

Detection of CVE-2022-39952 (FortiNAC) using Stamus Security Platform

On February 16, 2023, NIST published a Common Vulnerabilities and Exposure (CVE) alert identifying a vulnerability in the Fortinet FortiNAC zero-trust access control solution that can “allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted HTTP request.” This critical alert - CVE-2022-39952- applies to Fortinet FortiNAC versions 9.4.0, 9.2.0 through 9.2.5, 9.1.0 through 9.1.7, 8.8.0 through 8.8.11, 8.7.0 through 8.7.6, 8.6.0 through 8.6.5, 8.5.0 through 8.5.4, 8.3.7

A proof of concept (PoC) exploit was made available 21 February 2023 by Horizon3 on GitHub.

We recommend you upgrade any vulnerable systems as soon as possible.

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 are vulnerable.

DETECTION AND ESCALATION

Please follow the steps listed below in the Stamus Security Platform “[Hunt](#)” interface.

There are two detection mechanisms with multiple detection methods each that Stamus Security Platform provides in order to highlight possible CVE attempts or usage.

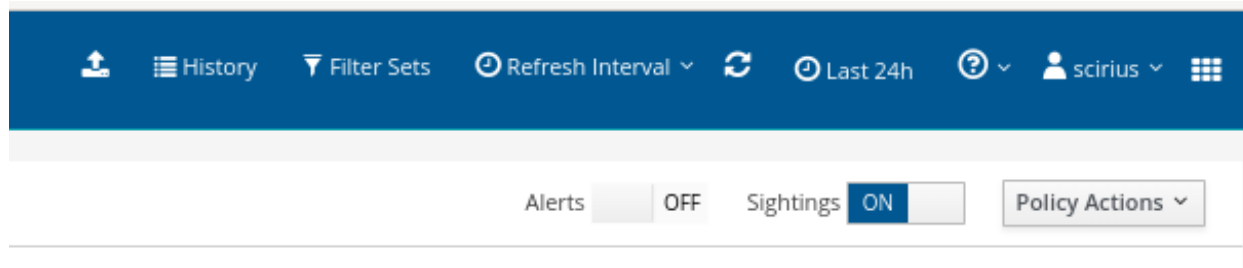
The first mechanism leverages Stamus Sightings and the second mechanism leverages specific CVE signature detection methods.

Mechanism 1: Using Sightings to Uncover an Attack

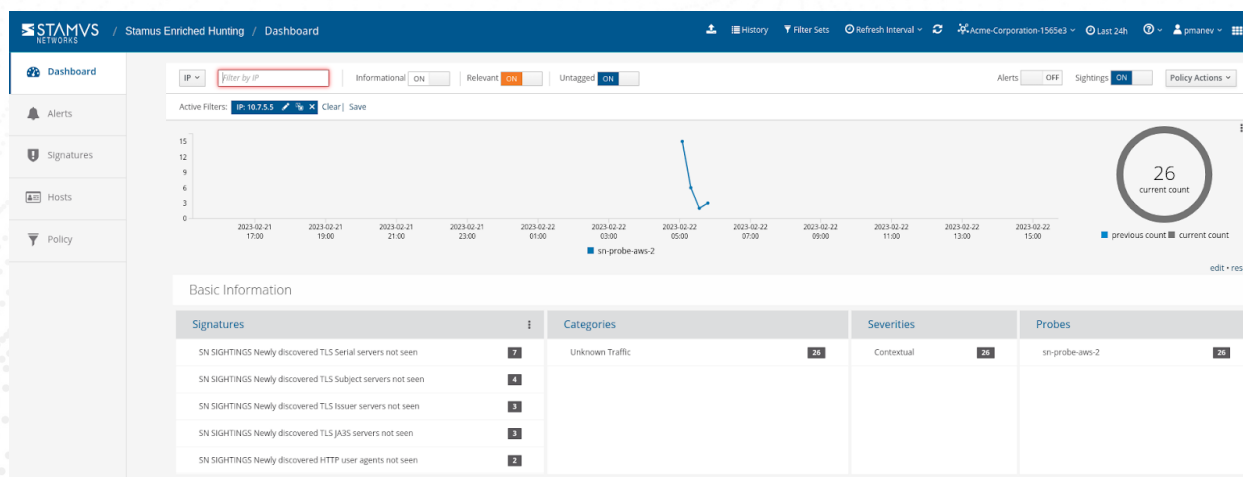
“Sightings” is a new feature in U38 that allows for Stamus customers to differentiate and detect new encrypted connections and data transfer never seen before in the enterprise.

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.



In the drop-down filter menu, select “IP” and type in the management IP of the Fortinet FortiNAC management web server. The screen example below shows a drop to 26 Sightings after switching off alerts:



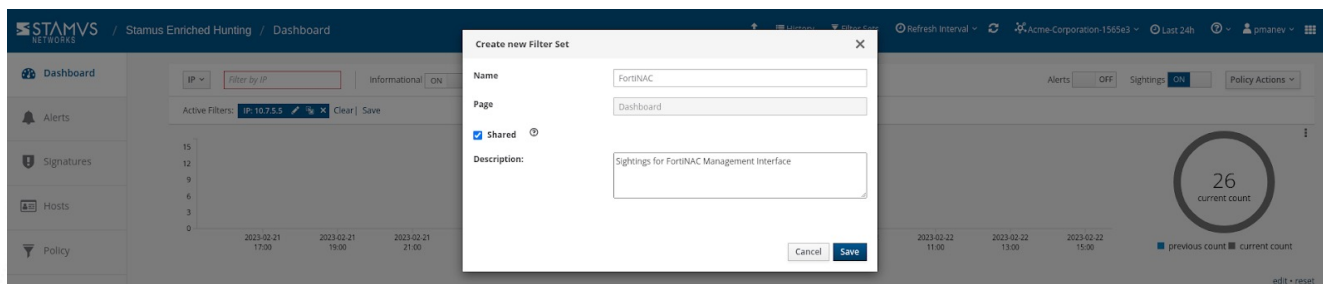
If we dive deeper into the Sightings (Clicking the 3 dots on the Signatures card) we can see all the Sightings are related to TLS, HTTP, or other internal protocols like SMB.

Now we can scroll down to the TLS information section and see a list of the relevant metadata such as SNI's, JA3, JA3S, user agents or HTTPS server editions. Looking at each one we can hover over them and click the "external info" icon to query VirusTotal for example for that specific SNI to see if it is compromised. This will give you a quick way to check for example unknown SNI's for this threat.

Create a Sightings Filter

To create a Sightings-based filter for a specific Fortinet FortiNAC management interface using the previously explained steps:

1. Click Save
2. You are now ready to review the results and events in the Dashboard, HostID and Alert views



How to Escalate and Webhook Notification

Please refer to the section entitled: Automated Escalation and Webhook Notification

Please note that with the escalation based on the created filter above, any and all new and previously unseen communications from that FortiNAC management interface will be highlighted and escalated.

Mechanism 2: Create a Filter for Signature Based Detection

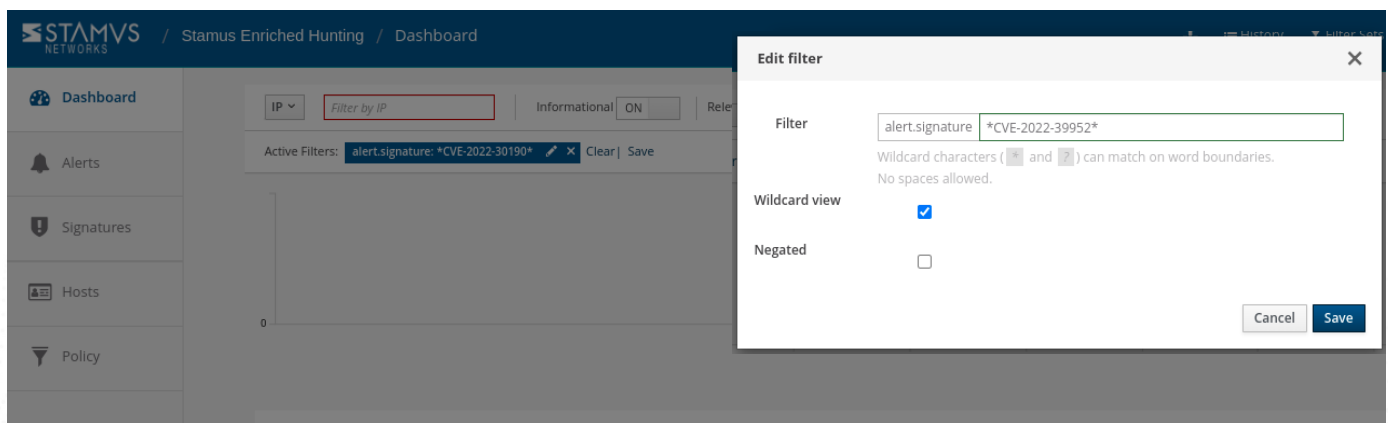
NOTE: Portions of this are not applicable to the Stamus Probe Management license tier

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 (*) at each end (for example: *CVE-2022-39952*)
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

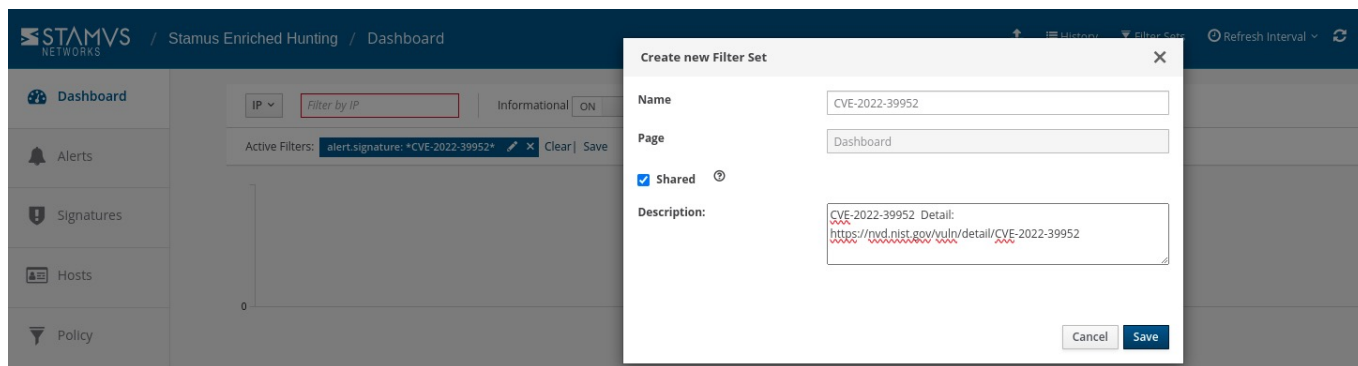
The example screenshot below shows how to do that for "CVE-2022-39952"



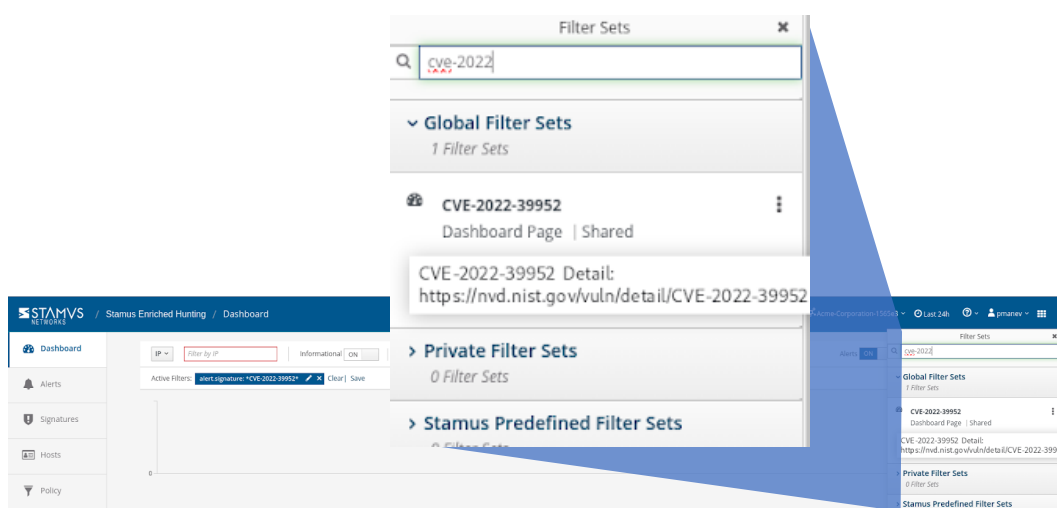
Save the Filter

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.



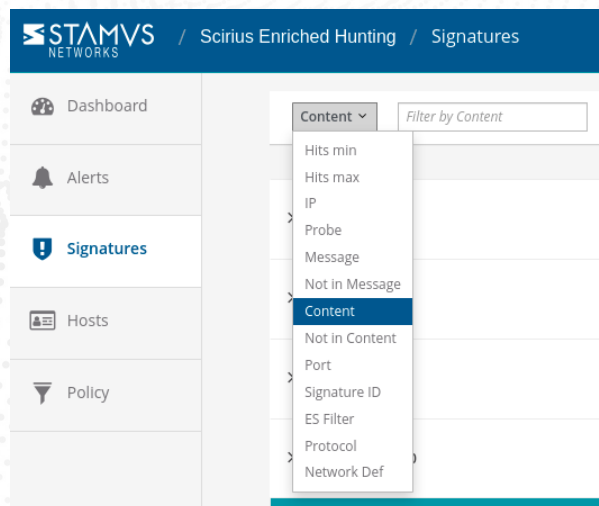
The newly created filter is now available in “Global Filter Sets” or “Private Filter Sets”

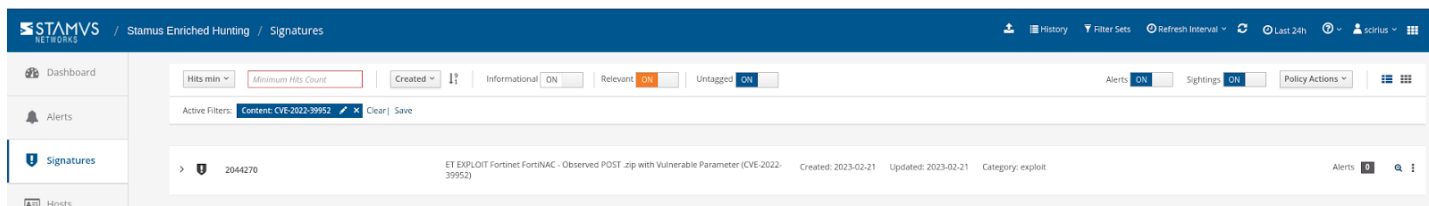


Review Detection Methods in Hunt

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-2022-39952), hit Enter





Automated Escalation and Webhooks Notification

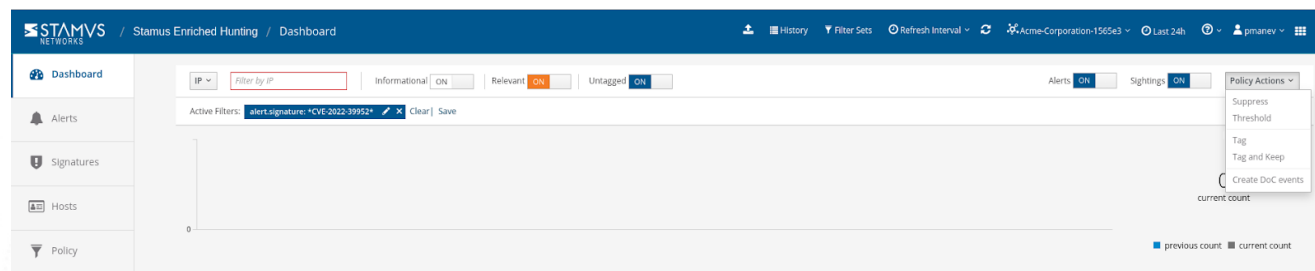
NOTE: Portions are not applicable to Stamus ND or Stamus Probe Management license tiers.

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 24 hours or 7 days ago, it will still be detected and escalated based on that custom filter.

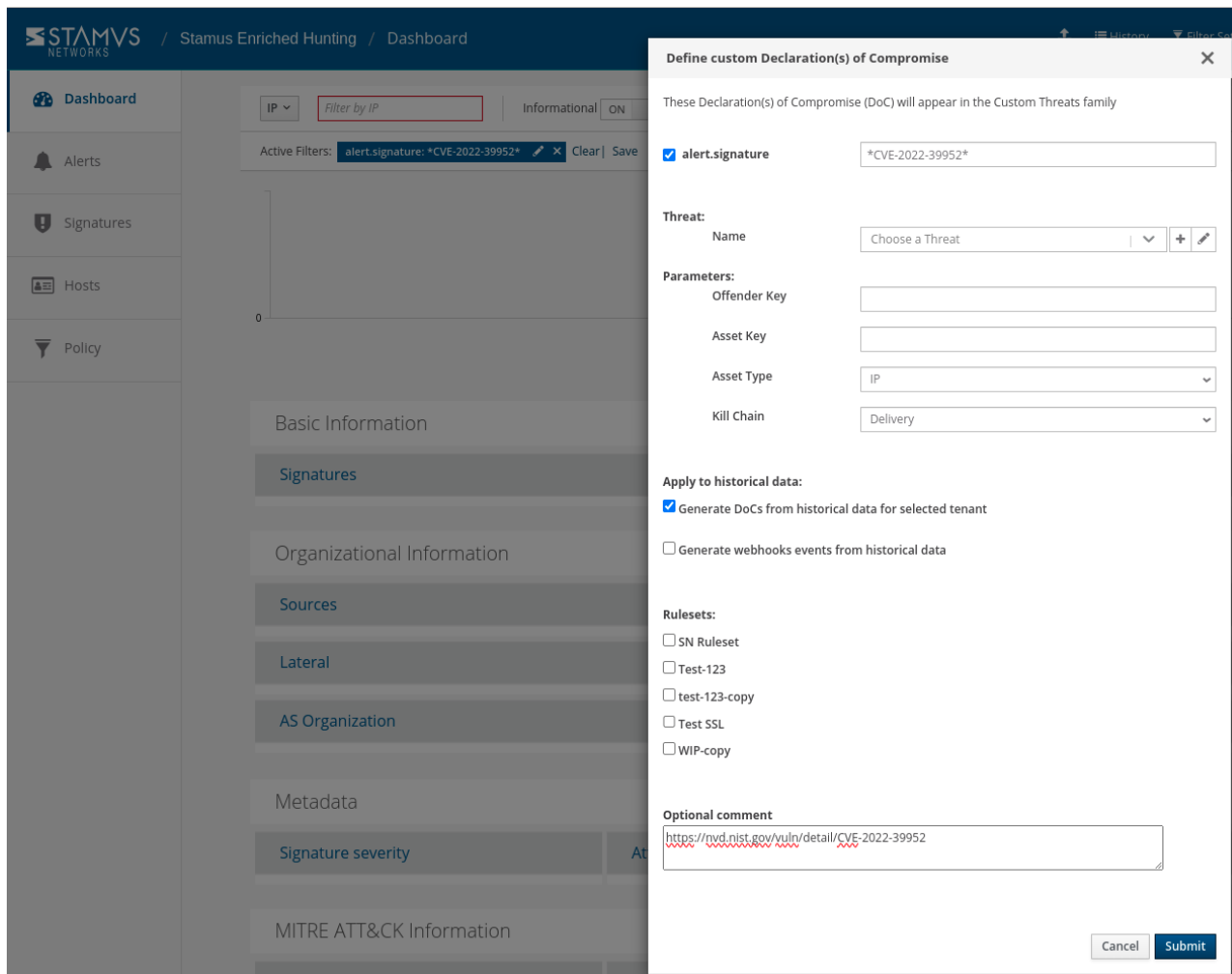
To do so:

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



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:



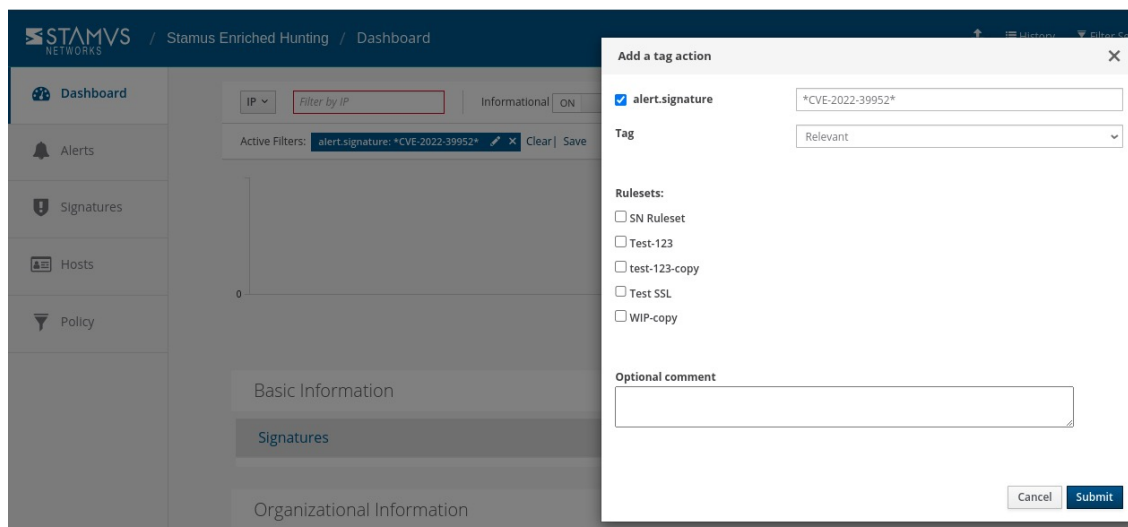
Automated Classification and Tagging

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)



Export Data - SIEM / Elasticsearch / Kibana

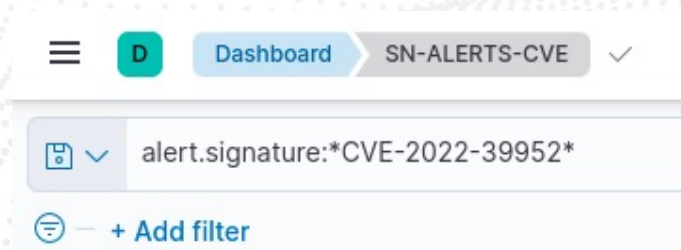
All data generated by Stamus Security Platform (with the Stamus ND/NDR license tiers), such as alerts, protocol transactions, sightings events or Host Insights information, may be exported and shared with any SIEM or SOAR system.

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. You can find a reference to all fields here <https://docs.stamus-networks.com/developer-corner/data-structure.html>

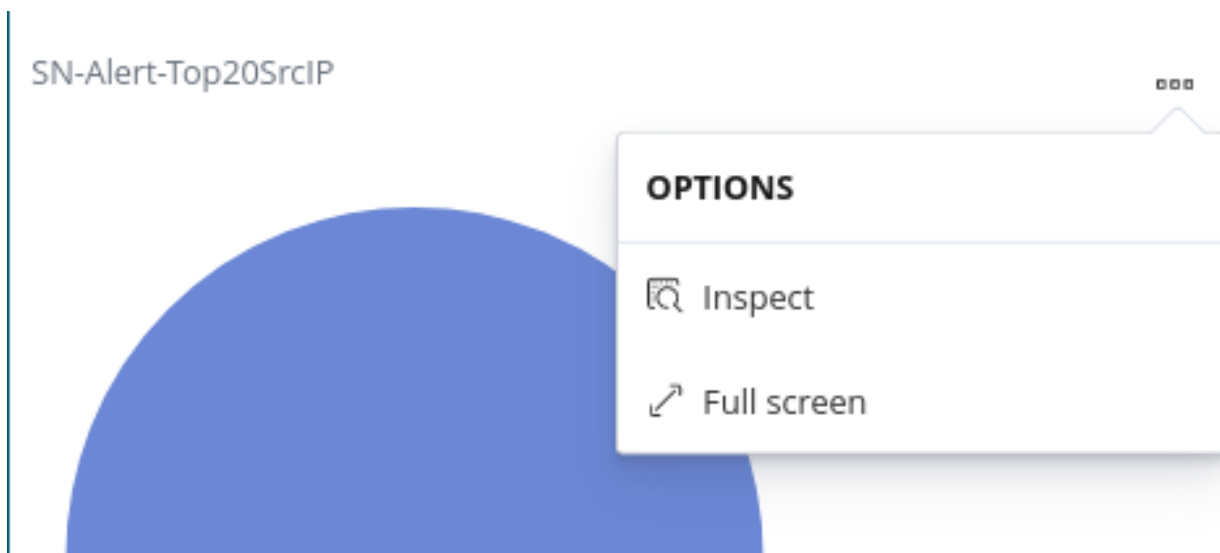
Any query of the Stamus Networks data (protocol transaction or alert logs) can be exported via a regular JSON log query or visualization export.

Example of Kibana query on alert events

To export CSV data from any info of the alerts you can open the SN-ALERT-CVE dashboard in Kibana, type in the filter "alert.signature.keyword:*CVE-2022-39952*", then you can export a CSV of any visualization using "Inspect" (see example below):



Click on "Inspect" in any visualization to export a CSV



Export Data - Splunk

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

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

Example of a Splunk query on alert events

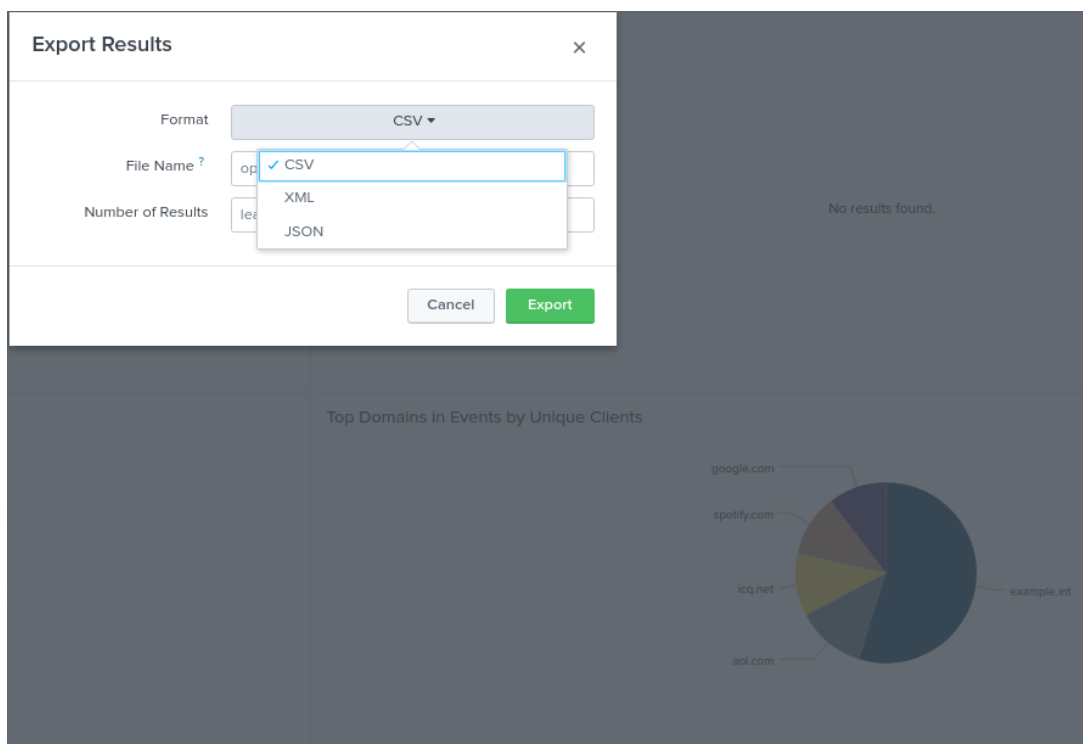
Splunk "event_type=alert "alert.signature"="*39952"



Protocol Transactions

Stamus Networks provides a free Splunk app <https://splunkbase.splunk.com/app/5262> that can be used to do specific “CVE-2022-39952” 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.



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.



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