Detection of CVE-2022-30190 (Follina) using Stamus Security Platform

Microsoft published a Common Vulnerabilities and Exposure (CVE) CVE-2022-30190 alert identifying a vulnerability in the Microsoft Support Diagnostic Tool (MSDT) that allows the user to run any arbitrary code EVEN if macro scripts are disabled in any Microsoft tool supporting MSDT (like Word for example) when opening a file containing the attack. This zero day is known to have been used by some attackers.

As of publication time, there is no patch available from Microsoft. We recommend you apply workarounds described in the Microsoft bulletin as soon as possible. https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

In the meantime, you may take the following steps to help determine if any of your systems have been attacked in the past, are currently under attack or vulnerable.

DETECTION AND ESCALATION

Please follow the steps listed below in the Stamus Security Platform at the Stamus ND/NDR license tiers (formerly Scirius Security Platform), “Hunt” interface.

Create a Filter

NOTE: Portions of this are not applicable to the Stamus Probe Management license tier

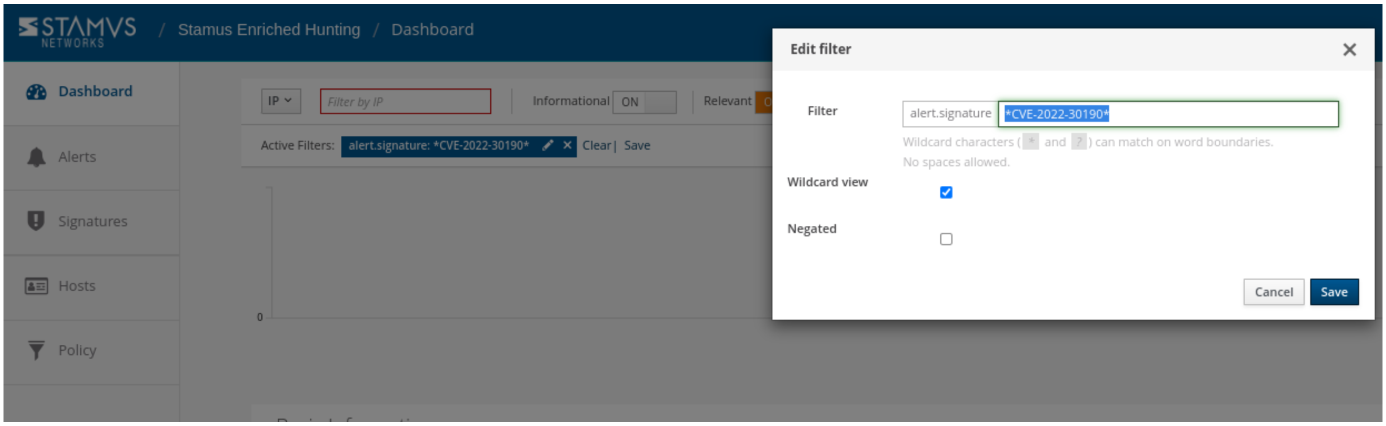
Any CVE number can be searched in the Hunt interface.

To create a filter:

1. In Hunt, click on the magnifying icon next to any signature (first group Signatures on the Dashboard tab).

2. Click on the pencil/Edit icon on the resulting filter displayed as "Active Filters:".
3. Type the CVE number or a text descriptor with a wildcard (*) it at each end (for example: *CVE-2022-30190* or *Follina*)
4. Select the checkbox "Wildcard view"
5. Click Save
6. You are now ready to review the results and events in the Dashboard, Host Insights and Alert views

The example screenshot below shows how to do that for "CVE-2022-30190"



Active Filters: alert.signature: *CVE-2022-30190*

Edit filter

Filter: alert.signature *CVE-2022-30190*

Wildcard characters (* and ?) can match on word boundaries. No spaces allowed.

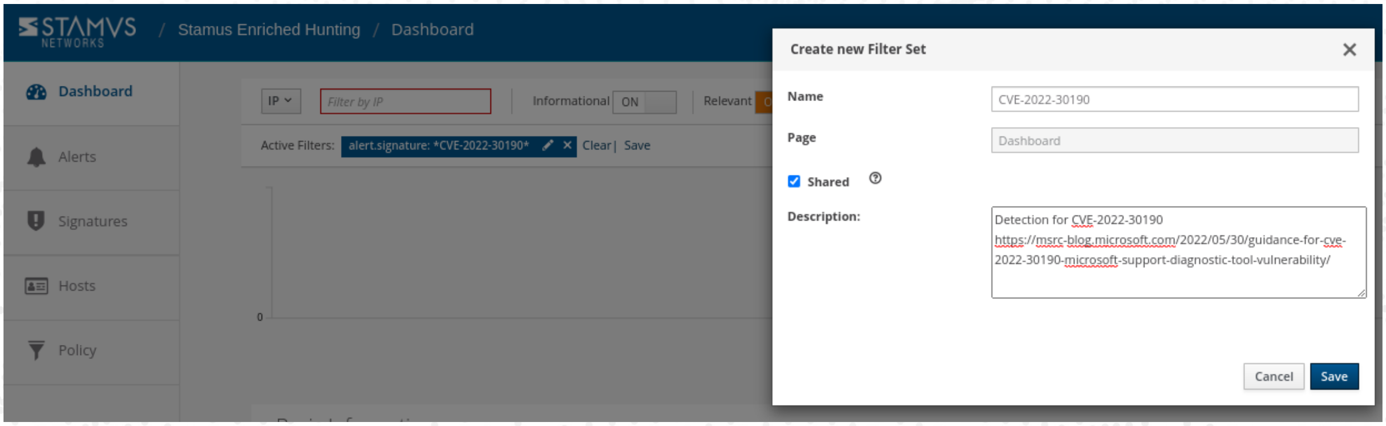
Wildcard view ☑

Negated □

Save the Filter

NOTE: some items described here are not applicable to Stamus Probe Management license tier

The resulting filter can be saved by simply clicking on the "Save" link on the right-hand side of the "Active filter". Check "Shared" in the resulting dialog box if you want to make the filter available to all users.



Active Filters: alert.signature: *CVE-2022-30190*

Create new Filter Set

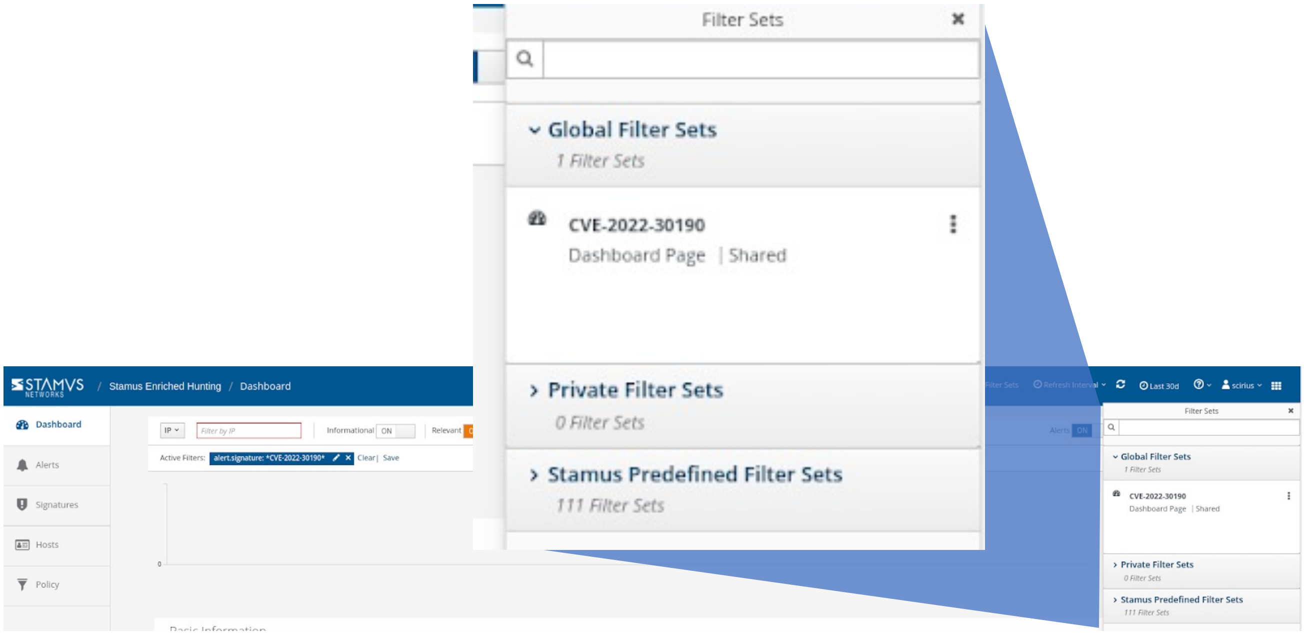
Name: CVE-2022-30190

Page: Dashboard

☑ Shared

Description: Detection for CVE-2022-30190
https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

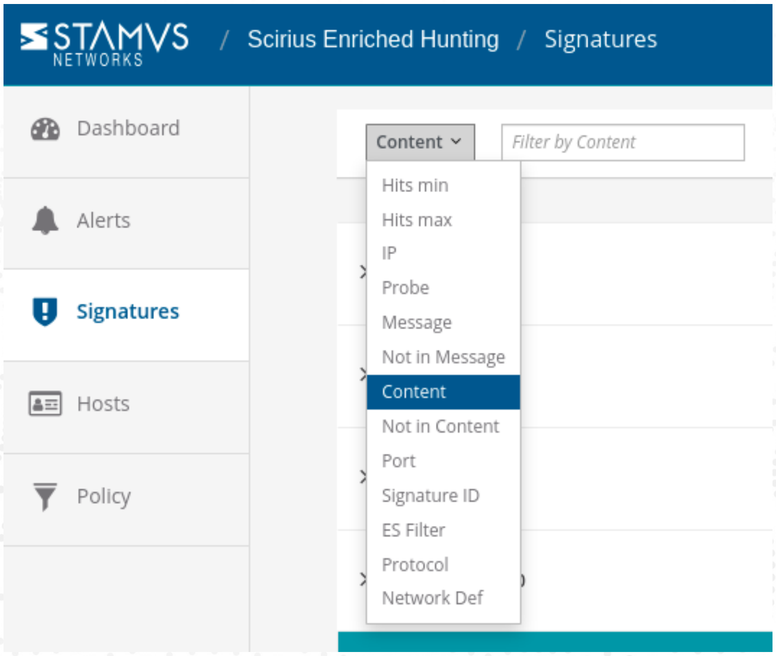
The newly created filter is now available in “Global Filter Sets” or “Private Filter Sets”

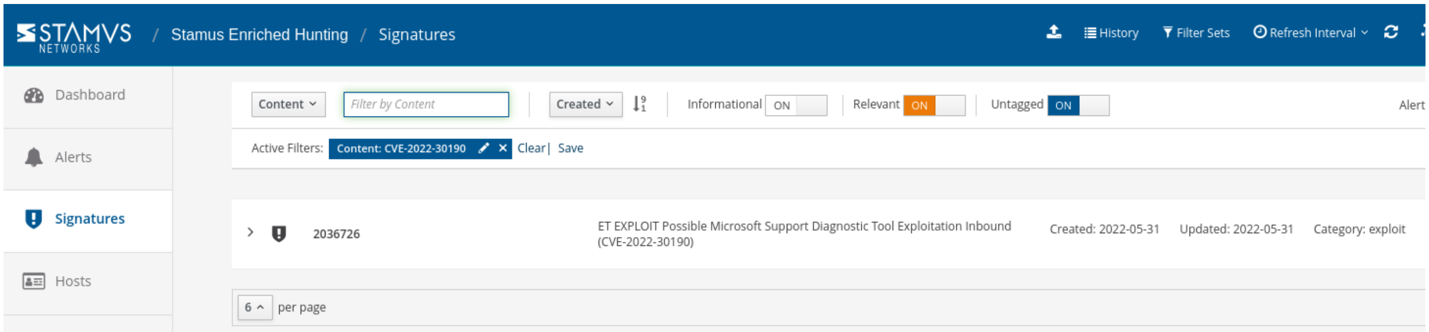


Review Detection Methods in Hunt

To review exactly what detection methods are available in Hunt for that specific vulnerability you can:

1. Head to the Signatures tab on the left-hand side in Hunt.
2. Select the “Content” option from the dropdown menu.
3. Type in the full CVE (i.e. CVE-2022-30190), hit Enter





Active Filters: Content: CVE-2022-30190

2036726 ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) Created: 2022-05-31 Updated: 2022-05-31 Category: exploit

6 per page

Automated Escalation and RestAPI Notification

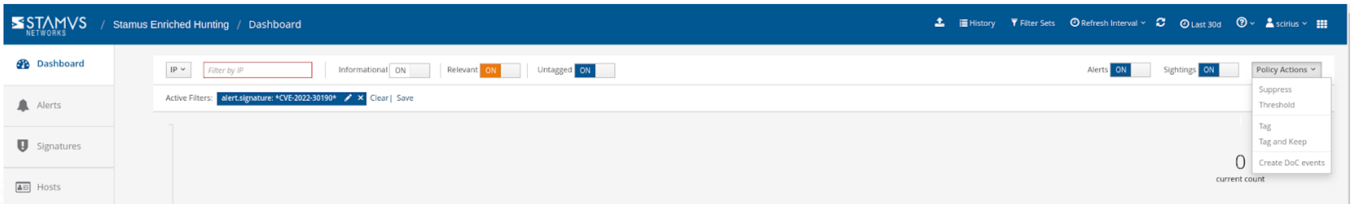
NOTE: Portions are not applicable to Stamus ND or Stamus Probe Management license tiers.

If needed, an automated escalation to a Declaration of Compromise™ (DoC) and webhooks is also possible, including from historical data.

For example, if it happened 24hrs or 7 days ago, it will still be detected and escalated based on that custom filter.

To do so:

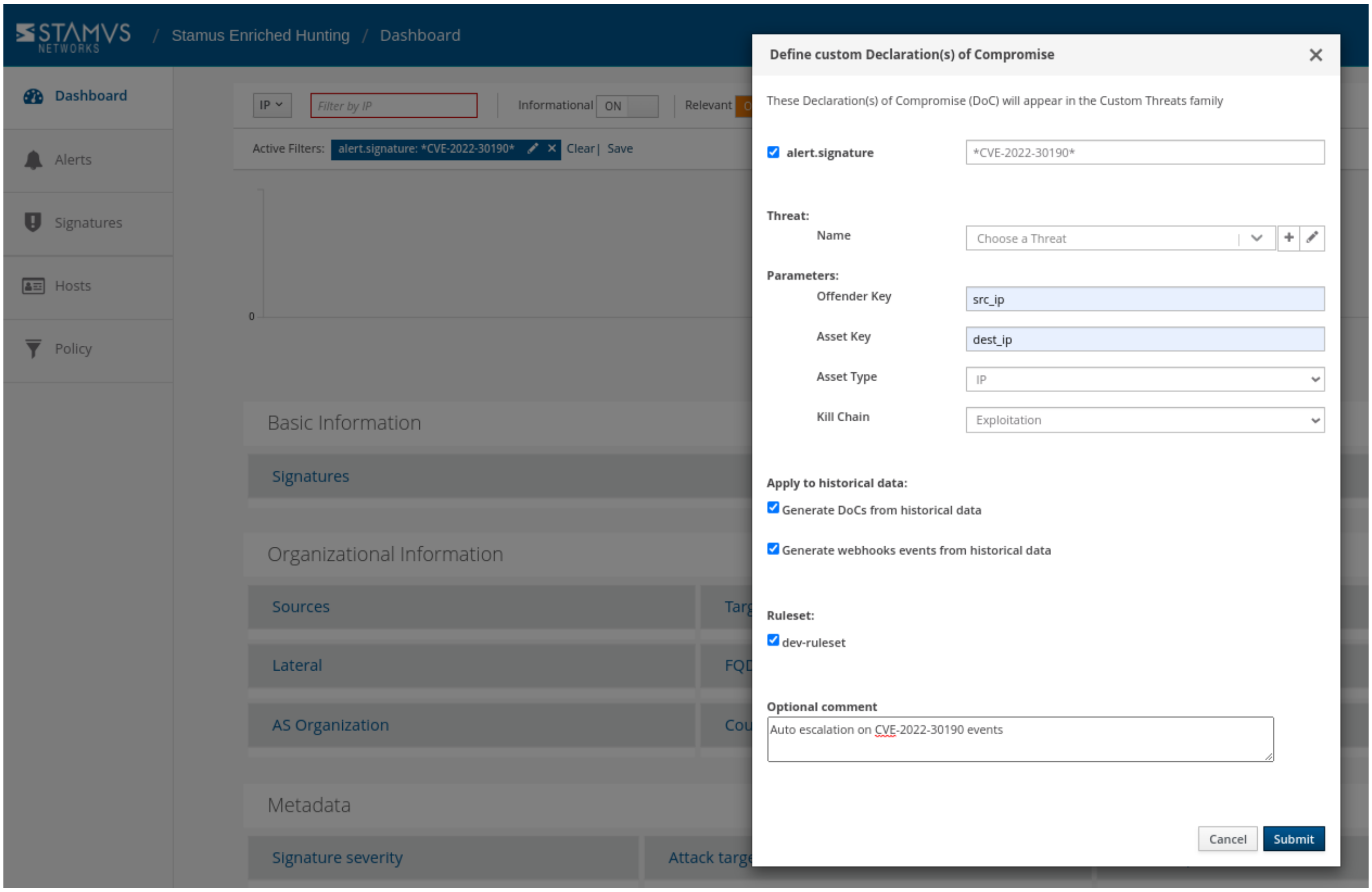
1. After creating your filter as above
2. From the right-hand side drop down menu, *Policy Actions*, select “Create DoC events”.



Active Filters: alert.signature: *CVE-2022-30190*

3. Choose the plus (+) next to the Threat: Name
4. Fill in the Threat Name, Description, and Additional information.
5. Enter an Offender Key (i.e. src_ip)
6. Enter an Asset Key (i.e. dest_ip)
7. Leave Asset Type “IP”
8. Set a Kill Chain phase (i.e. Exploit)
9. Select “Generate DoC events from historical data”. [This will make sure historical events are also checked]
10. If desired and webhooks are setup also select “Generate webhooks events from historical data”

The screenshot below shows the DoC event creation form:



Define custom Declaration(s) of Compromise ×

These Declaration(s) of Compromise (DoC) will appear in the Custom Threats family

☑ alert.signature: *CVE-2022-30190*

Threat:
Name: Choose a Threat

Parameters:
Offender Key: src_ip
Asset Key: dest_ip
Asset Type: IP
Kill Chain: Exploitation

Apply to historical data:
☑ Generate DoCs from historical data
☑ Generate webhooks events from historical data

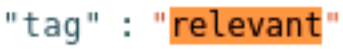
Ruleset:
☑ dev-ruleset

Optional comment
Auto escalation on CVE-2022-30190 events

Cancel | Submit

Automated Classification and Tagging

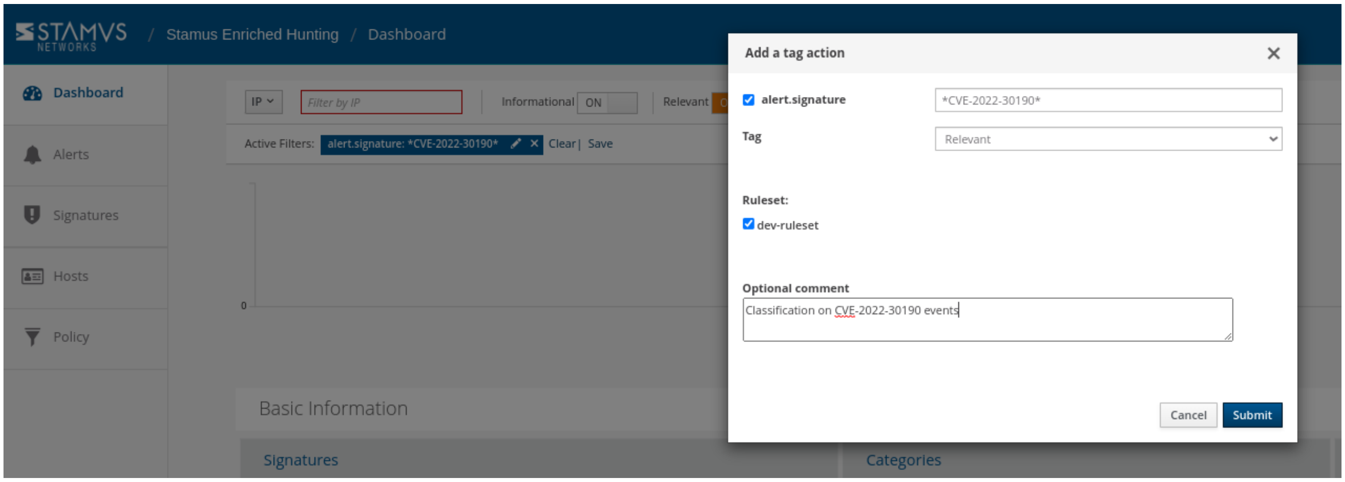
Auto Tagging all relevant events is also an option. This will allow for any logs (alerts or protocol transaction events related to the alerts) to have a “Relevant” tag inserted in the JSON logs:



```
"tag" : "relevant"
```

To do so:

1. After creating your filter as above.
2. From the right-hand side drop down menu - Policy Actions , Select “Tag”.
3. Add in an optional comment and select a ruleset.
4. Update the threat detection (upload button in the middle of the top bar on the Hunt page, on the left-hand side of History, Filter Sets)



Active Filters: alert.signature: *CVE-2022-30190* ✕ Clear | Save

Add a tag action ✕

☑ alert.signature: *CVE-2022-30190*

Tag: Relevant

Ruleset:

☑ dev-ruleset

Optional comment

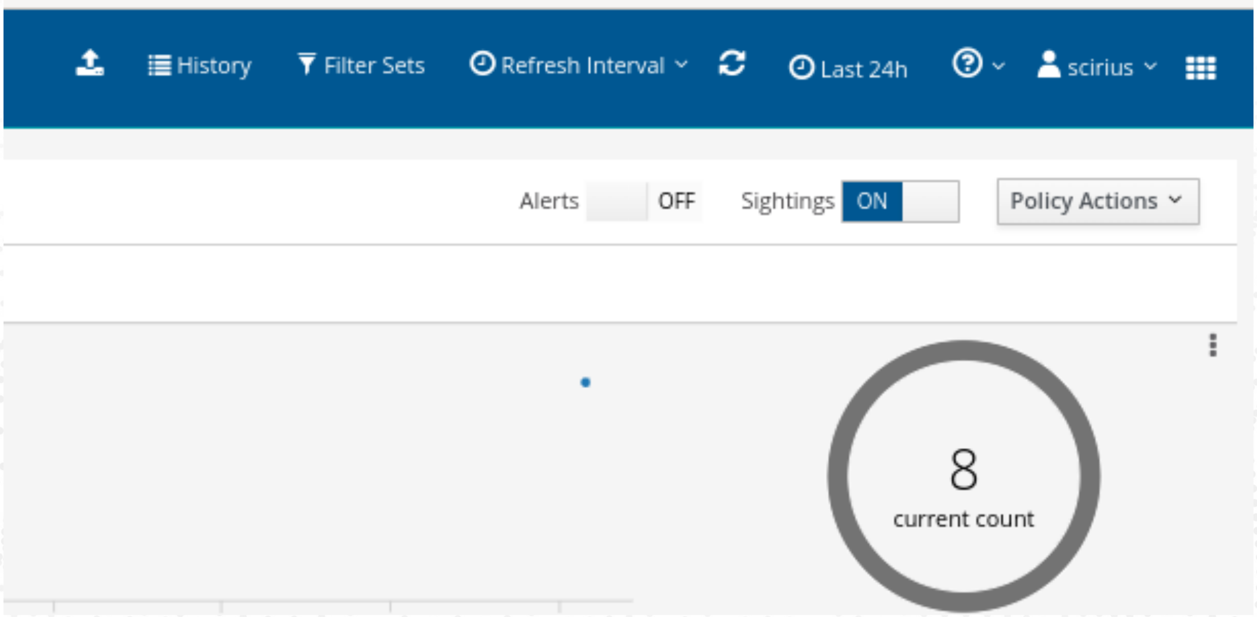
Classification on CVE-2022-30190 events

Using Sightings to Uncover an Attack

“Sightings” is a new feature in U38 that allows for Stamus customers to differentiate and detect new encrypted connections and data transfer never seen before in the enterprise.

Our research team has explored a publicly-available sample of an exploit to this vulnerability. And we have determined that by using the new “Sightings” functionality, Stamus users may quickly filter through the noise to identify new malicious TLS connections to known malicious domains.

Here’s how: In Hunt, disable Alerts view by switching off the Alert tab. This will filter results down to only Sightings. The screen below shows a drop to 8 Sightings after switching off alerts:

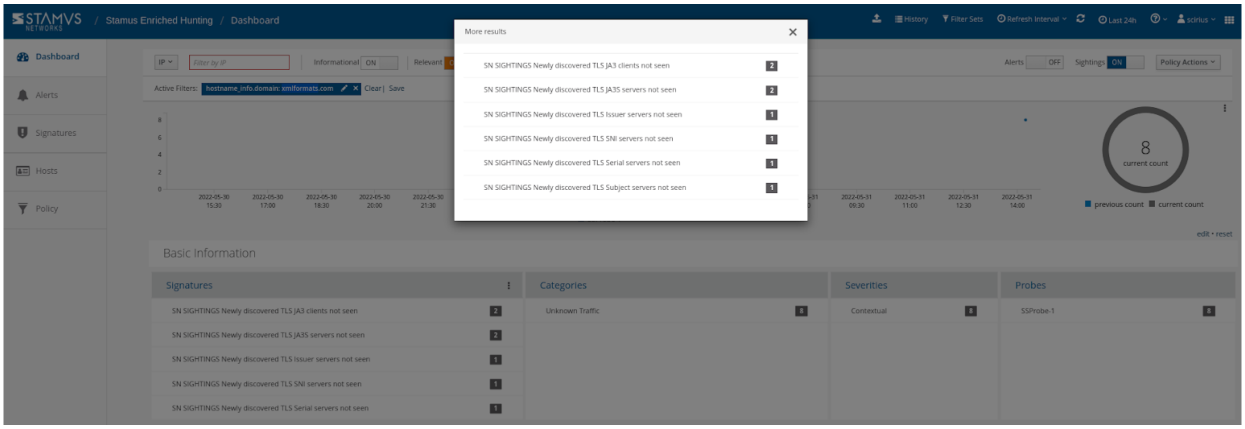


Alerts OFF

Sightings ON

8 current count

If we dive deeper into the Sightings (Clicking the 3 dots on the Signatures card) we can see all the Sightings are for TLS:

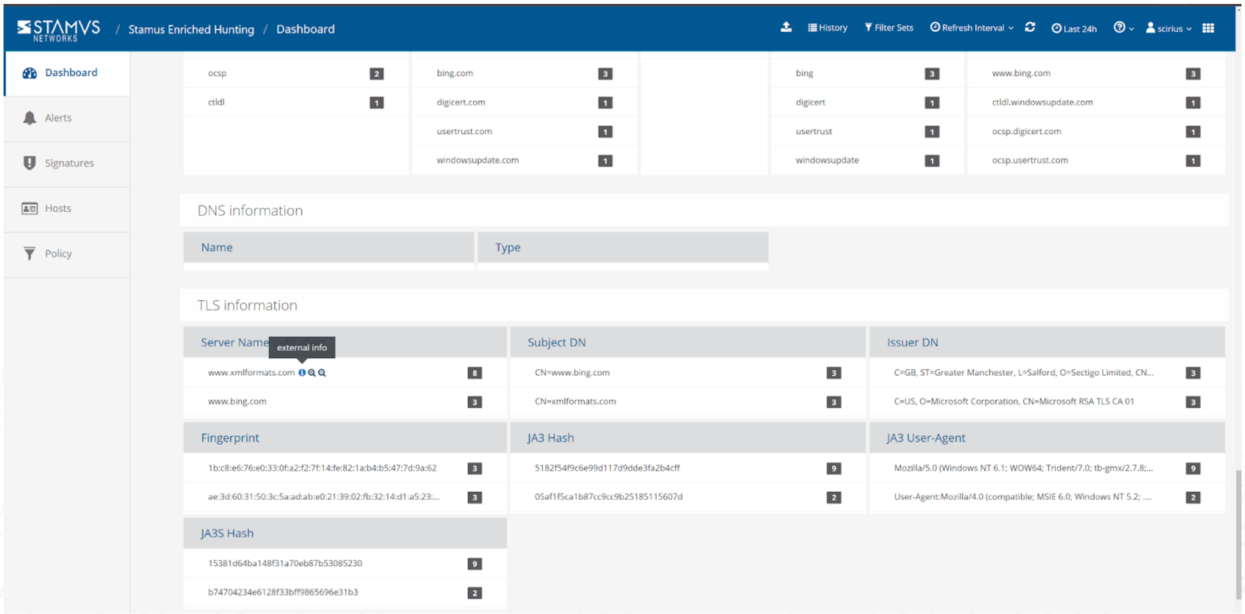


More results

SN SIGHTINGS Newly discovered TLS JA3 clients not seen	2
SN SIGHTINGS Newly discovered TLS JA3S servers not seen	2
SN SIGHTINGS Newly discovered TLS Issuer servers not seen	1
SN SIGHTINGS Newly discovered TLS SNI servers not seen	1
SN SIGHTINGS Newly discovered TLS Serial servers not seen	1
SN SIGHTINGS Newly discovered TLS Subject servers not seen	1

Signatures		Categories		Severities		Probes	
SN SIGHTINGS Newly discovered TLS JA3 clients not seen	2	Unknown Traffic	8	Contextual	8	SSProbe-1	8
SN SIGHTINGS Newly discovered TLS JA3S servers not seen	2						
SN SIGHTINGS Newly discovered TLS Issuer servers not seen	1						
SN SIGHTINGS Newly discovered TLS SNI servers not seen	1						
SN SIGHTINGS Newly discovered TLS Serial servers not seen	1						

Now we can scroll down to the TLS information section and see a list of SNI's. Looking at each one we can hover over them and click the "external info" icon to query VirusTotal for that SNI to see if it is compromised. This will give you a quick way to check unknown SNI's for this threat.



ocsp	2	bing.com	3	bing	3	www.bing.com	3
ctldl	1	digicert.com	1	digicert	1	ctldl.windowsupdate.com	1
		usertrust.com	1	usertrust	1	ocsp.digicert.com	1
		windowsupdate.com	1	windowsupdate	1	ocsp.usertrust.com	1

DNS information

Name	Type

TLS information

Server Name		Subject DN		Issuer DN	
www.xmlformats.com	8	CN=www.bing.com	3	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN...	3
www.bing.com	3	CN=xmlformats.com	3	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 01	3

Fingerprint		JA3 Hash		JA3 User-Agent	
1b:c8:e6:76:e0:33:0f:a2:f2:7f:14:fe:82:1a:b4:b5:47:7d:9a:62	3	5182f54f9c6e99d117d9dde3fa2b4cff	9	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; tb-gmx/2.7.8;...	9
ae:3d:60:31:50:3c:5a:ad:ab:e0:21:39:02:fb:32:14:d1:a5:23:...	3	05af1f5ca1b87cc9cc9b25185115607d	2	User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2;	2

JA3S Hash	
15381d64ba148f31a70eb87b53085230	9
b74704234e6128f33bff9865696e31b3	2

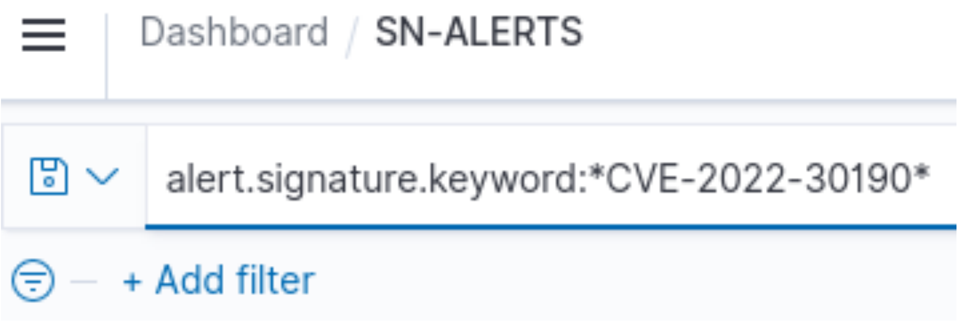
Export Data - SIEM / Elasticsearch / Kibana

All data generated by Stamus Security Platform (with the Stamus ND/NDR license tiers), such as alerts, protocol transactions, sightings events or Host Insights information, may be exported and shared with any SIEM or SOAR system.

Over 4000 fields are available -- from domain requests, http user agents used, hostnames, usernames logged in -- to encrypted analysis including JA3/JA3S fingerprinting, TLS certificates and more.

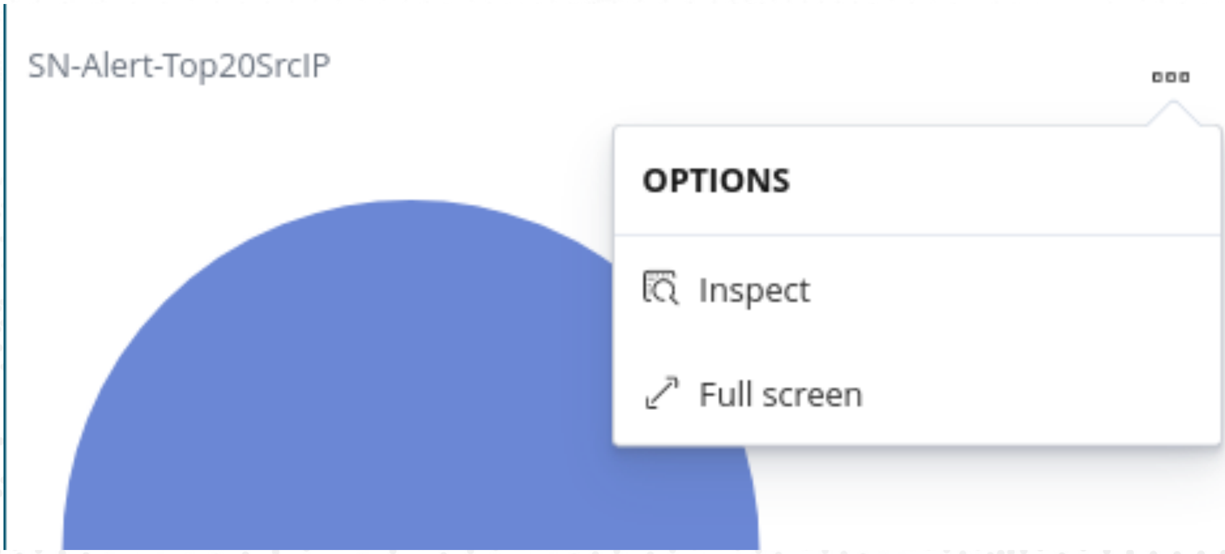
Any query of the Stamus Networks data (protocol transaction or alert logs) can be exported via a regular JSON log query or visualization export.
Example of Kibana query on alert events

To export CSV data from any info of the alerts you can open the SN-ALERT dashboard in Kibana, type in the filter “alert.signature.keyword:*CVE-2022-30190*” , then you can export a CSV of any visualization using “Inspect” (see example below):



alert.signature.keyword:*CVE-2022-30190*

Click on “Inspect” in any visualization to export a CSV



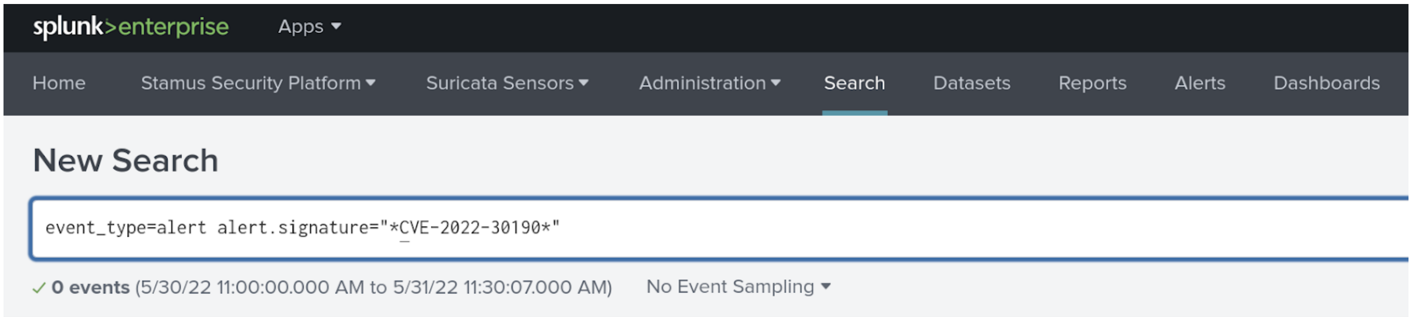
Export Data - Spunk

NOTE: portions of this section are not applicable to Stamus Probe Management.

Any query of the Stamus Networks data (protocol transaction or alert logs a like) in Splunk can be exported via a regular Splunk query or visualization export.

Example of a Splunk query on alert events

Splunk ″event_type=alert "alert.signature"="*CVE-2022-30190*"



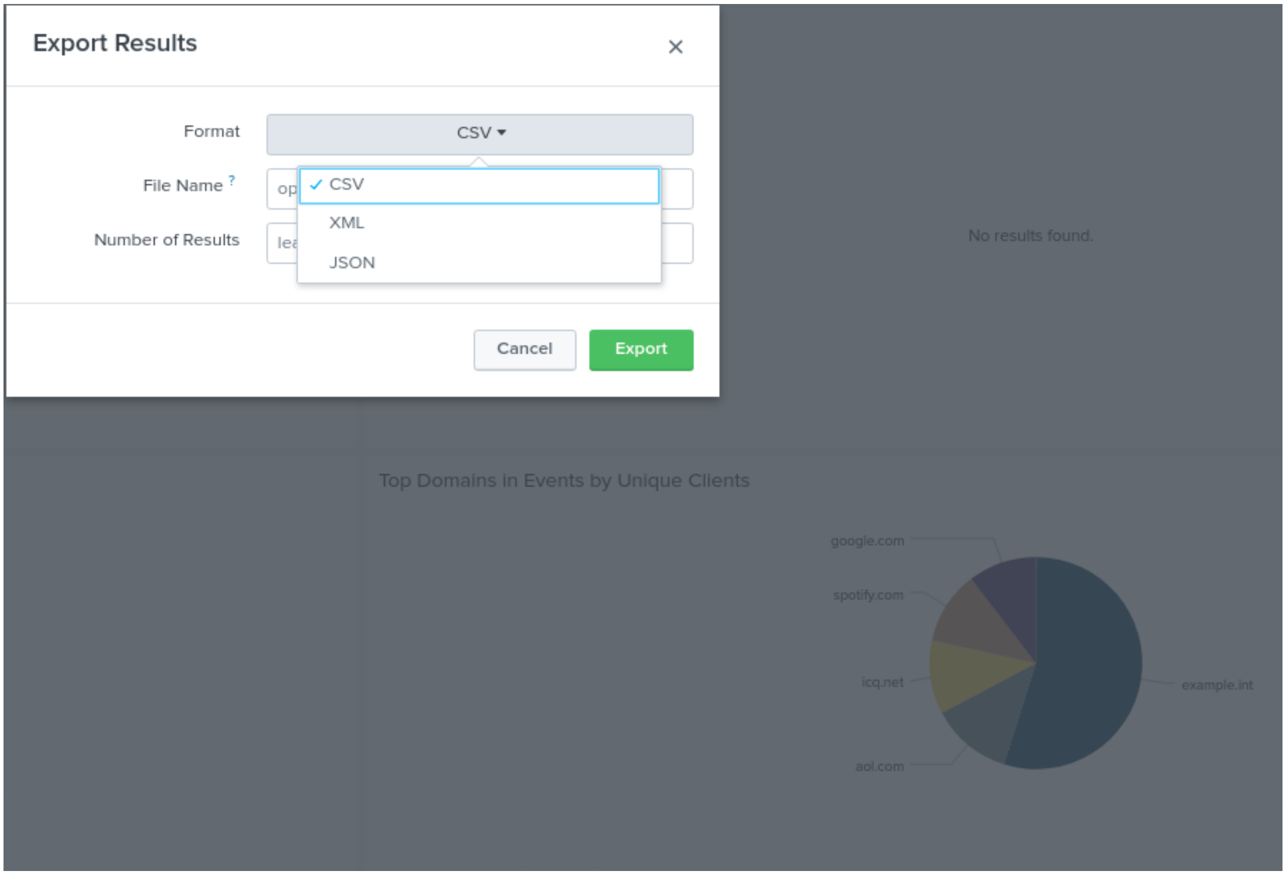
```
event_type=alert alert.signature="*CVE-2022-30190*"
```

✓ **0 events** (5/30/22 11:00:00.000 AM to 5/31/22 11:30:07.000 AM)   No Event Sampling ▾

Protocol transactions

Stamus Networks provides a free Splunk app https://splunkbase.splunk.com/app/5262 that can be used to do specific “CVE-2022-30190” searches.

If there are any Splunk visualizations queries that have supporting information for the CVE that needs to be exported, it can be done so by the native Splunk export functionality.



Export Results

Format: CSV

File Name ?: op

Number of Results: lea

Troubleshooting and Help

Please feel free to reach out to support@stamus-networks.com with any questions or feedback.

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMVS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com