Login

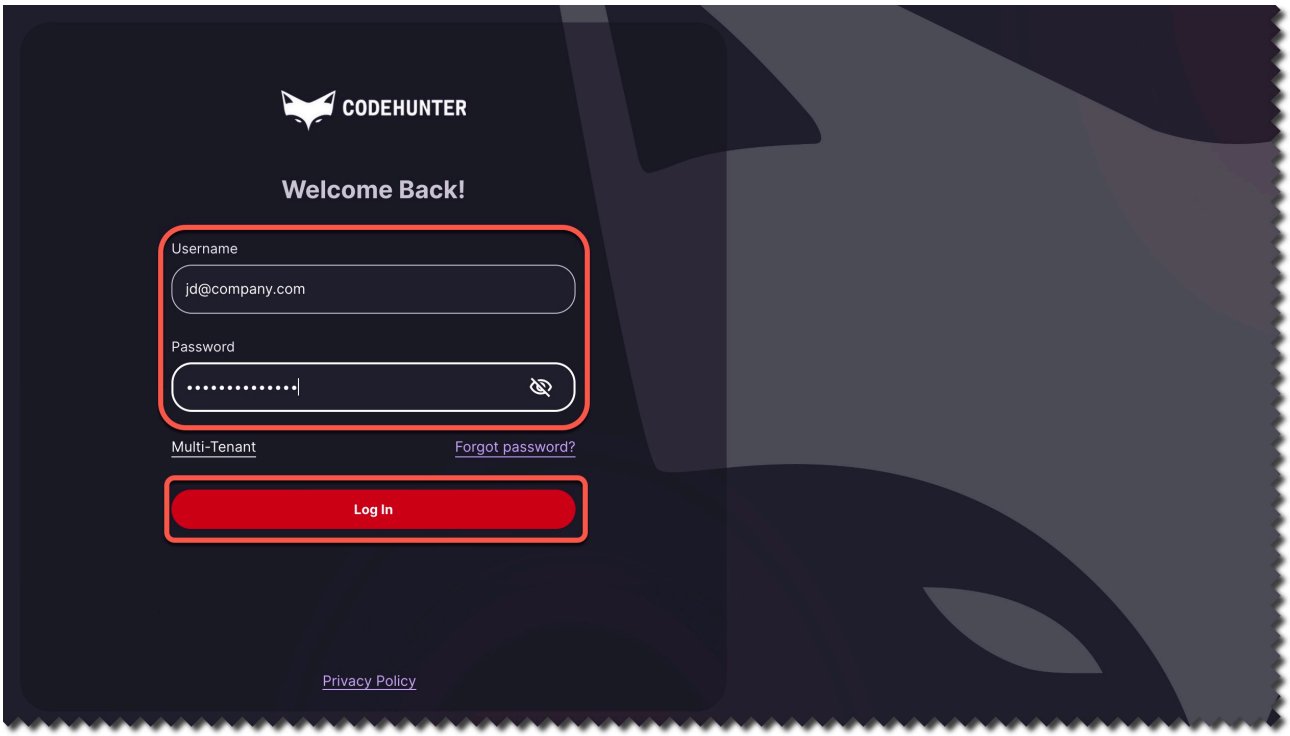
Updated on 12 Jan 2024 · 1 Minute to read · Contributors

> **Note**
>
> If a VPN is required to connect to your CodeHunter instance, ensure it's running before trying to log in. Contact your administrator for more information.

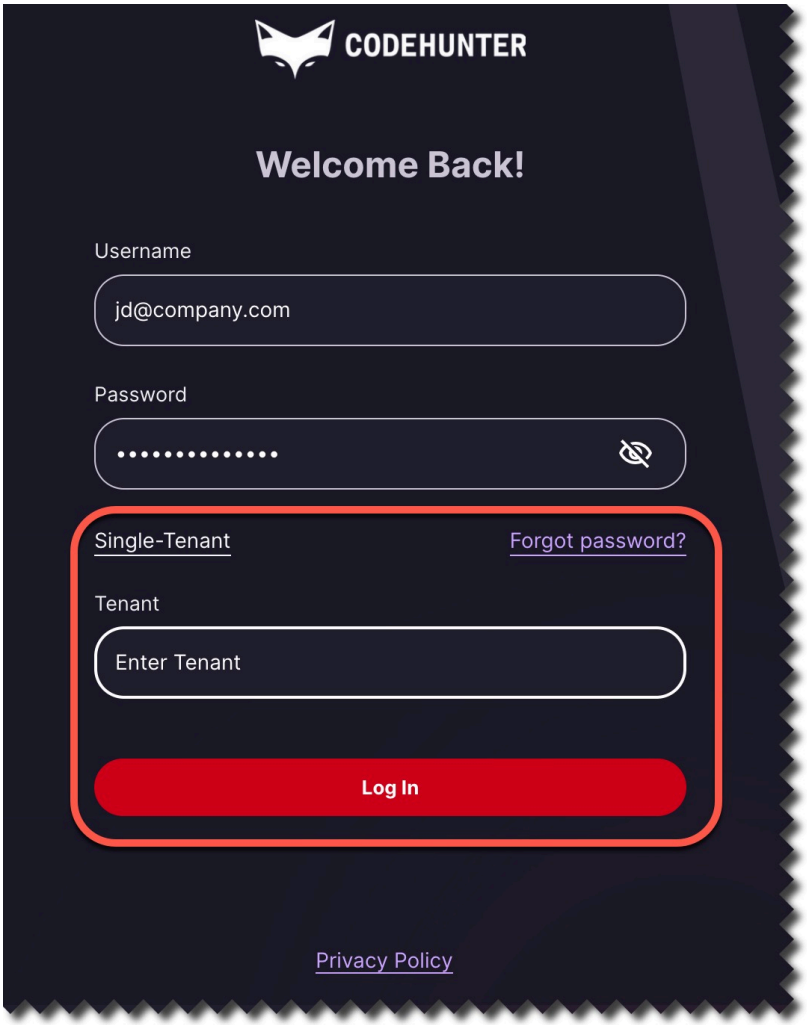
To login to your CodeHunter account, follow the steps below.

1. Type in the URL to your CodeHunter account in a browser.

2. On the login page, enter your **Username** and **Password**. Then, click **Log In**.



If you are not on a **Multi-Tenant**, click to change to **Single Tenant**, then enter the **Tenant** name.

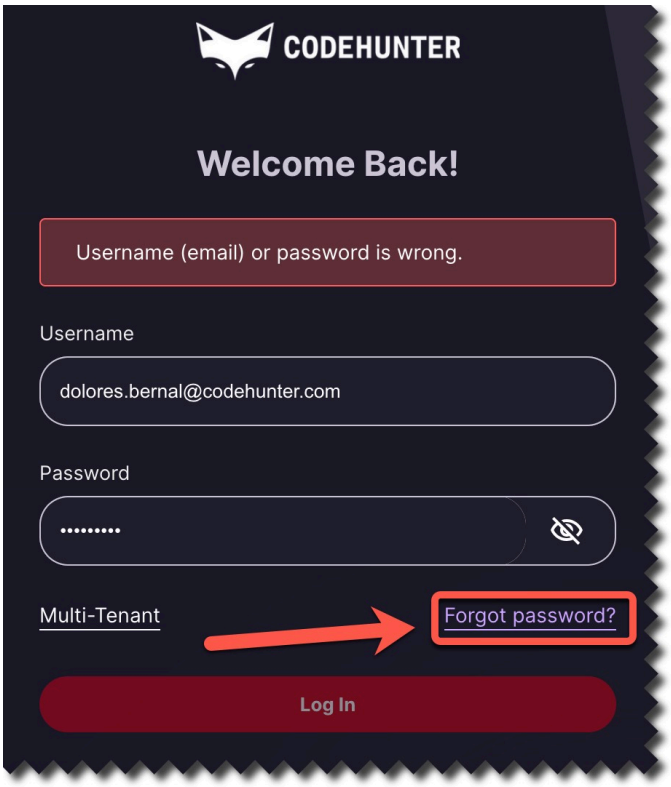


When you are done, click **Log In**.

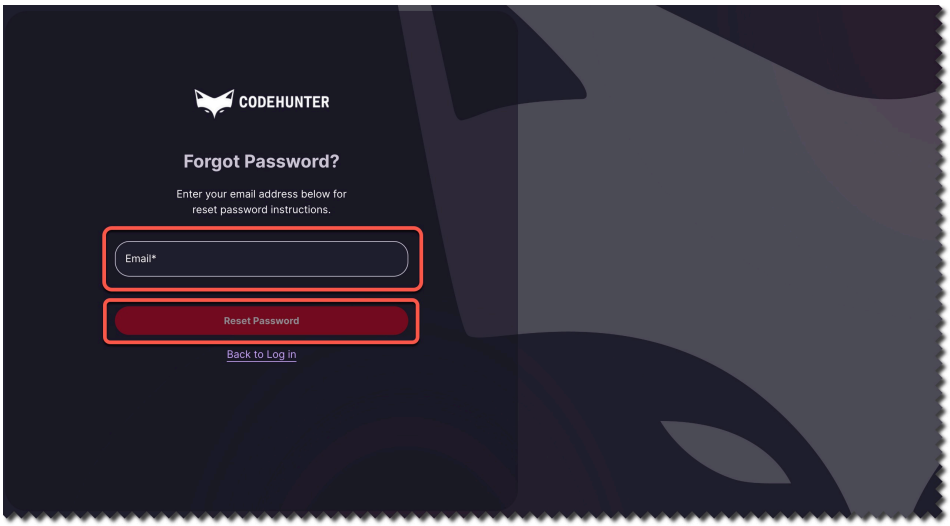
Forgot Password

If you are have trouble logging or have forgotten your password, follow these steps.

1. At the login page, click **Forgot Password?**



2. Next, provide your login email, then click **Reset Password**.



An email will be sent to your account to create a new password.

Previous
Contacting Support

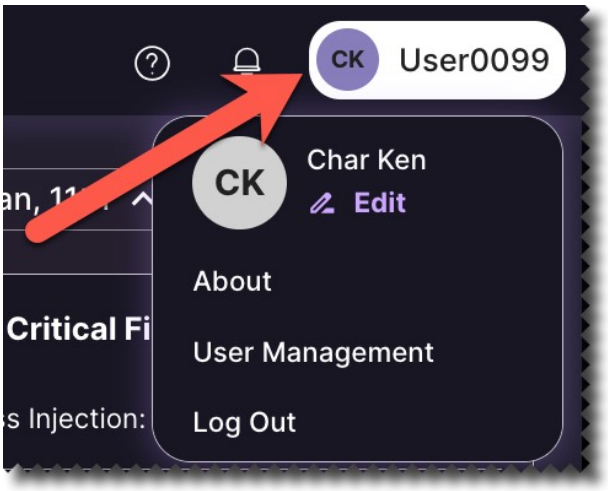
Next
User Profile Settings

User Profile Settings

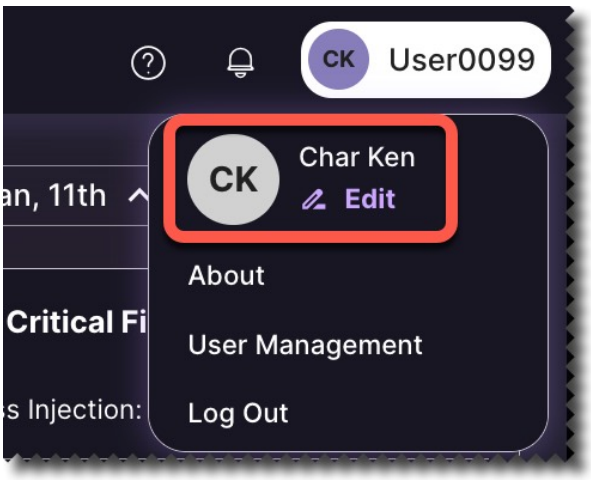
Updated on 12 Jan 2024 · 1 Minute to read · Contributors

You can add or modify you account's profile at any time. To do this, follow the steps below.

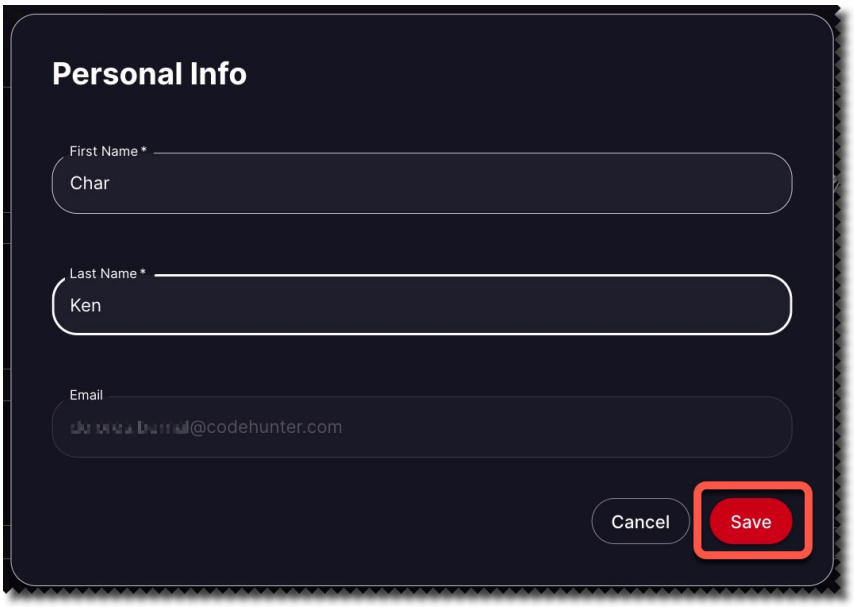
1. Click your avatar on the top right corner of the page.



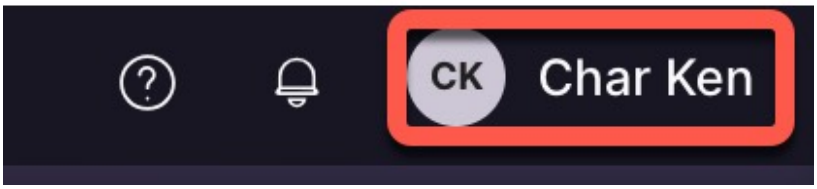
2. Next, click **Edit**.



3. In the dialog window, add or modify your **First Name** and **Last Name**. When you are done, click **Save**.

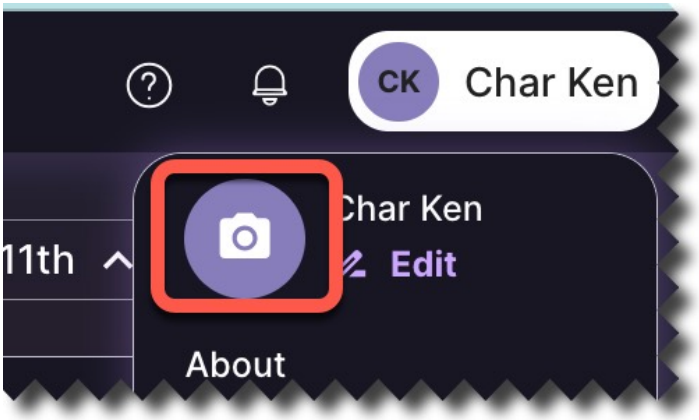


Your first and last name will now be visible on your avatar.

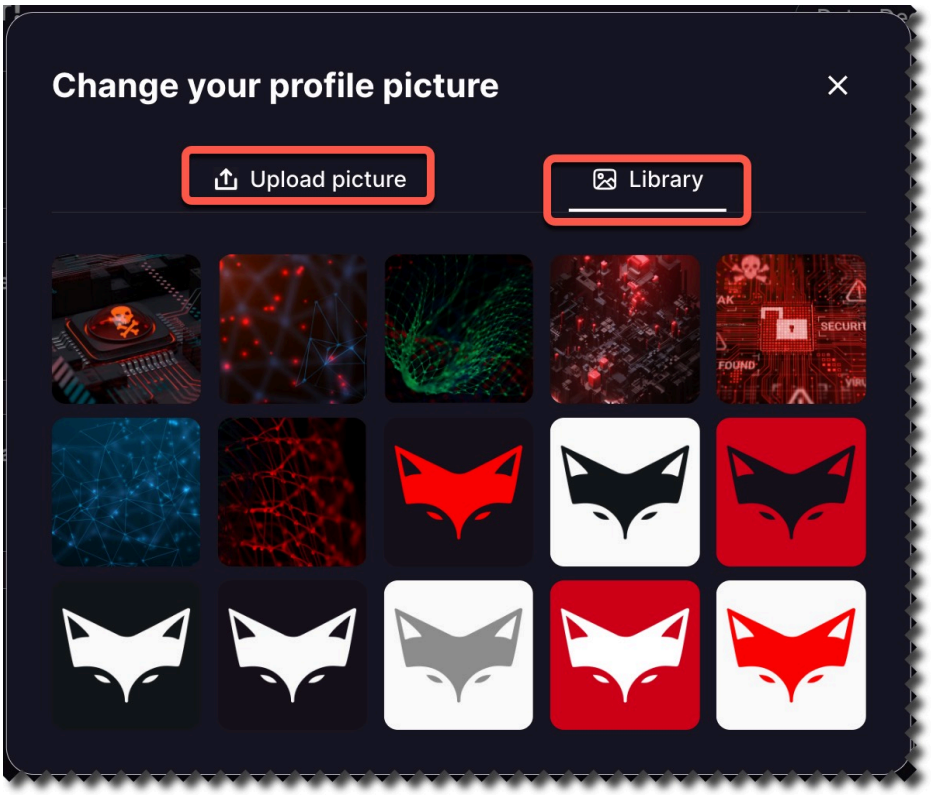


Changing Your Profile Photo

1. To change your profile photo, go to your user avatar and click on the photo icon.



2. Next, choose an image from our CodeHunter **Library**, or use one from your device by clicking **Upload picture**.



After selecting an image, it will appear as your avatar next to your username.

Previous
Login

Next
Adding Users

SentinelOne

Updated on 12 Jan 2024 · 2 Minutes to read · Contributors 

You need admin privileges to configure integrations.

CodeHunter and SentinelOne have partnered to provide native integration between the two applications.

You can automate the sending and receiving of security telemetry through this integration. The benefit is that when an incident is “Malicious” or “Suspicious” in the AI confidence status, the integration will automate the sending of those incidents to CodeHunter for further analysis.

When the file analysis results are ready, they will be appended to the Notes field of the incident and the SentinelOne console will display a notification for this.

To start the configuration process with SentinelOne, follow the steps below.

Retrieve Your SentinelOne Base URL

You will need to retrieve your SentinelOne Base URL is in order to successfully configure this integration.

a. Log in to your SentinelOne account. Once logged in, look for a Settings or Account section in the console.

b. Within the Settings or Account section, search for a category related to API or integrations. This is where you may find information about accessing SentinelOne services programmatically.

c. Look for the base URL or API endpoint information. This might be labeled as API URL, Integration URL, or something similar.

The base URL is the starting point for constructing API requests. It usually includes the protocol (https://) and the domain or IP address.

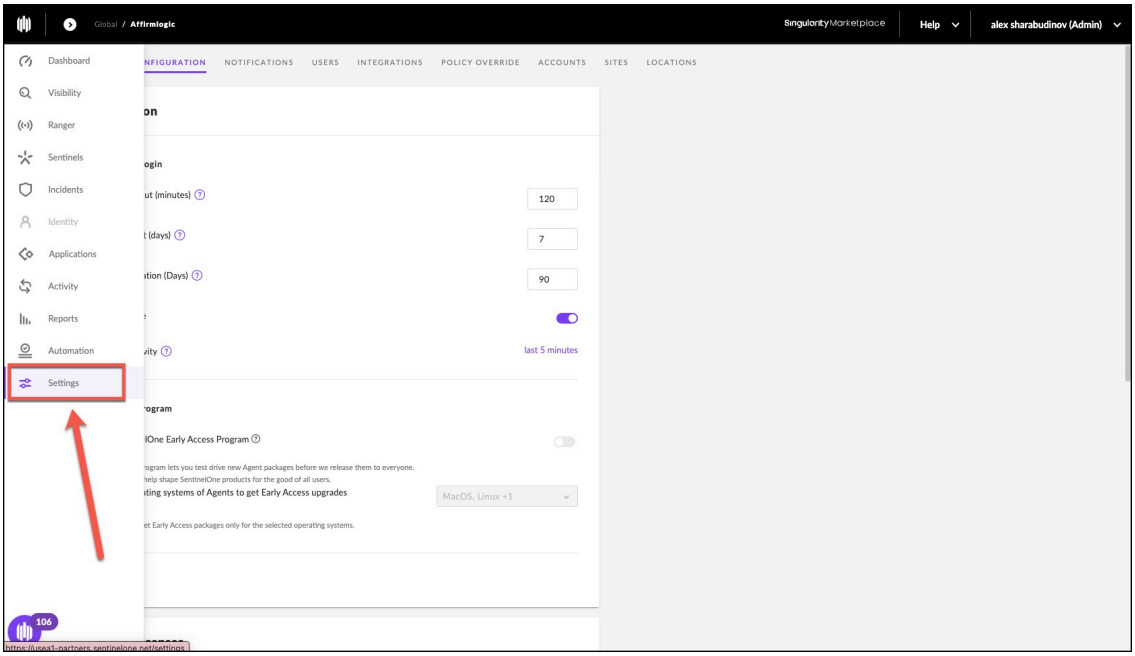
d. Once you've located the base URL, copy it to your clipboard.

The base URL could be formatted like this: https://<host>.sentinelone.net

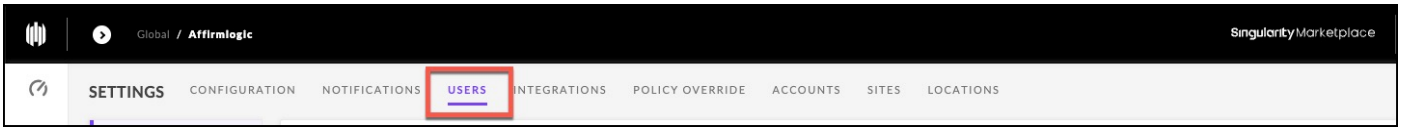
Generate API Token

Next, you will need to generate the API token. This token will be used to set up the integration with CodeHunter.

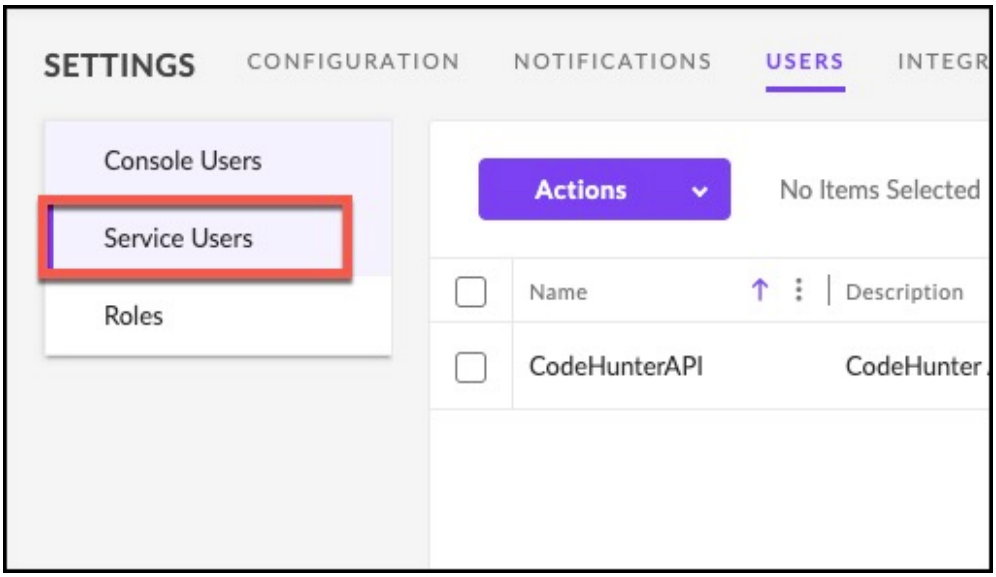
1. Log in to your SentinelOne management console and navigate to **Settings**.



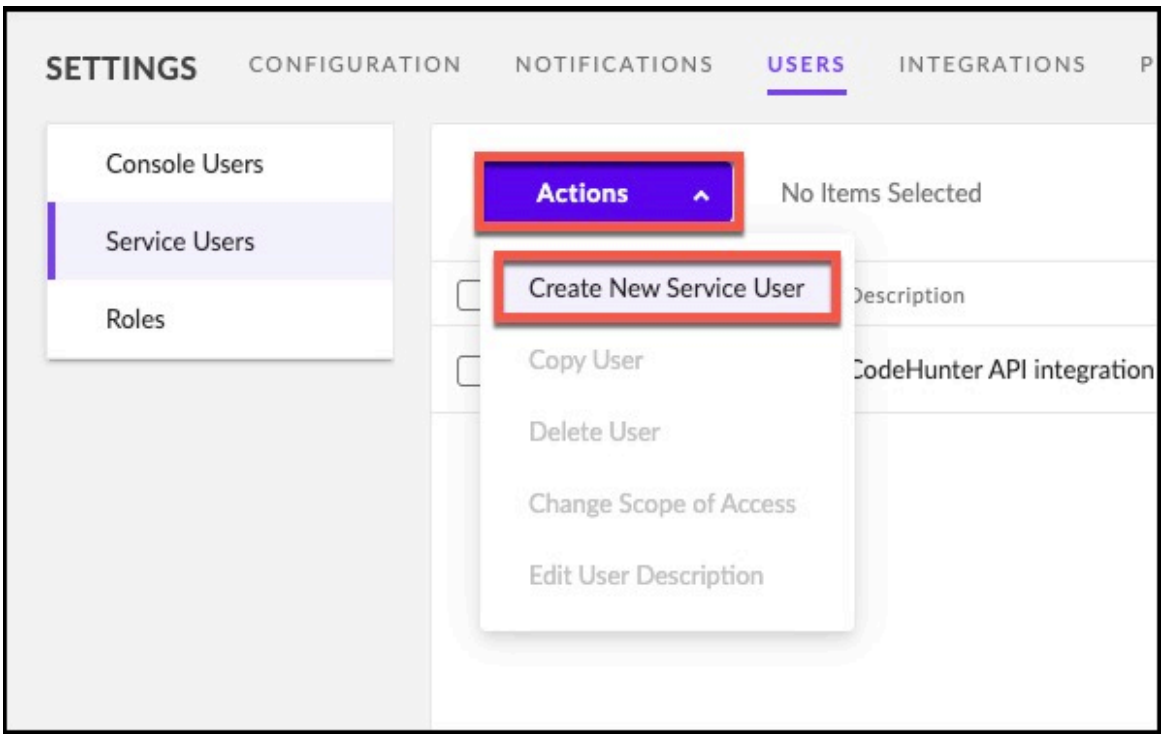
2. Click **Users**.



3. Click **Service Users** in the left panel.

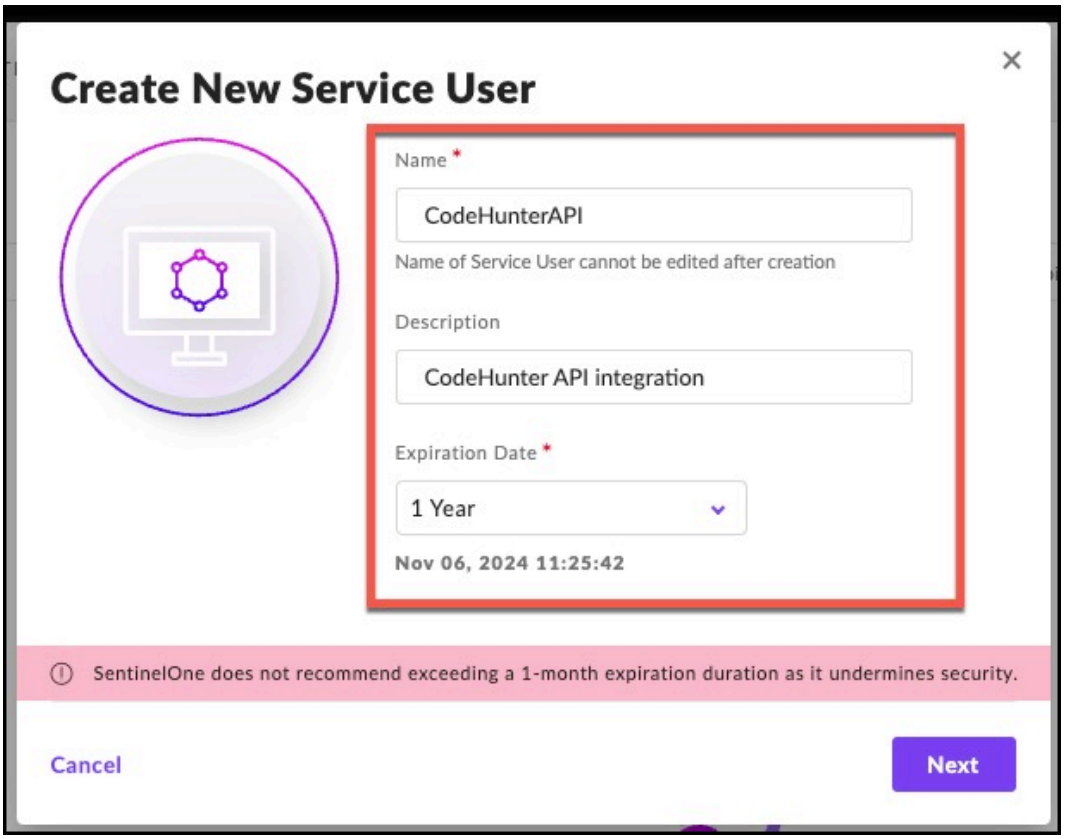


4. Click **Actions**, then **Create New Service User** from the drop-down menu.

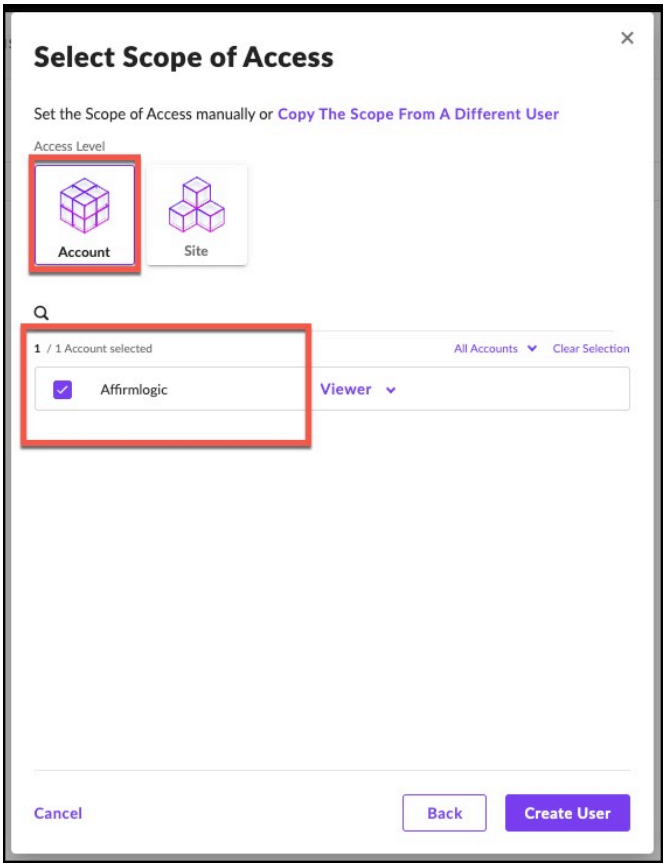


5. Type CodeHunterAPI in the **Name** field of the **Create New Service User** dialog box. Also, provide a **Description** such as CodeHunterAPI Integration. Finally, set the **Expiration Date** to 1 Year.

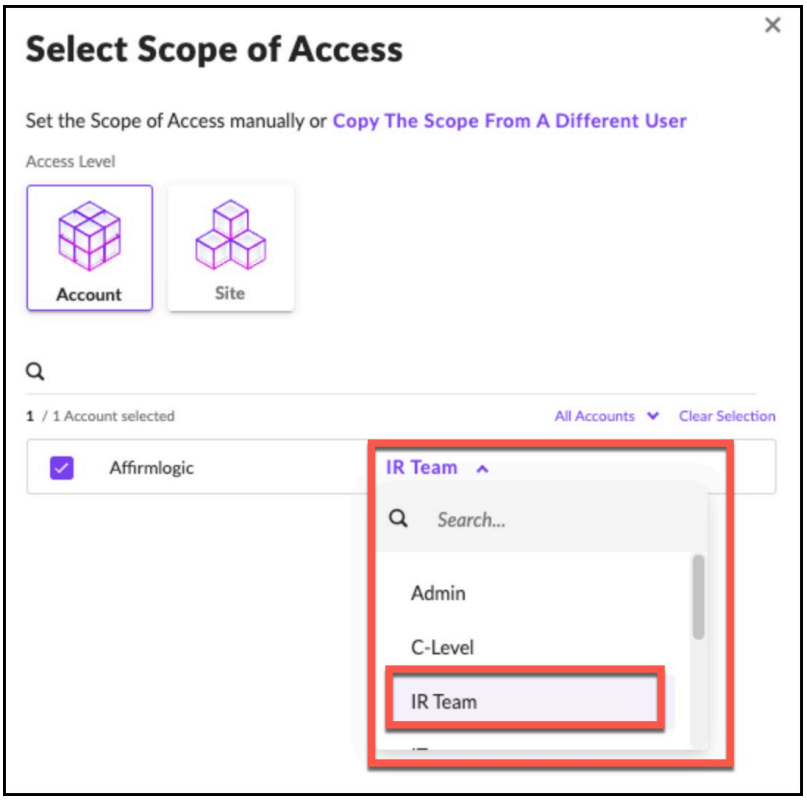
Click **Next** when you are done.



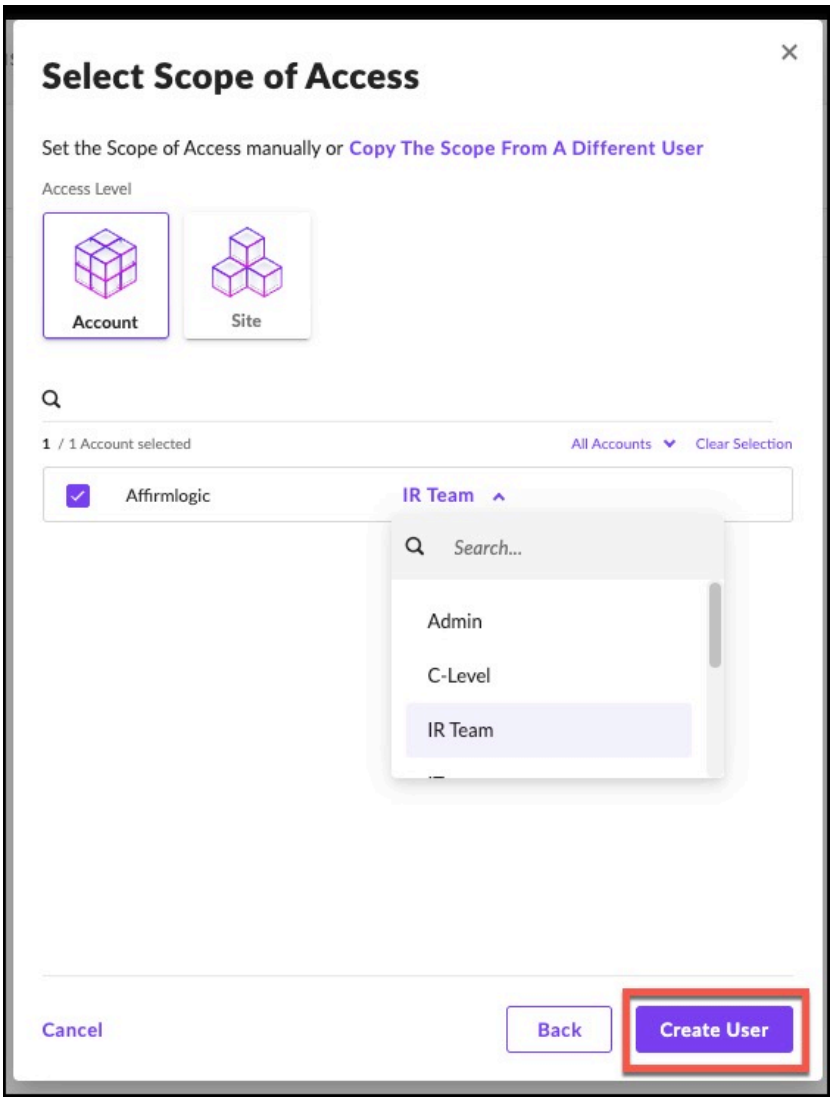
6. Select **Account** as the access level, then select the parent site, **Affirmlogic**.



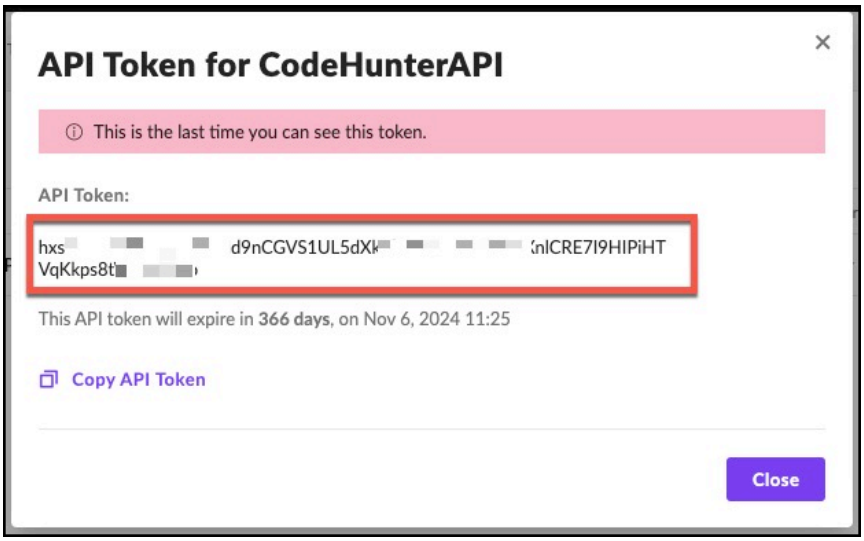
7. Set the role to **IR Team** from the drop-down menu.



8. Click **Create User**.

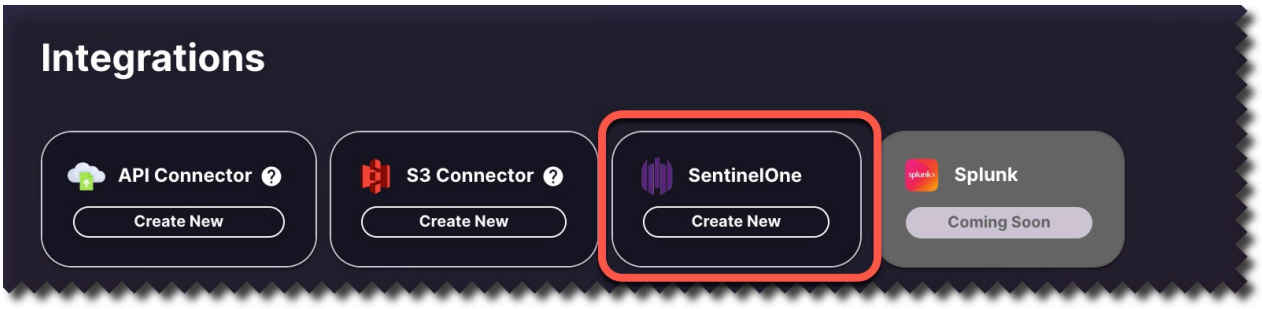


9. Save and copy the API Token information.



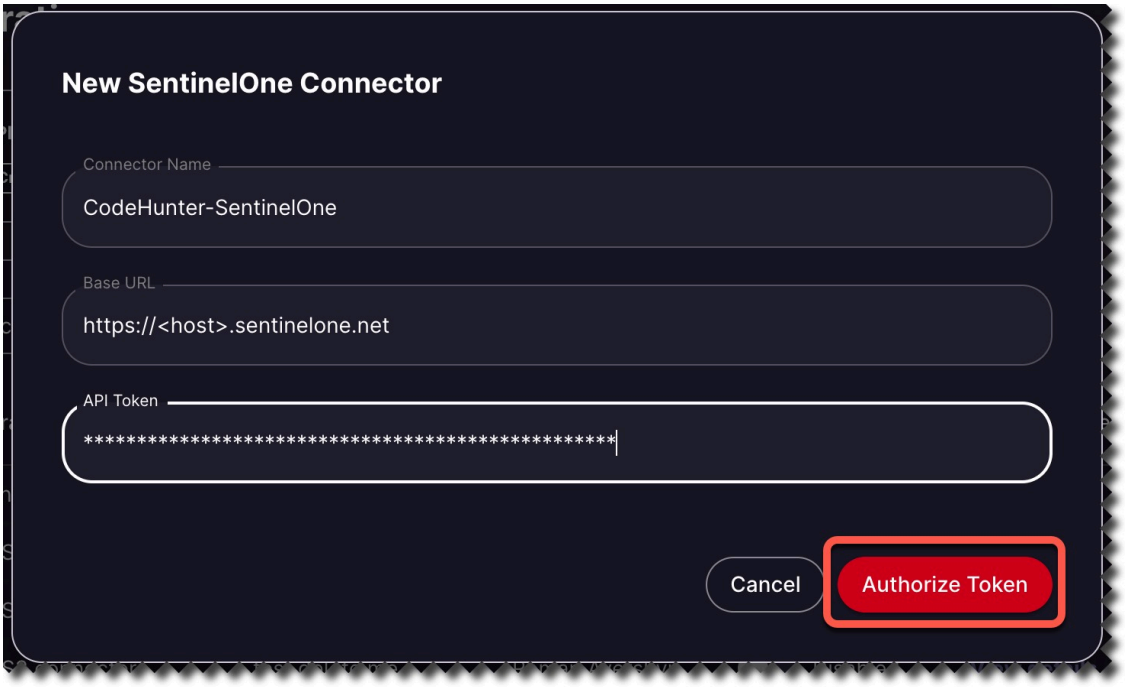
10. Next, log in to CodeHunter and navigate to **Integrations**.

11. Click **Create New** in the **SentinelOne** tile.

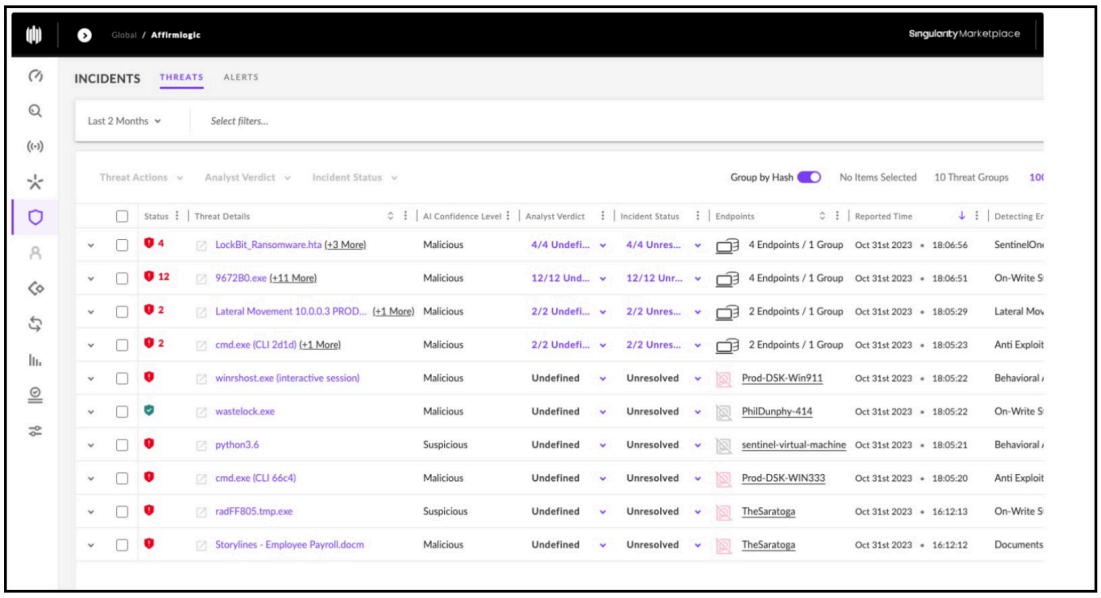


12. In the dialog box, provide a **Connector** name (e.g., SentionelOne Integration)

13. Next, paste the **Base URL** from Step 1 and **API Token** from Step 2 in the corresponding fields. Click **Authorize Token** when done.



SentinelOne Incident_type are viewable on the **Dashboard** tab.



FAQs

Q. Will the customer be notified if the token expires?
Answer: An email will be sent to the admin user prior to the 12 month expiration date.

Q. How does the analysis results work in the S1 console?
Answer: The CH results will be displayed in the Notes section of the incident.

Q. In the scenario that a customer has other incidents outside of SentinelOne do those ones need to be moved into S1 to be provided to CH?
Answer: Not necessarily. The manual upload action can be used.

Q. If a customer is not receiving the CH analysis results in the notes section of the incident will there be a link to the CH UI?
Answer: Yes, there is a link to the file that will navigate to CodeHunter application. The URL resolves to the dashboard page → file. Example URL: (https://mycodehunter.io/dashboard/sample/86e0eac8c5ce70c4b839ef18af5231b5f92e292b81e440193cdbdc7ed108049f)

← Previous
API and S3 Integrations

Next
Uploading Files

CodeHunter v1.1.6 (February 21, 2024)

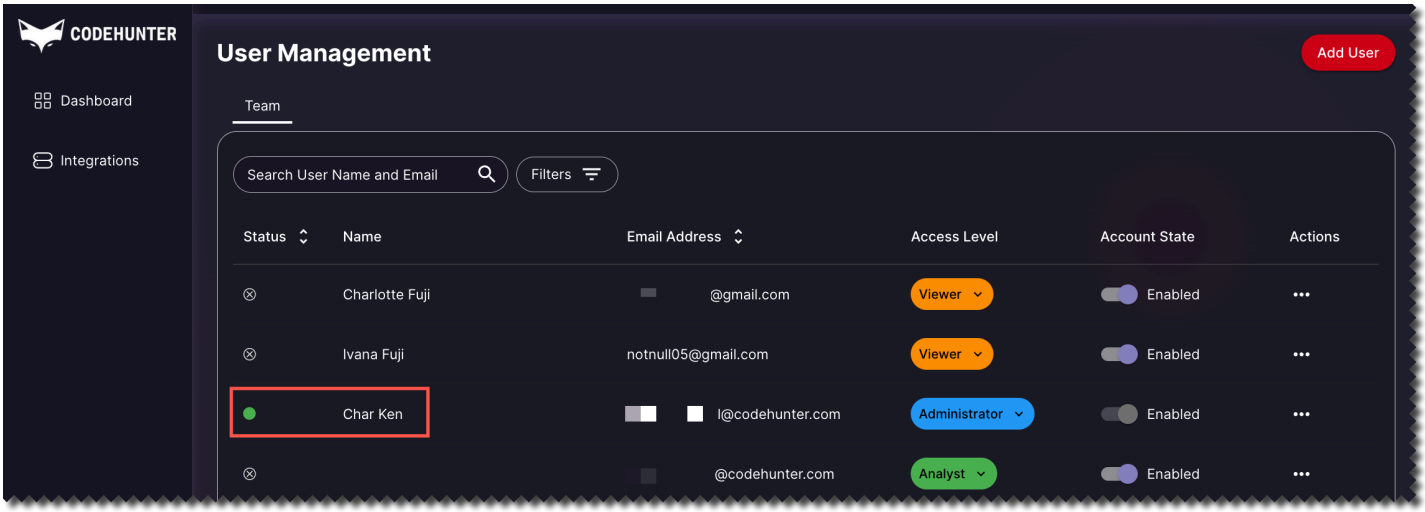
Updated on 29 Feb 2024 · 1 Minute to read · Contributors

What's New

User Management

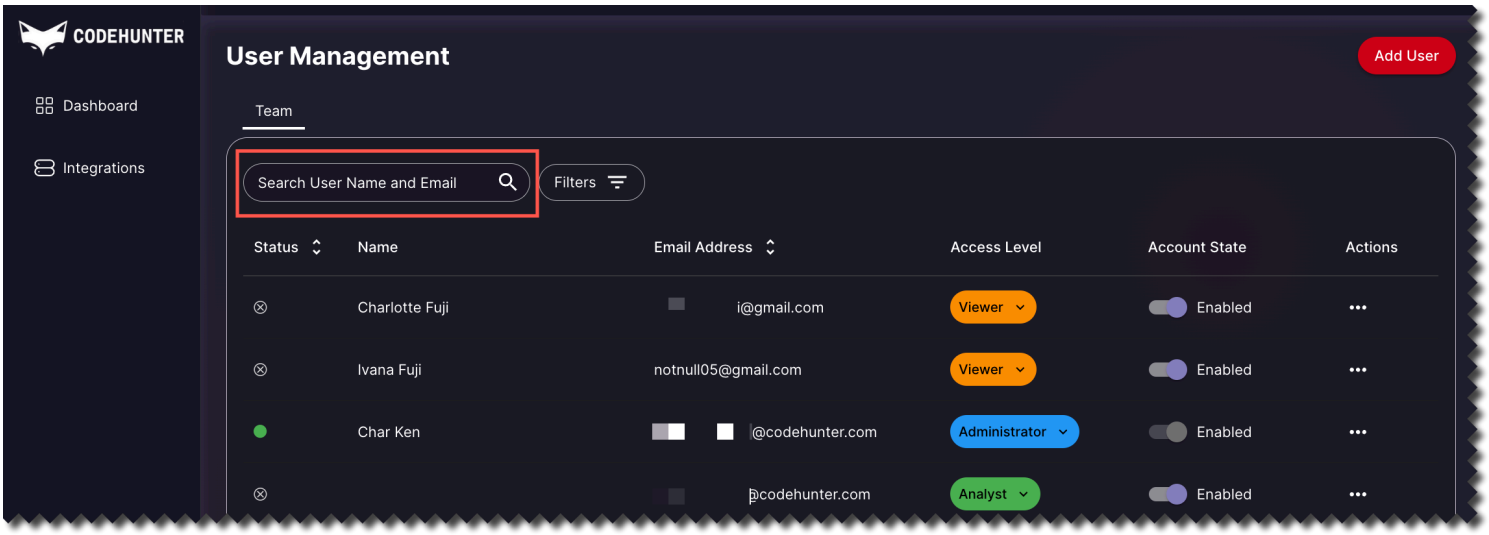
- **Online Status**

You now have the ability to view the status of users, indicating whether they are currently online or offline. Users who are online will be marked with a green dot next to their name.



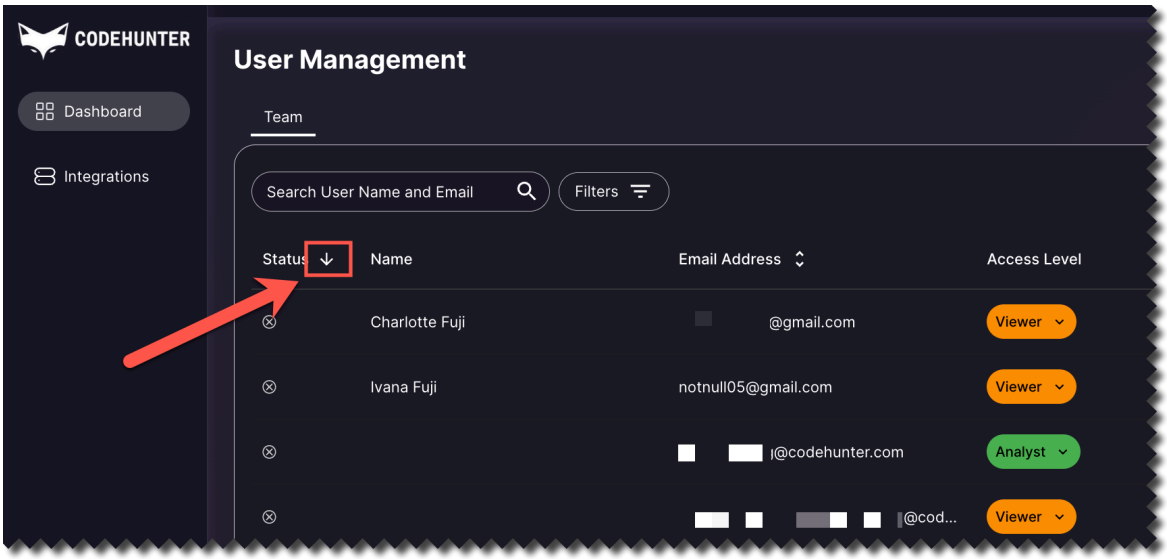
- **Search Users**

Explore a new feature that allows you to effortlessly search for users. Now, you can search for users using their usernames or email addresses.



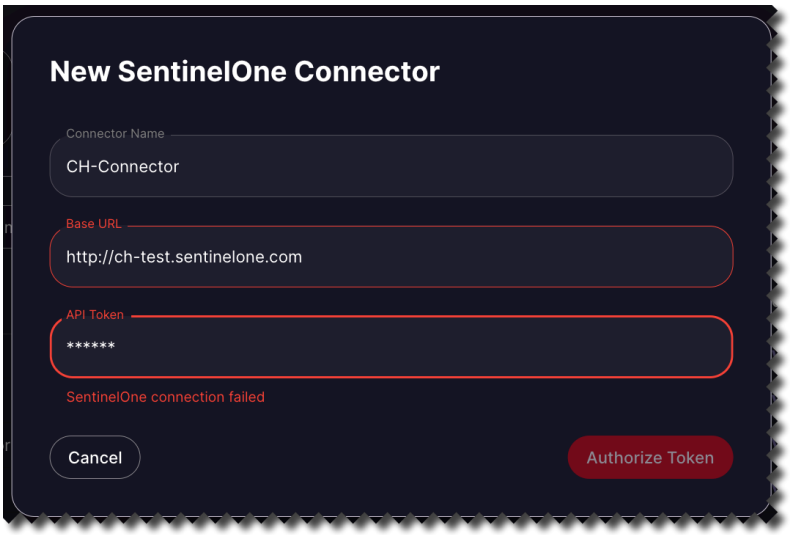
- **Sort Users**

You can now sort users by clicking the arrow next to Status on the **User Management** table.



SentinelOne Connector

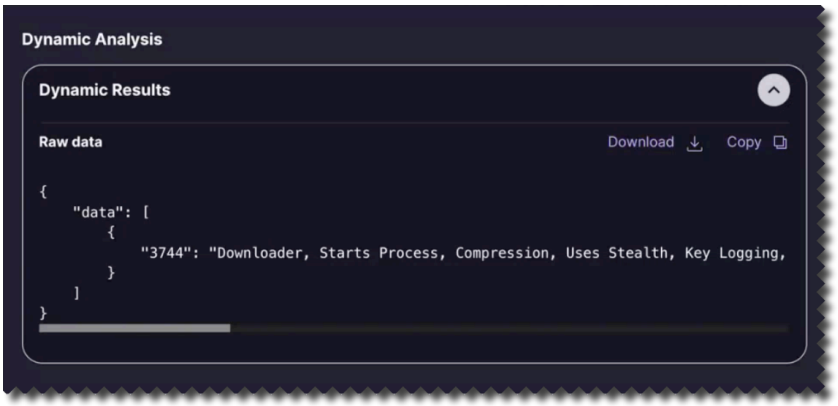
We eliminated the guesswork when configuring your new SentinelOne connector by introducing real-time validation. Whenever you attempt to create a new SentinelOne connector, error messages will prompt if the correct base URL and/or token are not used.



Enhancements

Malware Analysis

Enhancements have been made to the data in dynamic analysis results. Now, expect to see more actionable information to enhance the efficiency and effectiveness of your analyst work.



Bug Fixes

- Fixed a bug that prevented the analysis of Suspicious files on SentinelOne.
- Fixed an unexpected application error on the dashboard after trying to add a user already existing in the system.
- Fixed an issue that prevented all files in a folder from being ingested by the platform.

- Resolved an issue where the 'Back to Dashboard' link would disappear from the top of the page after users accessed a scanned file page for the second time.
- Fixed general displaying issues across the platform.

Previous
CodeHunter v1.1.17 (March 6, 2024)

Next
CodeHunter v1.1.5 (Feb. 5, 2024)

CodeHunter v1.1.17 (March 6, 2024)

Updated on 07 Mar 2024 · 1 Minute to read · Contributors

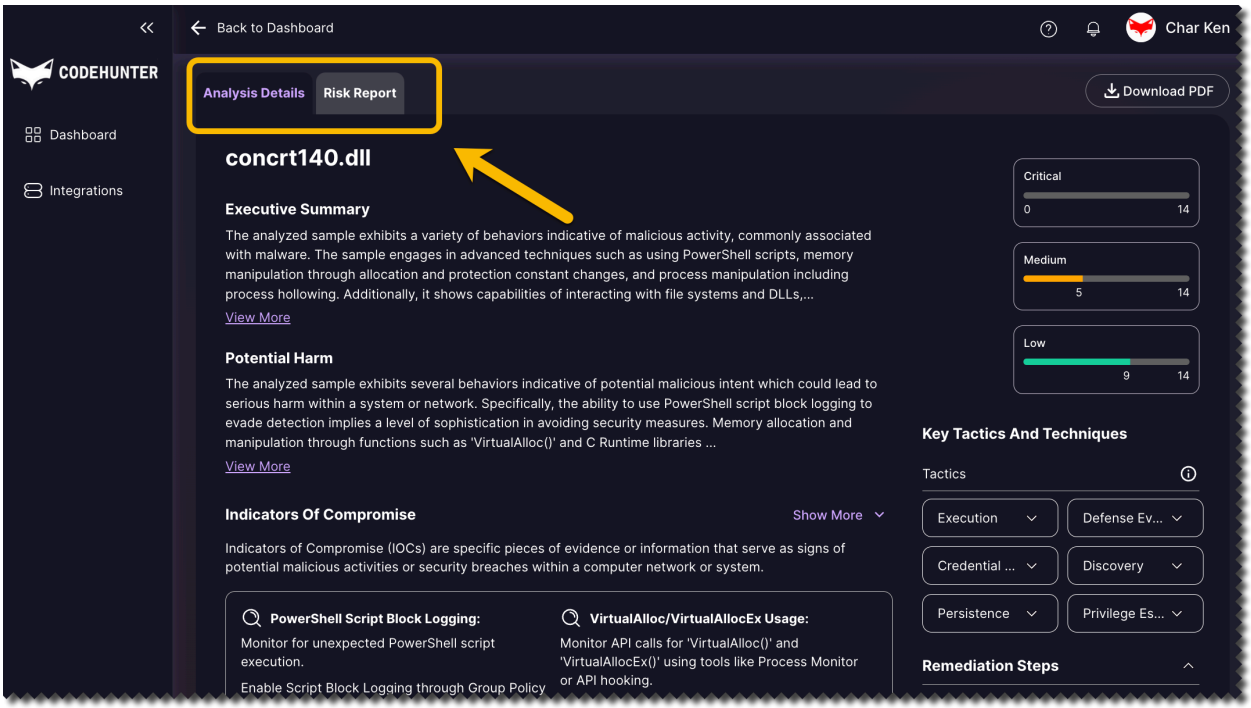
What's New

Risk Reports

- You can now generate risk reports for **Unknown** and **Known Bad** files. These reports provide an early indication of potential security incidents or vulnerabilities in a system. To learn more about how to generate risk reports, **click here**.

- We enhanced navigation for accessing generated risk reports. Now, when you click to view analysis results/details, you will see two tabs at the top of the page: **Analysis Details** and **Risk Report**.

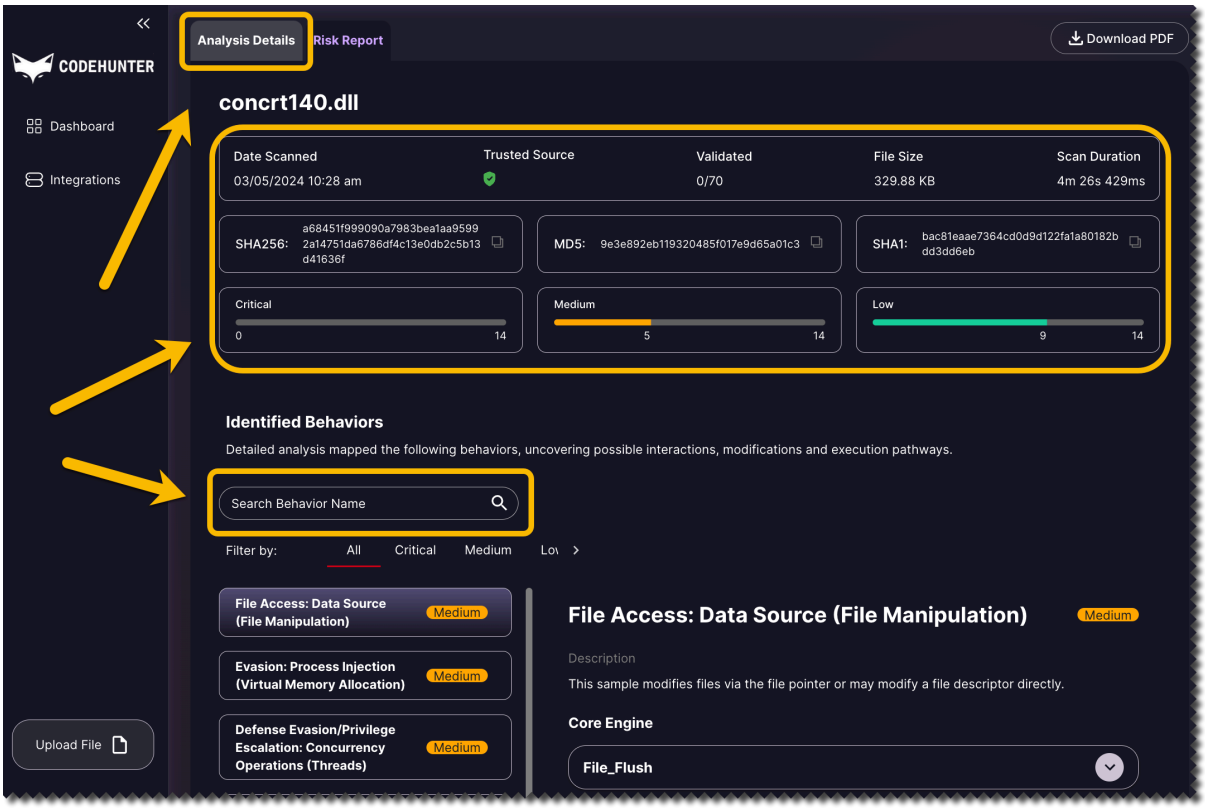
- In addition, the **Risk Reports** page has undergone a comprehensive redesign, enhancing its functionality to deliver crucial and streamlined information.



Analysis Details

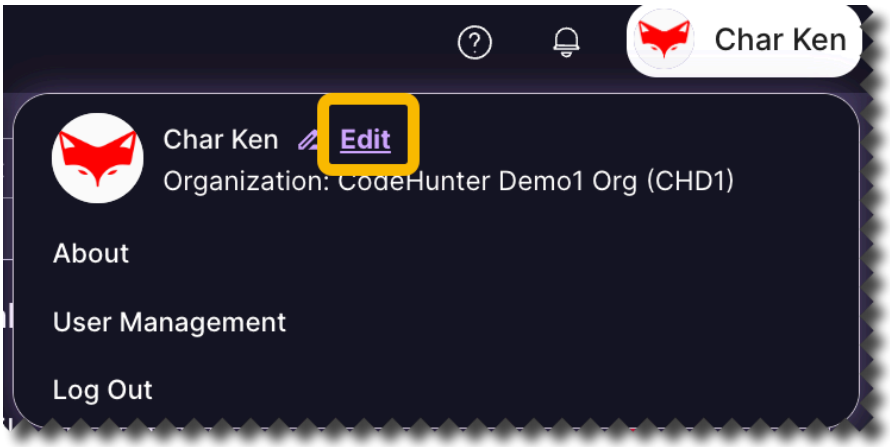
- We also redesigned the **Analysis Details** page, featuring a more logical organization of information related to the scanned file. This includes an improved display of hashes and a refined presentation of severity levels for functions identified within the file's code.

- Additionally, within the **Identified Behaviors** section, we've introduced a **Search Behavior Name** filter. This feature empowers you to effortlessly locate specific behaviors by utilizing keywords for a more refined and targeted experience.



Enhancements

- We've implemented a new feature that allows you to easily identify clickable elements in the user interface. Now, links are visually enhanced by appearing underlined for improved visibility and user interaction.



Bug Fixes

- Resolved Issue: Files loaded for analysis now correctly appear on the dashboard page of a new tenant.

- Resolved Issue: The 'Contact Support' link now correctly directs users to the appropriate support page, eliminating the redirection to the reset password page.

- Resolved Issue: Improved UI Responsiveness - Dashboard scaling no longer masks report items, ensuring a seamless and unobstructed user experience.

- Resolved Issue: The executive report summary no longer experiences truncation at the first "." symbol, ensuring comprehensive and accurate summaries.

Previous
CodeHunter v1.1.18 (March 28, 2024)

Next
CodeHunter v1.1.6 (February 21, 2024)

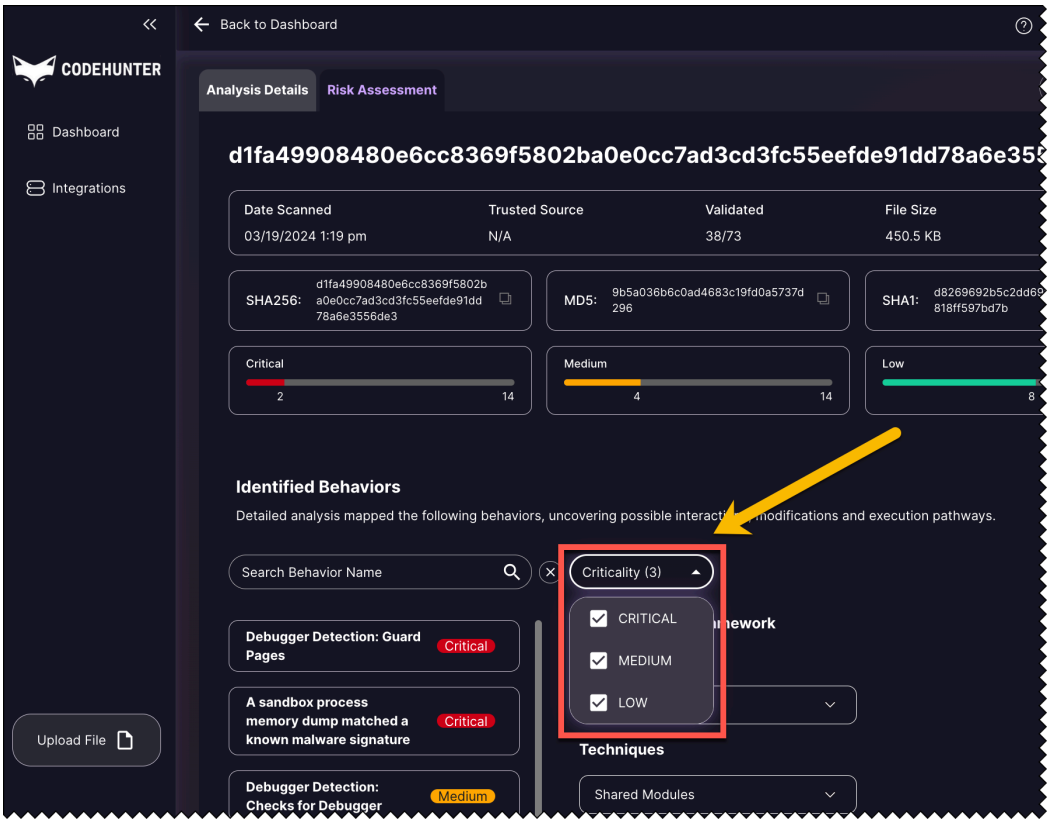
CodeHunter v1.1.18 (March 28, 2024)

Updated on 25 Mar 2024 · 1 Minute to read · Contributors

What's New

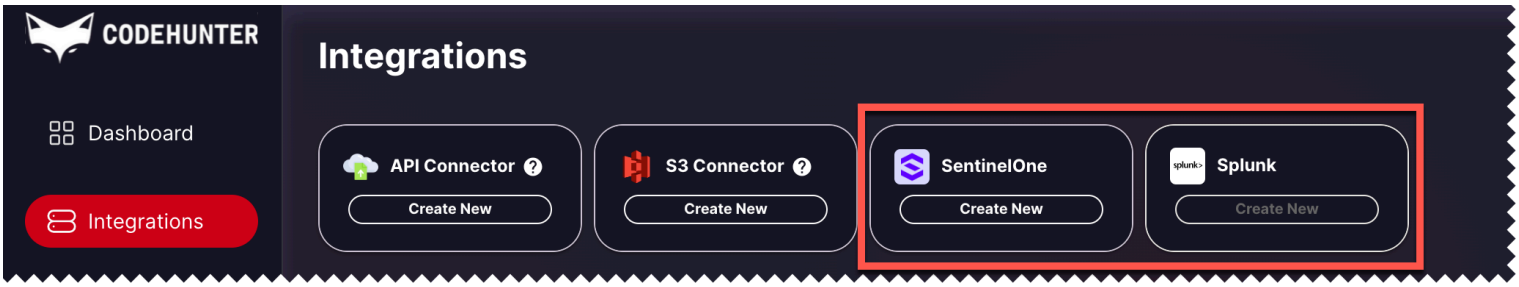
Analysis Details Section

- You can now sort file analysis code functions under **Identified Behaviors** by criticality. With this new filter, analysts can streamline their analysis process, focusing their attention on the most important aspects of the malware first.



Integrations

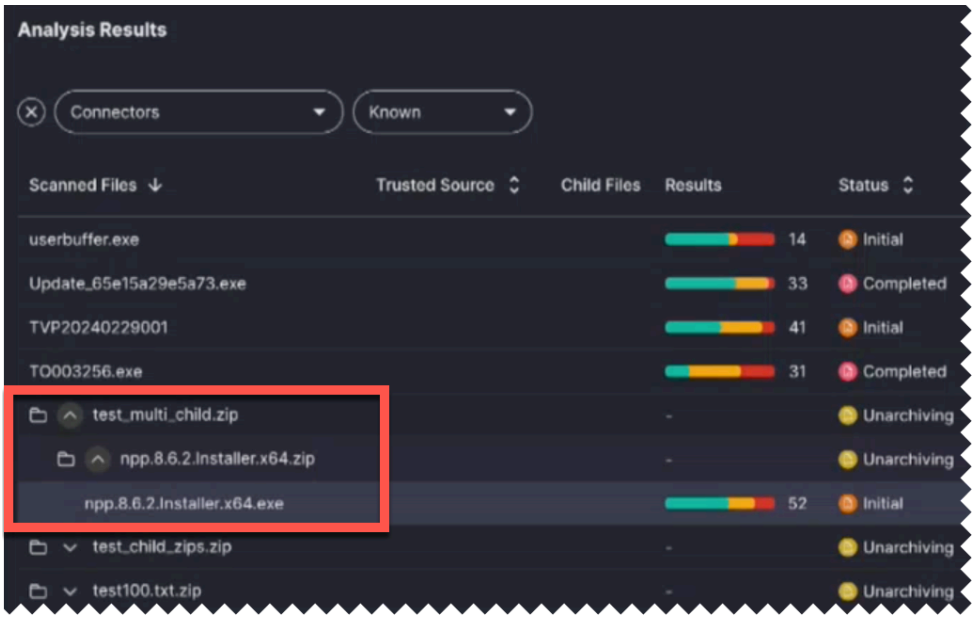
- We are excited to announce the release of our seamless Integration with Splunk, a leading platform for operational intelligence. This integration marks a significant milestone in our commitment to providing users with powerful tools for data analysis and insights.



Splunk Integration

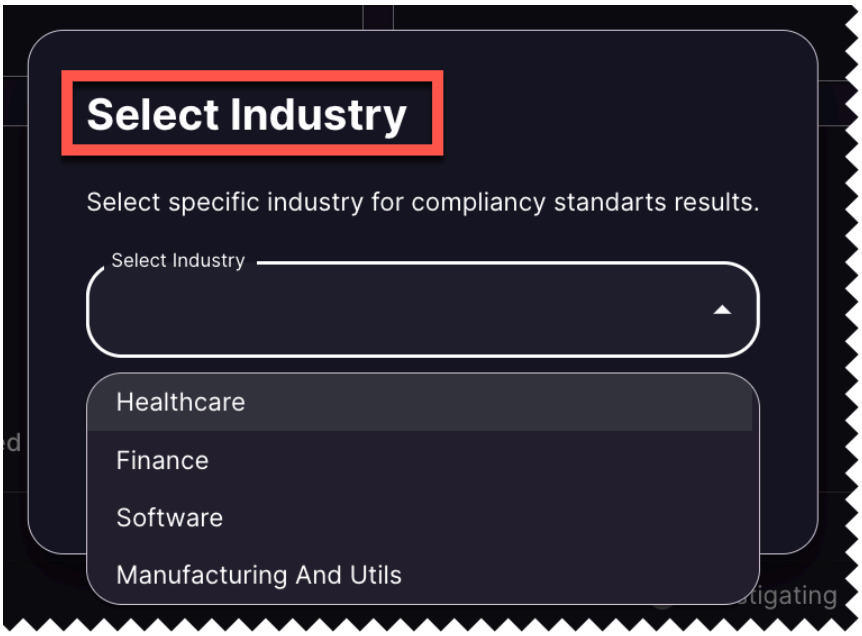
Analysis Summary Section

- Now, you can visualize child files in a hierarchical tree format when unarchiving zip files for analysis. This provides you and your team with a clear and organized representation of the file structure within the zip file. This capability enables users to quickly locate and focus on relevant files.

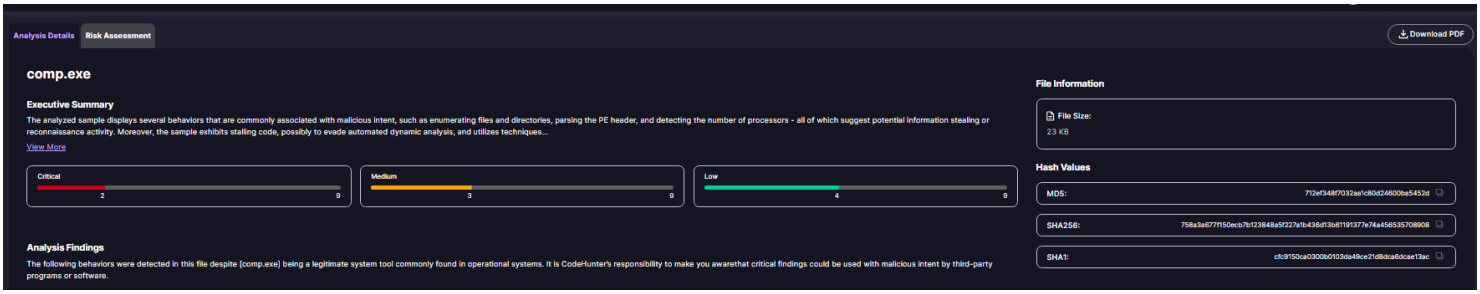


Reports

- Industry-specific reports are now available when generating a report from file analysis results. These reports will provide you with tailored insights relevant to your respective sector and help you gain a deeper understanding of how file analysis findings relate to your specific business domain.



- You can now generate a Risk Assessment executive report for analyzing known-good files signed by trusted sources. These reports offer comprehensive insights into the security posture and integrity of files with established trustworthiness.



Previous
Release Notes

Next
CodeHunter v1.1.17 (March 6, 2024)