

This guide walks you through creating and updating findings using the Security Command Center API.

Before you create and update findings, you need to complete the following:

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

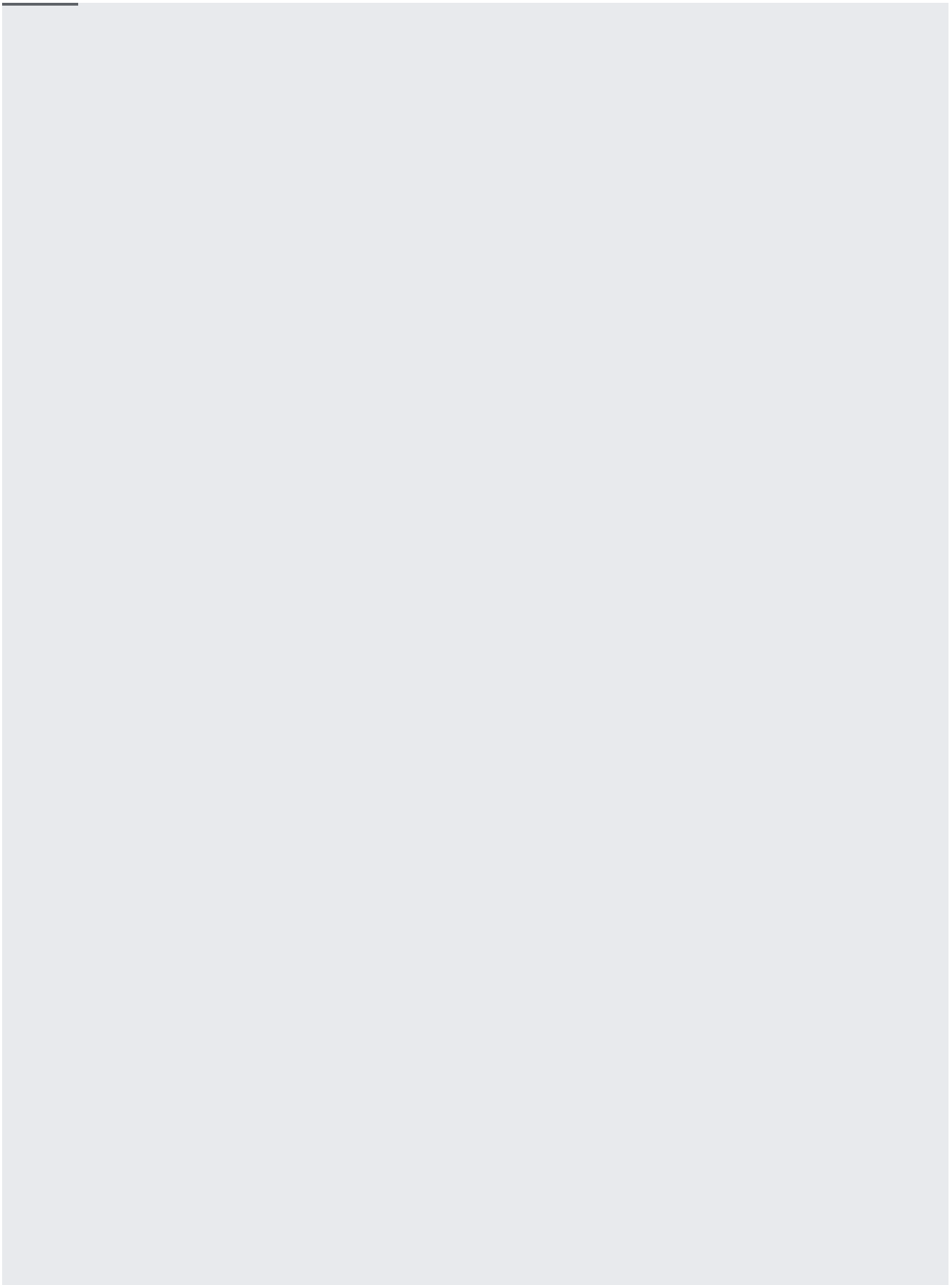
To complete this guide, you must have the Cloud Identity and Access Management (Cloud IAM) role `securitycenter.findingsEditor` for the security source. For more information, see [Access control](#) (/security-command-center/docs/access-control) and [Creating and managing security sources](#) (/security-command-center/docs/how-to-api-create-manage-security-sources).

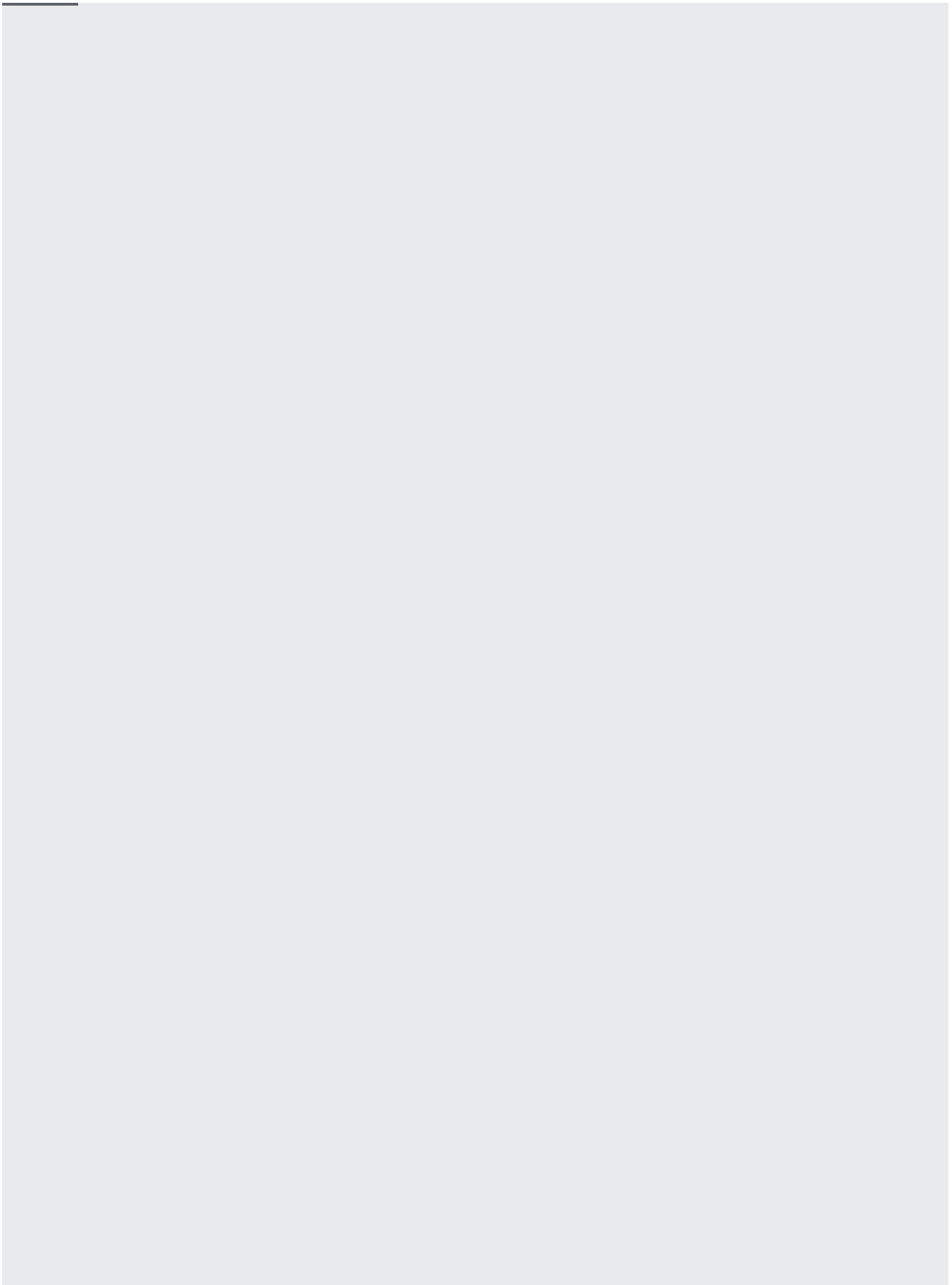
If you want to create findings with security marks, you must also have a Cloud IAM role that includes permissions for the kind of mark that you want to use:

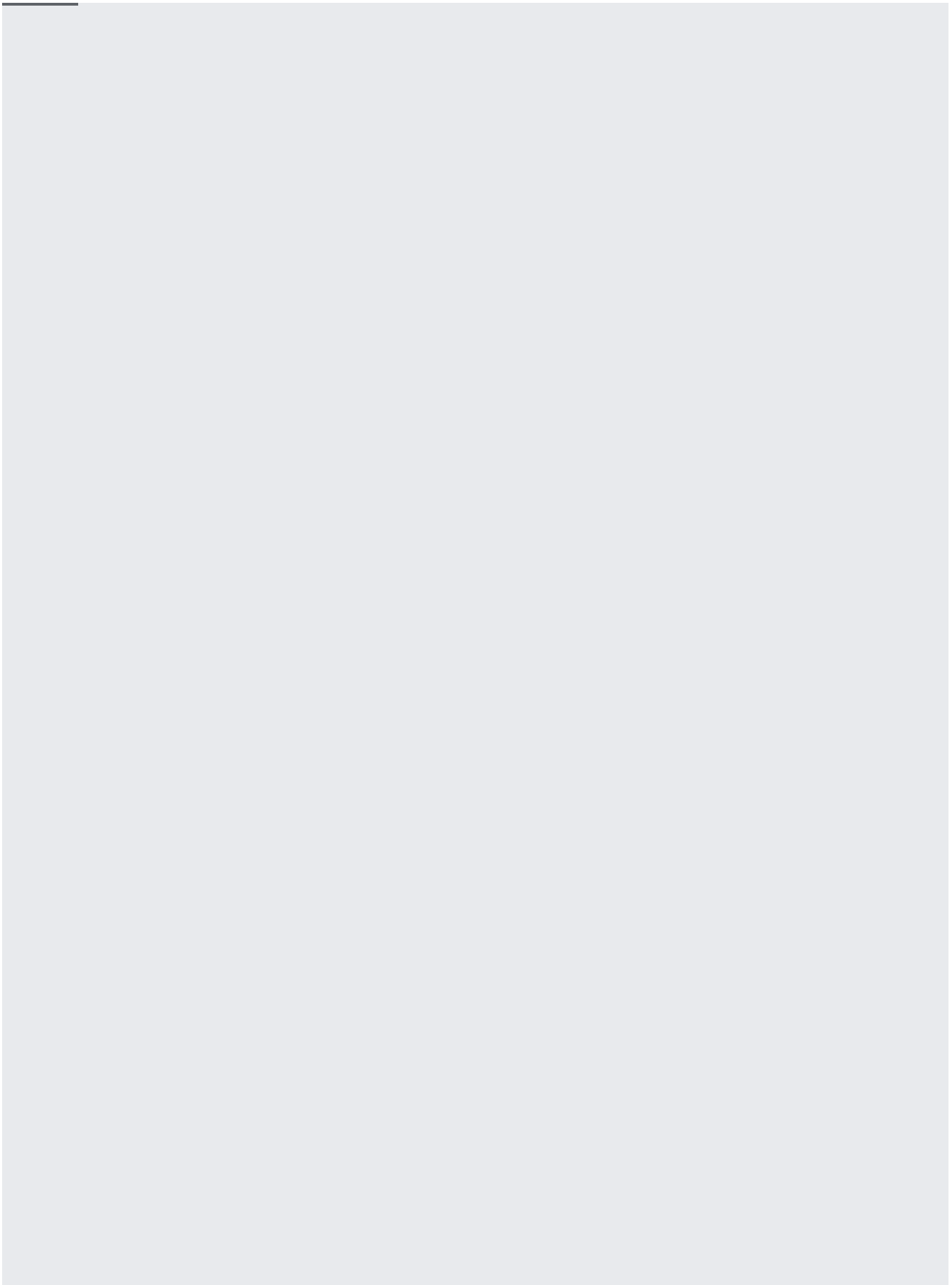
- Asset marks: **Asset Security Marks Writer**, `securitycenter.assetSecurityMarksWriter`
- Finding marks: **Finding Security Marks Writer**,
`securitycenter.findingSecurityMarksWriter`

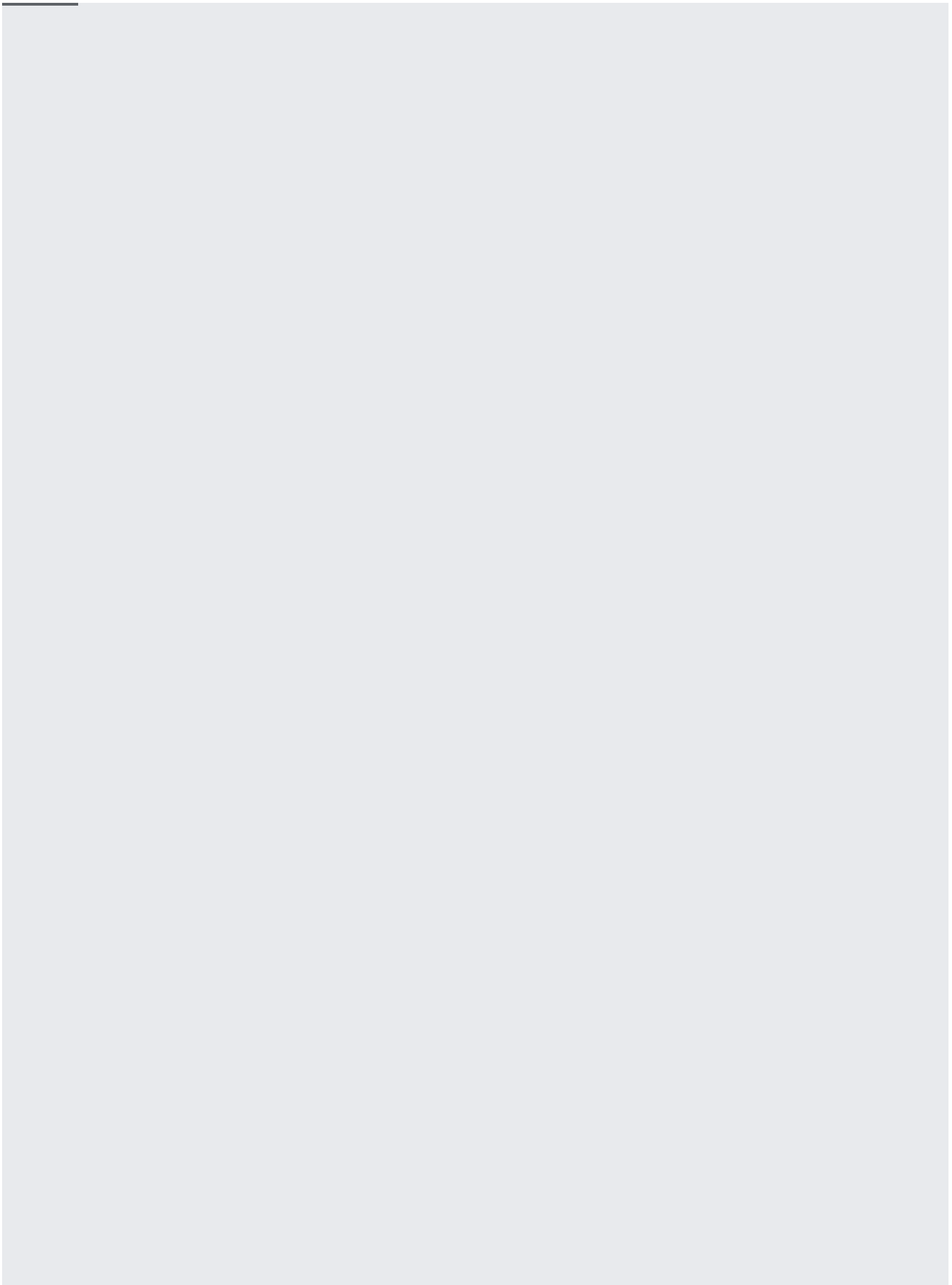
For more information about marks, see [Using Security Command Center security marks](#) (/security-command-center/docs/how-to-security-marks).

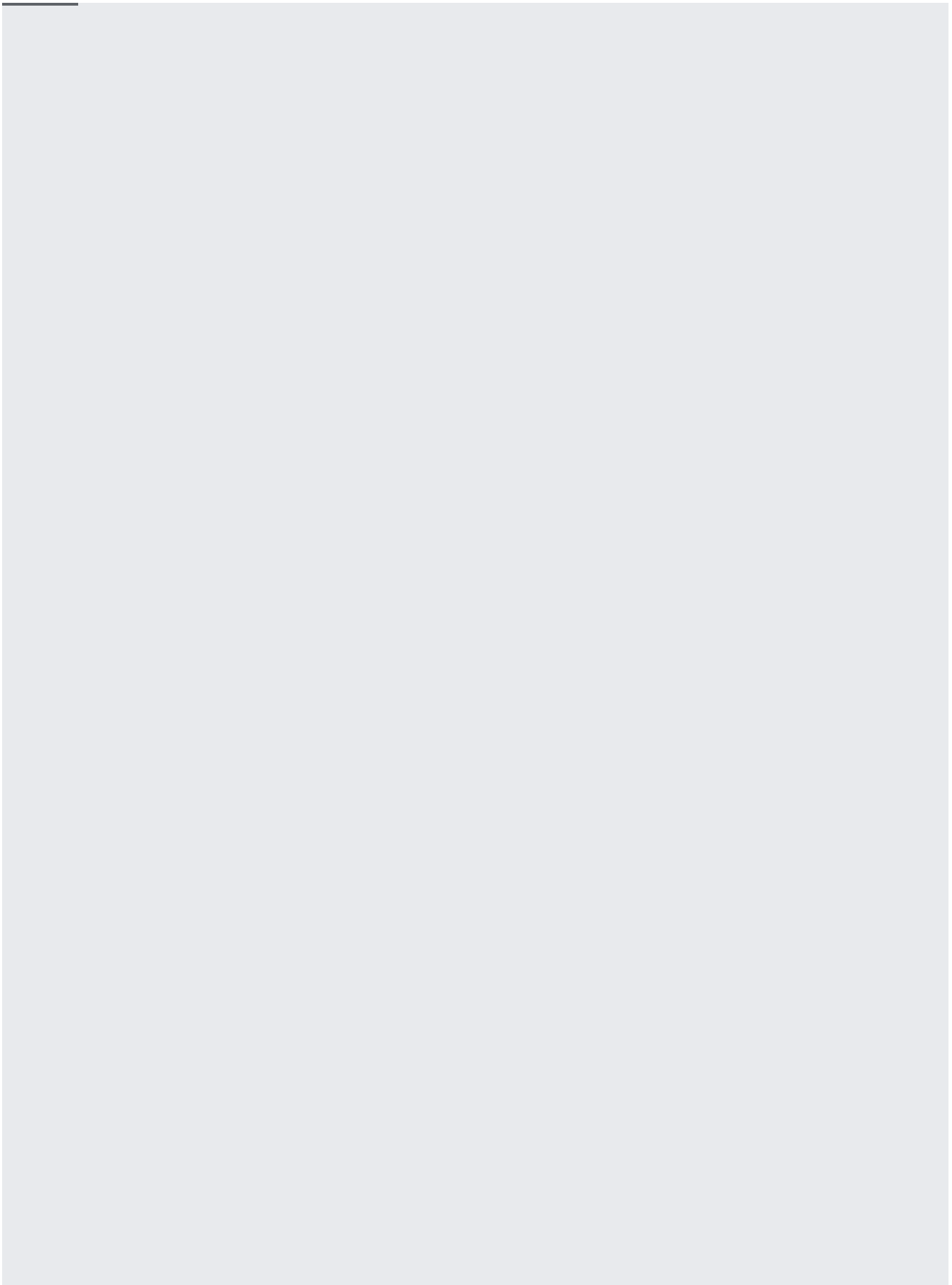
Create an active finding for a source.





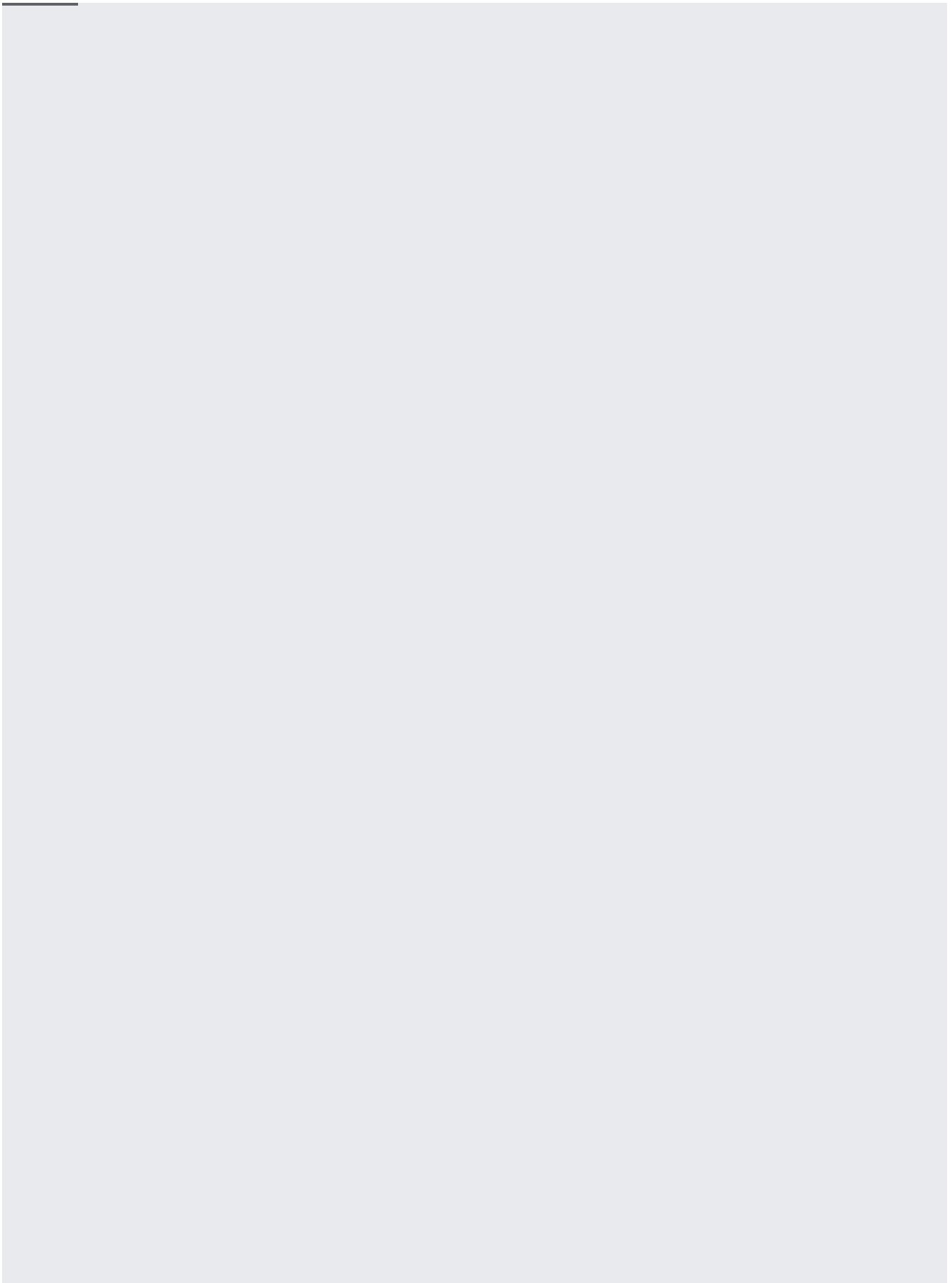


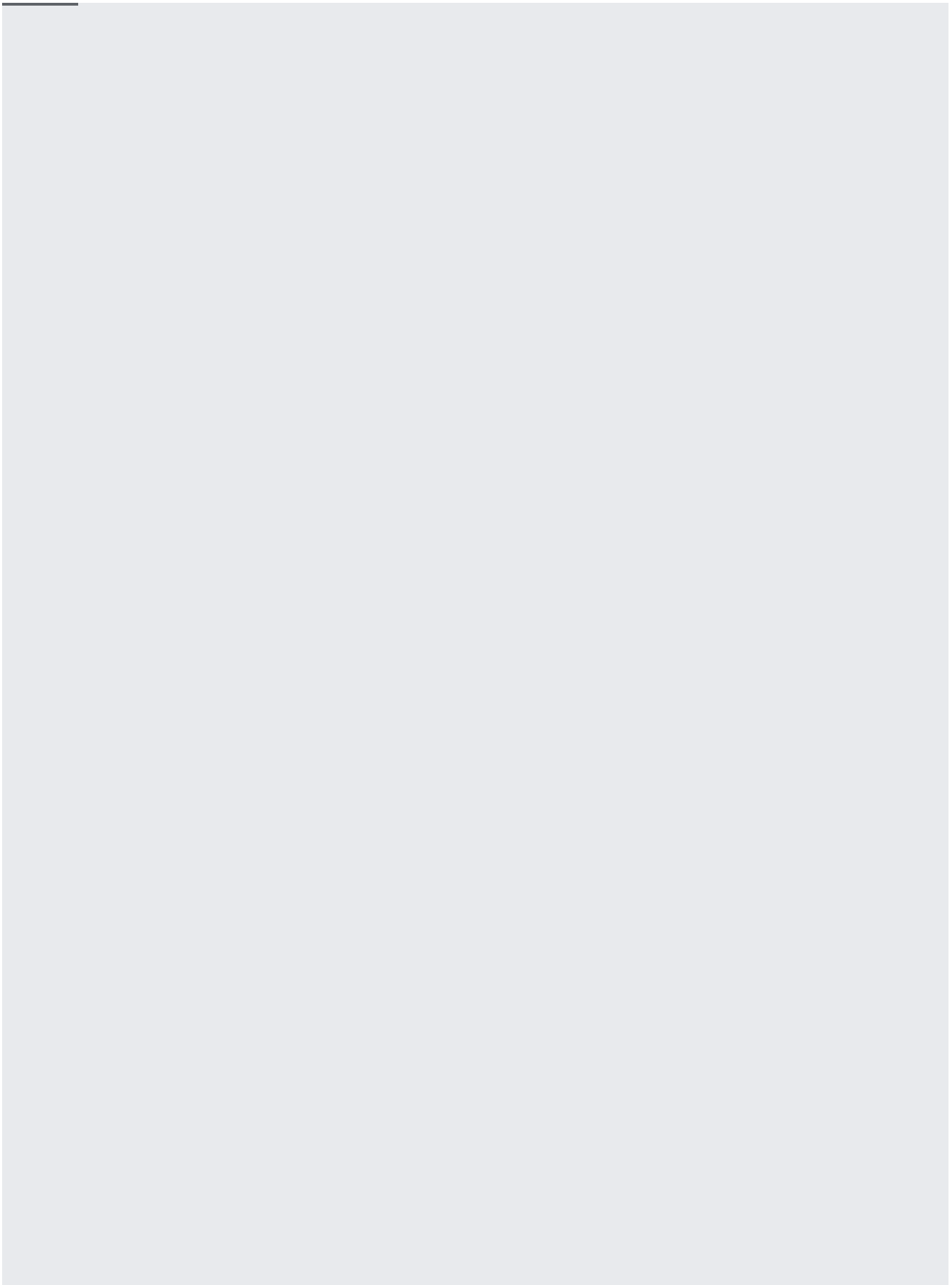


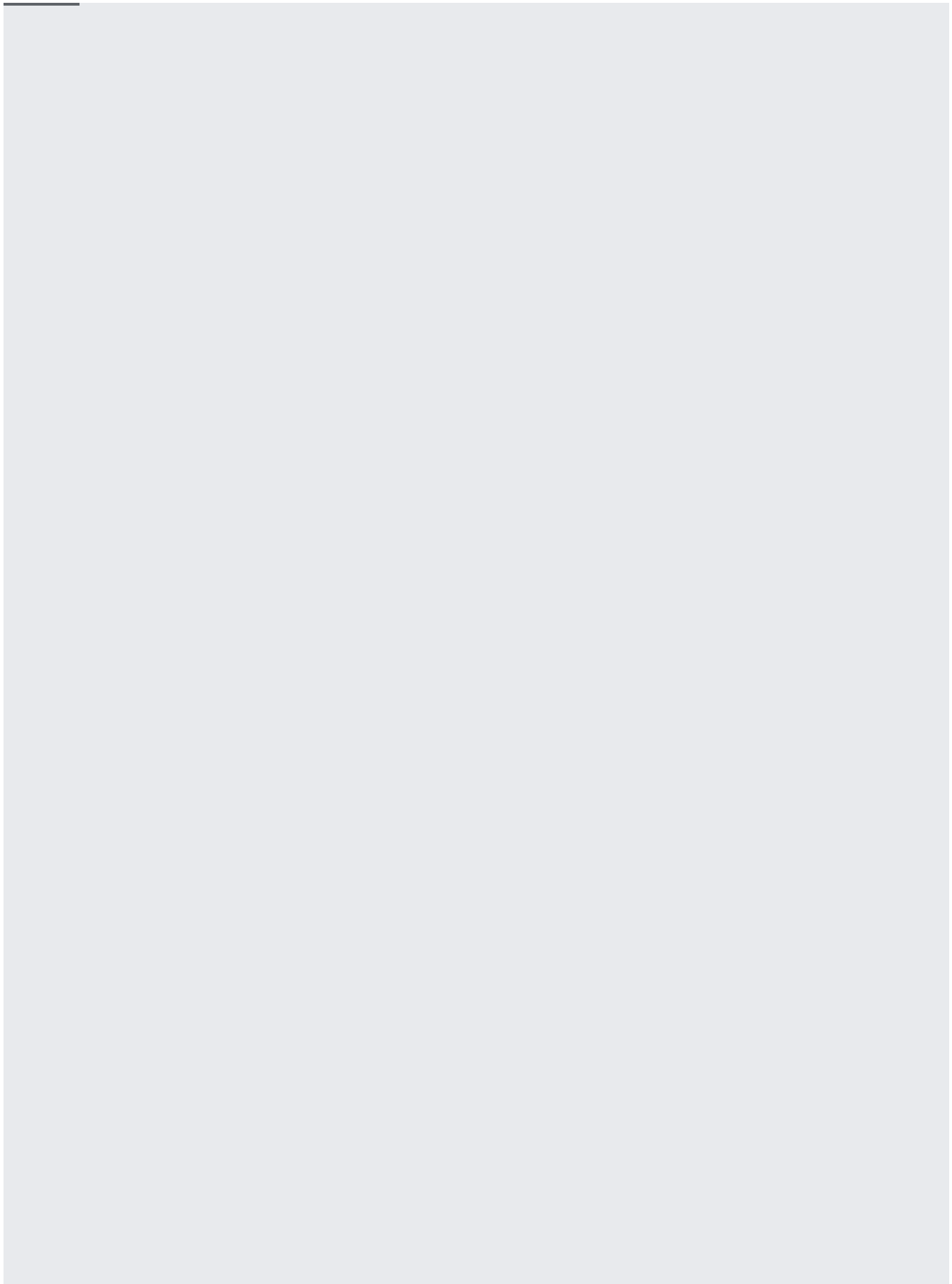


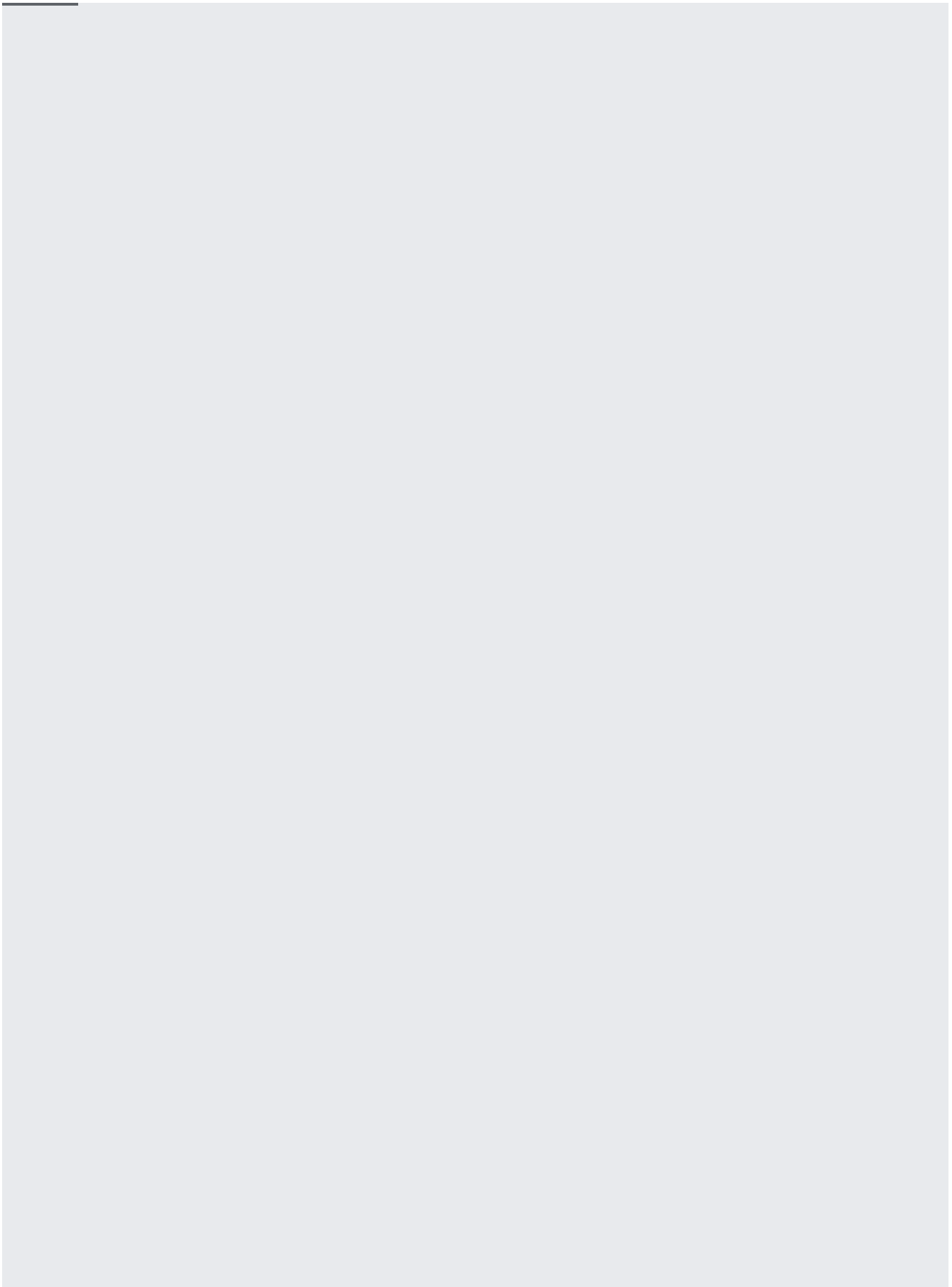
Security Command Center allows Sources to add context to findings through key-value metadata called "Source Properties." Source Properties can be initialized at creation time. The example below shows how to create a finding with source properties.

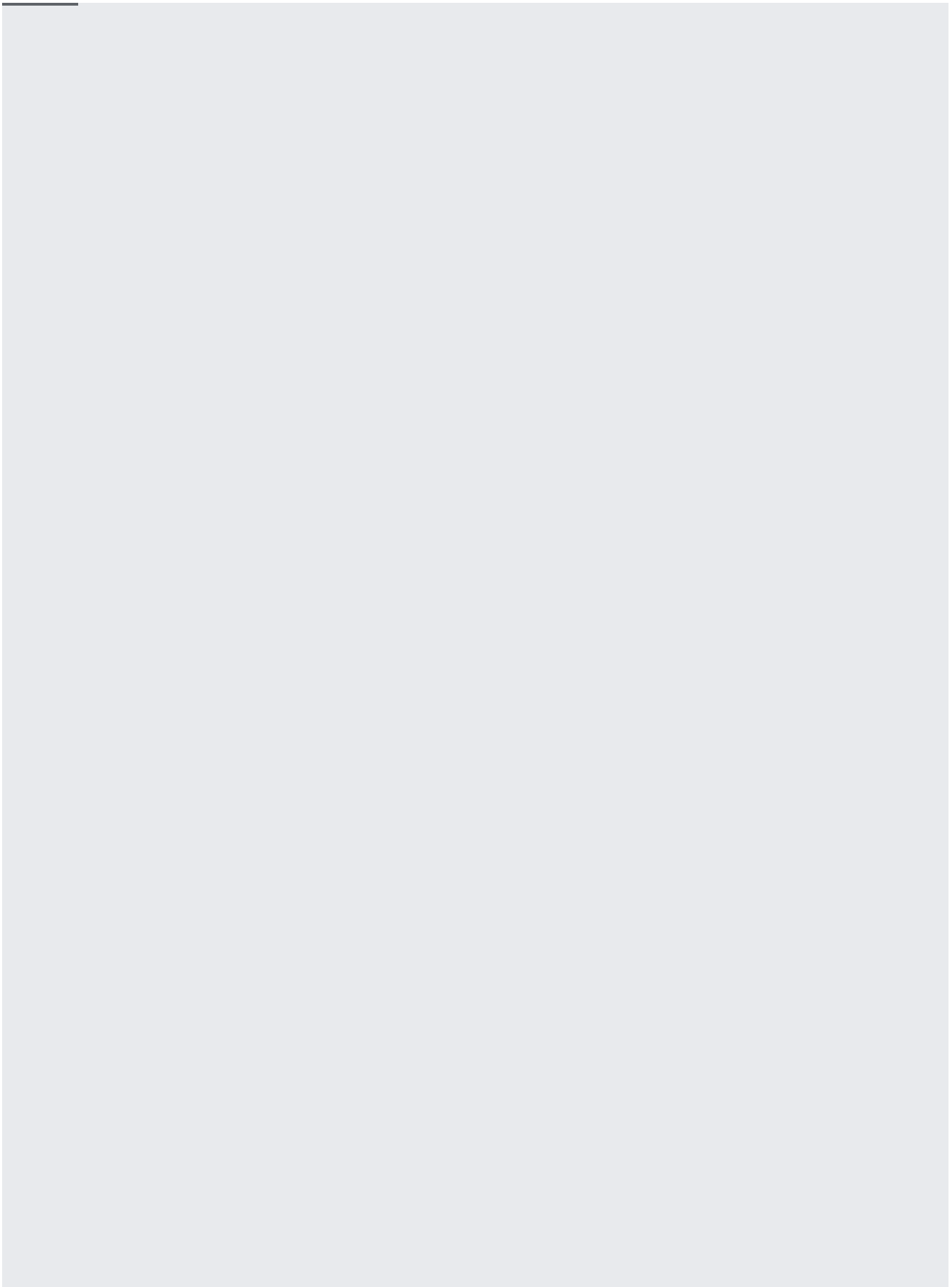
Create a finding with source properties. The length of the key names in the `source_properties` map must be from 1 to 255 characters, and must start with a letter and contain only alphanumeric characters or underscores. Security Command Center only supports values of boolean, number, and string.





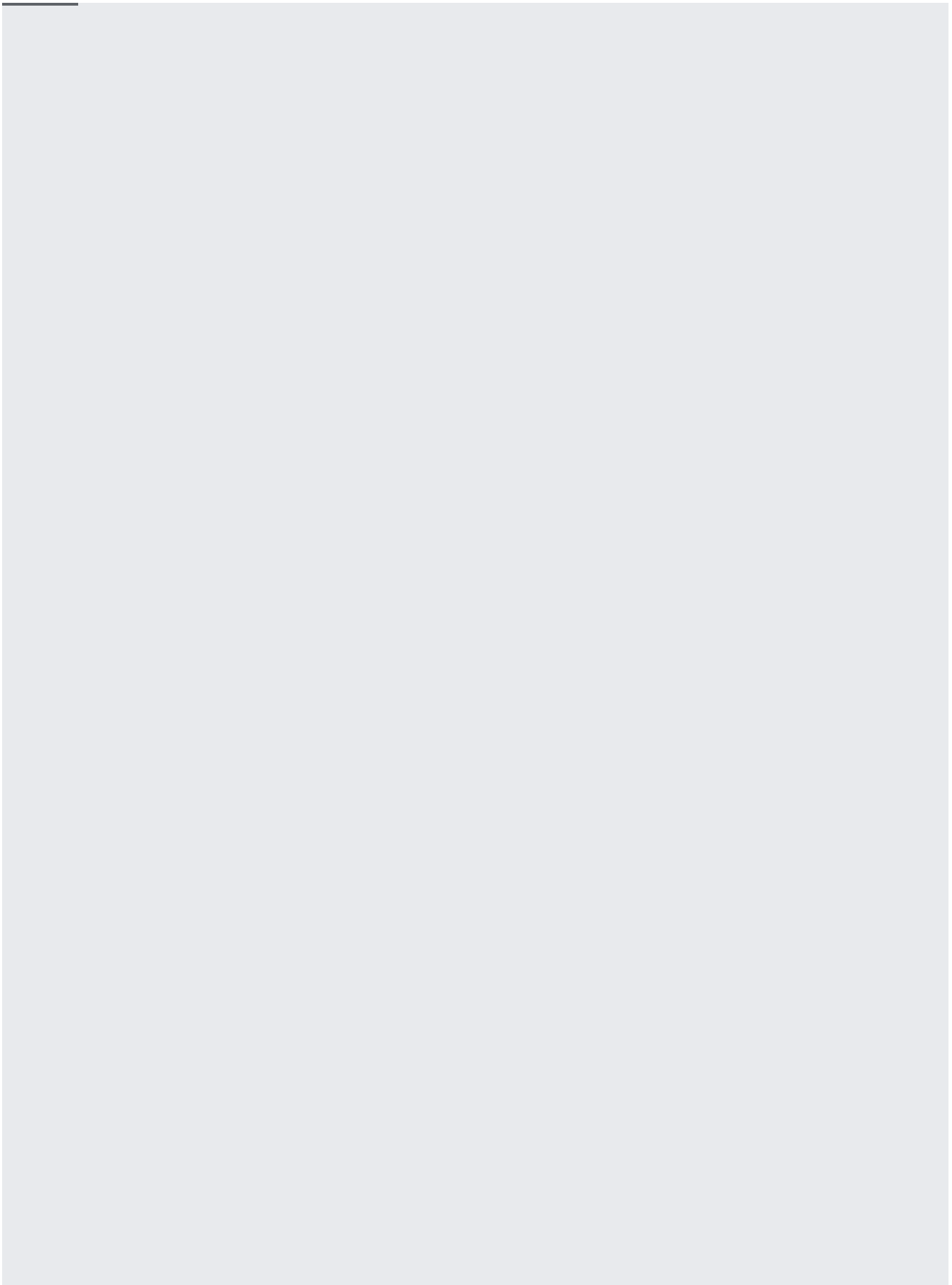


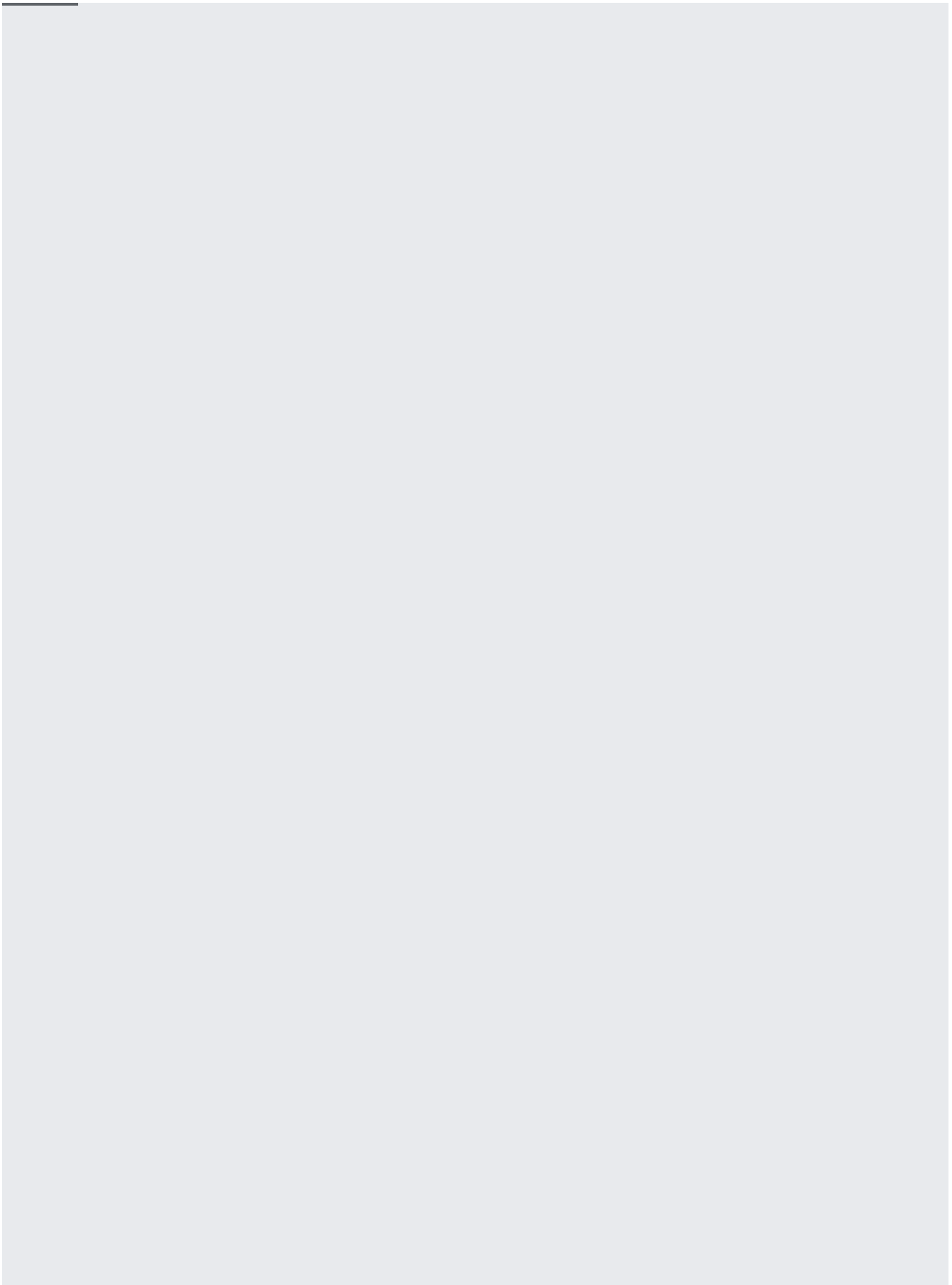


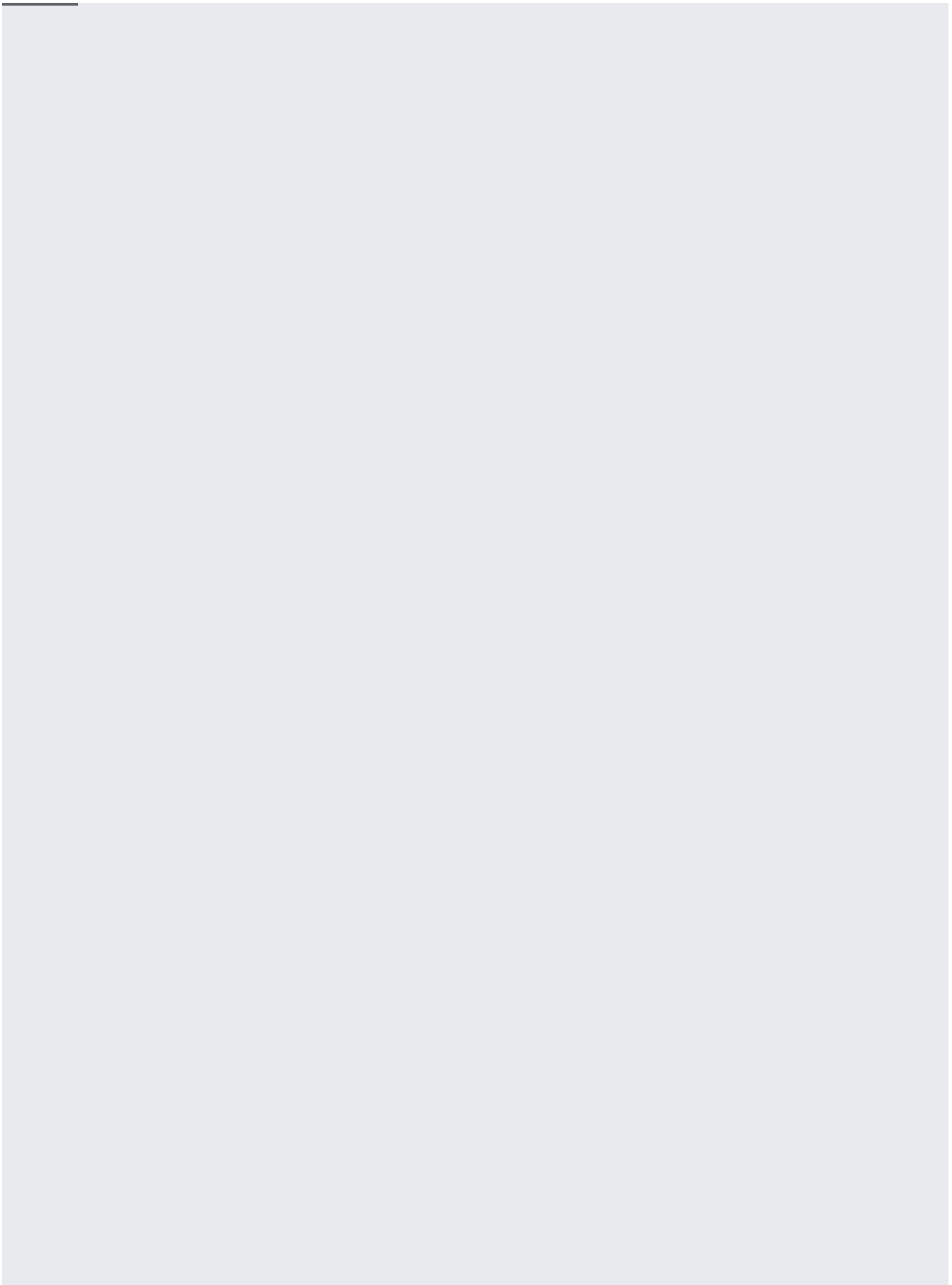


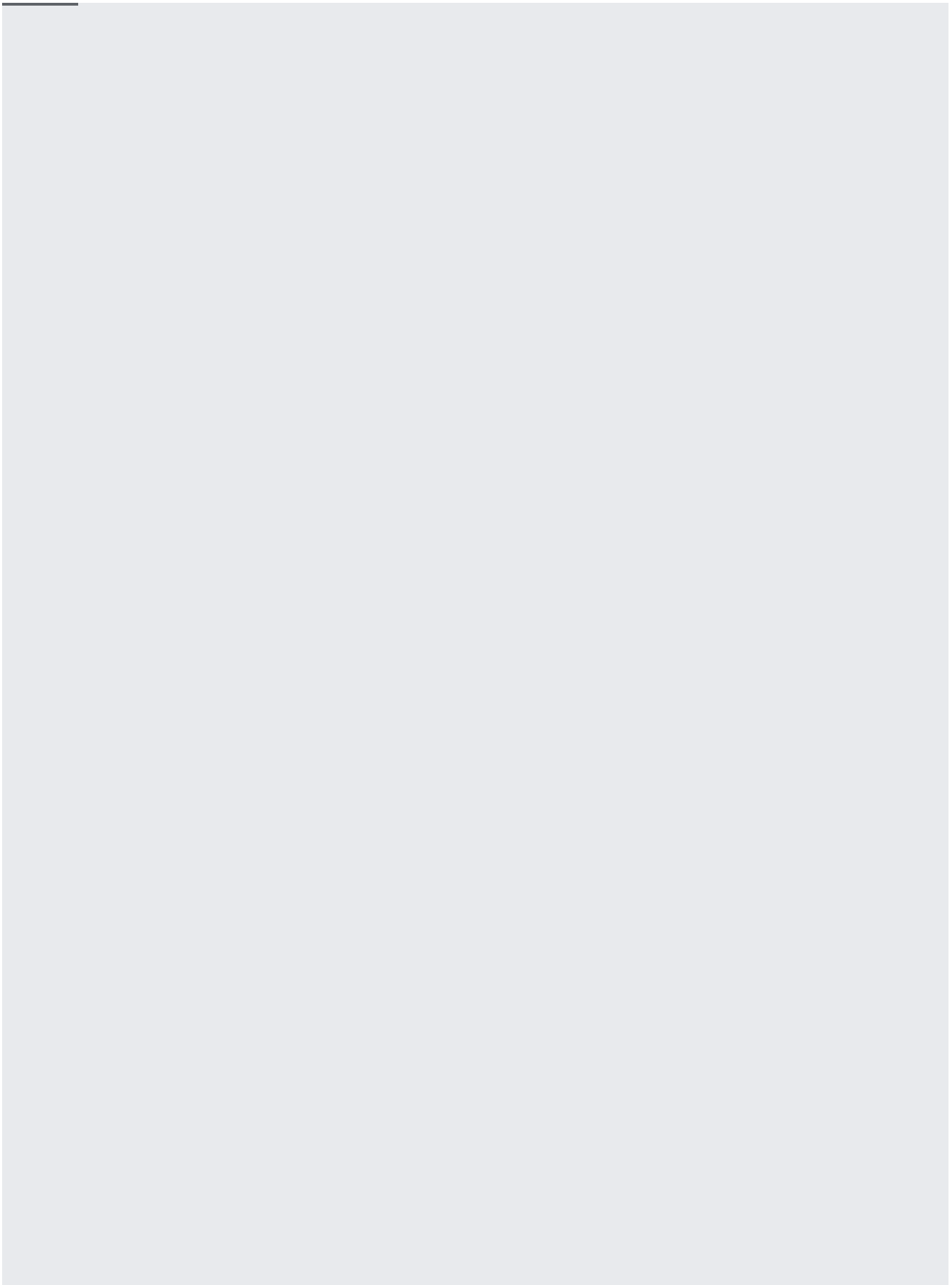
This example shows how to update individual source properties and the event time. It uses field masks to only update specific fields. Without the field masks, the new values replace all mutable fields on the finding.

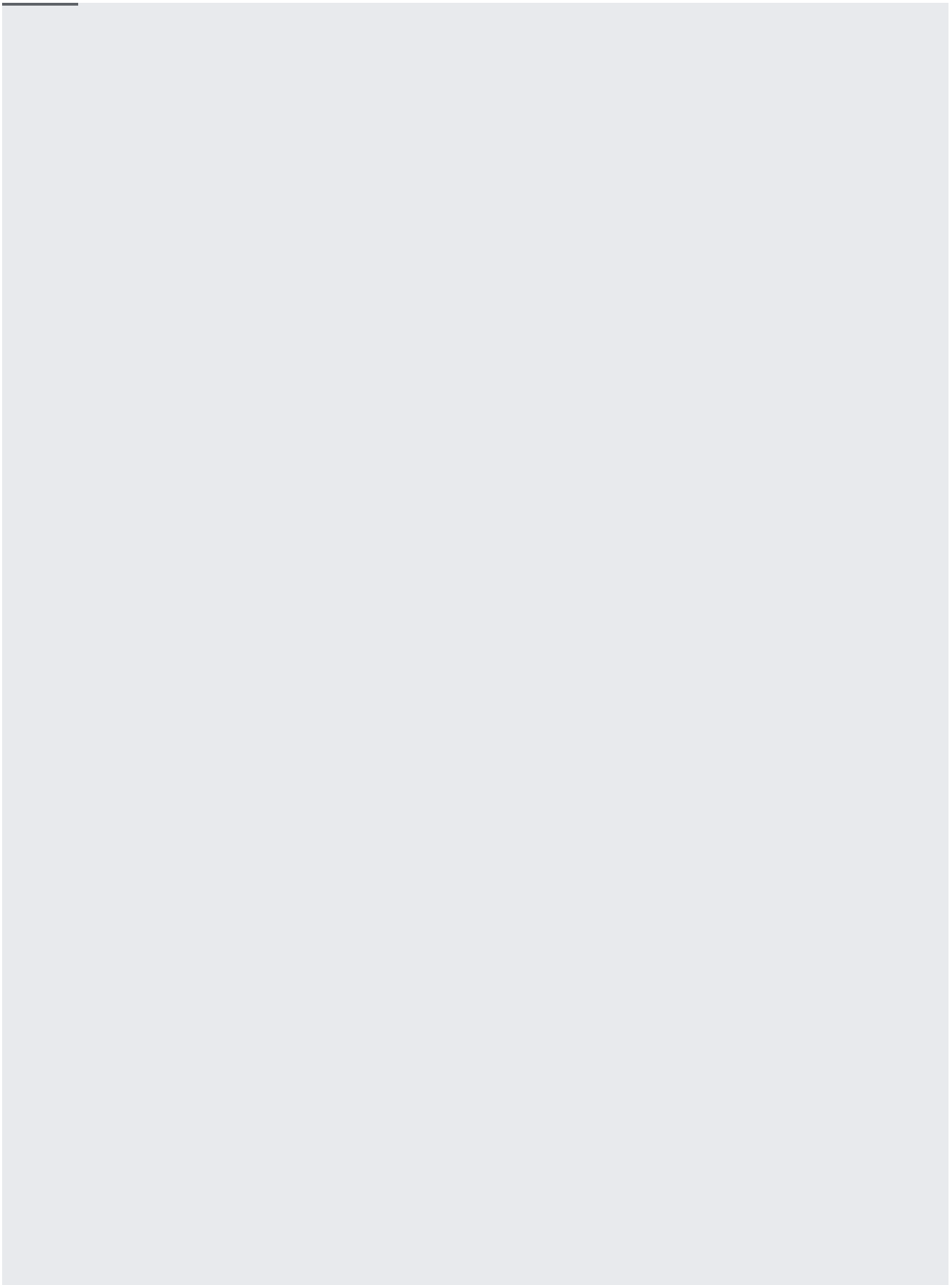
As with creating a new finding, the key names in the `source_properties` map must be between 1 and 255 characters, and must start with a letter and contain alphanumeric characters or underscores only. Security Command Center only supports values of boolean, number, and string.



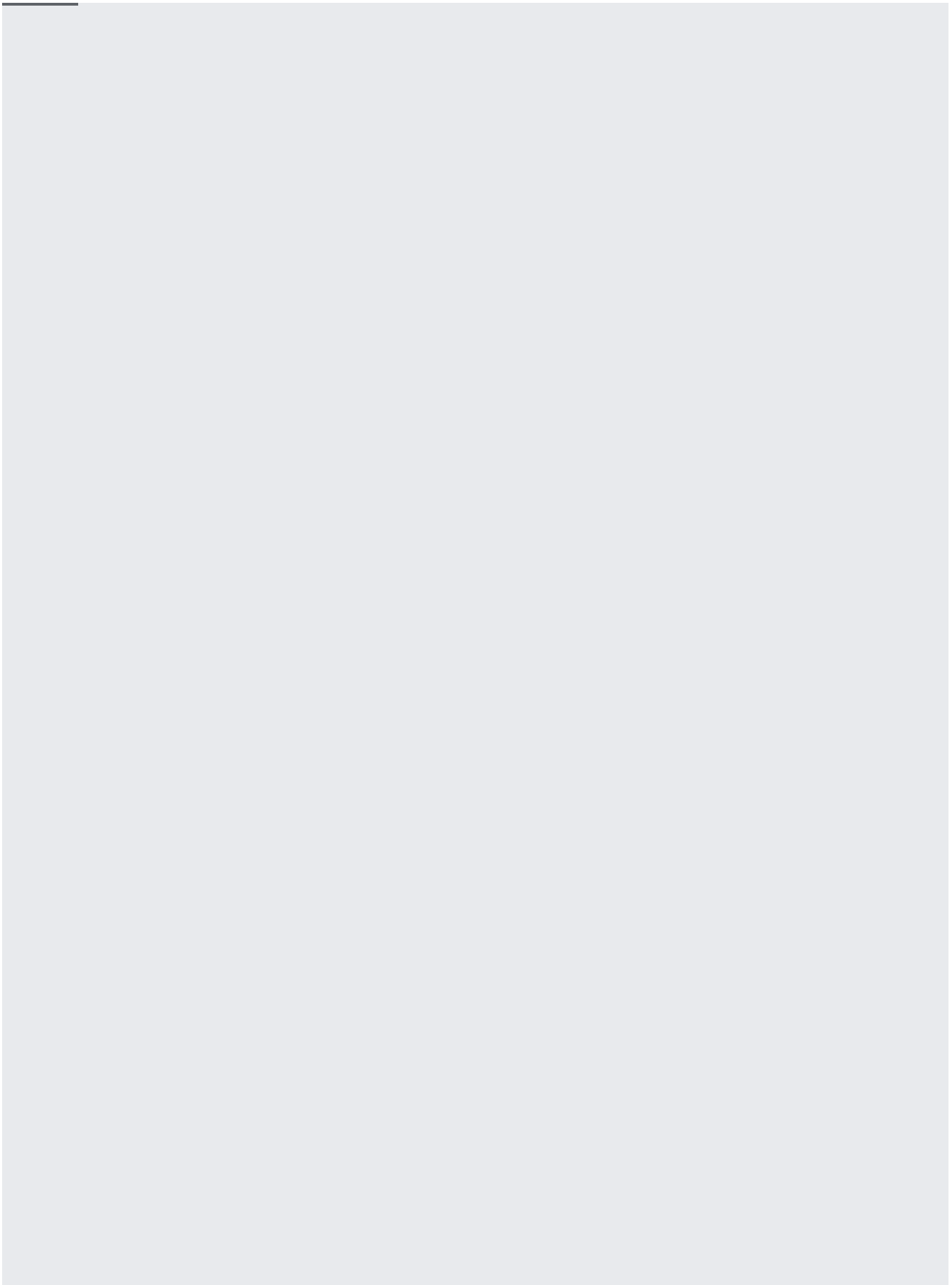


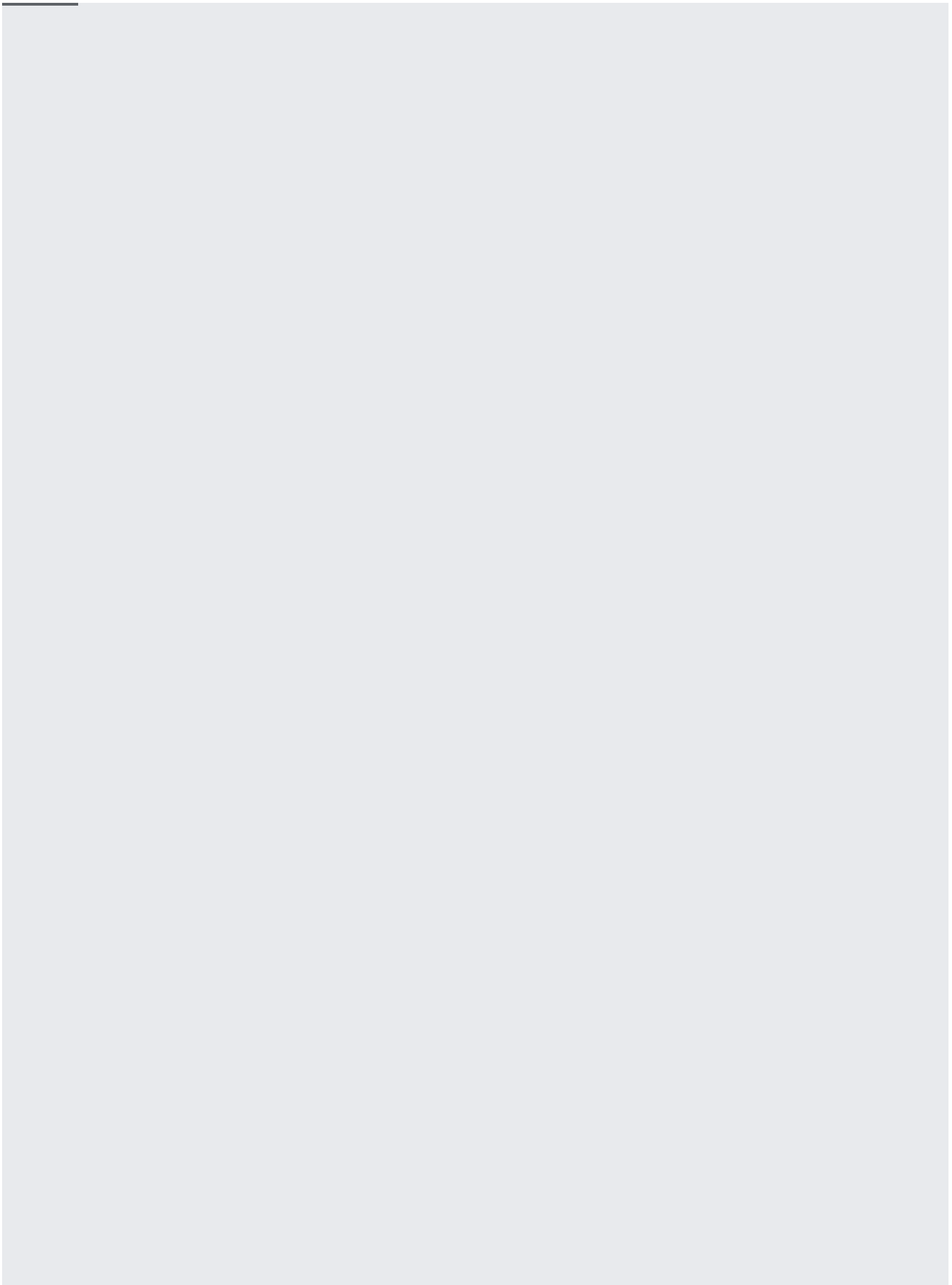


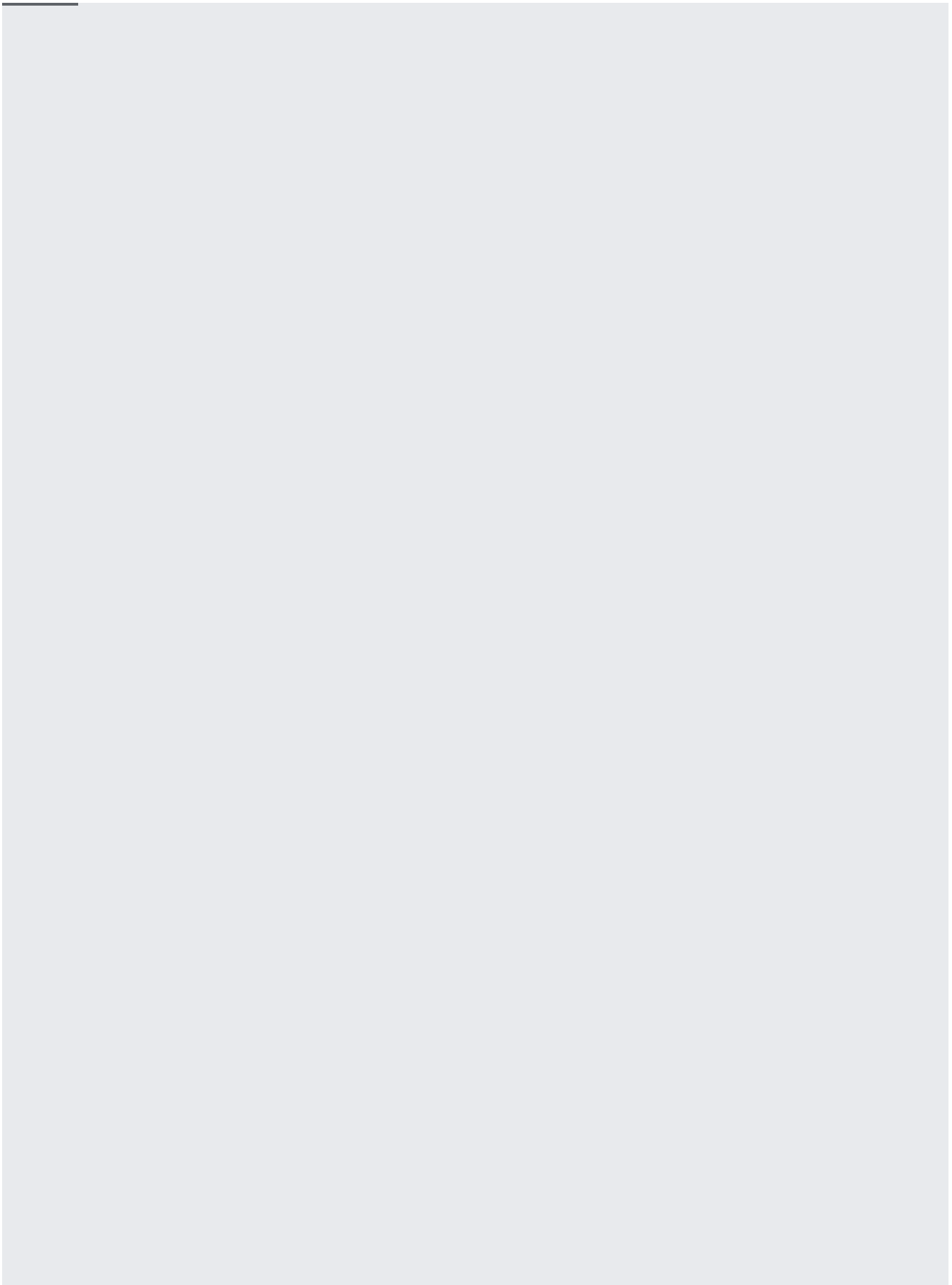




Security Command Center also provides an API to only update a finding's state. This API exists to provide a means of updating just the state of a finding. It is a simple API that also allows for permissioning principals to only be able to modify the state and no other aspect of a finding. The example below shows how to change a finding's state to inactive.







Creating and updating findings requires one of the following Cloud IAM permissions:

- Creating and updating findings: `securitycenter.findings.update`.
- Updating findings only: `securitycenter.findings.setState`.

If you can't create findings for a source, use the following code to confirm that your account has the required permissions listed in the [Before you begin](#) (`#before_you_begin`) section. If you don't have the necessary permissions, see [Creating and managing security sources](#) (`/security-command-center/docs/how-to-api-create-manage-security-sources`) to set up the appropriate Cloud IAM policies.

