The Prime Hunt

Browser Extension

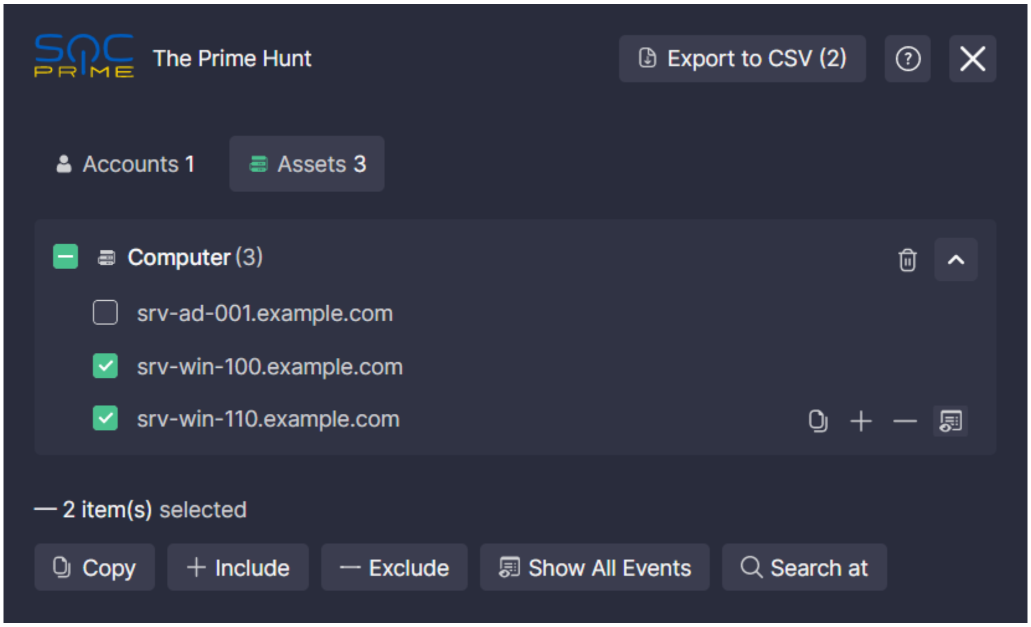
User Guide

Overview

The Prime Hunt is a browser extension for threat hunting. It introduces a One UI idea to simplify and speed up the investigation process regardless of the SIEMs or EDR in use. This is useful both for threat hunters starting off their careers and for seasoned professionals. The former can master the different security platforms and query languages faster, learning the right methodology from the very beginning, while the latter benefit from a streamlined workflow.

One UI for different technologies mirrors the concept of Sigma as a single language for cybersecurity. Sigma rules can be translated into multiple platform formats. This extension helps any threat hunter easily run and tune Sigma rule translations in those platforms, ensuring the community is Sigma-enabled. Meanwhile, sharing query hits (coming soon) helps the entire community measure and consolidate the MITRE ATT&CK® technique prevalence and rule quality.

With The Prime Hunt, you can easily see what accounts and assets are affected by the suspicious activity your query detects. Filter for or filter out query results by any field values with one click or look for all events related to them. Easily drill down to any CTI or any other sources that can help you in the investigation.



Computer (3)

- □ srv-ad-001.example.com
- ☑ srv-win-100.example.com
- ☑ srv-win-110.example.com

— 2 item(s) selected

If you have any questions, would like to give feedback, or need help, contact us at support@socprime.com.

Requirements

Supported browsers: Chrome, Firefox, Edge.
Supported security platforms: Microsoft Sentinel, Microsoft Defender for Endpoint.

Installation

Chrome

1. Open the three-dots menu and select **More Tools** > **Extensions**.
2. Make sure the **Developer mode** is **On**.
3. Click **Load unpacked** and select the **/dist/production/chrome** extension folder from your file system.

Firefox

1. Open the three-bars menu and select **Add-ons and Themes**.
2. Make sure the **Extensions** tab is selected on the left-side panel.
3. Click the gear icon on the right and select **Debug Add-ons**.
4. Click the **Load Temporary Add-on…** button and select the **/dist/production/firefox/manifest.json** file from your file system.

Edge

1. Open the three-dots menu and select **Extensions**.
2. Make sure the **Developer mode** is **On**.
3. Click **Load unpacked** and select the **/dist/production/edge** extension folder from your file system.

Compilation

You can install a compiled version of the extension for your browser from the `dist` folder or compile it yourself from the source files. To compile the extension:

1. Install Yarn from here: https://classic.yarnpkg.com/lang/en/docs/install
2. Run console commands in your source root folder:

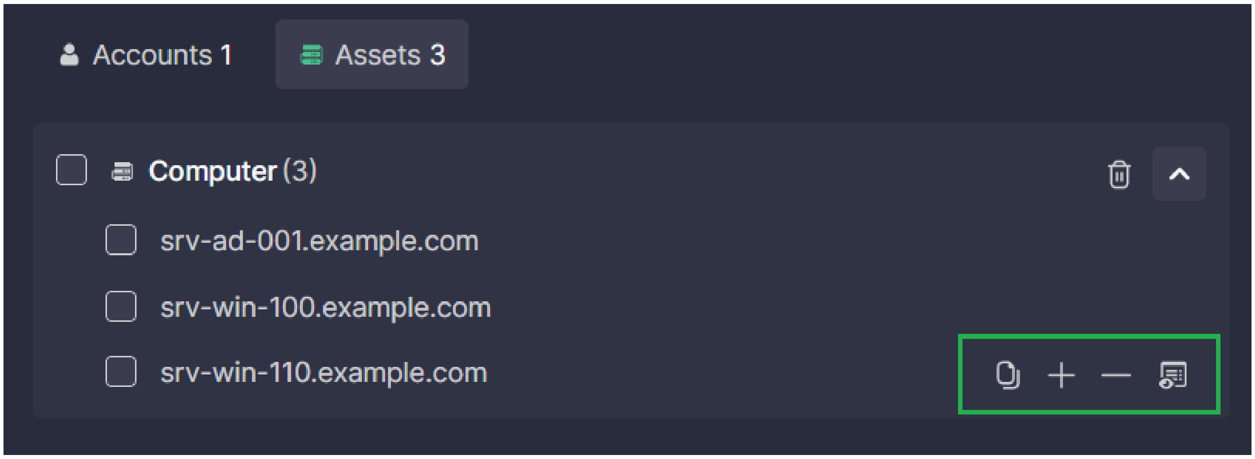
```
yarn install
yarn extension --mode=development|production
```

How to Use

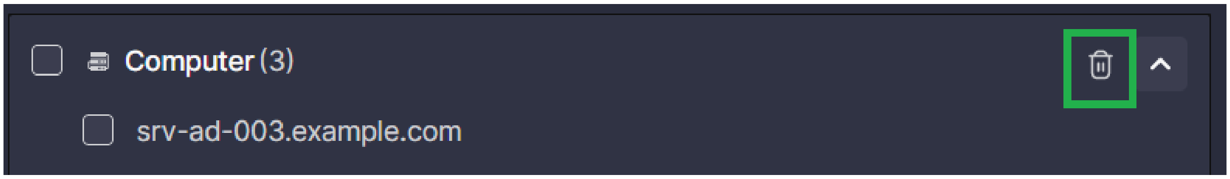
1. Go to your SIEM/EDR/XDR environment and start the extension from the Extensions panel next to the address bar. You can resize the extension's window by dragging its edges. To move the window, hover over the extension's name and drag it.

   Note:
   The position and size of the extension's window are stored as the `the-prime-hunt--extension--position` key in the local storage of your browser (developer tools > Application > Local Storage > your security platform). If you delete the value of the key (right-click > Delete), the default position and size are used.

2. Run a query in your SIEM/EDR/XDR environment. If there are results, the extension lists the accounts and assets affected by the suspicious activity.
3. In the extension, click the down arrow on a tab to show results.
4. Hover over a result:



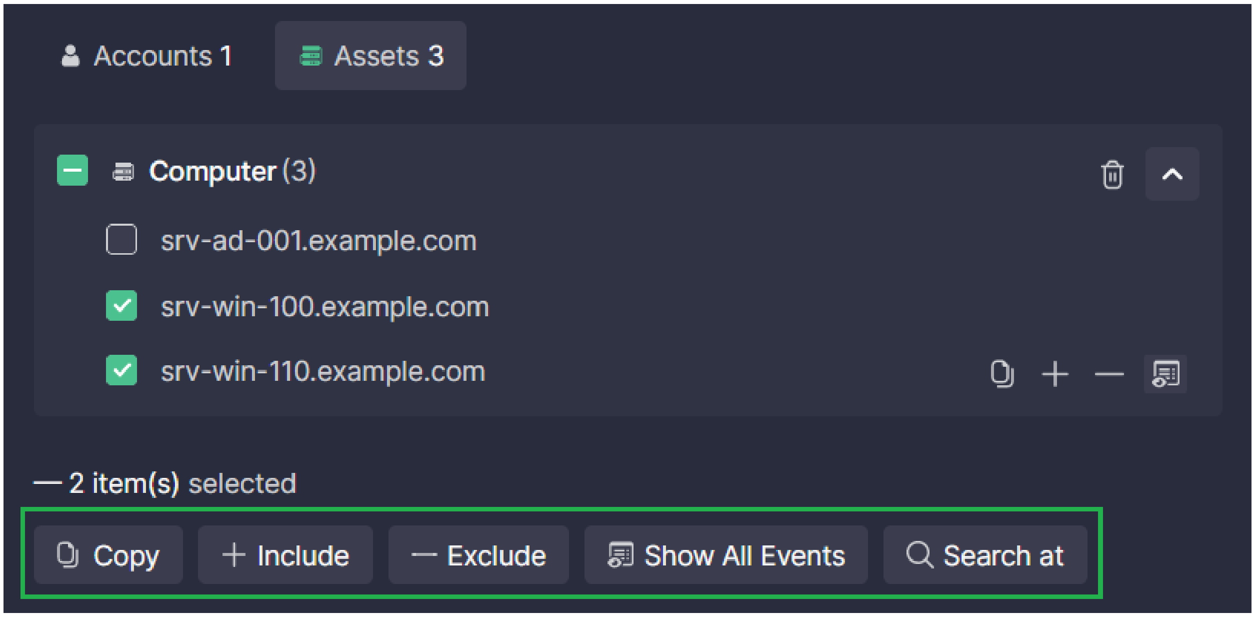
- Click the copy icon to copy the result to the clipboard
- Click the plus icon to include the account/asset in the search
- Click the minus icon to exclude the account/asset from the search
- Click the eye-and-list icon to search for all events that involve the account/asset
- To add a field to the active tab in the extension, click on the field in your security platform holding the Alt (Option on Mac) key. To remove a field from the extension, click on the remove icon next to the field.



Note:
The fields that have been added manually are stored as the `the-prime-hunt--extension--watchers` key in the local storage of your browser (developer tools > Application > Local Storage > your security platform). If you delete the value of the key (right-click > Delete), only the default fields are used again.

5. You can also select multiple results by setting the checkboxes next to them. In this case, bulk action buttons appear at the extension’s footer:
    - Click the **Copy** button to copy the selected accounts/assets to the clipboard
    - Click the **Include** button to include the selected accounts/assets in the search
    - Click the **Exclude** button to exclude the selected accounts/assets from the search

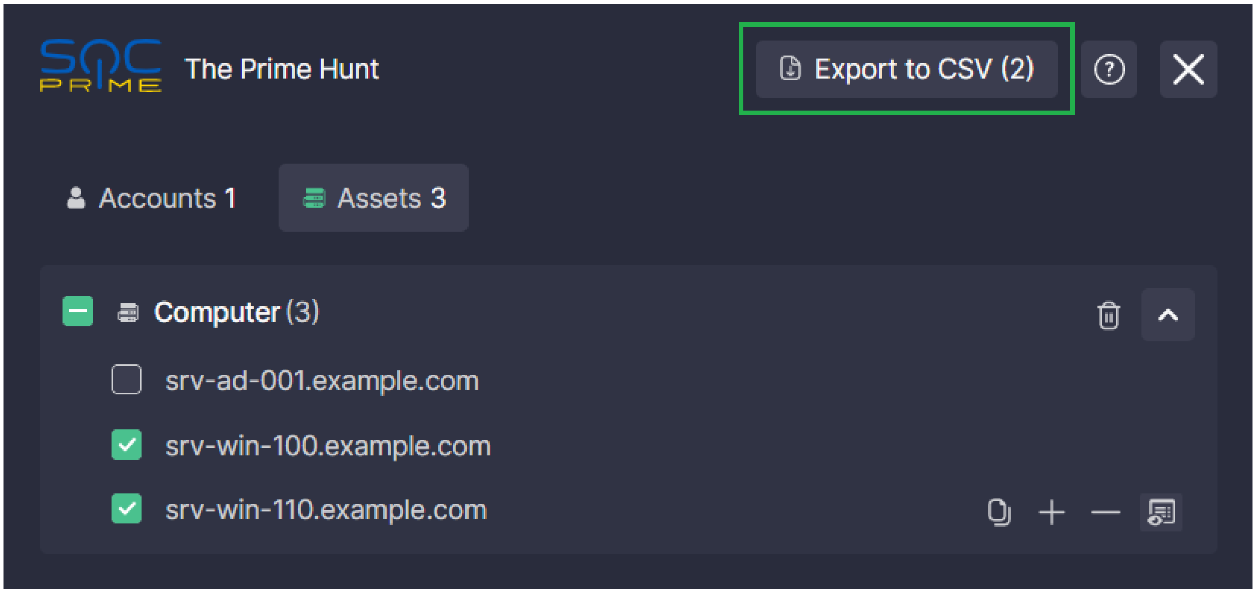
- Click the **Show All Events** button to search for all events that involve the selected accounts/assets
- Click the **Search At** button and select a CTI source to analyze the selected accounts/assets. Default options include VirusTotal, VirusTotal Enterprise, and Anomali. You can customize or remove any menu item, add your OpenCTI credentials, or add a new integration in **Search Settings**



☐ srv-ad-001.example.com
☑ srv-win-100.example.com
☑ srv-win-110.example.com

— 2 item(s) selected

- Optionally, export the selected results as a CSV



Computer (3)

□ srv-ad-001.example.com

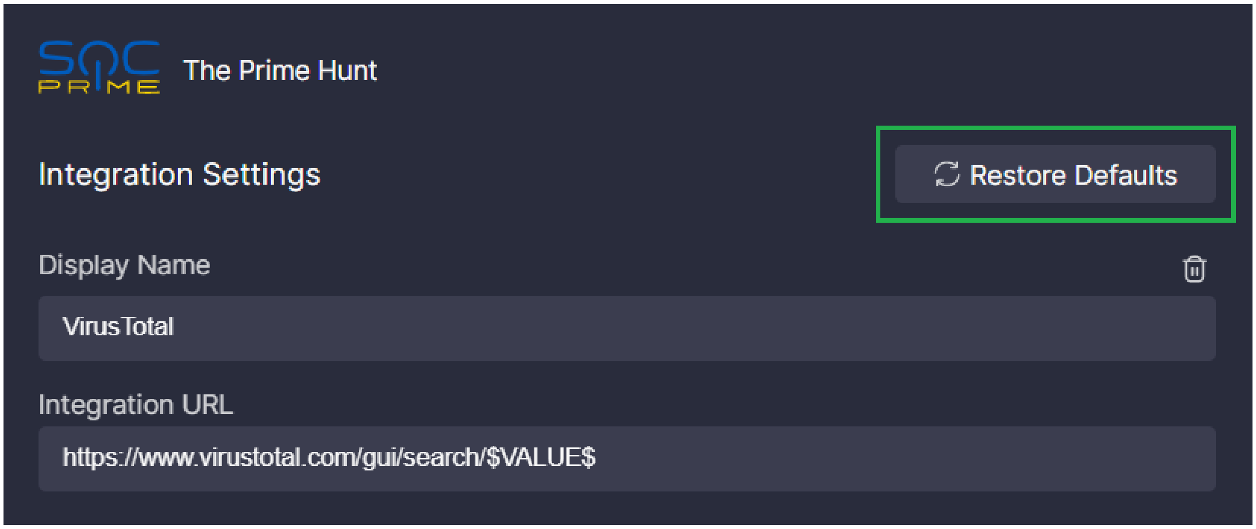
☑ srv-win-100.example.com

☑ srv-win-110.example.com

6. If you need to reset the extension, go to the Extensions page in your browser's settings and click **Reload** (or the related icon). Reloading does not affect the custom settings of position and size of extension, integrations, and watching fields (to reset them you should clear specific keys in your browser's local storage.)

Search Settings

Custom integration names and URLs are stored as the `the-prime-hunt--extension--integrations` key in the local storage of your browser (developer tools > Application > Local Storage > your security platform). If you delete the value of the key (right-click > Delete) or click **Restore Defaults** in the extension's UI, the default names and URLs are used.



Integration Settings

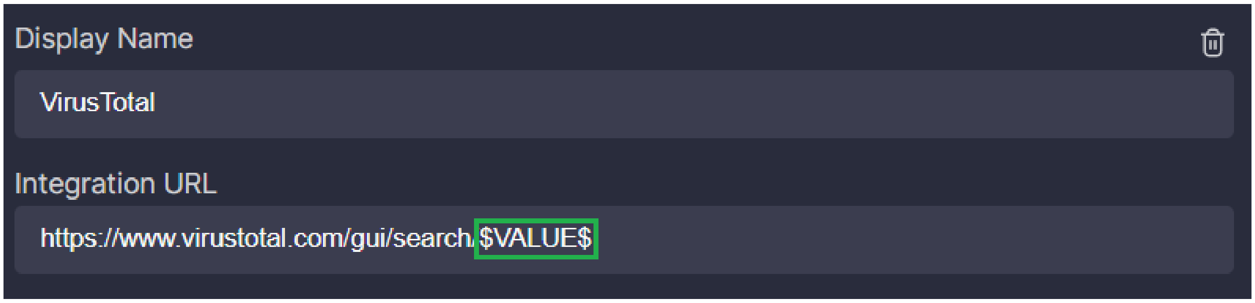
Display Name: VirusTotal

Integration URL: https://www.virustotal.com/gui/search/$VALUE$

By default, when you select an option in the **Search At** dropdown menu, an analysis of each selected result is opened in a new tab. The only exception is VirusTotal Enterprise where a single new tab is opened for all results. By default, the browser blocks opening multiple tabs, so please allow pop-ups when prompted to do so.

Opening multiple results in a single or multiple tabs is defined by the `$VALUE$` and `$VALUES$` markers in the integration URL:

- `$VALUE$`: each result is opened in a separate new tab
- `$VALUES$`: all results are opened in a single new tab

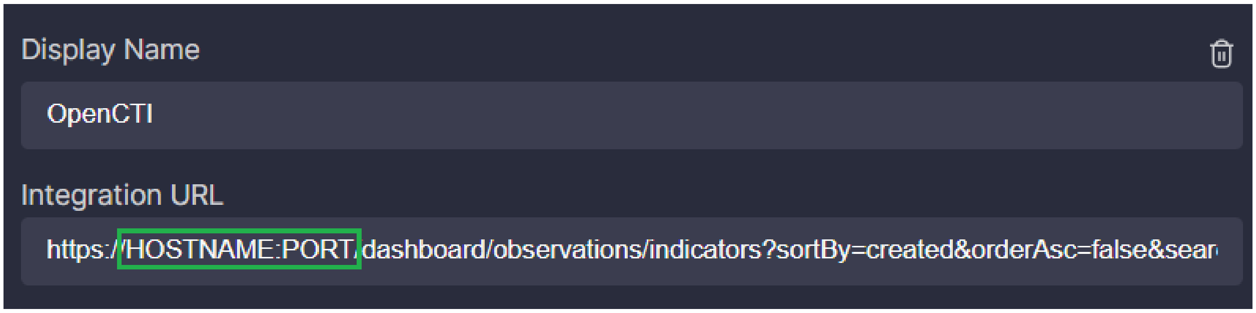


Display Name: VirusTotal

Integration URL: https://www.virustotal.com/gui/search/$VALUE$

Customize this marker to change the behavior.

To use the OpenCTI integration, replace the `HOSTNAME:PORT` placeholder in the OpenCTI integration URL with the hostname and port of your account.



Display Name

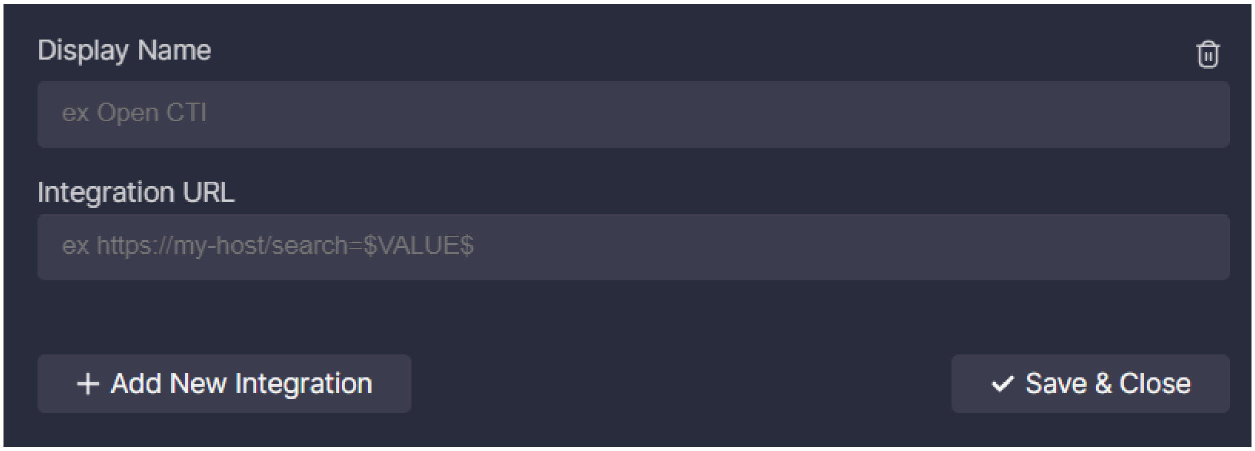
OpenCTI

Integration URL

https://HOSTNAME:PORT/dashboard/observations/indicators?sortBy=created&orderAsc=false&sear

You can add an integration with any service. To create a new integration:

1. Click **Add New Integration**.
2. Enter the display name that will be shown in the **Search At** menu.
3. Enter the integration URL.
4. Click **Save & Close**.



Display Name

ex Open CTI

Integration URL

ex https://my-host/search=$VALUE$

To delete an integration, click the remove icon next to it.

NOTE: The Prime Hunt browser extension does not send any data outside your laptop/browser. It works only with the data that is on the page of your browser.