

# 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](mailto:info@nsslabs.com)  
[www.nsslabs.com](http://www.nsslabs.com)

© 2017 NSS Labs, Inc. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, e-mailed or otherwise disseminated or transmitted without the express written consent of NSS Labs, Inc. ("us" or "we").

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. "You" or "your" means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.

The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.

NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.

This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.

All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.

<b>Chapter 1: Introduction</b>	<b>1</b>
What is CAWS	1
List of Security Product Types Tested in CAWS	1
List of Applications Tested in CAWS	2
List of Platform (Operating Systems) Tested in CAWS	2
<b>Chapter 2: Licensing</b>	<b>3</b>
Trial	3
Converting a Trial License to a Paid License	3
<b>Chapter 3: Registering for CAWS</b>	<b>4</b>
Register	4
<b>Chapter 4: Organizations</b>	<b>6</b>
Using Global Search	7
Editing your Profile	8
Change Password	9
End User License Agreement	10
User Account Settings	10
Inviting Users	10
Deleting Users	12
License	12
<b>Chapter 5: Global Dashboard</b>	<b>13</b>
Filters	14

Global Country Chart .....	14
Key Performance Indicators .....	15
Scanned URLs .....	15
Drive By Exploits .....	15
Scanned Files .....	15
File Exploits .....	15
Using Global Search .....	16
<b>Chapter 6: Threats .....</b>	<b>17</b>
Exploits .....	17
Connections .....	17
Processes .....	18
Filters .....	19
Using Global Search .....	19
Threat Details Page .....	19
Overview .....	20
Processes .....	20
Shellcode .....	20
Chain of Events .....	21
<b>Chapter 7: Submissions .....</b>	<b>22</b>
URL Scan .....	22
File Scan .....	22

Using Global Search .....	24
<b>Chapter 8: Analyze .....</b>	<b>25</b>
Filters .....	25
Using Global Search .....	25
Security Profiles .....	26
Creating a Security Profile .....	26
Overview .....	27
Unique Threats Targeting Applications .....	28
Total Tested Against Security Products .....	28
Bypassing Threats .....	28
Total Bypassed by Security Products .....	28
Targeted Applications .....	28
Security Products .....	28
Applications .....	29
Bypassed Applications .....	29
Bypassed Applications Families .....	29
Top Exploited Application .....	30
Top Exploited Platform .....	30
Targeted Applications Over Time .....	30
Sources .....	30
Top Threats .....	30

Top Outbound Connections .....	30
<b>Chapter 9: Help and support .....</b>	<b>31</b>

## 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](mailto: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.

The image shows a registration form for CAWS. At the top, the CAWS logo is displayed in a light blue font. Below the logo, the text "REGISTER FOR A FREE FULLY FUNCTIONAL CAWS TRIAL" is shown in a smaller, light blue font. The form itself is a dark gray rectangle with a light blue border. Inside the form, there are four input fields with light blue placeholder text: "WORK EMAIL", "CONFIRM WORK EMAIL", "PASSWORD (MIN 8 CHARS)", and "CONFIRM PASSWORD". Below the input fields, there are two small light blue dots. At the bottom of the form, there are two buttons: "BACK" and "NEXT", both in light blue text.

2. Enter your work email address.
3. Confirm your email address.
4. Enter your desired password.

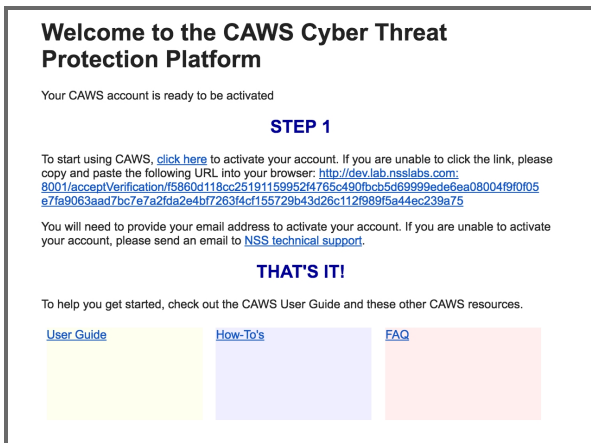
**Note:** Password must have the following characteristics:

- 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.

The screenshot shows the CAWS interface. The top left header displays 'CAWS 3.0.0.3554-dev' and the user email '+cawstest123@gmail.com'. The left sidebar has a menu with 'ORGANIZATIONS' selected. Below the menu is a search bar and a list of items: 'ORGANIZATIONS' and 'CAWS test - 1 accounts[s]'. The main content area is titled 'Organizations' and has tabs for 'DETAILS', 'ACCOUNT USERS', 'INVITE USERS', and 'LICENSE'. The 'DETAILS' tab is active, showing the 'ORGANIZATION DETAILS' form. The form includes fields for NAME, ADDRESS, ADDRESS 2, CITY, COUNTRY, PRIMARY CONTACT NAME, PRIMARY CONTACT PHONE, and ZIP. A 'CREATE ORGANIZATION' button is at the bottom.

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**.

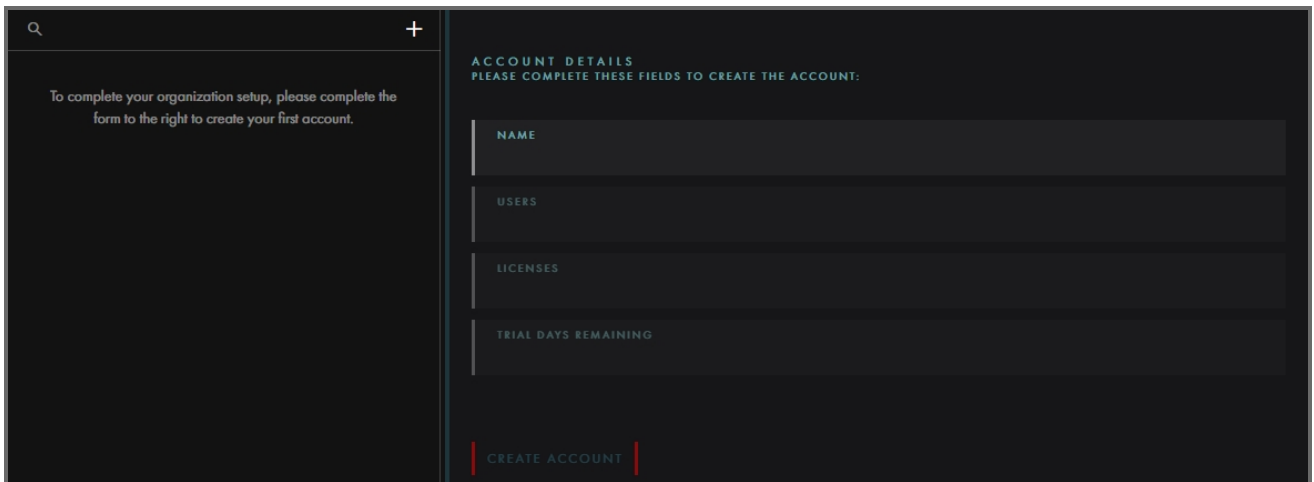
**To add an organization:**

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.



The screenshot shows a dark-themed user interface. On the left, there is a sidebar with a search icon (magnifying glass) and a plus sign (+). The main area on the right is titled 'ACCOUNT DETAILS' and 'PLEASE COMPLETE THESE FIELDS TO CREATE THE ACCOUNT:'. Below the title, there are four input fields labeled 'NAME', 'USERS', 'LICENSES', and 'TRIAL DAYS REMAINING'. At the bottom of the form is a button labeled 'CREATE ACCOUNT'.

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**.

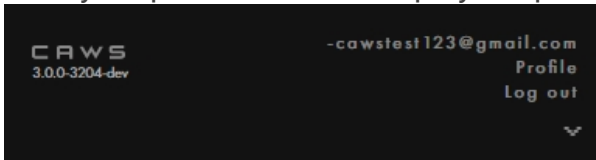


The screenshot shows a dark-themed search bar. It contains a magnifying glass icon followed by a vertical bar, indicating the search input area.

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

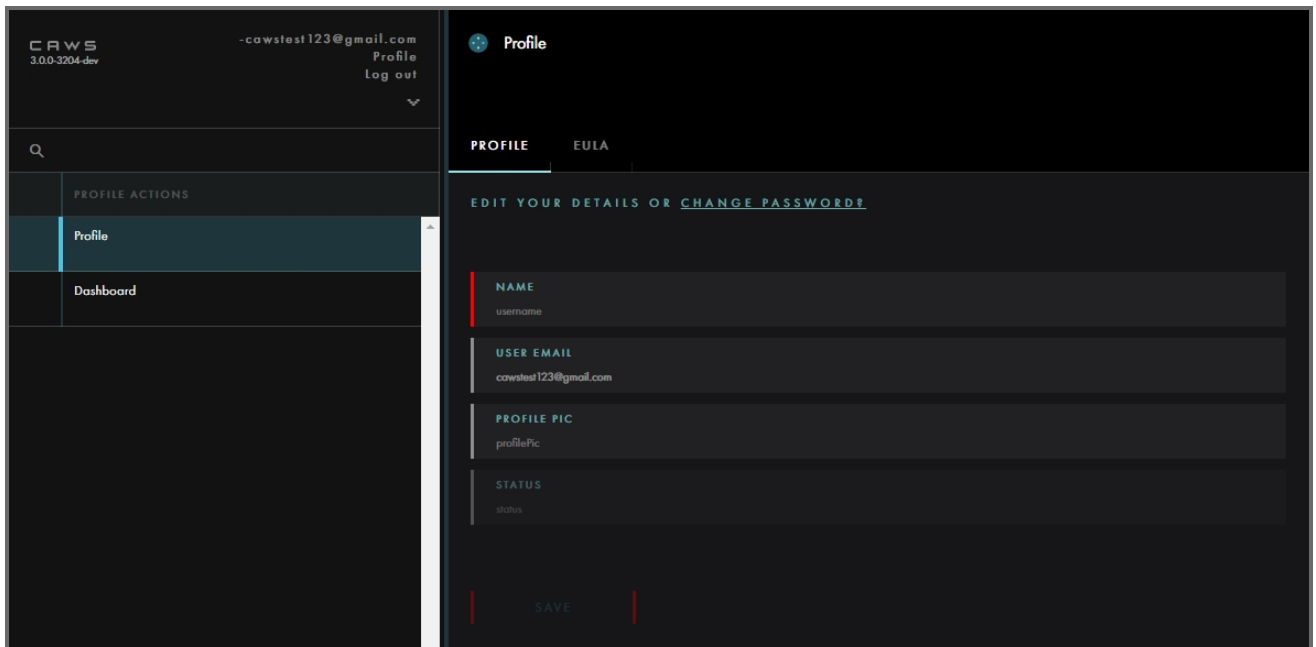
## Editing your Profile

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



### To edit your profile:

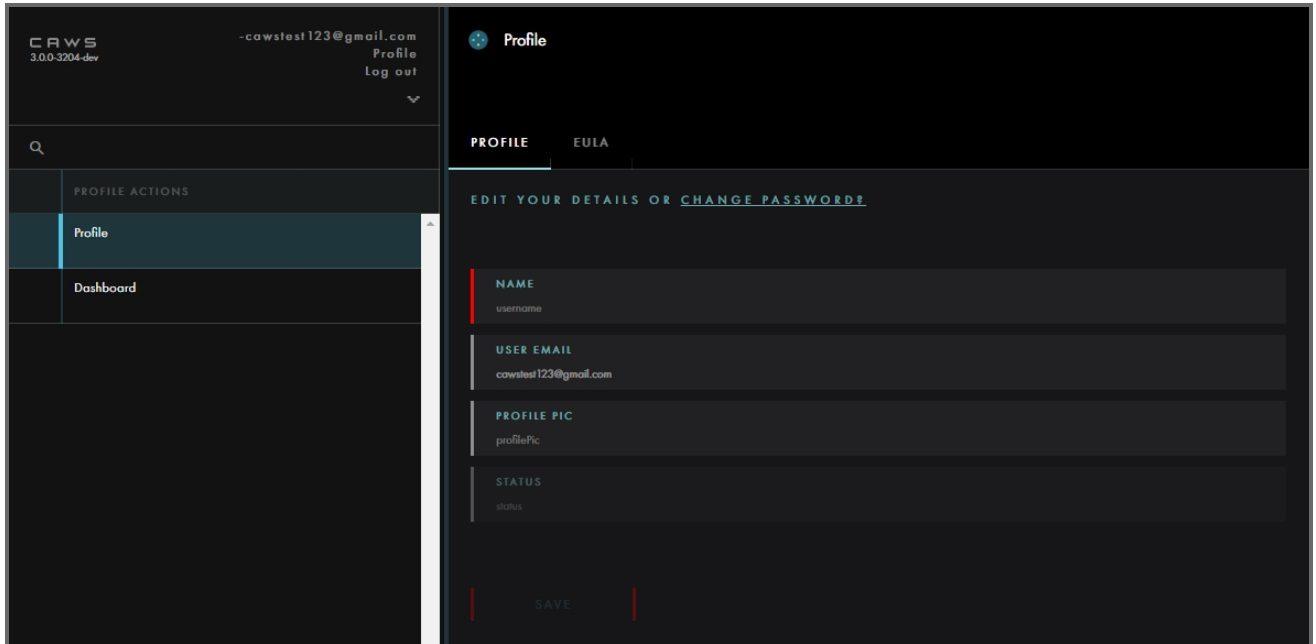
1. Click **Profile** from the drop-down menu. The Profile page displays.



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/1b5dbbe4af4f09130edf78b0ddfab4329bdaffc8ae28313ff224dd63233781858e49ac3145540e641e645a177f2c2d979c1050a8ed47d5f22e3a9c0deaac3f10>

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](#).

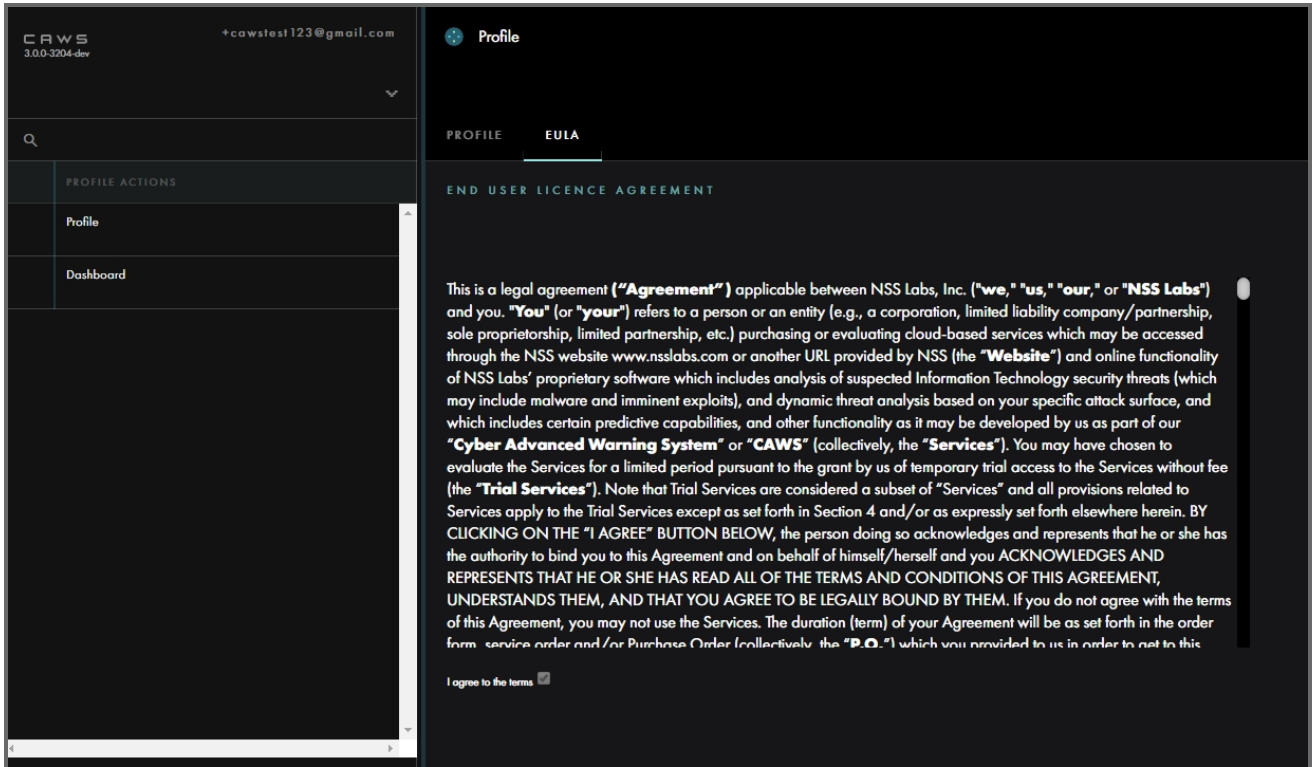
Best regards,  
NSS Labs

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

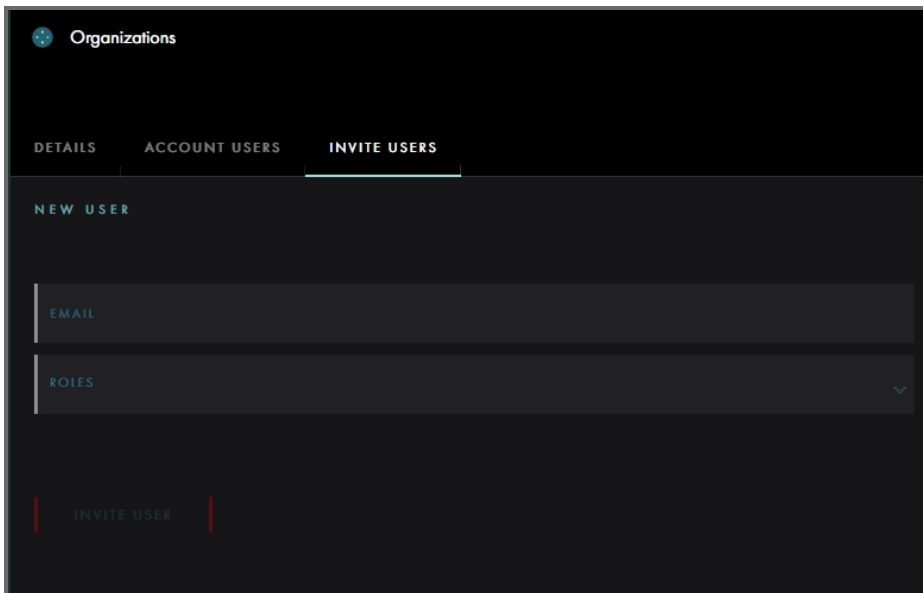
### Inviting Users

CAWS allows you to invite users.

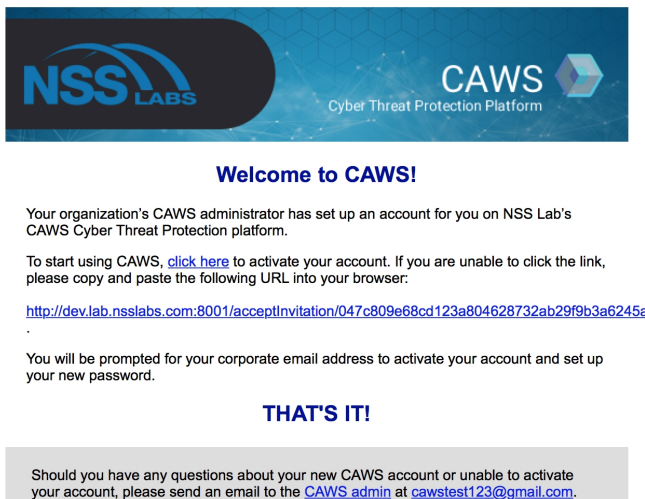


### To invite users:

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.

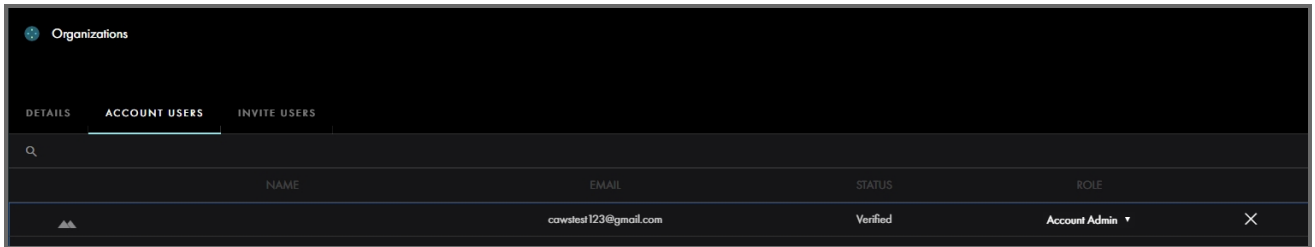


6. Click the link in the email and then enter and confirm your password.
7. Click **Save**.

## Deleting Users

To delete a user:

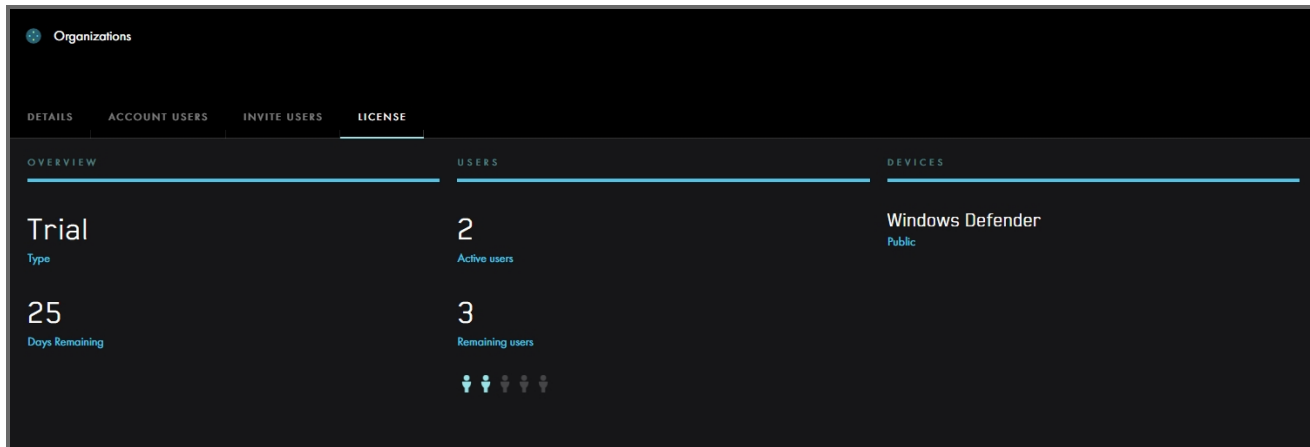
1. From the menu bar, click **Organizations**.
2. Select the **Account User** tab.



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.




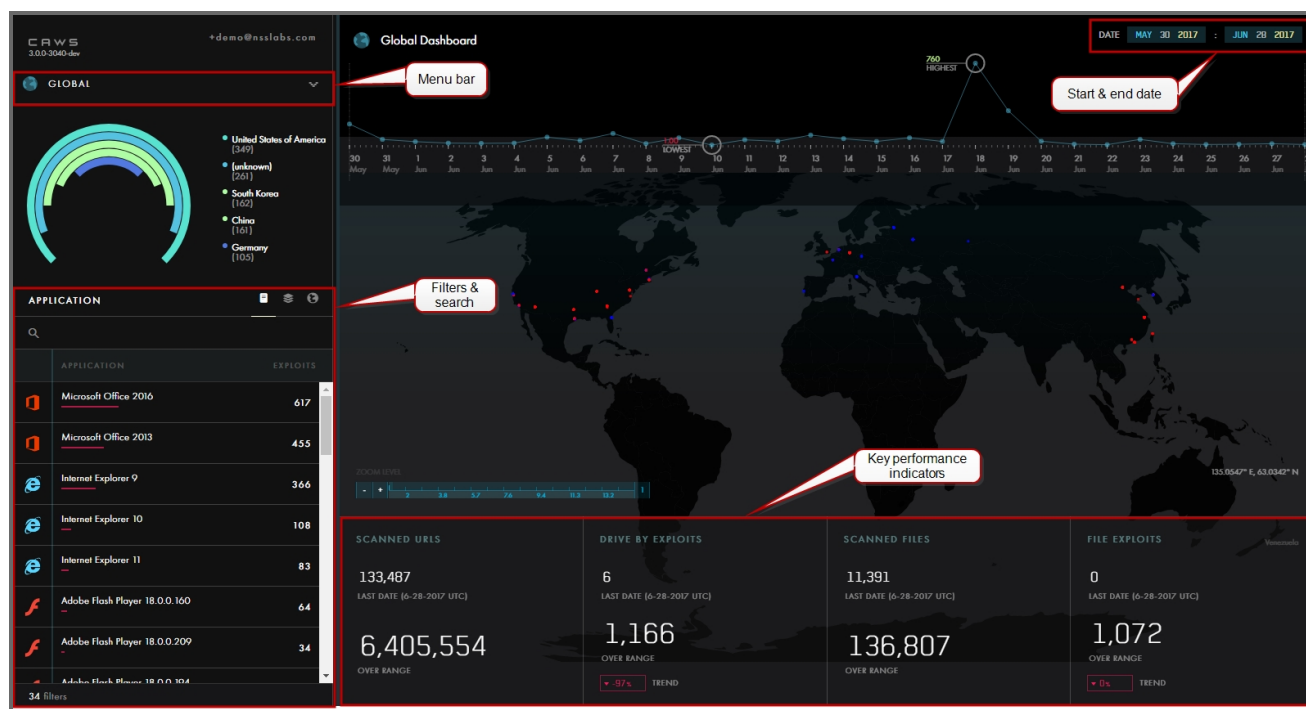
## CHAPTER 5: GLOBAL DASHBOARD

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.

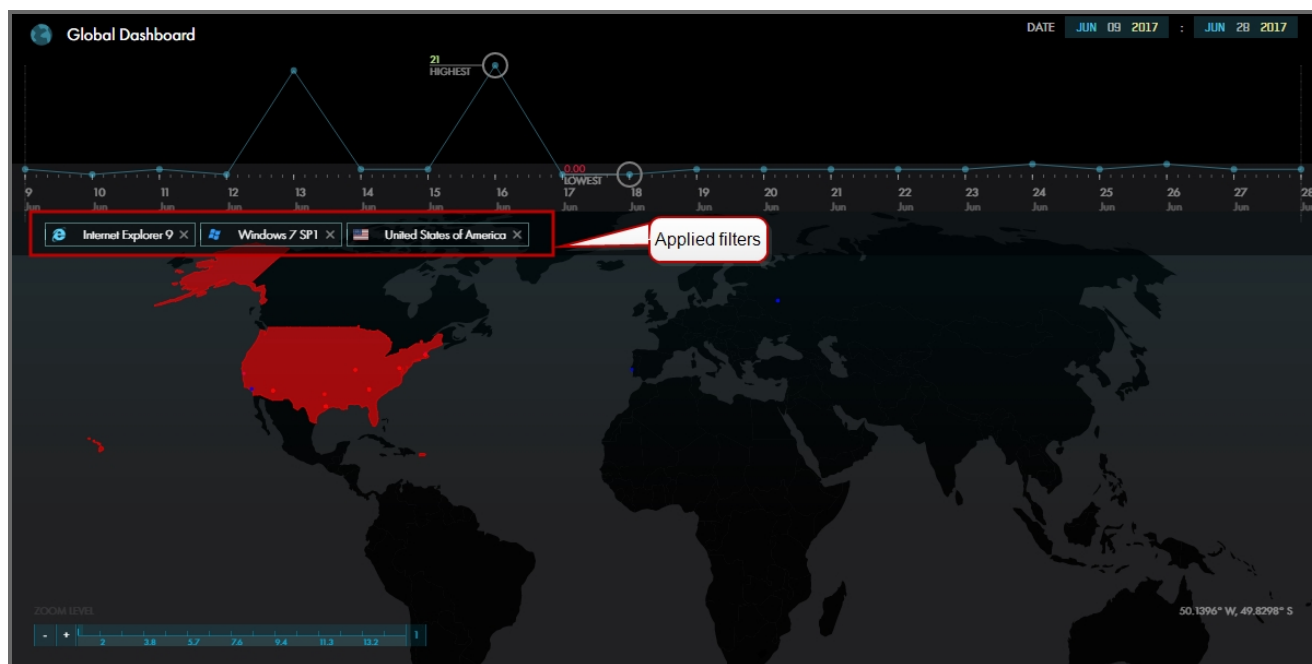
CAWS generates new data for the start and end date range specified. There are pre-defined filters available: 30 days, 90 days, Year, and All. When using a filter, CAWS uses the current date as the end date.

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.

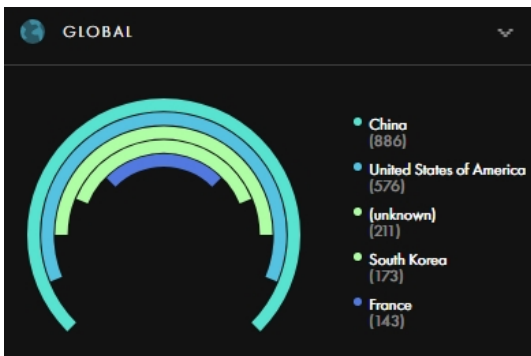


Click **X** to remove the applied filter.

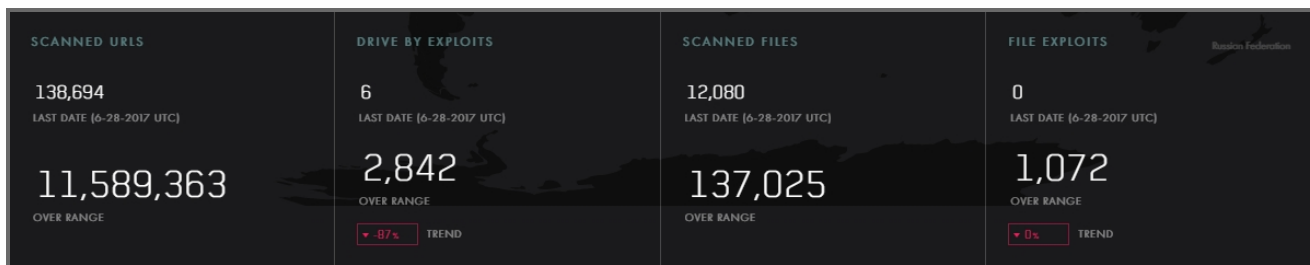
You can search within the filters and the search applies to all filters, not just the one selected. The total number of filters found displays at the bottom.

## 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**.



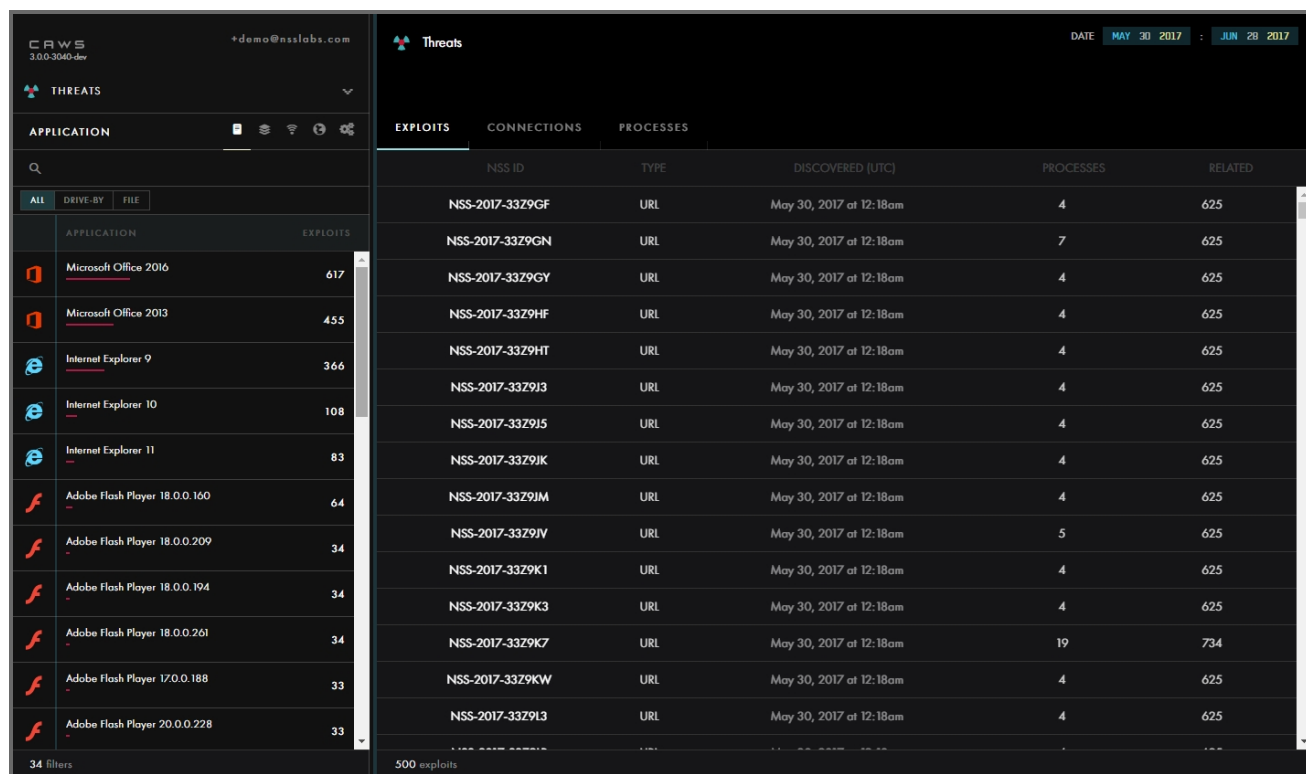
- To perform a global search, from any page type **Ctrl + F** and the global search opens.

## 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.



The screenshot shows the CROWS 3.0.0-3040-dev interface. The left sidebar has a 'THREATS' section with an 'APPLICATION' filter. The main panel is titled 'Threats' and shows a date range from May 30, 2017, to Jun 28, 2017. Below the title are tabs for 'EXPLOITS', 'CONNECTIONS', and 'PROCESSES'. The 'EXPLOITS' tab is active, displaying a table with columns: NSS ID, TYPE, DISCOVERED (UTC), PROCESSES, and RELATED. The table lists 19 exploits, all of type 'URL', discovered on May 30, 2017, at 12:18am. The applications targeted include Microsoft Office 2016, Microsoft Office 2013, Internet Explorer 9, Internet Explorer 10, Internet Explorer 11, and various versions of Adobe Flash Player. The number of processes and related exploits are also listed for each entry.

NSS ID	TYPE	DISCOVERED (UTC)	PROCESSES	RELATED
NSS-2017-33Z9GF	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9GN	URL	May 30, 2017 at 12:18am	7	625
NSS-2017-33Z9GY	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9HF	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9HT	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9J3	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9J5	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9JK	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9JM	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9JV	URL	May 30, 2017 at 12:18am	5	625
NSS-2017-33Z9K1	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9K3	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9K7	URL	May 30, 2017 at 12:18am	19	734
NSS-2017-33Z9KW	URL	May 30, 2017 at 12:18am	4	625
NSS-2017-33Z9L3	URL	May 30, 2017 at 12:18am	4	625

### Connections

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

CROWS  
3.0.0.3064-dev

\*cowtest123@gmail.com

THREATS

APPLICATION

Q

ALL

DRIVE-BY

FILE

APPLICATION

EXPLOITS

Microsoft Office 2016

617

Microsoft Office 2013

455

Internet Explorer 9

412

Internet Explorer 10

147

Internet Explorer 11

92

Adobe Flash Player 18.0.0.160

78

Adobe Flash Player 18.0.0.194

38

Adobe Flash Player 18.0.0.261

38

Adobe Flash Player 17.0.0.188

37

Adobe Flash Player 20.0.0.228

37

Adobe Flash Player 18.0.0.209

37

Adobe Flash Player 17.0.0.169

37

Adobe Flash Player 17.0.0.191

37

Adobe Flash Player 18.0.0.241

36

34 filters

Threats

DATE

MAY 30 2017

JUL 14 2017

EXPLOITS

CONNECTIONS

PROCESSES

ADDRESS

LAST (UTC)

PORT

CONNECTIONS

0.0.0.0

Jun 29, 2017 at 12:00am

80

312

121.40.176.63

Jun 7, 2017 at 12:00am

80

107

211.110.1.86

Jun 13, 2017 at 12:00am

80

101

78.47.1.194

Jun 7, 2017 at 12:00am

80

59

69.50.130.106

Jun 17, 2017 at 12:00am

80

56

184.168.171.163

Jun 9, 2017 at 12:00am

80

52

194.58.40.252

Not Applicable

80

49

192.185.41.211

May 30, 2017 at 12:00am

80

38

78.47.1.221

Jun 7, 2017 at 12:00am

80

37

45.32.136.84

Not Applicable

80

36

116.251.205.28

Not Applicable

80

32

182.92.166.254

Jun 7, 2017 at 12:00am

80

30

116.126.142.209

May 31, 2017 at 12:00am

80

26

192.185.32.157

May 30, 2017 at 12:00am

80

26

168.235.251.214

Not Applicable

80

24

34.197.200.120

Jun 5, 2017 at 12:00am

80

24

108.167.183.232

Jun 5, 2017 at 12:00am

80

22

69.64.37.219

May 30, 2017 at 12:00am

80

22

68.65.122.198

Jun 7, 2017 at 12:00am

80

21

75 connections

Processes

Processes displays the list of files found

CROWS  
3.0.0.3064-dev

\*cowtest123@gmail.com

THREATS

APPLICATION

Q

ALL

DRIVE-BY

FILE

APPLICATION

EXPLOITS

Microsoft Office 2016

617

Microsoft Office 2013

455

Internet Explorer 9

251

Internet Explorer 10

140

Internet Explorer 11

72

Adobe Flash Player 18.0.0.160

63

Adobe Flash Player 20.0.0.228

27

Adobe Flash Player 18.0.0.194

27

Adobe Flash Player 17.0.0.191

27

Adobe Flash Player 18.0.0.261

27

Adobe Flash Player 17.0.0.188

26

Adobe Flash Player 18.0.0.209

26

Adobe Flash Player 17.0.0.169

26

Adobe Flash Player 17.0.0.190

26

34 filters

Threats

DATE

JUN 06 2017

JUL 06 2017

EXPLOITS

CONNECTIONS

PROCESSES

FILE

DISCOVERED (UTC)

MD5

SHA1

MAUFOCUS

RELATED

cmd.exe

Jul 5, 2017 at 1:32pm

AD789C14083852BC532FBA5948342B98

EE8CBF12D87C4D388F0984F69BED2E91682920...

no

198

cmd.exe

Jun 20, 2017 at 3:03pm

D752C96401E2540A443C599154FC6FA9

00667A0F0CDD5E9DA697E9FF54CEDDD449259...

no

613

powershell.exe

Jun 20, 2017 at 3:03pm

6D7B0EC562C19E46803C2EC69F7BC85D

A9D3B2DED5EC2DA6C8F48F795437469961D3A...

no

605

WINWORD.EXE

Jun 20, 2017 at 3:03pm

306353AF8A61D271859690CC0D67DF015

A3ED879087B11F8351C7FAC2053D9F696321582...

no

607

powershell.exe

Jun 29, 2017 at 8:41am

92F44E405D816AC55D97E3BFE38132FA

04C5D2B4DA9A0F3FABA45702D4256CEE42D8C...

no

459

WINWORD.EXE

Jun 23, 2017 at 11:32pm

AF3519EE7B156EEE1159E4E040E68558

B41D046FDAFC209C8B6E22F81921652757C85F8...

no

454

ieplone.exe

Jul 5, 2017 at 12:16pm

7116680C7C62709EE818DDC69EF26B93

DAB44ACF3103CD0E4C0F8071E83CFE9B45EBCB...

no

88

cmd.exe

Jun 20, 2017 at 3:03pm

0FEC5F30E705EADAEAE59144F2FB12DC

A4D7B99EB7169198B47448E135D489A1100BA70...

no

119

wscript.exe

Jul 5, 2017 at 1:32pm

D1AB72D82BEDD2F25D33DA3DA0D4B16

860265276829B42B8C4B077E5C651DEF9C81B6...

no

92

cmd.exe

Jul 5, 2017 at 1:35pm

3E30EF769BC47B9B16515E866EFF1E2F

86549432678D5F300219F192CC0B8A4082977...

no

27

test.exe

Jul 5, 2017 at 1:35pm

01E8D50726D2FA186E039490F93BC5A6

FB1C26307AD30EF2023E2115AD8F7DE3DC265...

yes

58

cacript.exe

Jun 29, 2017 at 8:41am

F36B7461FECDFC763FDEFA3A3352CD45

D1B9BA6FD3AA56896F5375136798FE9DFC927F...

no

24

100488293.exe

Jul 5, 2017 at 7:22am

96E90CE7290790E88F8906EFC3F2ECAF

220DA3806D8A7238E30C839C08D19FA43C57...

yes

45

net1.exe

Jul 4, 2017 at 3:15pm

2041012726EF7C95ED51C15C56545A7F

387577CDB38B9FCE983DC42CFF456A332870...

no

24

net.exe

Jul 4, 2017 at 3:15pm

B9A4DAC2192FD78CDA097BF679F6E7B2

9A544E2094273741AA2D3FEA0AF303AF2B587...

no

24

ieplone.exe

Jul 5, 2017 at 1:32pm

CAF61908B1684761D8356389F059B53

C60762352B265D08C5A9FDA0C9315AF91EE081...

no

23

run32.exe

Jul 5, 2017 at 12:17pm

511388EEA3E2C21EC4AD0932C71762A8

8939CF35447822D02C6E6F443446ACC118F986...

no

44

cmd.exe

Jul 5, 2017 at 1:35pm

5996C79F852BDE3FA110F7396654AE42

AC4D87E771010698DC8211F289ABCF7D670...

no

27

opache2.exe

Jul 5, 2017 at 1:32pm

1F95D260FF05B7F6D3610C97E78F6F0

8745154453B7FC6AE60FE32ABC72CB17CE2A...

yes

38

204 processes



## 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.

Threat Details for NSS-2017-35XDXT

NSS-2017-35XDXT





Located in  
China

Coordinates:  
39.928900° N, 116.388300° E

Organization  
Hangzhou Alibaba Advertising C...

ASN  
37963

ASO  
Hangzhou Alibaba Advertising C...

ISP  
Hangzhou Alibaba Advertising C...

OVERVIEWPROCESSESSHELLCODECHAIN OF EVENTS

DISCOVERED  
Jun 6, 2017 at 12:19am

IP ADDRESS  
182.92.166.254

URL  
hxxp://beisimu.com/index.php

SCOPE  
4  
SPAWNED PROCESSES  
9  
RELATED THREATS

TARGET PLATFORM  
Windows 7 SP1  
WINDOWS

262 days  
AT RISK

TARGET BROWSER  
Internet Explorer 9  
INTERNET EXPLORER

262 days  
AT RISK

Processes

Processes displays the process files found in the threat.

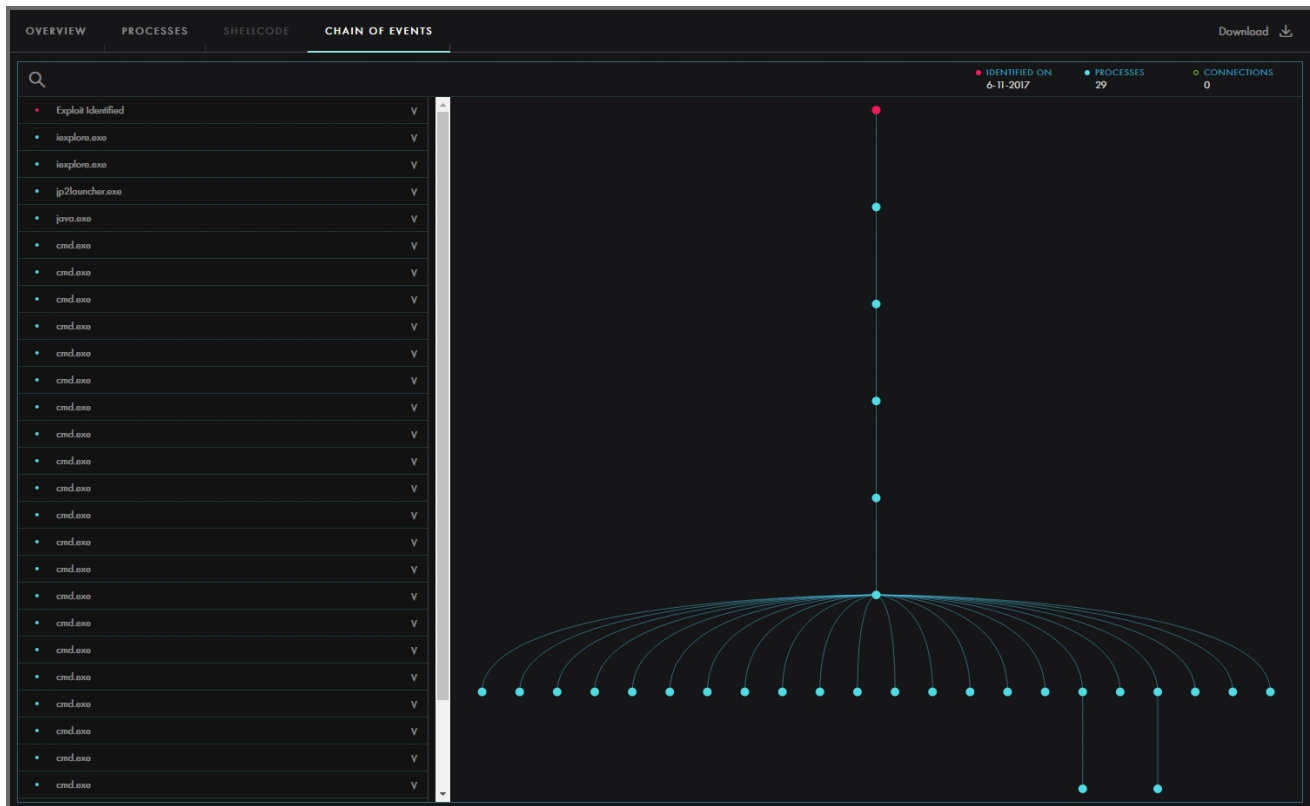
OVERVIEWPROCESSESSHELLCODECHAIN OF EVENTS				
FILE		MD5		SHA1
iexplore.exe		7116680C2C62709EE81BDDC69EF26B93		DAB44ACF3103CD0E4C0F8071E83CFE9B45E...
iexplore.exe		7116680C2C62709EE81BDDC69EF26B93		DAB44ACF3103CD0E4C0F8071E83CFE9B45E...
cmd.exe		AD7B9C14083B52BC532FBA5948342B98		EE8CBF12D87C4D388F09B4F69BED2E916829..

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).

The screenshot shows a web interface for submitting a URL for analysis. It is divided into four main sections: 'File or URL', 'Platforms', 'Browsers', and 'Submit URL'.

- File or URL:** Contains instructions to enter a URL or drag a file. It lists supported file extensions (.doc, .docx, .xls, .xlsx, .csv, .ppt, .pptx, .pdf, .mp3, .mp4, .m4a, .wav, .avi, .mov) and states that files must have a name with no more than 100 characters and a maximum size of 10MB. Below this is a text input field labeled 'URL' with 'google.com' entered and a small 'X' icon to clear the field.
- Platforms:** Has the instruction 'Select the Platforms you would like us to test your URL against.' It includes 'SELECT ALL' and 'CLEAR ALL' buttons. Two options are listed: 'Windows 7' (selected with a checked checkbox) and 'Windows 10' (unchecked).
- Browsers:** Has the instruction 'Select the browsers you would like us to test your URL against.' It also includes 'SELECT ALL' and 'CLEAR ALL' buttons. Five options are listed: 'Firefox 50.0.1' (checked), 'Firefox 50.0.2' (unchecked), 'Google Chrome 53.0.2785.101' (checked), 'Google Chrome 54.0.2840.59' (unchecked), and 'Internet Explorer' (unchecked).
- Submit URL:** Features a large blue 'SUBMIT' button.

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.

**File or URL**

Enter a URL into the field below to analyze a URL.

Drag a file in the blue dashed box or click it to submit a file for analysis.

Supported file extensions: .doc, .docx, .xls, .xlsx, .csv, .ppt, .pptx, .pdf, .mp3, .mp4, .m4a, .wav, .avi, .mov.

Files must have a name with no more than 100 characters and have a maximum size of 10MB.

**Platforms**

Select the Platforms you would like us to test your URL against.

☒ Windows 7

☐ Windows 10

**Applications**

Select the applications you would like us to test your URL against.

☐ Adobe Reader DC 2015.007.20033

☒ Adobe Reader 9.4

☐ Adobe Reader DC 2015.020.20039

**Submit File**

**FILENAME** X

CAWS User Guide.pdf

5. Click **Submit**.

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

SUBMISSIONS		Previous Submission Results				
		SUBMITTED (UTC)	RESPONSE (UTC)	RESULT	USER	BROWSER
		Jul 5, 2017 at 8:05pm	Jul 5, 2017 at 8:09pm	NSS-2017-3FM35G	cawtest123@gmail.com	Internet Explorer 9
		Jul 5, 2017 at 8:05pm	Jul 6, 2017 at 1:04pm	Clean	cawtest123@gmail.com	Internet Explorer 11

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
<a href="#">NSS-2017-3FM35G</a>	<a href="http://www.aac63.pw">http://www.aac63.pw</a>	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	<a href="http://www.aac63.pw">http://www.aac63.pw</a>	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**.

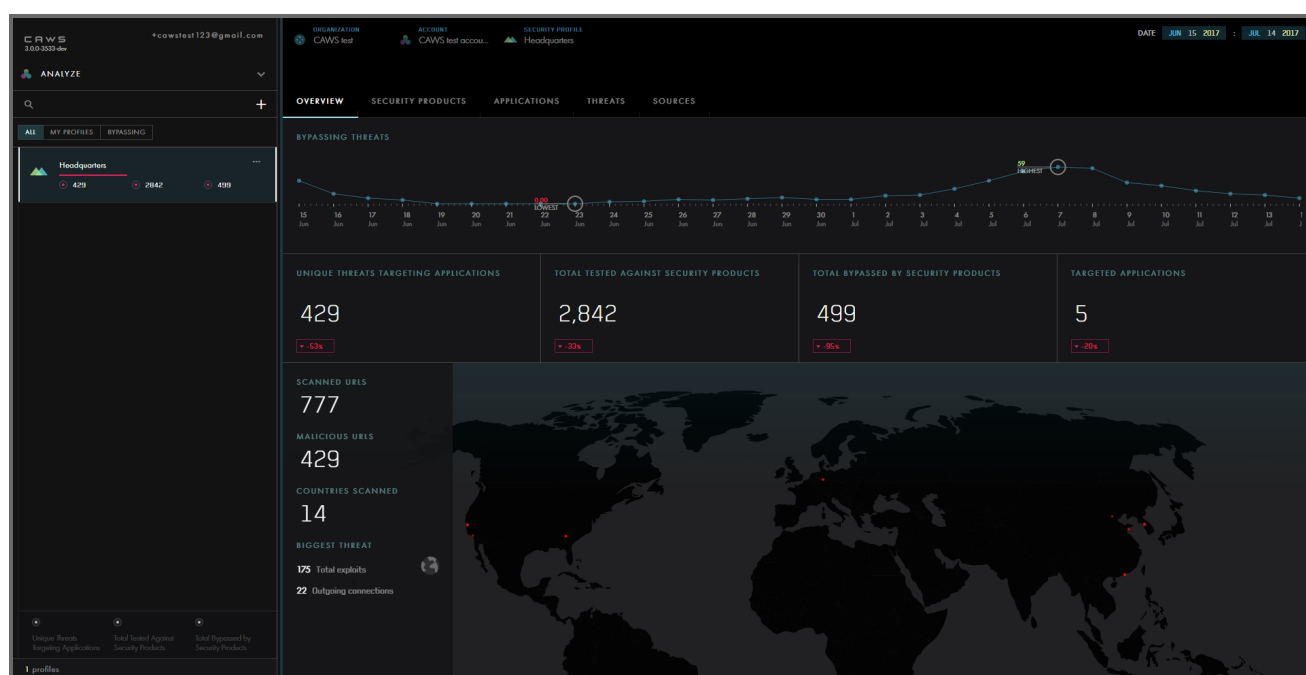


- To perform a global search, from any page type **Ctrl + F** and the global search opens.

## 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 bypassed 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.

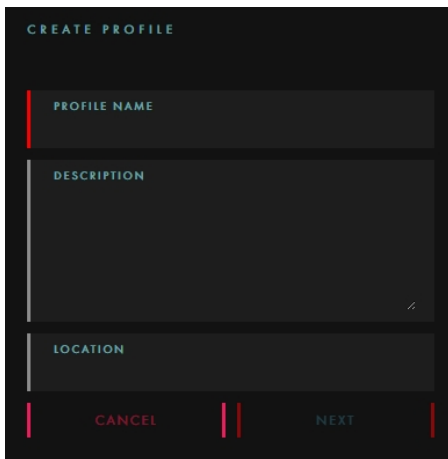
## Security Profiles

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

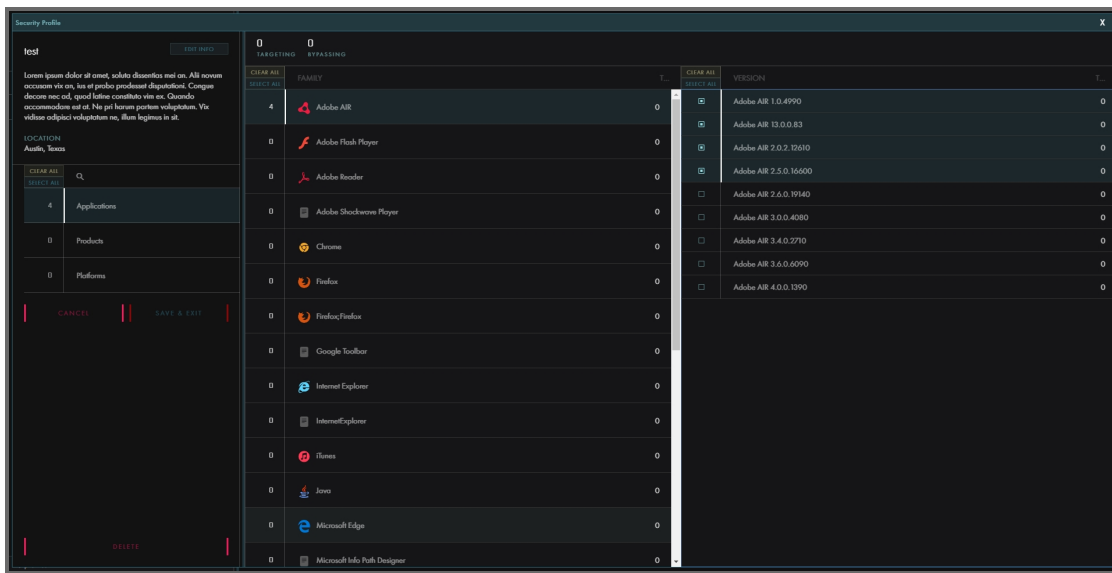
**To create a security profile:**

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

A dark-themed form titled 'CREATE PROFILE' in teal. It contains three input fields: 'PROFILE NAME' (a single-line text box), 'DESCRIPTION' (a multi-line text area with a small icon in the bottom right), and 'LOCATION' (a single-line text box). At the bottom, there are two buttons: 'CANCEL' in red and 'NEXT' in teal, separated by two vertical red bars.

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

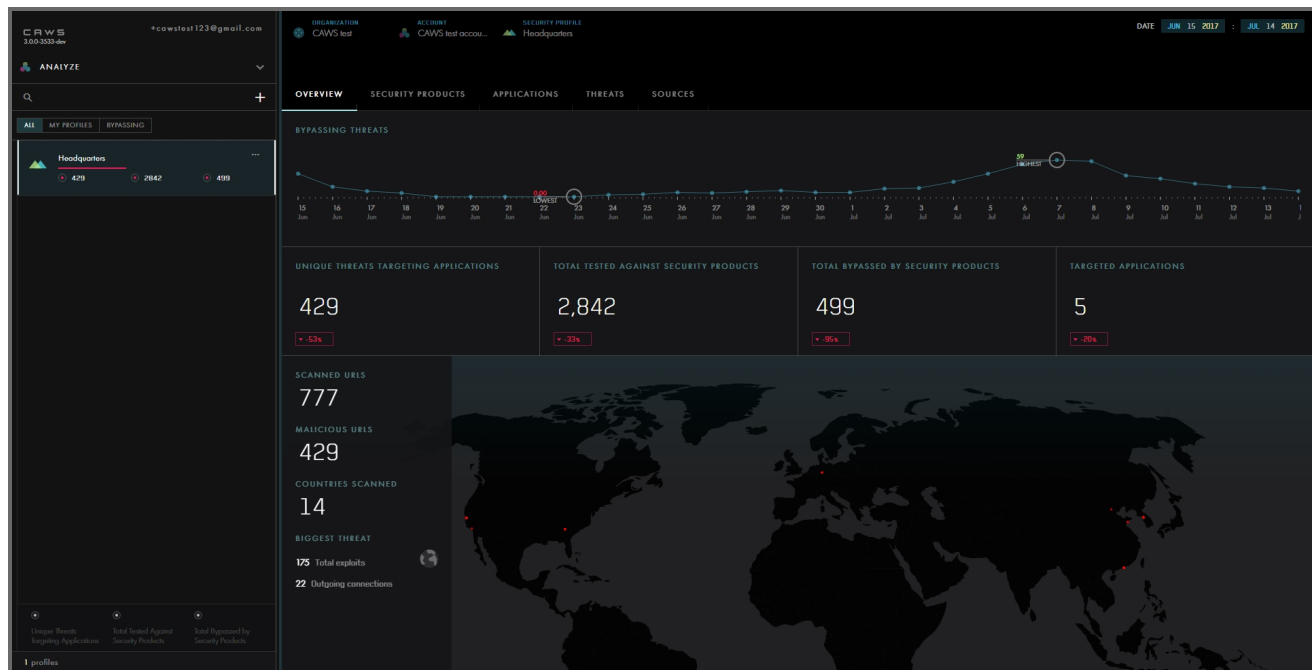




7. Select the **Applications** associated with the security profile by selecting **Application** in the left panel, selecting an item in the Application family column and then selecting the appropriate versions.
8. Select the **Products** associated with the security profile by selecting **Products** 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

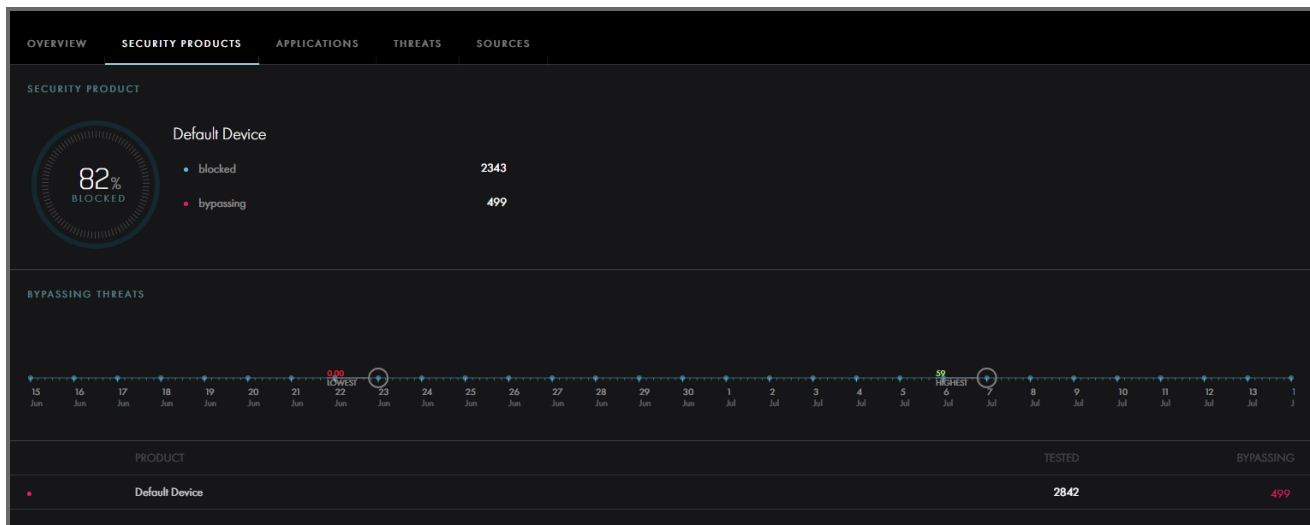
Displays the number of exploits that have bypassed all security products associated with the selected profile.

## Targeted Applications

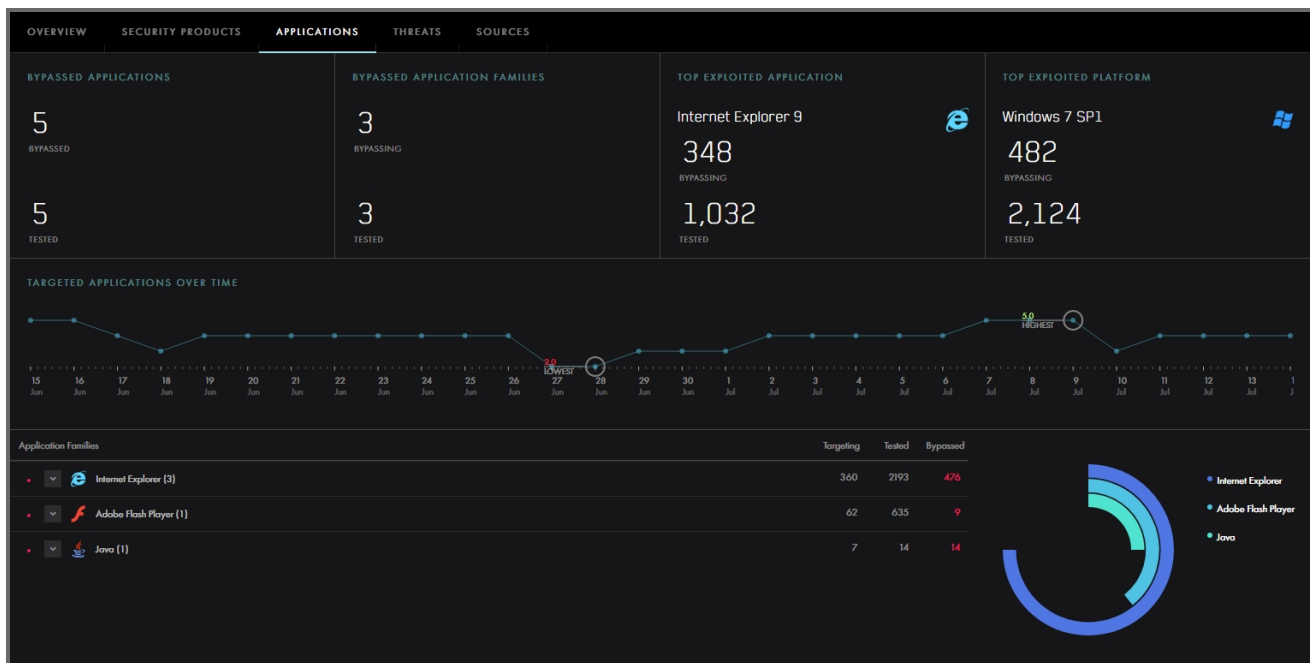
Summarizes attacks on the top applications the specified time period. Mouse over to view the total number of attacks for that application.

## 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.

The screenshot displays the NSS Labs website. The top navigation bar includes the NSS Labs logo, a search icon, and links for RESEARCH LIBRARY, CAWS LOGIN, CAWS DEMO, and a shopping cart. Below this, a secondary menu lists SECURITY TEST, CAWS THREAT PROTECTION PLATFORM, RESEARCH & ADVISORY, COMPANY, and RESOURCES. The main content area features the title "CAWS Cyber Threat Protection Platform" and a "Support Information" section. Under "Documents", there are links for User Guide, API Guide, and Release Notes. Under "Contact Information", the email support@nsslabs.com is provided. A large, stylized graphic of a hexagonal shield with circuitry is centered on the page. On the right side, a vertical sidebar contains icons for CONTACT, LIBRARY, SHOP, and DEMO. At the bottom, a footer contains detailed navigation links for SECURITY TEST, CAWS THREAT PROTECTION PLATFORM, RESEARCH & ADVISORY, COMPANY, and RESOURCES, along with the NSS Labs logo and address: 206 Wild Basin Road, Building A, Suite 200, Austin, TX 78746. A chat bubble from "NSS Labs" is visible in the bottom right corner, saying "Thanks for visiting NSS Labs, how may we help you?".

**NSS LABS**

RESEARCH LIBRARY CAWS LOGIN CAWS DEMO

SECURITY TEST CAWS THREAT PROTECTION PLATFORM RESEARCH & ADVISORY COMPANY RESOURCES

### CAWS Cyber Threat Protection Platform

#### Support Information

**Documents**

- User Guide
- API Guide
- Release Notes

**Contact Information**

Email: [support@nsslabs.com](mailto:support@nsslabs.com)

**CONTACT**

**LIBRARY**

**SHOP**

**DEMO**

**NSS LABS**

206 Wild Basin Road  
Building A, Suite 200  
Austin, TX 78746

**SECURITY TEST**

- Overview
- Endpoint Security
- Network Security
- Breach Security

**CAWS THREAT PROTECTION PLATFORM**

- Overview
- Threat Discovery & Analysis
- Threat Intelligence Enrichment

**RESEARCH & ADVISORY**

- Overview
- Research Library
- Pricing & Packaging

**COMPANY**

- About
- Team
- News & Events
- [Careers](#)

**RESOURCES**

- Resource Center
- Blog
- Research Library

**NSS LABS**

206 Wild Basin Road  
Building A, Suite 200  
Austin, TX 78746

NSS Labs  
Thanks for visiting NSS Labs, how may we help you?

Write a reply...