attached to the parent Cloud Security Command Center (Cloud SCC) resource. Security marks are scoped within a Cloud SCC organization – they can be modified and viewed by all users who have proper permissions on the organization.

## JSON representation

## JSON representation

### Fields

name	<p><b>string</b></p> <p>The relative resource name of the SecurityMarks. See: <a href="https://cloud.google.com/apis/design/resource_names#relative_resource">https://cloud.google.com/apis/design/resource_names#relative_resource</a> (<a href="https://cloud.google.com/apis/design/resource_names#relative_resource">https://cloud.google.com/apis/design/resource_names#relative_resource</a>)</p> <p>Examples: "organizations/{organization_id}/assets/{asset_id}/securityMa "organizations/{organization_id}/sources/{source_id}/findings/{findingId}</p>
marks	<p><b>map (key: string, value: string)</b></p> <p>Mutable user specified security marks belonging to the parent resource. Cf follows:</p> <ul style="list-style-type: none"> <li>• Keys and values are treated as case insensitive</li> <li>• Keys must be between 1 - 256 characters (inclusive)</li> <li>• Keys must be letters, numbers, underscores, or dashes</li> <li>• Values have leading and trailing whitespace trimmed, remaining charac between 1 - 4096 characters (inclusive)</li> </ul> <p>An object containing a list of "key": value pairs. Example: { "name": "mass": "1.3kg", "count": "3" }.</p>

Creates a finding.

	Filters an organization or source's findings and groups them by their specified properties.
	Lists an organization or source's findings.
	Creates or updates a finding.
	Updates the state of a finding.
	Updates security marks.