CAWS CONTINUOUS SECURITY VALIDATION PLATFORM USER GUIDE

Version 3.0

Version 2.3, 7/17/2017

NSS Labs, Inc.
206 Wild Basin Road
Building A, Suite 200
Austin, TX 78746 US
info@nsslabs.com
www.nsslabs.com

CHAPTER 1: INTRODUCTION

This User Guide introduces you to the Continuous Security Validation Platform threat awareness and dynamic modeling suite. Use this guide to learn how to activate your account and navigate the suite.

The CAWS platform includes the following modules:

- Global Dashboard
- Analyze
- Submissions
- Threats
- Organizations

What is CAWS

CAWS is the only cloud-based continuous security validation platform that lets you build organization-specific profiles, which mirrors the specific security products deployed to protect them. The platform provides enterprises a public validation lane and a private validation lane options.

- The public validation lane option enables enterprises to validate how well their security controls are performing against vendor recommended settings including out-of-the-box configuration and tuning.
- The private validation lane option offers enterprises the ability to customize specific categories of product against enterprise specific configuration and tuning

List of Security Product Types Tested in CAWS

- Next Generation FireWall (NGFW)
  - Barracuda F280
  - Cisco Firepower NGFWv
  - Check Point 5900 -NGFW
  - Forcepoint 5206
  - Fortinet 500D
  - Juniper SRX1500
  - Palo Alto Networks 5020
  - Sophos S230
  - Sophos XG 750
  - Sonicwall SM9400
  - Trend Micro Tipping Point 2200T
  - Watchguard M4600
  - Watchguard XTM535
  - Watchguard XTM1525

- Next Generation Intrusion Prevention Systems (NGIPS):
  - Cisco Firepower NGIPSv
  - Checkpoint 13800 -NGIPS
  - IBM XGS 5100
  - McAfee NS9100
  - Trend Micro TippingPoint 7500NX
  - Trustwave TS500
- Secure Web Gateway (SWG)
  - Forcepoint V1000G4 - SWG
  - McAfee WG5500

List of Applications Tested in CAWS

- Adobe Flash Player
- Adobe Reader
- Browser
  - Google Chrome
  - FireFox
  - Internet Explorer
  - Microsoft Edge
- Media Players
  - iTunes
  - Quick Time Player
  - VLC Player
  - Windows Media Player
- Java
- SilverLight
- Microsoft Office 2013 and 2016

List of Platform (Operating Systems) Tested in CAWS

- Windows7 SP1
- Windows 8
- Windows 8.1
- Windows10

CHAPTER 2: LICENSING

Continuous Security Validation Platform offers two subscription license levels: Trial and Paid.

Trial

A trial license provides:

- A trial license is started when a new user registers and creates an organization
- One organization per email address
- Five accounts per organization
- Five users per account
- Access to only demo security product

To see information about your trial license, go to **Organizations** and then click the **License** tab.

Converting a Trial License to a Paid License

To convert your trial license to a paid license, please contact our Sales department at Sales@nsslabs.com or 512-485-1144.

CHAPTER 3: REGISTERING FOR CAWS

There are several methods to get started with the Continuous Security Validation Platform: register as a new organization or get invited to join an existing organization. Once you register, you receive an email message containing a hyperlink to the Continuous Security Validation Platform login page. You must activate your account within 72 hours of receiving the email, or the link expires. If your link expires, request a new activation email on the login page.

Register

To register for CAWS:

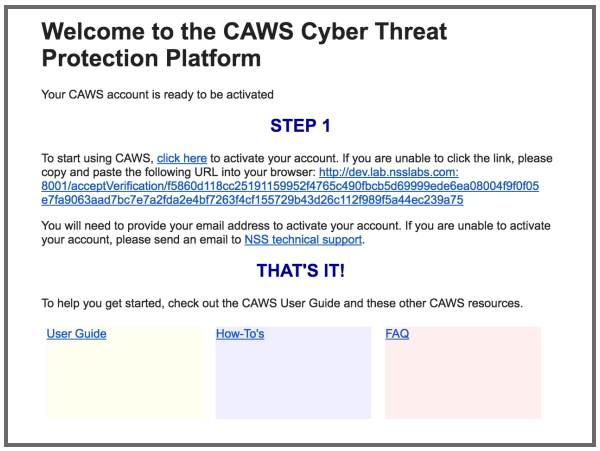
1. From the CAWS landing page, click **Register**. The Register page displays.

2. Enter your work email address.
3. Confirm your email address.
4. Enter your desired password.
   Note: Password must have the following characteristics:
   - At least 8 characters or longer
   - At least one uppercase letter
   - At least one lowercase letter
   - At least one numeral or special character
5. Retype the password into the **Confirm Password** field.

6. Click **Next**.
7. Click **Register** after verifying your email address.

To activate your account:

1. Click the hyperlink in the system-generated email from CAWS. The website displays the CAWS login page.



If the link is not active, copy the web address in the email and paste it into the address field of a browser window. CAWS supports Internet Explorer 11, Edge, and Safari.

2. Enter your password.
3. Click **Login**.
4. Read the end user agreement, scrolling to the end. Select **I agree to the terms** and then click **Submit Agreement**.

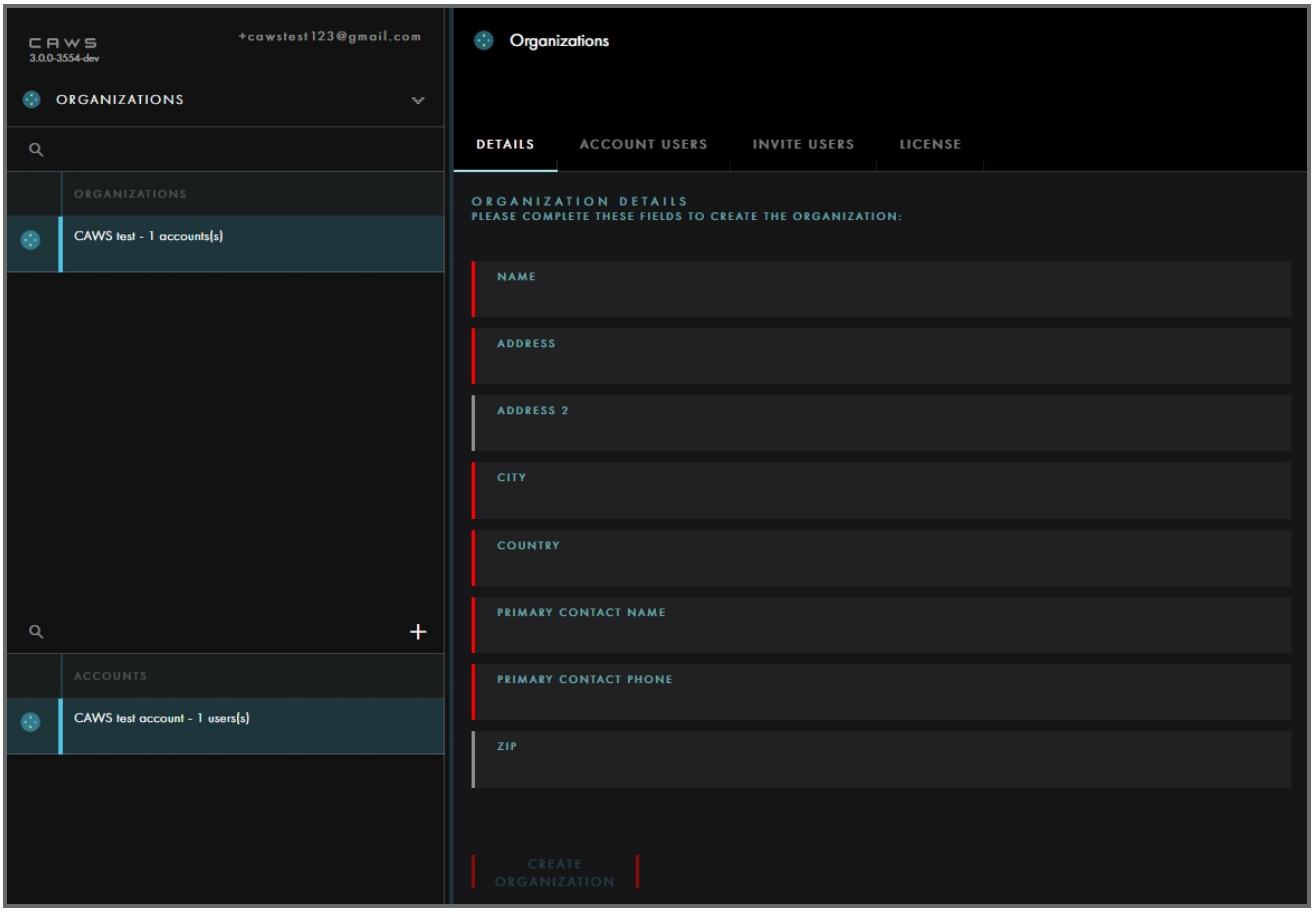
User accounts used when you authenticate are session specific. This means that they can only be used by one session at a time, whether that session is a browser session or a session you started from a Python script, for example. If you try to use the same user account to generate a login token from two different sessions, the most recent session will invalidate the first session. For this reason, we recommend you create a user as part of your account dedicated to API usage if you plan on using the API extensively.

CHAPTER 4: ORGANIZATIONS

The CAWS Organizations menu allows you to add and edit organizations, accounts, and users. You must create an organization and at least one account.

To create an organization:

1. From the menu bar, click **Organizations**. The Organizations page displays.



2. Enter the name of your organization.
3. Enter the address, city, state, and zip of your organization.
4. Enter the primary contact name and phone number.
5. Select the country from the list.
6. Click **Create Organization**.

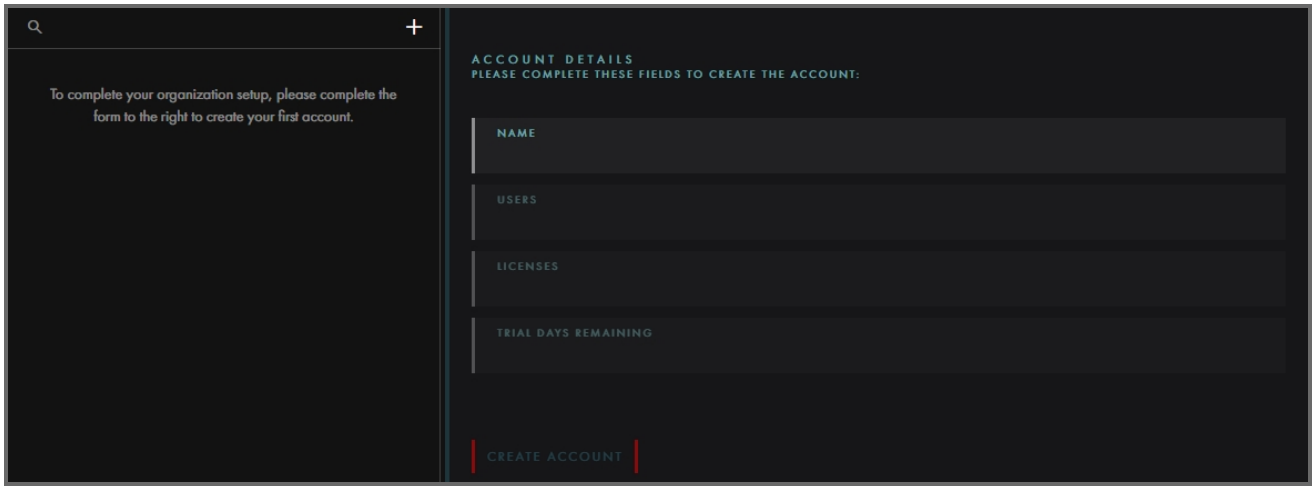
To add an organization:

1. From the menu bar, click **Organizations**.
2. Click the **+** symbol in the left-hand pane.

To create an account:

Note: You must have an existing organization.

1. From the menu bar, click **Organizations**.
2. Select an organization from the list.
3. Click the **+** symbol. The Account Details page displays.



4. Enter the name of the account.
5. Click **Create Account**.

Using Global Search

Use the search function to search for organizational information.

To perform a search:

- To perform a search, enter the search term in the Search field and press **Enter**.

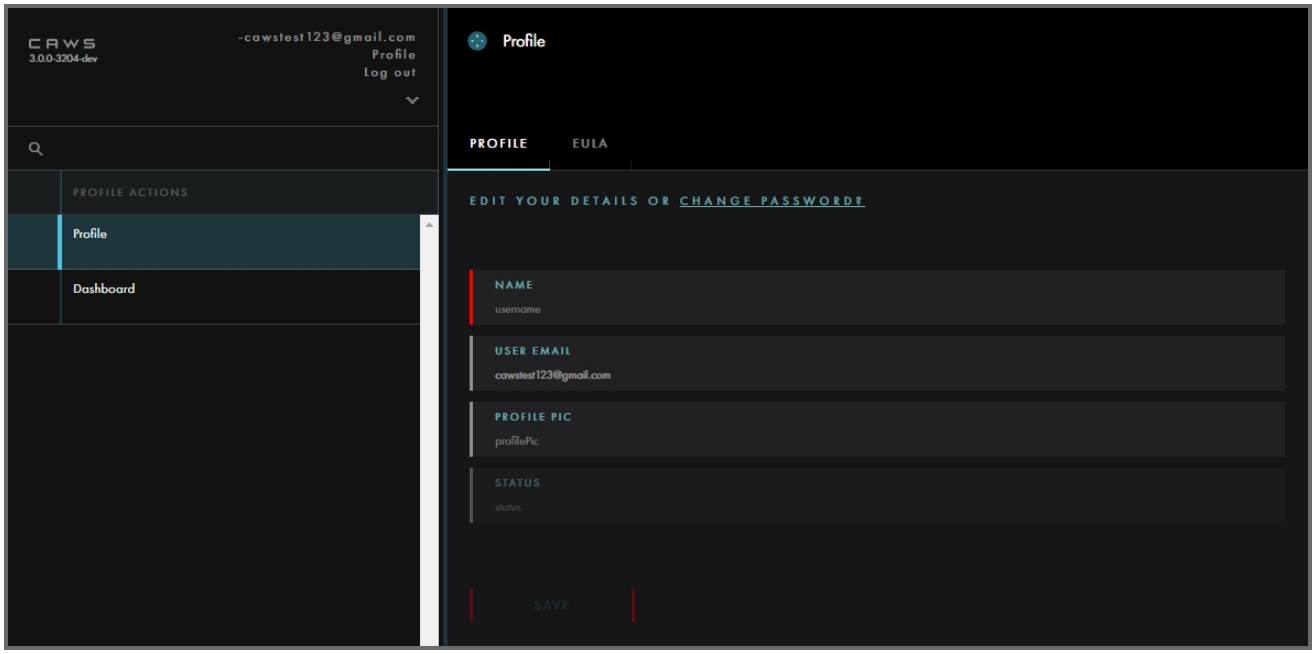
- To perform a global search, from any page type **Ctrl + F** and the global search opens.

Editing your Profile

Click your profile name to display the profile and log out options.

To edit your profile:

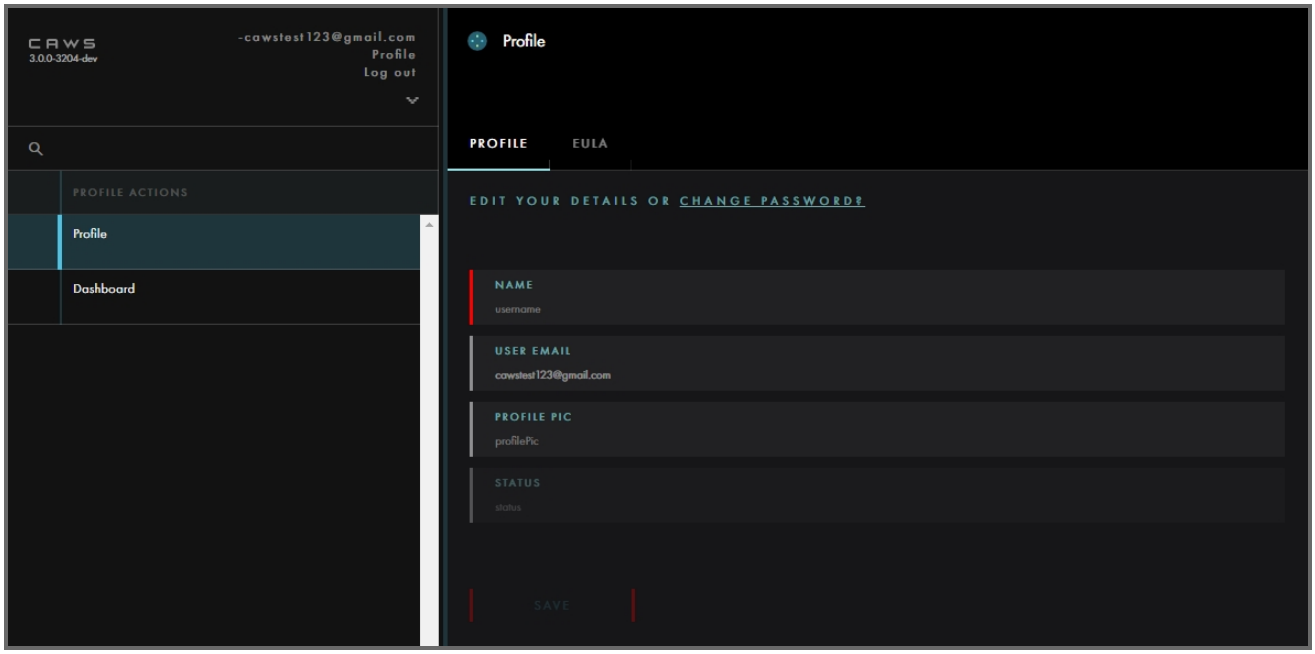
1. Click **Profile** from the drop-down menu. The Profile page displays.



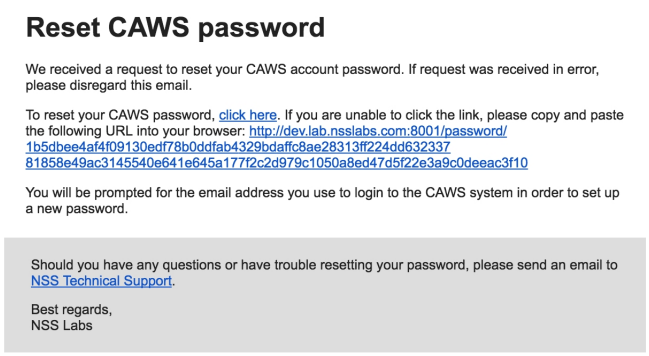
2. Select **Profile** in the Profile Actions area.
3. Make your edits to your profile.
4. Click **Save**.

Change Password

1. Click **Profile** from the drop-down menu. The Profile page displays.



3. Click **Change Password**. An email is sent with instructions and a link to change your password.



Reset CAWS password

We received a request to reset your CAWS account password. If request was received in error, please disregard this email.

To reset your CAWS password, click here. If you are unable to click the link, please copy and paste the following URL into your browser: http://dev.lab.nsslabs.com:8001/password/1b5dbee4af4f09130edf78b0ddfab4329bdaffc8ae28313ff224dd63233781858e49ac3145540e641e645a177f2c2d979c1050a8ed47d5f22e3a9c0deeac3f10

You will be prompted for the email address you use to login to the CAWS system in order to set up a new password.

Should you have any questions or have trouble resetting your password, please send an email to NSS Technical Support.

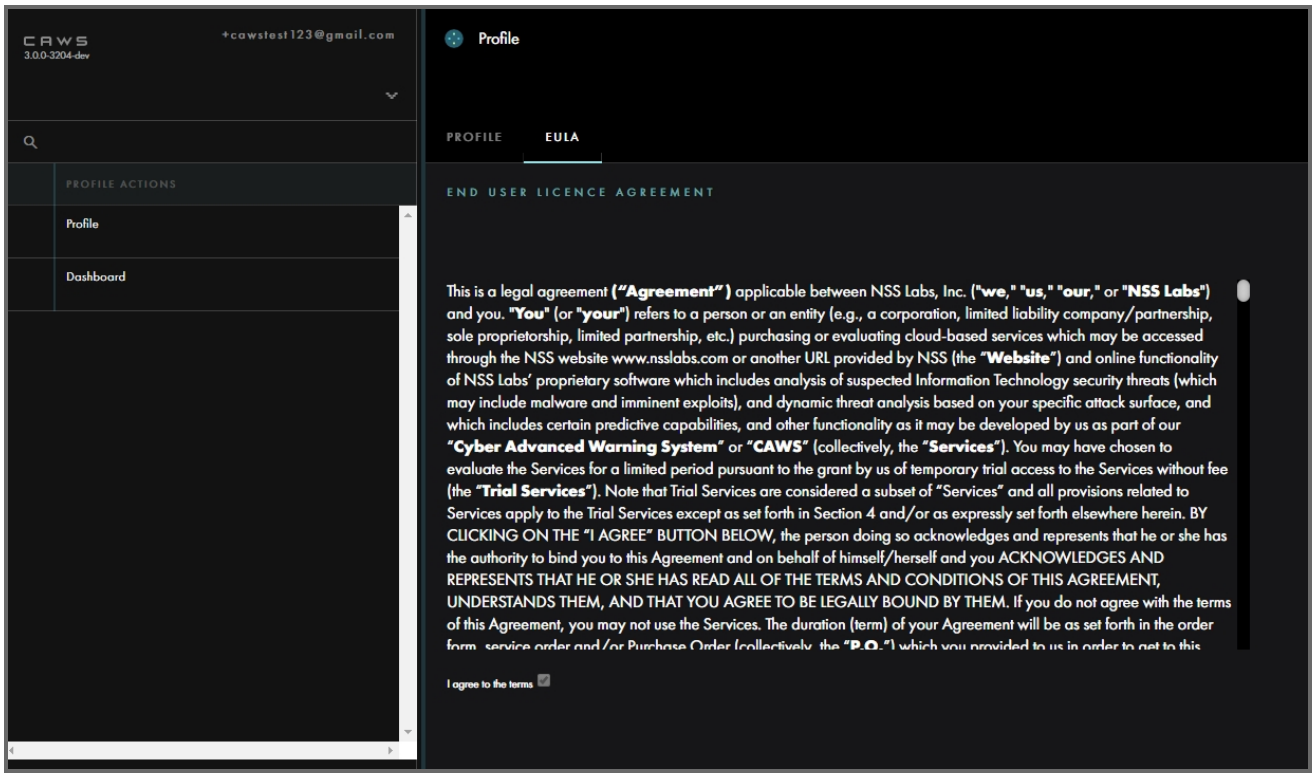
Best regards,
NSS Labs

2. Enter your new password. **Note**: Minimum of eight characters.
3. Confirm your new password.
4. Click **Save**.

End User License Agreement

To view the End User License Agreement (EULA):

1. Click **Profile** from the drop-down menu. The Profile page displays.



2. Select the **EULA** tab to view the full agreement.

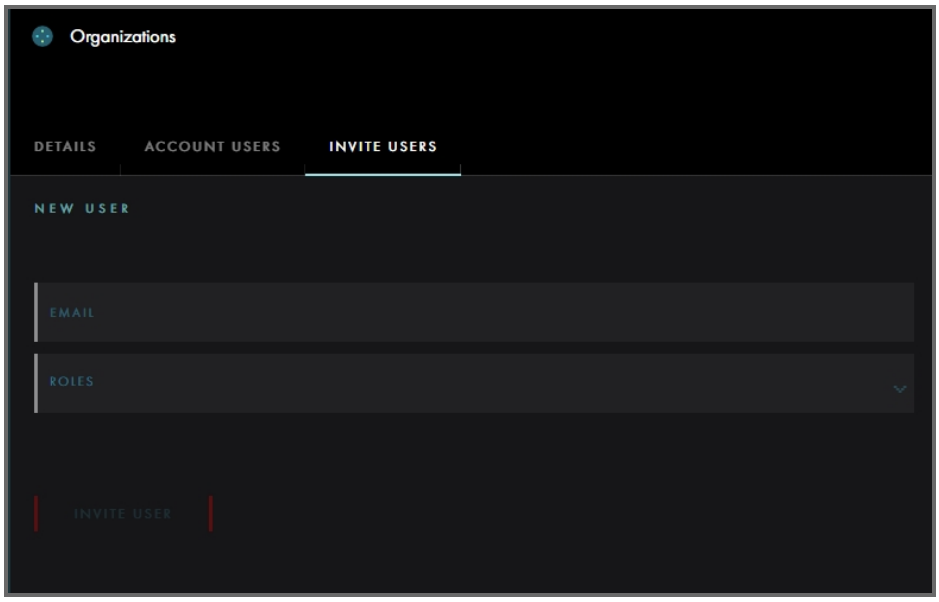
User Account Settings

Inviting Users

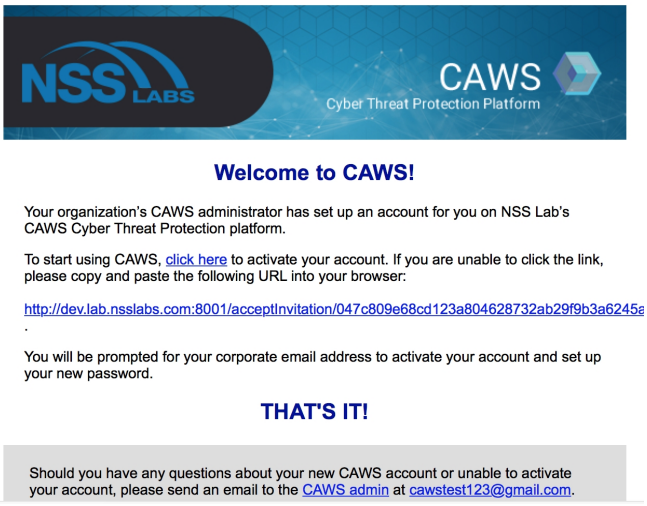
CAWS allows you to invite users.

To invite users:

1. From the menu bar, click **Organizations**.



2. Select the **Invite Users** tab.
3. Enter an **email address** for the new user.
4. Select a **role**.
5. Click **Invite User**. An email is sent inviting the user to start using CAWS.

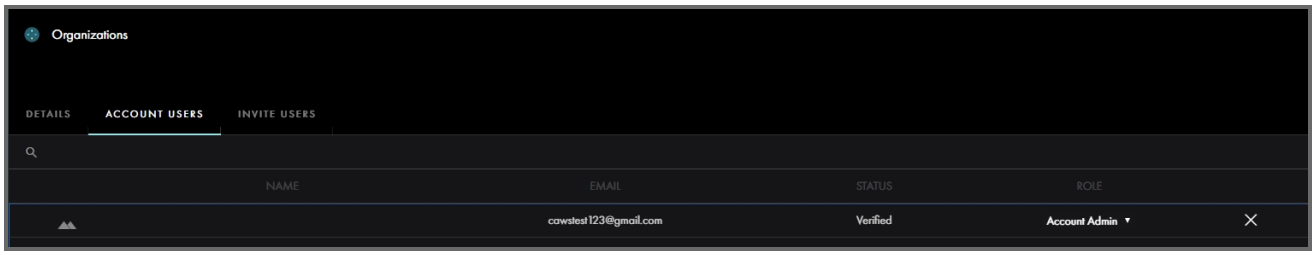


6. Click the link in the email and then enter and confirm your password.
7. Click **Save**.

Deleting Users

To delete a user:

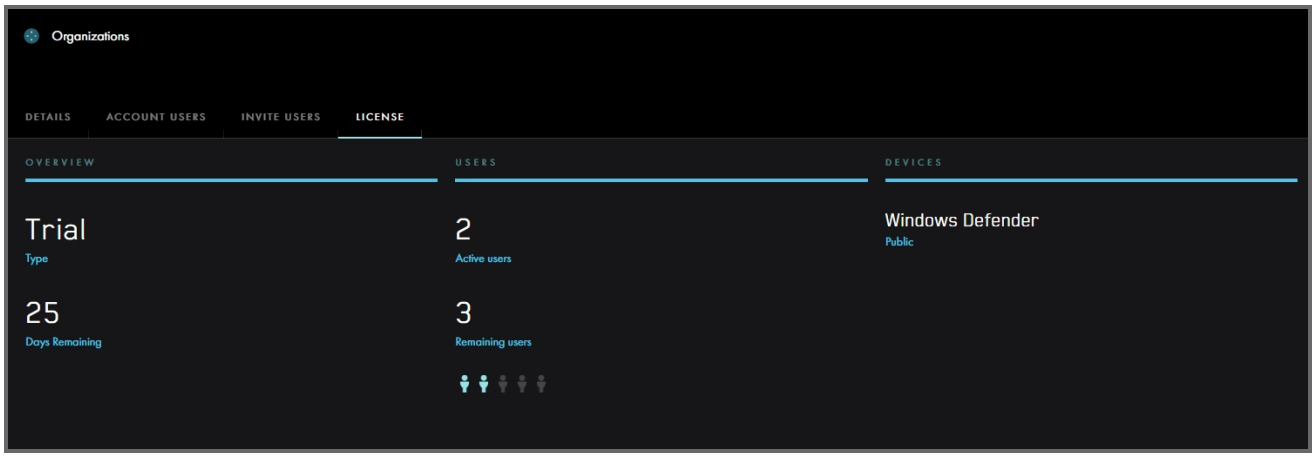
1. From the menu bar, click **Organizations**.
2. Select the **Account User** tab.



3. Click the **X** at the end of the row of the user you want to delete.
4. Click **OK** to confirm you want to revoke access for this user.

License

The license tab displays information about your trial license. You can see the type of license you have, how many days you have remaining, how many users you have active and remaining, and the security device selected.



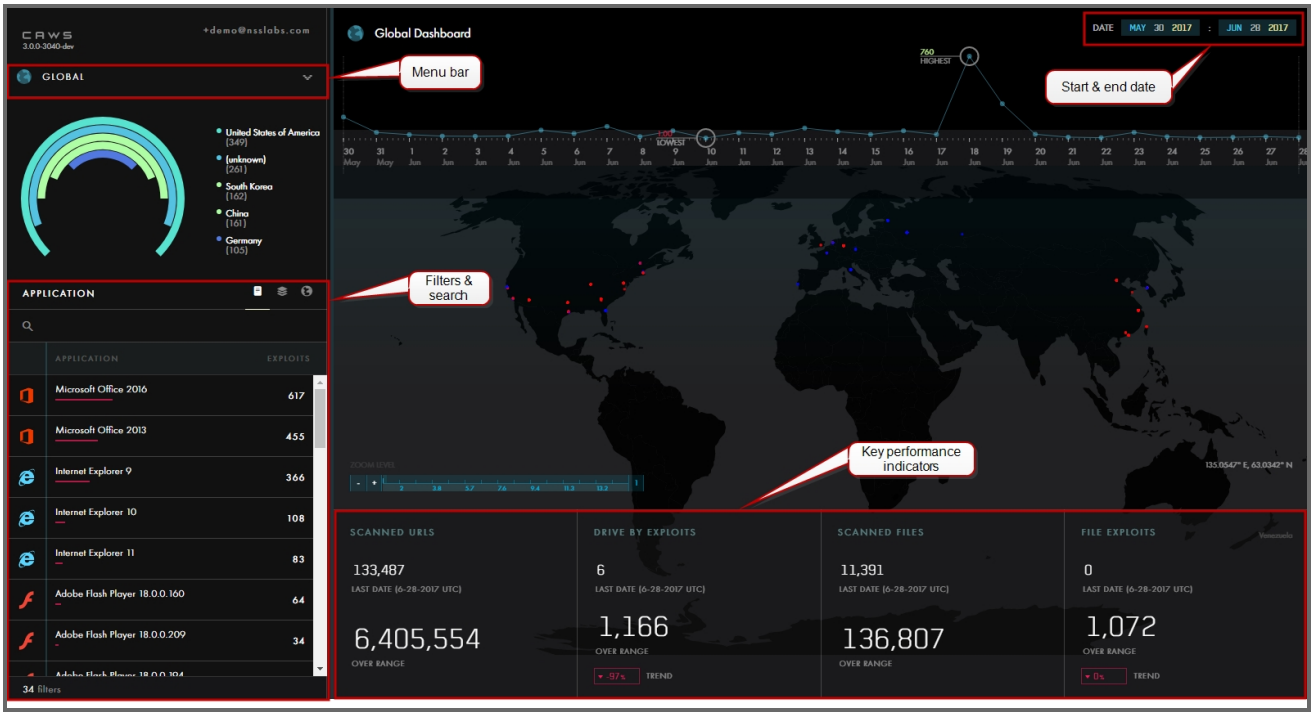
CHAPTER 5: GLOBAL DASHBOARD

When you log into CAWS, the Global Dashboard default home page summarizes information about how many exploits were found in every application, operating system platform, and country for the time frame chosen. By default, it is set to 30 days.

You can view information on exploits, such as the country and point of origin, and how many connections points that exploit has.

The menu bar on the left side of the page contains options for accessing each CAWS module.

To expand the menu bar, click the  arrow.



Data panes in CAWS are interactive, allowing you to view the data in different ways or to view additional information. You can scroll to zoom in to view more detailed information. Clicking the number of exploits opens the Threat Details page.

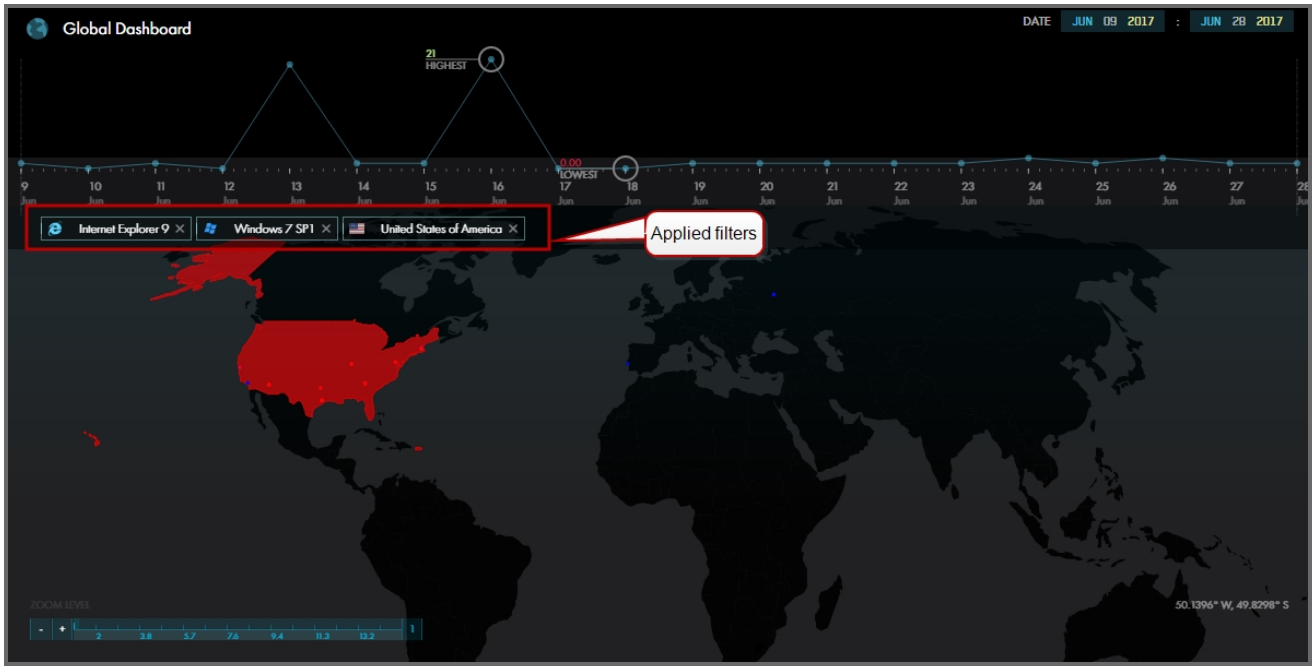
CAWS generates new data for the start and end date range specified. There are pre-defined filters available: 30 days, 90 days, Year, and All. When using a filter, CAWS uses the current date as the end date.

The world map shows red and blue dots. The red dots are the origin point of each threat found in that country, and the blue dots are the connection points where the command and control servers are located. Moving over the map displays the geographical location in the bottom right of the map. You can focus into the world map using the zoom function. You can click a location on the map and see the exploits information for that country at the bottom of the page.

Filters

Filters are “and” between application, platform, and country. They are “or” within each filter. For example, you want to see threats between a given date range, originated in the United States, with application Internet Explorer 9 and platform of Windows 7.

Filter	Definition
Application	Displays the applications and the total number of exploits found per application during the specified time period.
Platform	Displays the platforms associated with the threat and the total number of exploits found per platform during the specified time period.
Country	Displays the countries associated with the threat and the total number of exploits found per country during the specified time period.

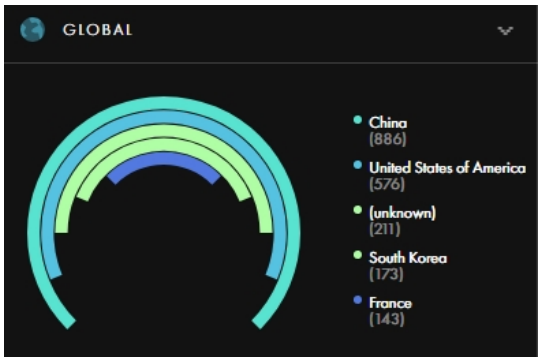


Click **X** to remove the applied filter.

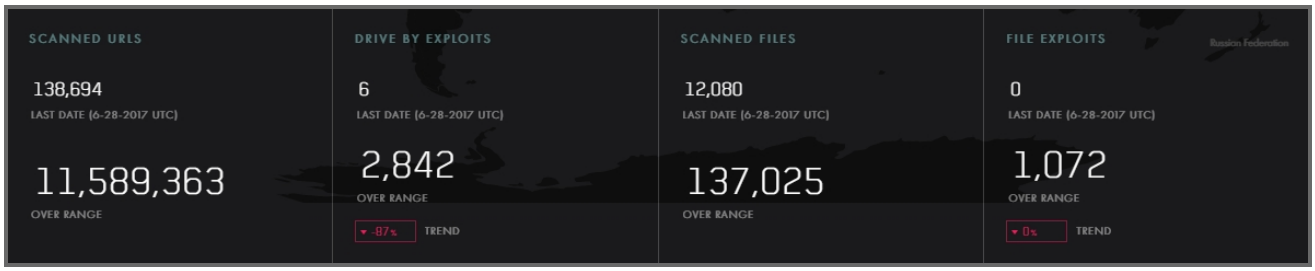
You can search within the filters and the search applies to all filters, not just the one selected. The total number of filters found displays at the bottom.

Global Country Chart

The Global Country chart displays the number of exploits in the five top countries who have exploits hosted.



Key Performance Indicators



Scanned URLs

Last Date - Displays the number of URLs found hosting exploits during the specified end date.

Over Range - Displays the number of URLs found hosting exploits during the specified start and end time period.

Drive By Exploits

Last Date - Displays the number of exploits caused by visiting a URL CAWS detected during the specified end date.

Over Range - Displays the total number of exploits caused by visiting a URL detected during the specified start and end time period.

Trend - Displays the percentage difference during the specified start and end time period.

Scanned Files

Last Date - Displays the number of files scanned during the specified end date.

Over Range - Displays the number of files scanned during the specified start and end time period.

File Exploits

Last Date - Displays the number of exploits hidden in a file that CAWS detected during the specified end date.

Over Range - Displays the total number of new, unique exploits CAWS detected during the specified start and end time period.

Trend - Displays the percentage difference during the specified start and end time period.

Using Global Search

Use the search function to search by MD5 hashes, URLs, NSS IDs, and IP addresses.

To perform a search:

- To perform a search, enter the search term in the Search field and press **Enter**.

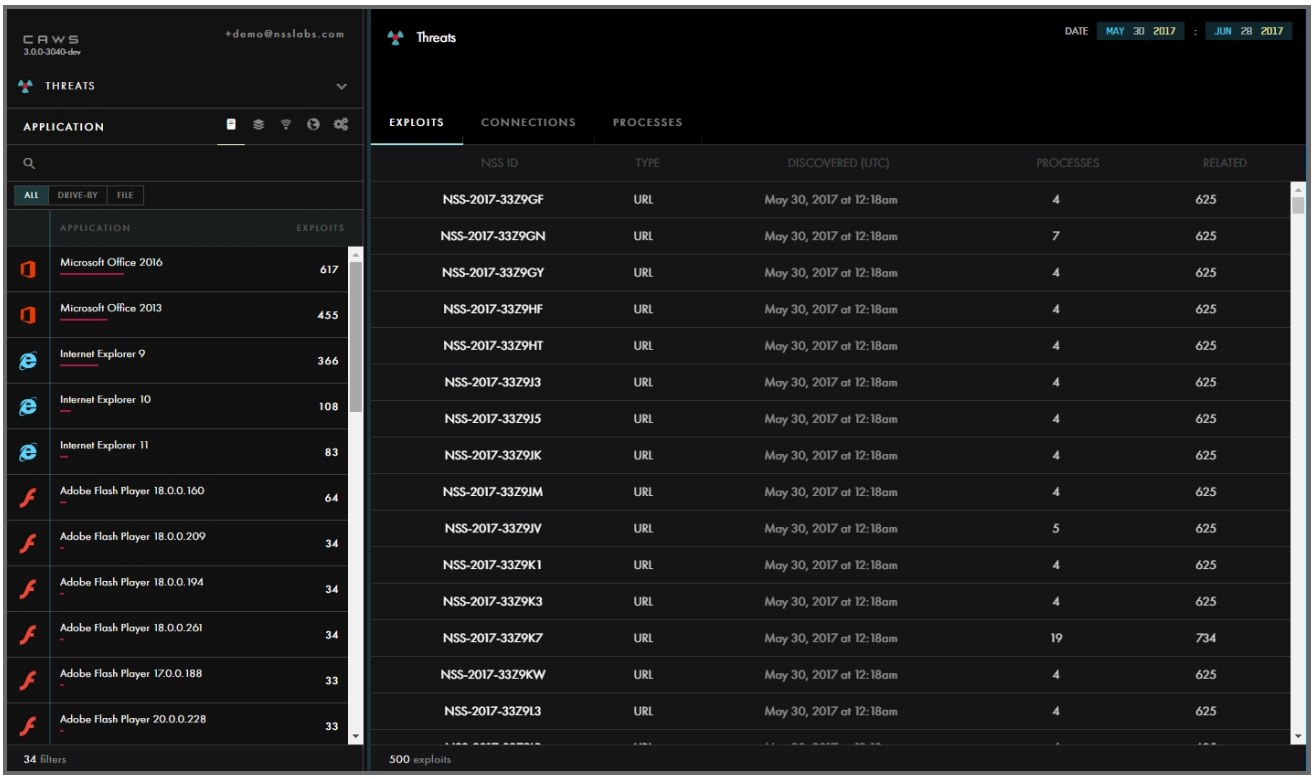
- To perform a global search, from any page type **Ctrl + F** and the global search opens.

CHAPTER 6: THREATS

Threats shows a summary of the threats found within the time period specified and the applications targeted.

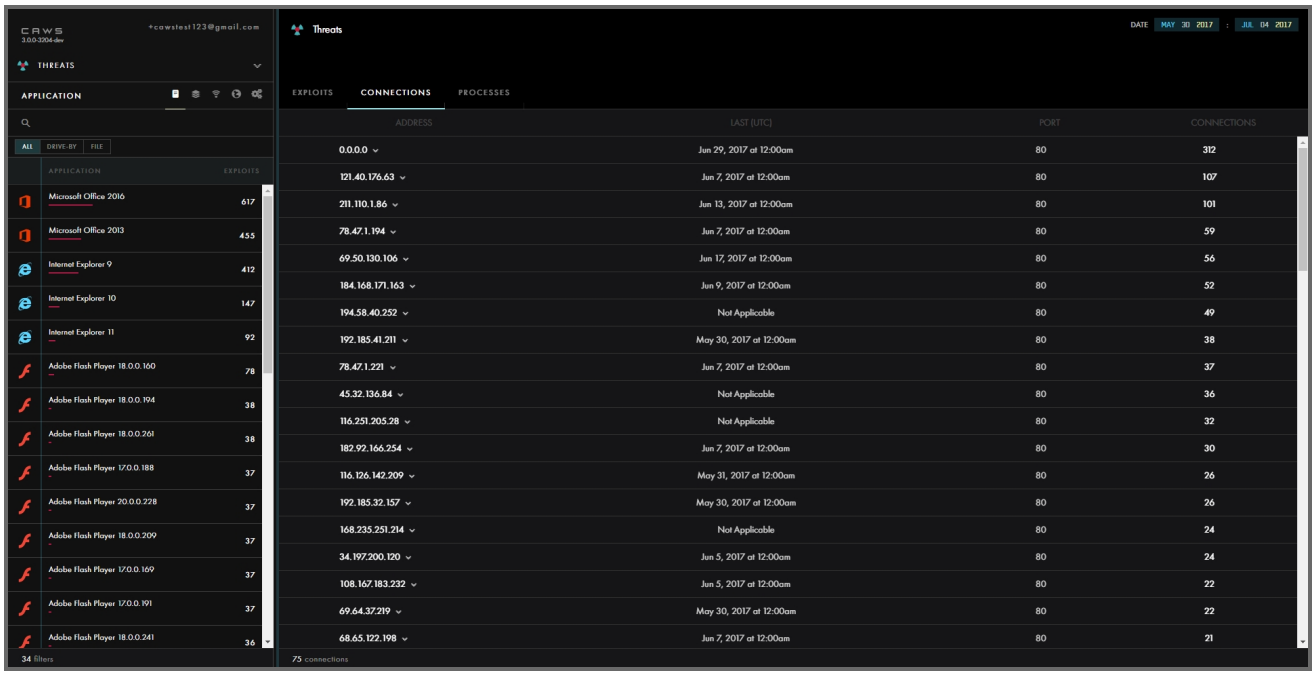
Exploits

The Exploits page displays specific information about an individual threat, such as the NSS ID, type, date discovered, the number of processes and related exploits.



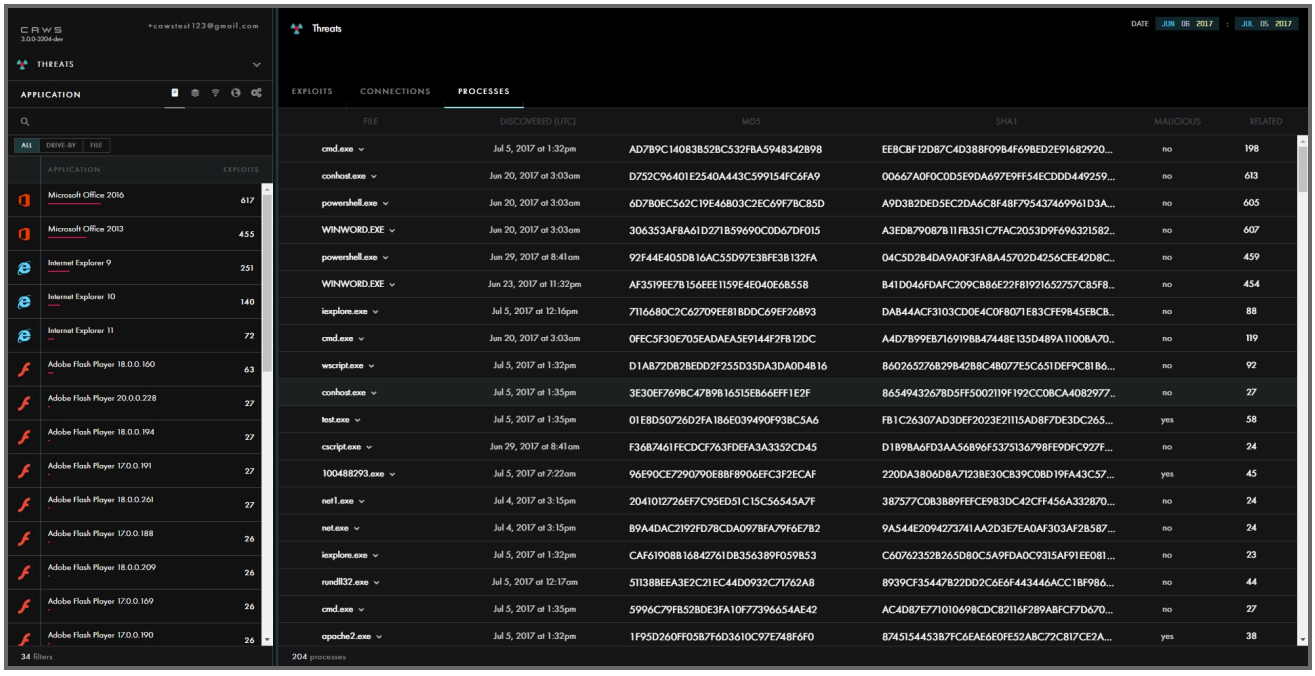
Connections

List of unique IP addresses, ports, and number of connections associated with the threat.



Processes

Processes displays the list of files found



Filters

Filter	Definition
Application	Displays the applications and the total number of exploits found per application during the specified time period.
Platform	Displays the platforms associated with the threat and the total number of exploits found per platform during the specified time period.
IP	Displays the IP addresses associated with the threat and the total number of exploits found per IP during the specified time period.
Country	Displays the countries associated with the threat and the total number of exploits found per country during the specified time period.
Process	Displays the processes associated with the threat and the total number of exploits found per process during the specified time period.
Drive-By	Displays the total number of exploits caused by clicking or visiting a URL.
File	Displays the application file with the exploit.

Filters are “and” between application, platform, IP, country and process. They are “or” within each filter. For example, you want to see threats between a given date range, originated in the United States, with application Internet Explorer 9 and platform of Windows 7.

Using Global Search

Use the search function to search by MD5 hashes, URLs, NSS IDs, and IP addresses.

To perform a search:

- To perform a search, enter the search term in the Search field and press **Enter**.

- To perform a global search, from any page type **Ctrl + F** and the global search opens.

Threat Details Page

You can open a Threat Details page from the Global Dashboard and Threats page.

- In Threats, click any NSS ID hyperlink to open the Threat Details page.
- In the Global Dashboard, click on the number of File Exploits or Drive By Exploits found. Click any NSS ID hyperlink to open the Threat Details page.
- To close the Threat Details page, click the **X** in the right-hand corner.

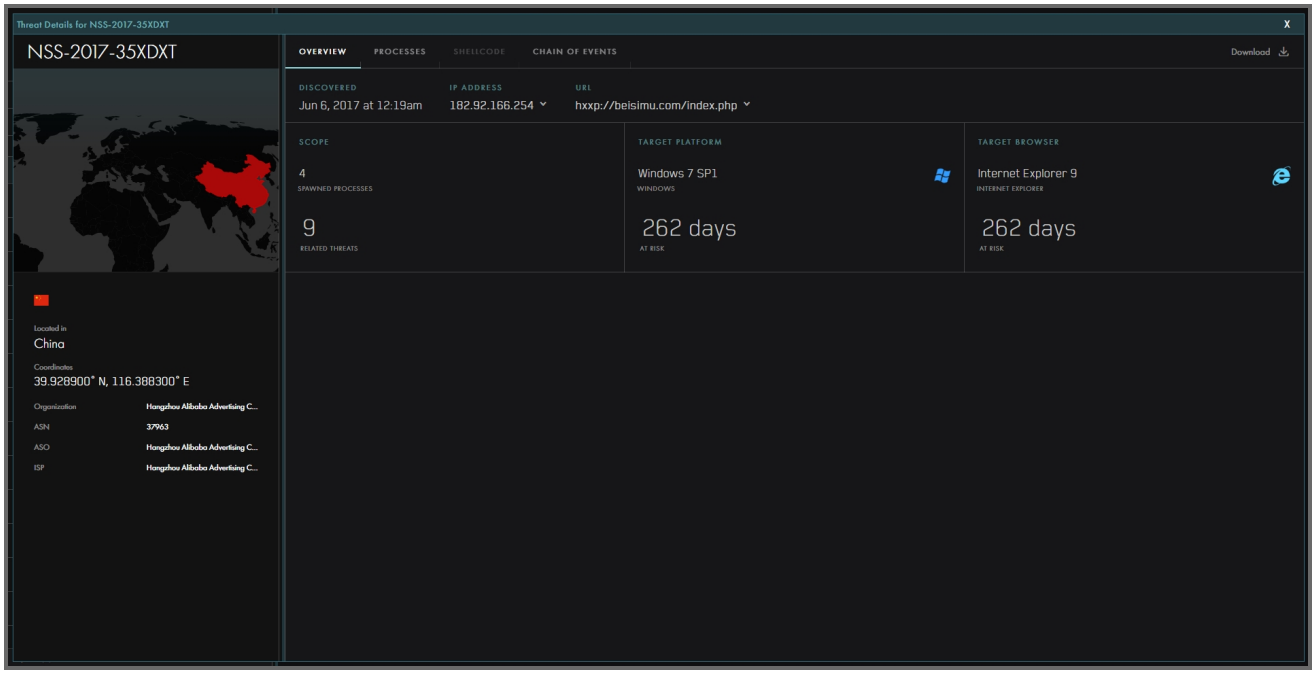
- Use the **Download** function to download a Packet Capture (PCAP) file, Session Archive Zip (SAZ), or Shellcode file so you can perform your own analysis.

Overview

The **Overview** tab displays specific information about an individual threat, such as when it was discovered, IP address, and the URL, etc.

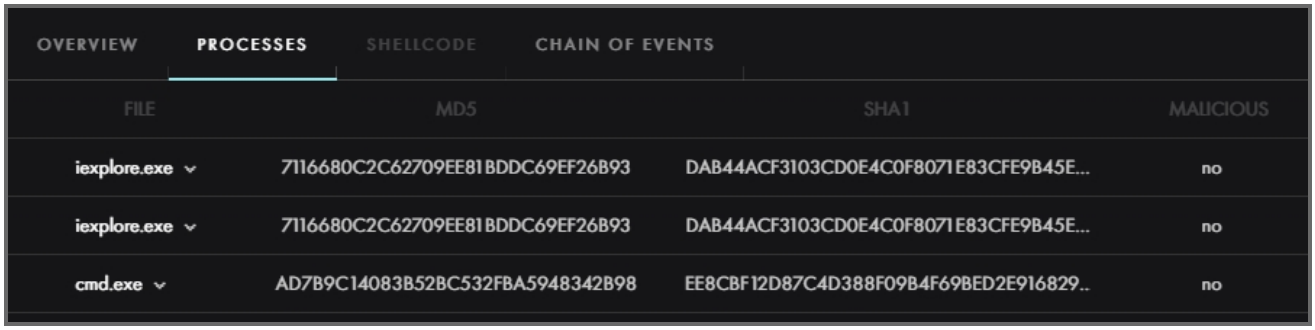
The Files section displays hash information about files associated with the threat.

Click the ▾ arrow next to the IP Address and URL to view related threats, VirusTotal information.



Processes

Processes displays the process files found in the threat.

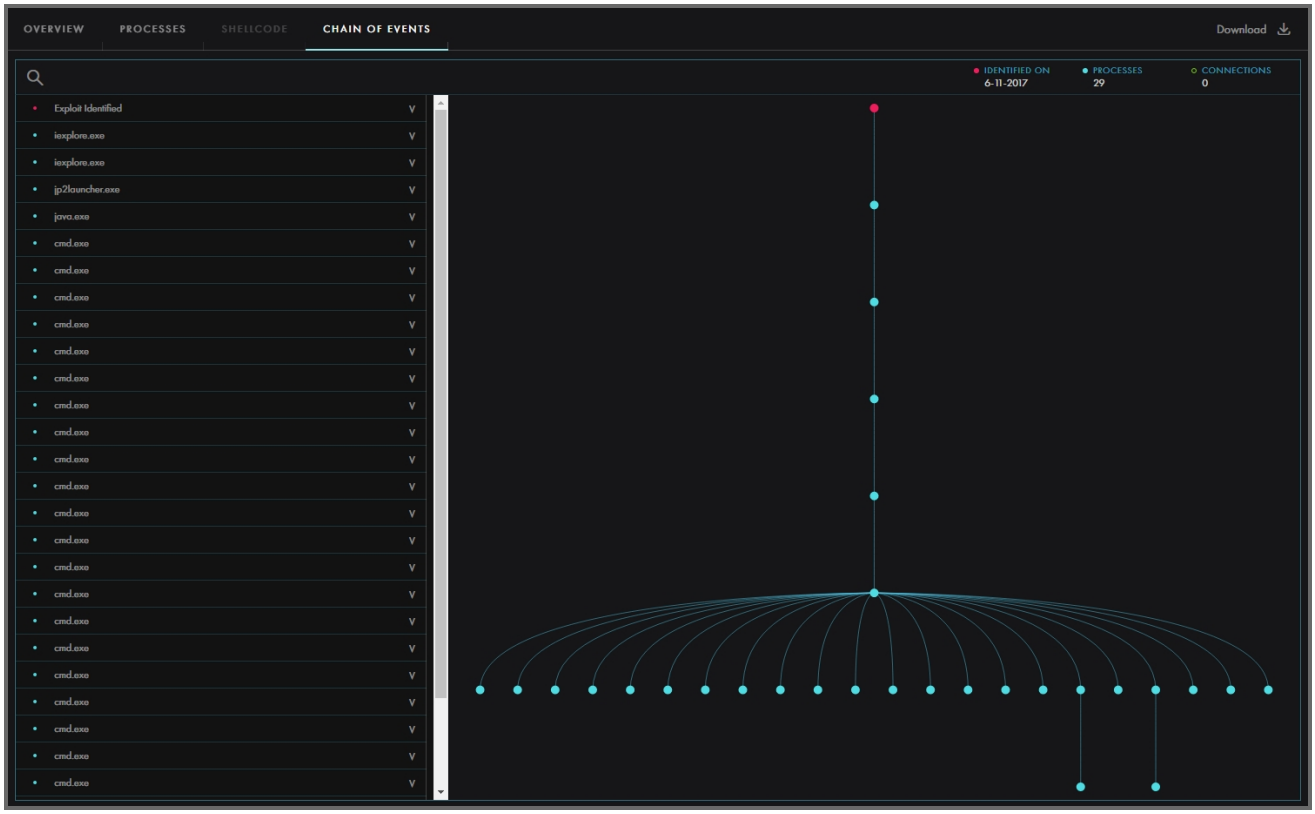


Shellcode

Displays a list of captured exploits that contain new shellcode captures. The list displays the NSS ID, detection time stamp, platform, targeted application, file count, and connection count.

Chain of Events

The **Chain of Events** tab displays a step-by-step playback of events for an exploit. This allows you to visualize the sequence of events leading up to and during an exploitation.



To view a chain of events, click an individual event in the Exploit list.

Clicking an individual item allows you to drill down for more information on each event.

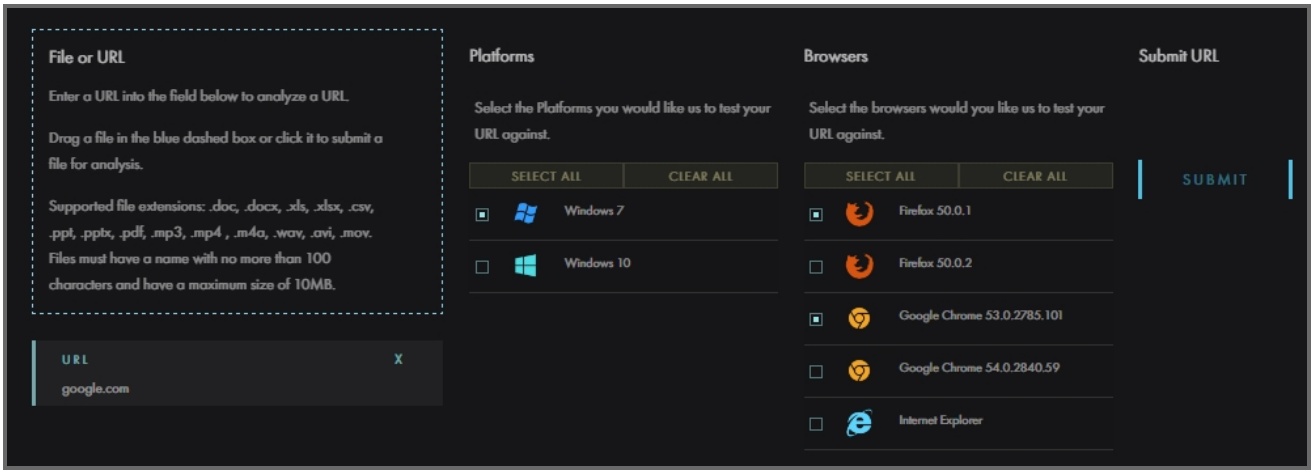
CHAPTER 7: SUBMISSIONS

The Submissions feature allows you to submit URLs or files (Office, PDF, and media) for exploit analysis.

URL Scan

To submit a URL:

1. From the menu bar, click **Submissions**.
2. Type a URL in the **URL** field.
3. Select the platform(s) you would like to use to test your URL against.
4. Select the browser(s).



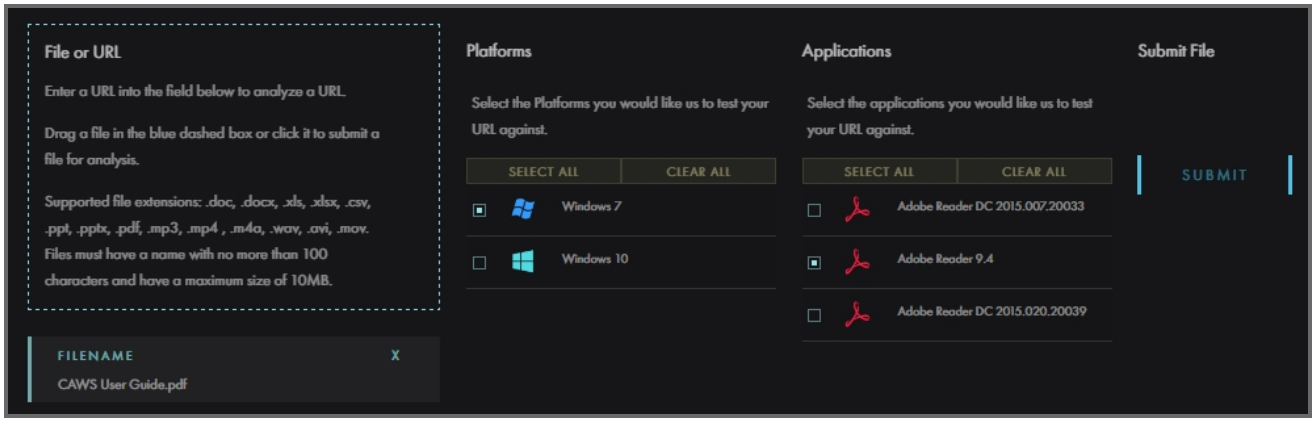
5. Click **Submit**.

File Scan

You can upload custom files to be scanned for exploit detection by CAWS. The following are supported file extensions: .doc, .docx, .xls, .xlsx, .csv, .ppt, .pptx, .pdf, .mp3, .mp4 , .m4a, .wav, .avi, .mov. The file name must be 100 characters or less in length. The maximum file size 10MB.

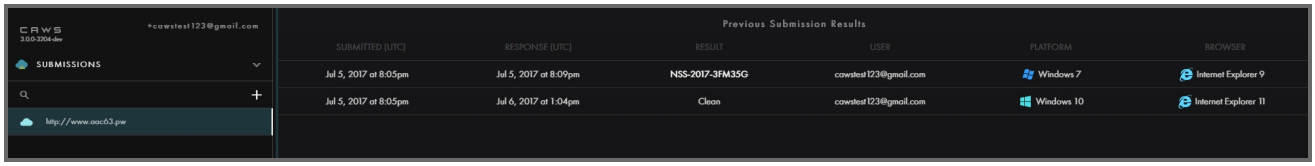
To submit a file:

1. From the menu bar, click **Submissions**. The Submit File or URL page displays.
2. Click the blue dashed box and select a file, or drag and drop the file onto the blue dashed box.
3. Select the platform(s) you would like to use to test your file against.
4. Select the application(s) you would like to use to test your file against. The Applications displayed are dependent on the type of file uploaded.



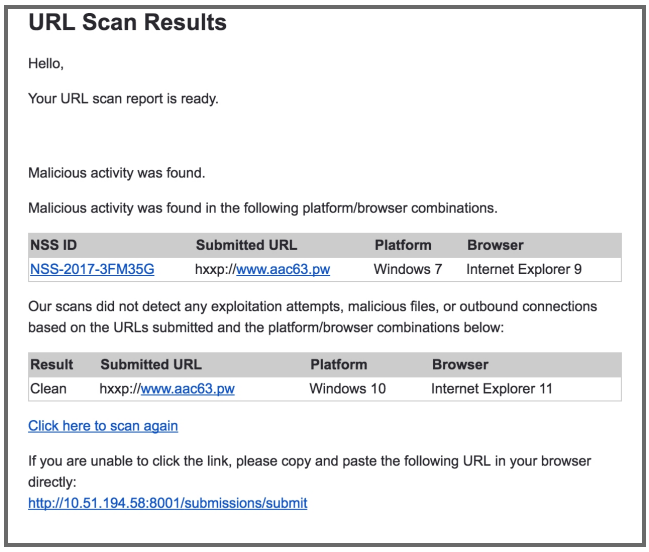
5. Click **Submit**.

Previously submitted files display on the left hand side of the page.



Status	Definition
Queued	File or URL was submitted to be scanned.
Syncing	File or URL is in the process of being scanned and results are being updated.
Clean	The submitted file or URL is not malicious.
NSS ID	The submitted file or URL is malicious. You can drill down to find out more information.

The following is a sample email you receive after submitting a file or URL to be scanned.



URL Scan Results

Hello,

Your URL scan report is ready.

Malicious activity was found.

Malicious activity was found in the following platform/browser combinations.

NSS ID	Submitted URL	Platform	Browser
NSS-2017-3FM35G	hxxp://www.aac63.pw	Windows 7	Internet Explorer 9

Our scans did not detect any exploitation attempts, malicious files, or outbound connections based on the URLs submitted and the platform/browser combinations below:

Result	Submitted URL	Platform	Browser
Clean	hxxp://www.aac63.pw	Windows 10	Internet Explorer 11

Click here to scan again

If you are unable to click the link, please copy and paste the following URL in your browser directly:
http://10.51.194.58:8001/submissions/submit

Using Global Search

Use the search function to search by MD5 hashes, URLs, NSS IDs, and IP addresses.

To perform a search:

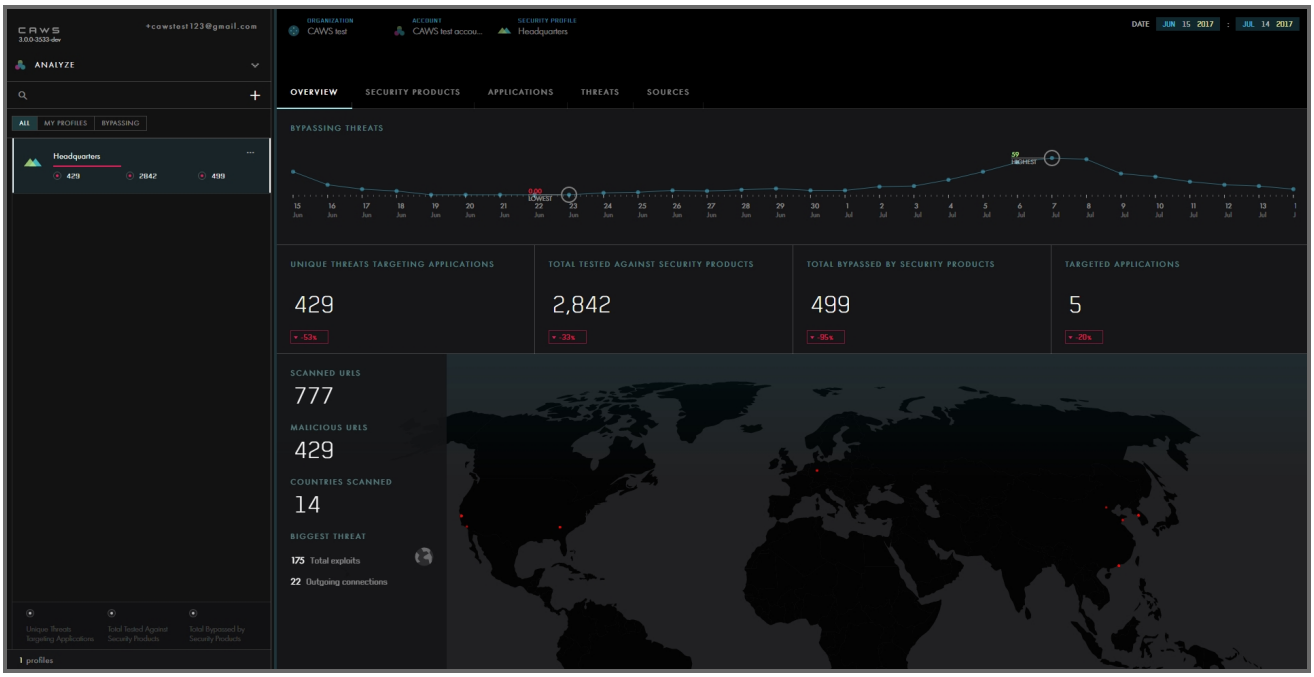
- To perform a search, enter the search term in the Search field and press **Enter**.

- To perform a global search, from any page type **Ctrl + F** and the global search opens.

CHAPTER 8: ANALYZE

Analyze allows you to view and understand how your existing security profiles are performing, and to compare security products and applications against your live data. Here are a few examples of how analyzing can be used to improve security:

- Situational awareness: Monitor which applications are being targeted by threat actors and determine how exploits relate to failures in deployed security products. This information helps prioritize security policy changes, patch cycles, and security product updates.
- Compare security profiles: Evaluate up to three different security products side by side to compare their efficacy against current threats and exploits.



Filters

Filter	Definition
My Profile	Displays profile information for the current user.
Bypassed Threats	Displays the security profiles that have bybassed threats.

Using Global Search

Use the search function to search by MD5 hashes, URLs, NSS IDs, and IP addresses.

To perform a search:

- To perform a search, enter the search term in the Search field and press **Enter**.

- To perform a global search, from any page type **Ctrl + F** and the global search opens.

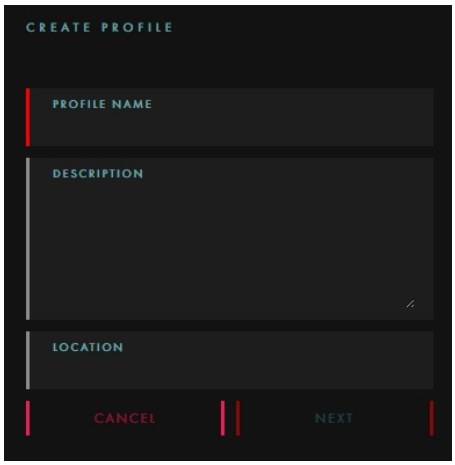
Security Profiles

Use security profiles to associate application groups and protection devices with a specific location in your organization. You can create multiple security profiles to compare your current security product to various competitors.

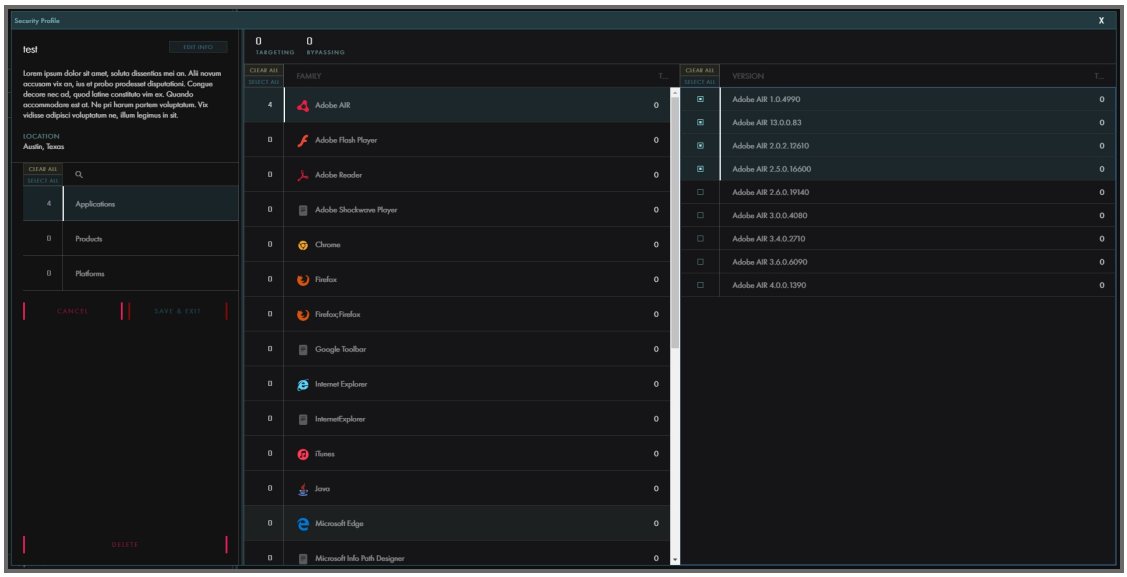
Creating a Security Profile

To create a security profile:

1. From the menu bar, click **Analyze**. The Analyze page displays.
2. Click the **+** symbol. The Create Profile page displays.



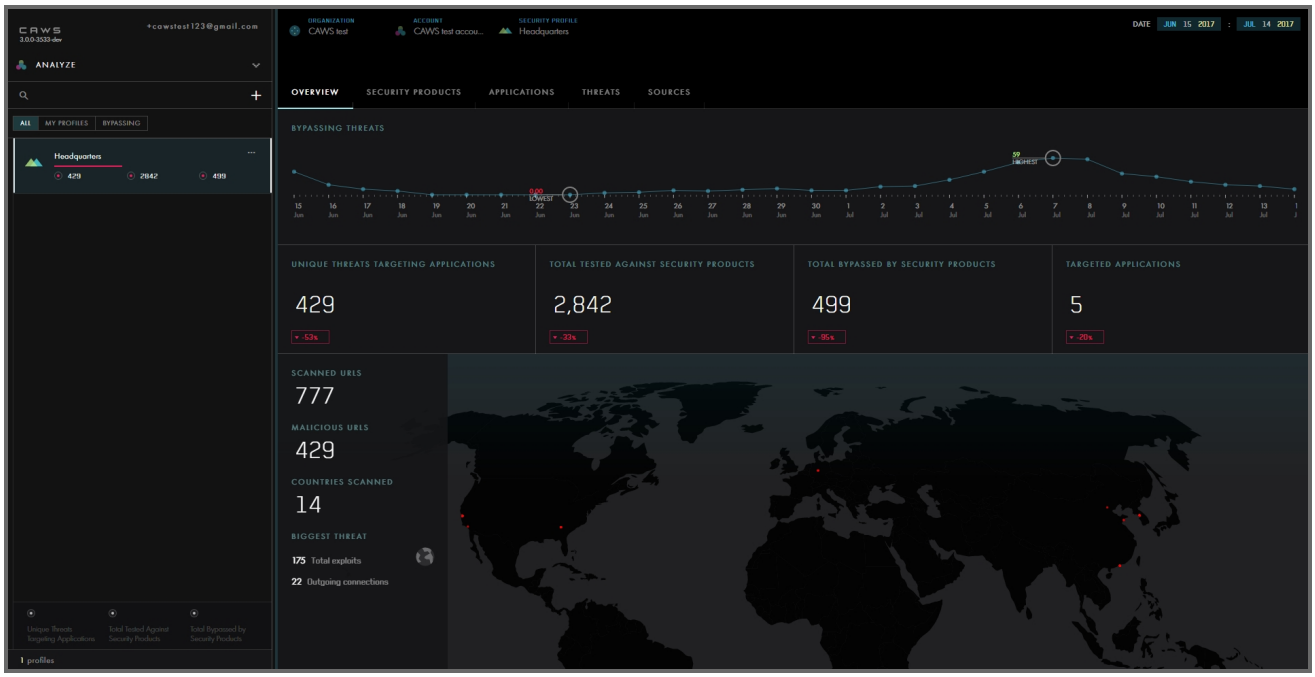
3. Enter a **Profile Name**.
4. Enter a **Description**.
5. Enter the **Location**.
6. Click **Next**.



7. Select the **Applications** associated with the security profile by selecting **Application** in the left panel, selecting an item in the Application family column and then selecting the appropriate versions.
8. Select the **Products** associated with the security profile by selecting **Products** in the left panel, selecting an item in the Family column and then selecting the appropriate version. **Note**: You can only select one product per profile.
9. Select the **Platforms** associated with the security profile by selecting **Platforms** in the left panel, selecting an item in the Family column and then selecting the appropriate versions.
10. Click **Save & Exit.**

Overview

Displays the threats that are bypassed on a daily basis for the selected profile.



Unique Threats Targeting Applications

Displays the total number of unique threats targeting the selected applications associated with this security profile.

Total Tested Against Security Products

Displays the total number of exploits found that are not bypassed.

Bypassing Threats

Displays a count of exploits that have bypassed all security products associated with this security profile.

Total Bypassed by Security Products

Displays the number of exploits that have bypassed all security products associated with the selected profile.

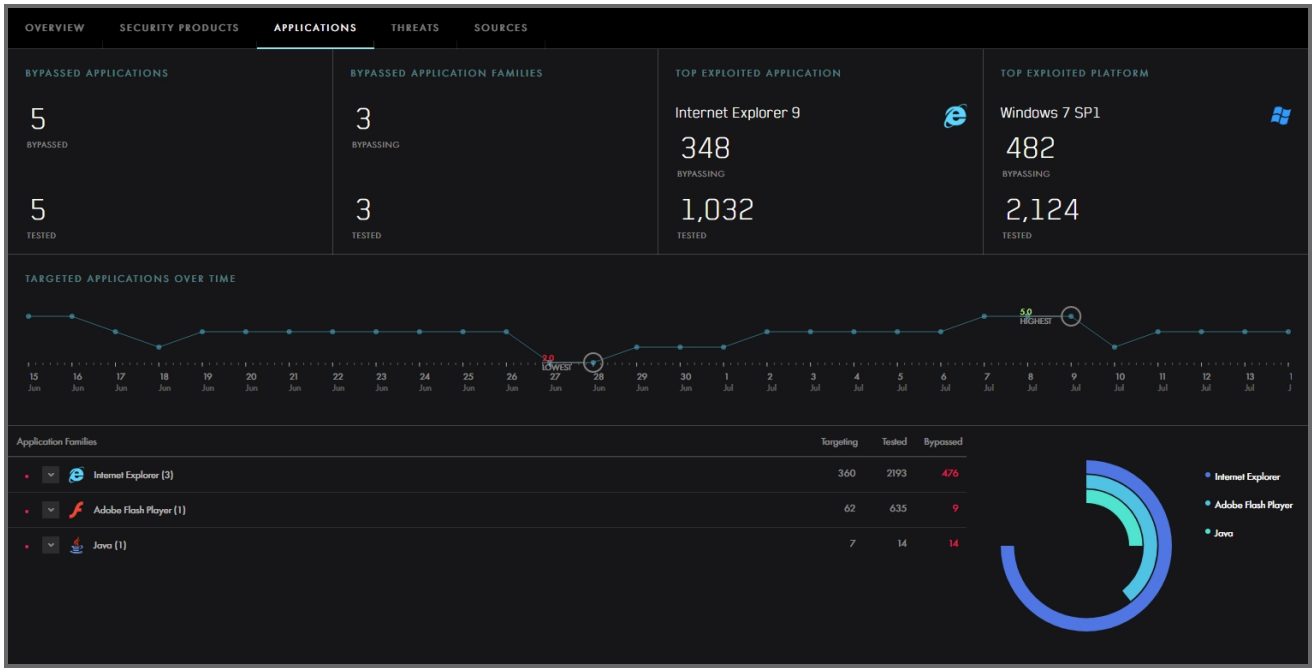
Targeted Applications

Summarizes attacks on the top applications the specified time period. Mouse over to view the total number of attacks for that application.

Security Products

Displays the bypass percentage against the security product selected.

Applications



Bypassed Applications

Displays the number of applications bypassed and tested.

Bypassed Applications Families

Displays the number of applications targeted by malicious threats.

Top Exploited Application

Displays the highest targeted application and the number of exploits bypassing this application.

Top Exploited Platform

Displays the highest targeted platform the specified time period.

Targeted Applications Over Time

Summarizes attacks on the top applications over the specified time period. Mouse over a point to view the total number of exploits for that application.

Sources

Displays the top threats and the country hosting the threat and the top outbound connections where they are opening connections to.

Top Threats

Displays the number of top threats and where they are originating.

Top Outbound Connections

Displays where the top threats are making connections.

CHAPTER 9: HELP AND SUPPORT

From the menu bar, click Help and support to access support for CAWS Continuous Security Validation Platform.