Technical Brief

Detection of CVE-2022-39952 (FortiNAC) using Clear NDR™

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 Clear NDR™ "Hunt" interface.

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

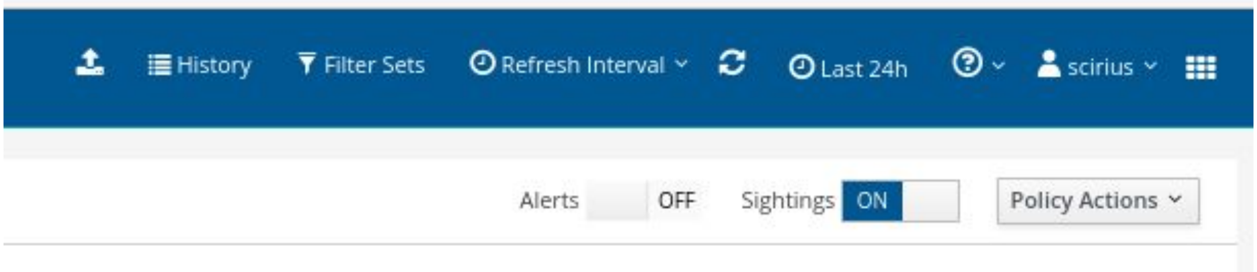
The first mechanism leverages Stamus Sightings and the second mechanism leverages specific CVE signature detection methods.

Mechanism 1: Using Sightings to Uncover an Attack

“Sightings” is a feature first available in U38 that allows for Stamus Networks 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, Clear NDR users may quickly filter through the noise to identify new malicious TLS connections to known malicious domains.

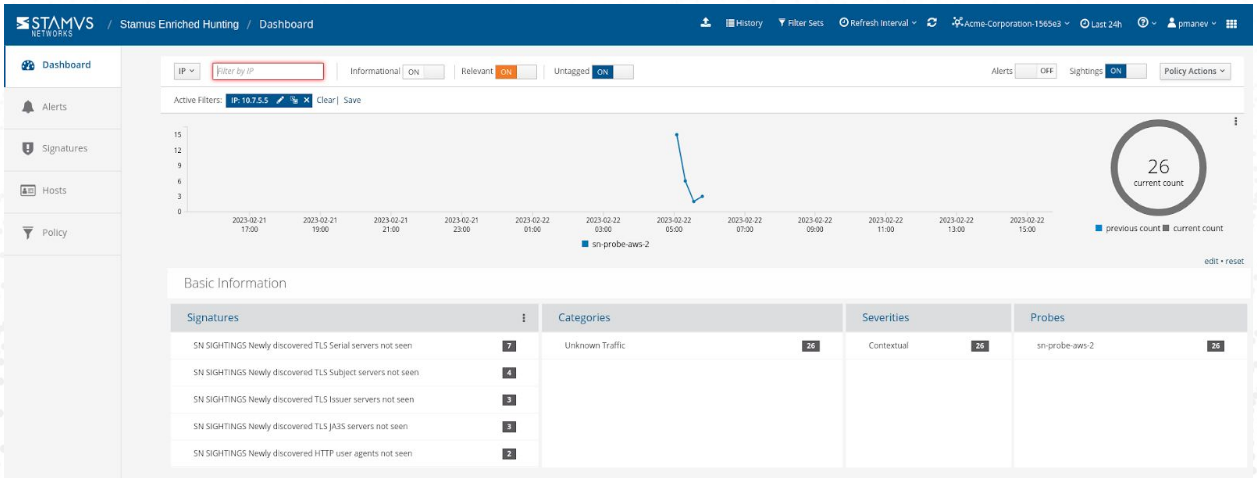
Here’s how: In Hunt, disable Alerts view by switching off the Alert tab. This will filter results down to only Sightings.



Alerts OFF

Sightings ON

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:



Informational ON

Relevant ON

Untagged ON

Alerts OFF

Sightings ON

Active Filters: IP: 10.7.5.5

Basic Information

Signatures	
SN SIGHTINGS Newly discovered TLS Serial servers not seen	7
SN SIGHTINGS Newly discovered TLS Subject servers not seen	4
SN SIGHTINGS Newly discovered TLS Issuer servers not seen	3
SN SIGHTINGS Newly discovered TLS JA3S servers not seen	3
SN SIGHTINGS Newly discovered HTTP user agents not seen	2

Categories	
Unknown Traffic	26

Severities	
Contextual	26

Probes	
sn-probe-aws-2	26

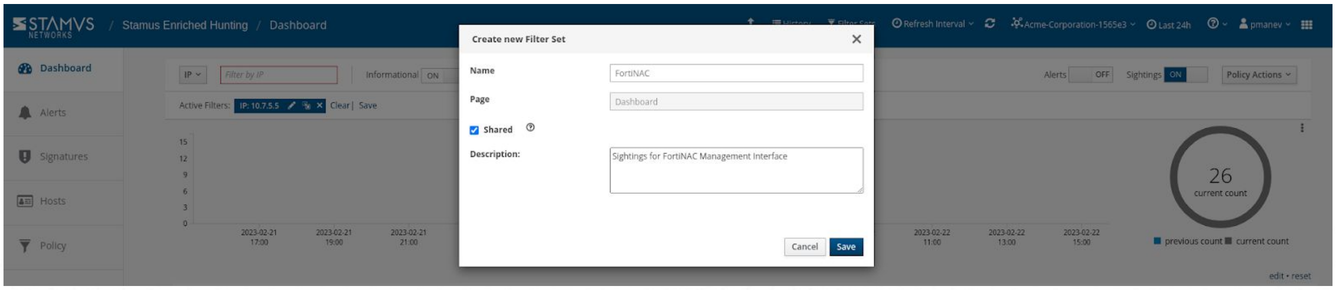
If we dive deeper into the Sightings (Clicking the 3 dots on the Signatures card) we can see all the Sightings are related to TLS, HTTP, or other internal protocols like SMB.

Now we can scroll down to the TLS information section and see a list of the relevant metadata such as SNI's, JA4, JA4S, 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



Create new Filter Set

Name: FortiNAC

Page: Dashboard

☑ Shared

Description: Sightings for FortiNAC Management Interface

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

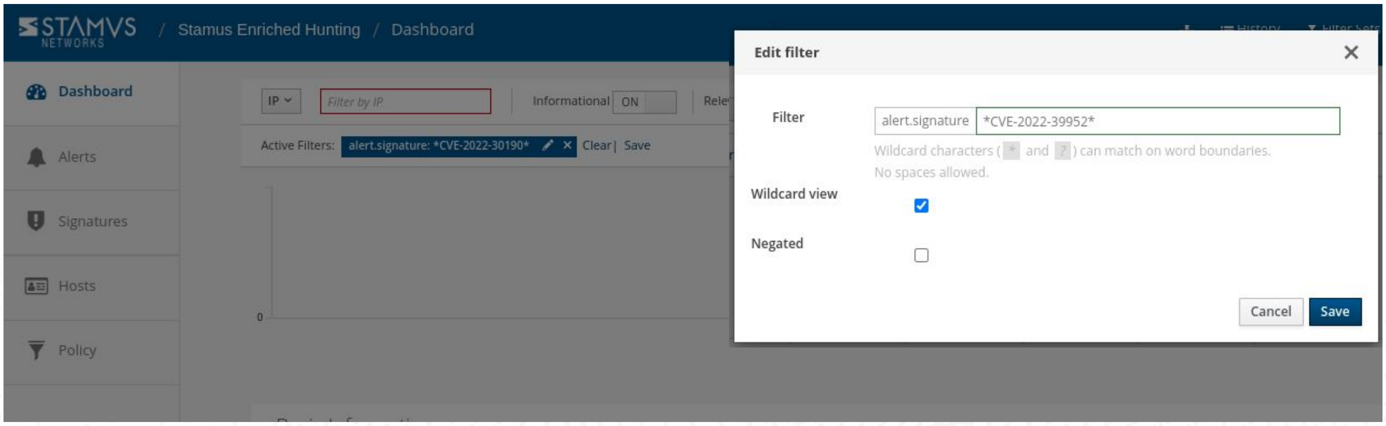
NOTE: Portions of this are not applicable to the Stamus Probe Management license tier

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 (*) it 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”



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

Edit filter

Filter: alert.signature *CVE-2022-39952*

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

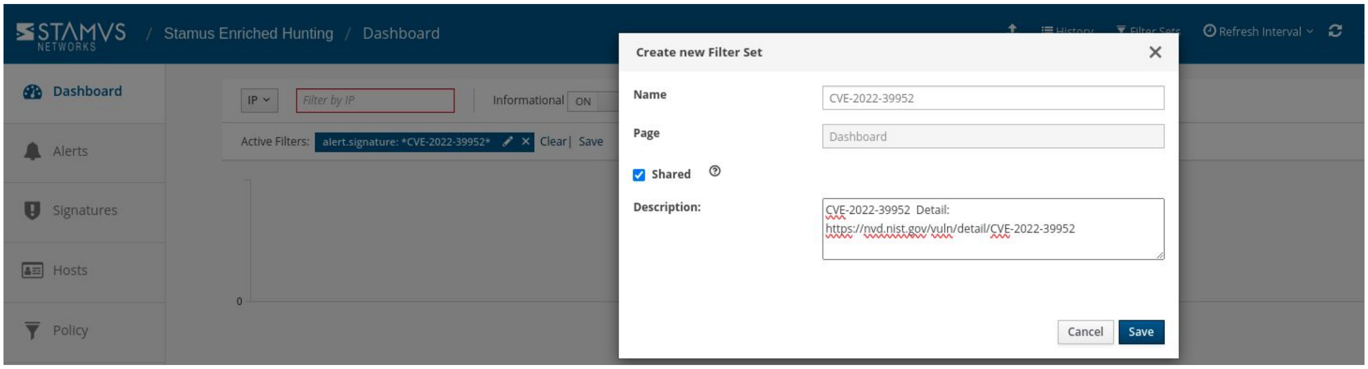
Wildcard view ☑

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.



Create new Filter Set

Name: CVE-2022-39952

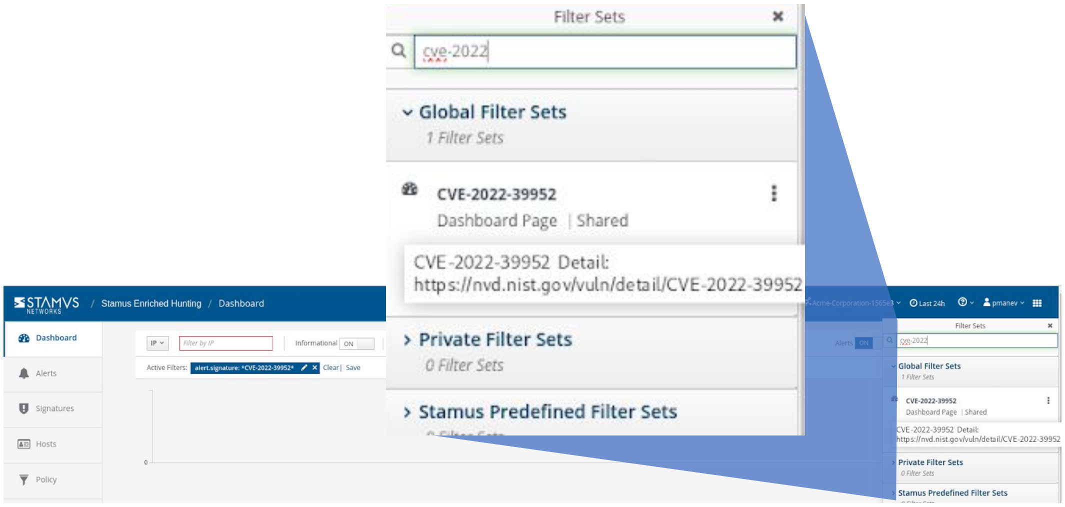
Page: Dashboard

☑ Shared

Description: CVE-2022-39952 Detail: https://nvd.nist.gov/vuln/detail/CVE-2022-39952

Cancel Save

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



Filter Sets

cve-2022

Global Filter Sets
1 Filter Sets

CVE-2022-39952
Dashboard Page | Shared

CVE-2022-39952 Detail:
https://nvd.nist.gov/vuln/detail/CVE-2022-39952

Private Filter Sets
0 Filter Sets

Stamus Predefined Filter Sets

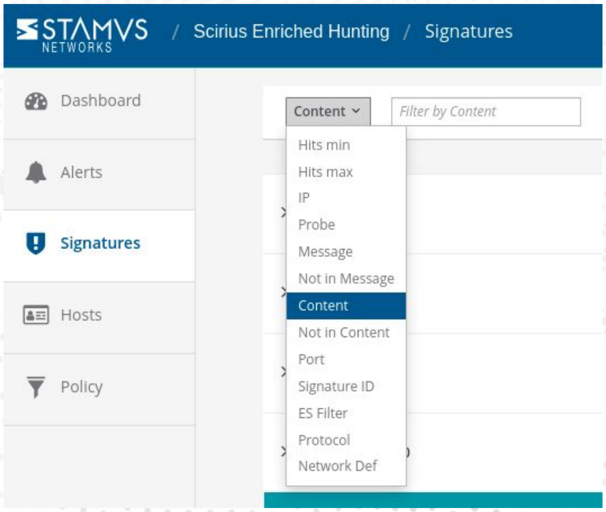
Review Detection Methods in Hunt

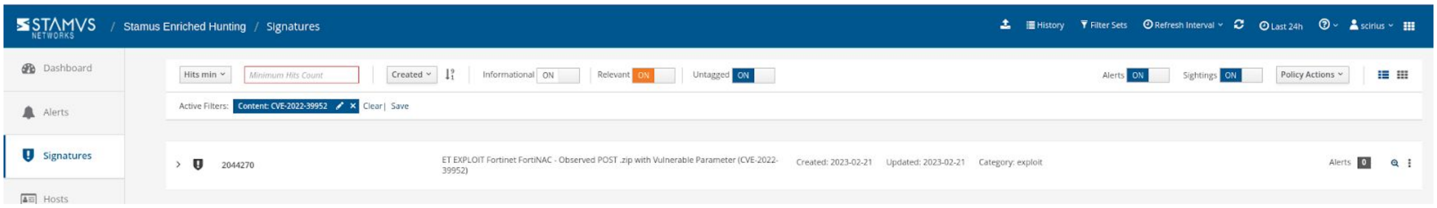
To review exactly what detection methods are available in Hunt for that specific vulnerability you can:

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





Informational ON Relevant ON Untagged ON Alerts ON Sightings ON

Active Filters: Content: CVE-2022-39952 Clear| Save

2044270 ET EXPLOIT Fortinet FortiNAC - Observed POST .zip with Vulnerable Parameter (CVE-2022-39952) Created: 2023-02-21 Updated: 2023-02-21 Category: exploit Alerts 0

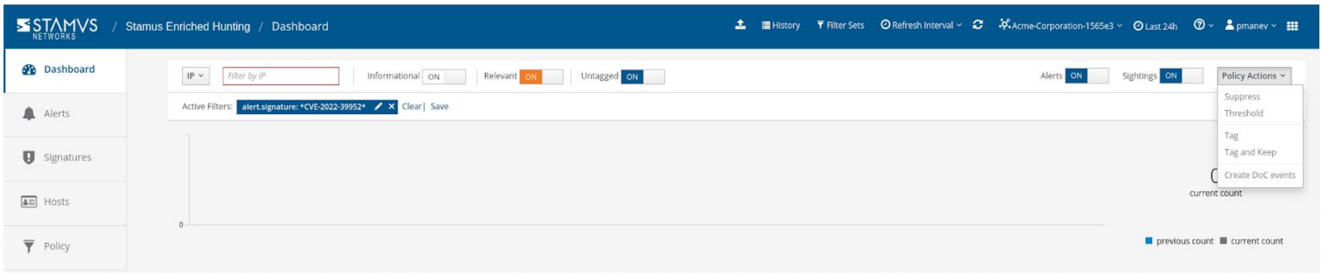
Automated Escalation and Webhooks Notification

NOTE: Portions are not applicable to older 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”.

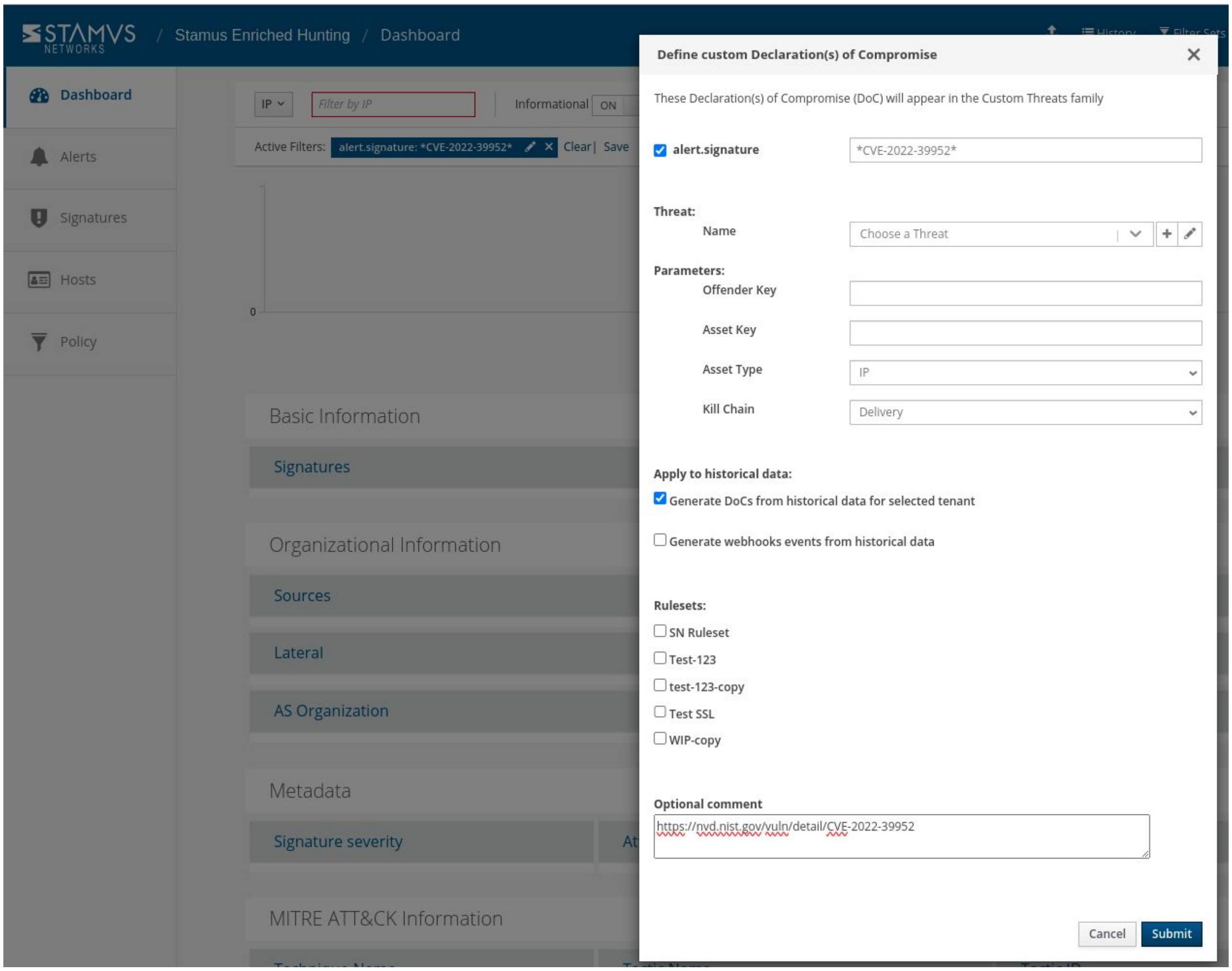


Informational ON Relevant ON Untagged ON Alerts ON Sightings ON

Active Filters: alert.signature: *CVE-2022-39952* Clear| Save

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-2022-39952*

Threat:

Name: Choose a Threat

Parameters:

Offender Key:

Asset Key:

Asset Type: IP

Kill Chain: Delivery

Apply to historical data:

☑ Generate DoCs from historical data for selected tenant

☐ Generate webhooks events from historical data

Rulesets:

☐ SN Ruleset
☐ Test-123
☐ test-123-copy
☐ Test SSL
☐ WIP-copy

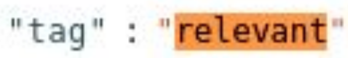
Optional comment

https://nvd.nist.gov/vuln/detail/CVE-2022-39952

Cancel | Submit

Automated Classification and Tagging

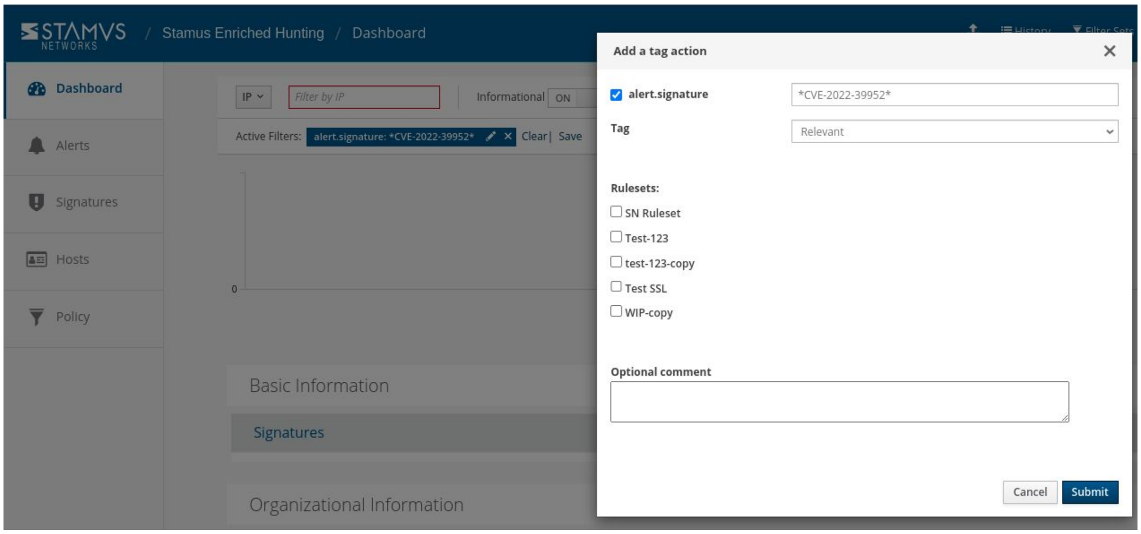
Auto Tagging all relevant events is also an option. This will allow for any logs (alerts or protocol transaction events related to the alerts) to have a “Relevant” tag inserted in the JSON logs:



```
"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-2022-39952*

Add a tag action

☑ alert.signature: *CVE-2022-39952*

Tag: Relevant

Rulesets:

□ SN Ruleset
□ Test-123
□ test-123-copy
□ Test SSL
□ WIP-copy

Optional comment

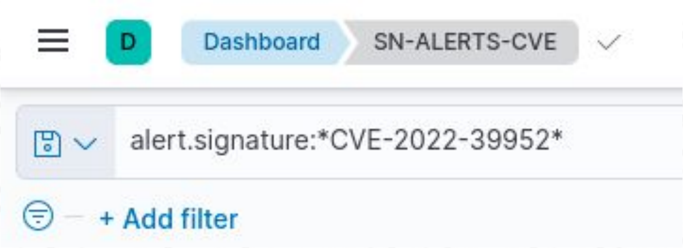
Export Data - SIEM / Elasticsearch / Kibana

All data generated by Clear NDR – Enterprise, 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 JA4/JA4S fingerprinting, TLS certificates and more. You can find a reference to all fields here https://docs.stamus-networks.com/developer-corner/data-structure.html

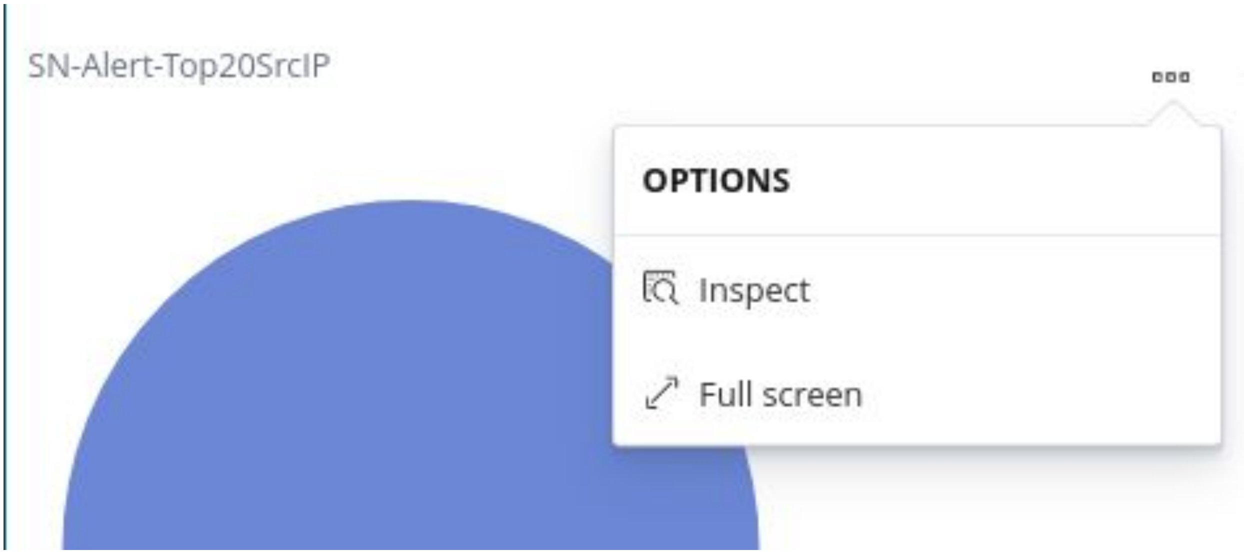
Any query of the Stamus Networks data (protocol transaction or alert logs) can be exported via a regular JSON log query or visualization export.
Example of Kibana query on alert events

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):



alert.signature:*CVE-2022-39952*

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



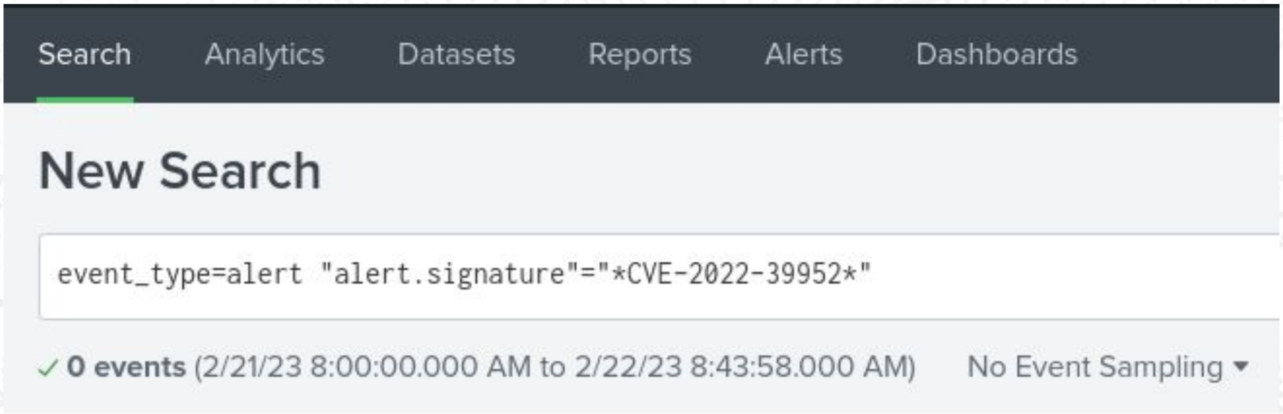
Export Data - Spunk

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

Any query of the Clear NDR 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"



```
event_type=alert "alert.signature"="*CVE-2022-39952*"
```

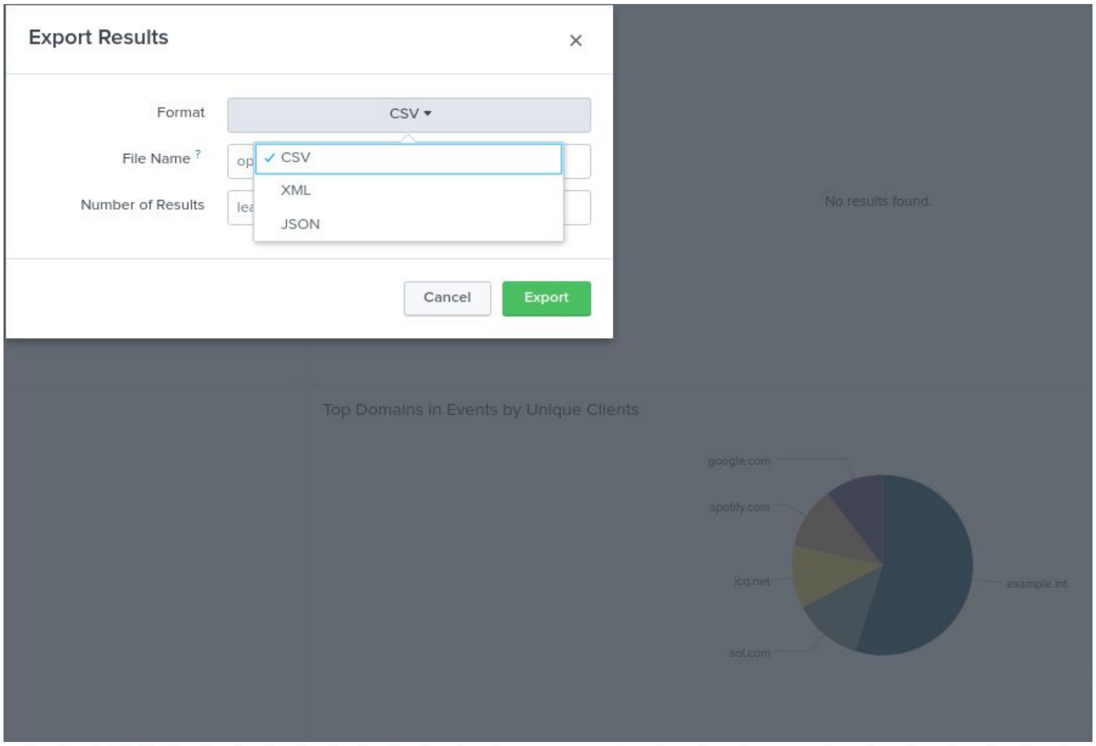
✓ **0 events** (2/21/23 8:00:00.000 AM to 2/22/23 8:43:58.000 AM)

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-2022-39952” 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.



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 that cyber defense is bigger than any single person, platform, company, or technology. That’s why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world’s most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

STAMUS 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