Filters an organization or source's findings and groups them by their specified properties.

To group across all sources provide a `-` as the source id. Example: /v1/organizations/{organization_id}/sources/-/findings

`POST`
`https://securitycenter.googleapis.com/v1/{parent=organizations/*/sources/*}/findings:group`

The URL uses gRPC Transcoding (https://github.com/googleapis/googleapis/blob/master/google/api/http.proto) syntax.

Parameters

`parent`	`string` Required. Name of the source to groupBy. Its format is "organizations/[organization_id]/sources/[source_id]". To groupBy across all sources provide a source_id of `-`. For example: organizations/{organization_id}/sources/-

The request body contains data with the following structure:

JSON representation

JSON representation

Fields	
`filter`	`string` Expression that defines the filter to apply across findings. The expression is a list of one or more restrictions combined via logical operators **`AND`** and **`OR`**. Parentheses are supported, and **`OR`** has higher precedence than **`AND`**. Restrictions have the form **`<field> <operator> <value>`** and may have a **`-`** character in front of them to indicate negation. Examples include: • name • sourceProperties.a_property • securityMarks.marks.marka The supported operators are: • **`=`** for all value types. • **`>`**, **`<`**, **`>=`**, **`<=`** for integer values. • **`:`**, meaning substring matching, for strings. The supported value types are: • string literals in quotes. • integer literals without quotes. • boolean literals **`true`** and **`false`** without quotes. The following field and operator combinations are supported: • name: **`=`** • parent: **`=`**, **`:`**

Fields	
	• resourceName: =, : • state: =, : • category: =, : • externalUri: =, : • eventTime: =, >, <, >=, <= Usage: This should be milliseconds since epoch or an RFC3339 string. Examples: "eventTime = "2019-06-10T16:07:18-07:00"" "eventTime = 1560208038000" • securityMarks.marks: =, : • sourceProperties: =, :, >, <, >=, <= For example, **`sourceProperties.size = 100`** is a valid filter string.
`groupBy`	**`string`** Required. Expression that defines what assets fields to use for grouping (including **`stateChange`**). The string value should follow SQL syntax: comma separated list of fields. For example: "parent,resourceName". The following fields are supported: • resourceName • category • state • parent The following fields are supported when compareDuration is set: • stateChange

Fields	
`readTime`	`string (`Timestamp (https://developers.google.com/protocol-buffers/docs/reference/google.protobuf#google.protobuf.Timestamp)`format)` Time used as a reference point when filtering findings. The filter is limited to findings existing at the supplied time and their values are those at that specific time. Absence of this field will default to the API's version of NOW. A timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds. Example: "`2014-10-02T15:01:23.045123456Z`".

Fields	
`compareDuration`	`string (Duration` (https://developers.google.com/protocol-buffers/docs/reference/google.protobuf#google.protobuf.Duration) `format)` When compareDuration is set, the GroupResult's "stateChange" attribute is updated to indicate whether the finding had its state changed, the finding's state remained unchanged, or if the finding was added during the compareDuration period of time that precedes the readTime. This is the time between (readTime - compareDuration) and readTime. The stateChange value is derived based on the presence and state of the finding at the two points in time. Intermediate state changes between the two times don't affect the result. For example, the results aren't affected if the finding is made inactive and then active again. Possible "stateChange" values when compareDuration is specified: • "CHANGED": indicates that the finding was present at the start of compareDuration, but changed its state at readTime. • "UNCHANGED": indicates that the finding was present at the start of compareDuration and did not change state at readTime. • "ADDED": indicates that the finding was not present at the start of compareDuration, but was present at readTime. If compareDuration is not specified, then the only possible stateChange is "UNUSED", which will be the stateChange set for all findings present at readTime. If this field is set then **`stateChange`** must be a specified field in **`groupBy`**. A duration in seconds with up to nine fractional digits, terminated by '`s`'. Example: "`3.5s`".
`pageToken`	`string` The value returned by the last **`GroupFindingsResponse`**; indicates that this is a continuation of a prior **`findings.group`** call, and that the system should return the next page of data.

Fields	
pageSize	number The maximum number of results to return in a single response. Default is 10, minimum is 1, maximum is 1000.

If successful, the response body contains data with the following structure:

Response message for group by findings.

JSON representation

Fields	
groupByResults[]	object (GroupResult (/security-command-center/docs/reference/rest/v1/GroupResult)) Group results. There exists an element for each existing unique combination of property/values. The element contains a count for the number of times those specific property/values appear.

Fields	
`readTime`	`string (Timestamp` (https://developers.google.com/protocol-buffers/docs/reference/google.protobuf#google.protobuf.Timestamp) `format)` Time used for executing the groupBy request. A timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds. Example: "`2014-10-02T15:01:23.045123456Z`".
`nextPageToken`	`string` Token to retrieve the next page of results, or empty if there are no more results.
`totalSize`	`number` The total number of results matching the query.

Requires the following OAuth scope:

- `https://www.googleapis.com/auth/cloud-platform`

For more information, see the Authentication Overview (https://cloud.google.com/docs/authentication/).

Requires the following Cloud IAM (https://cloud.google.com/iam/docs) permission on the `parent` resource:

- `securitycenter.findings.group`

For more information, see the Cloud IAM Documentation (https://cloud.google.com/iam/docs).