Improving Google Chrome security

Scenario: Users in your organization use Google’s Chrome browser. To improve the security around this, you use the security event reporting that Google Chrome provides from Chrome browsers directly to the Google Admin console. The events reported cover a wide range of use cases which help to detect and mitigate several classes of attacks, possible vulnerabilities and any user misbehavior within managed Google Chrome browsers.

Using the Google Admin console, you can add Splunk as a Chrome Reporting connector to send these events to Splunk HTTP Entry Connector. The Google Admin console and APIs allow administrators to configure which events send to Splunk Cloud through custom filtering.

By using Splunk as a Chrome Reporting Connector, you can enhance the security of the Chrome browser through integrating with Splunk to receive events (such as malware transfer, unsafe site visit, password reuse, and password change) and selecting specific data sets to be processed.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Security analyst
- Technologies: Splunk Cloud Platform or Splunk Enterprise
- Add-on: Google Chrome Add-on for Splunk

How to use Splunk software for this use case

Depending on what information you have available, you might find it useful to identify some or all of the following:

- Malware transfer via Google Chrome
- Content transfer to or from Google Chrome
- Unscanned content shared to or from Google Chrome
- Sensitive data transferred via Google Chrome
- Unsafe site visit by Google Chrome user
- Enterprise password reused via Google Chrome outside corporate resources
- Google account passwords changed via Google Chrome

Results

Events that appear should be investigated further and assessed against your existing organizational policies.
Additional resources

These additional Splunk resources might help you understand and implement this use case:

- Splunk Docs: Set up and use HTTP Event Collector in Splunk Web