Technical Brief

Uncovering Cisco Breach IoCs with Clear NDR™

On August 10, 2022, Cisco announced that on May 24 it became aware of a potential compromise.

Included in the breach report (https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html) is the following list of 14 domain IoCs that Cisco has determined were involved in the attack. You may query your Clear NDR data – specifically Alert, DNS, HTTP, or TLS logs – to see if any devices on your network have queried or visited these potentially dangerous domains.

cisco-help[.]cf
cisco-helpdesk[.]cf
ciscovpn1[.]com
ciscovpn2[.]com
ciscovpn3[.]com
devcisco[.]com
devciscoprograms[.]com
helpzonecisco[.]com
kazaboldu[.]net
mycisco[.]cf
mycisco[.]gq
mycisco-helpdesk[.]ml
primecisco[.]com
pwresetcisco[.]com

We recommend using your Clear NDR to determine if any of the IOC domains or IP addresses listed in the Cisco bulletin have been queried or contacted from within your environment.

Stamus Networks provides historical network protocol transaction and flow record logging that makes it easy for a security practitioner to discover if a questionable domain or IP address has previously been visited from within your organization.

This Technical Brief explains how to find the initially-compromised host and shows you how to search the protocol and transaction logs to determine if any device has attempted to query or contact the IOCs listed in the Cisco bulletin.

Clear NDR supports several different mechanisms for identifying these IoCs. Please review each of these and select the mechanism best for your particular tech stack.

From Clear NDR "Stamus Enriched Hunting" Interface

- Finding the first occurrence via Stamus *Sightings*
- Saving the Stamus Enriched Hunting filter

From third party systems

- Using Kibana to query the Elasticsearch database
- Using Splunk queries
- Using REST API commands

NOTE: Queries shown in this document will be limited by the retention level of the data. By default, that is 14 days.

FROM “STAMUS ENRICHED HUNTING” INTERFACE

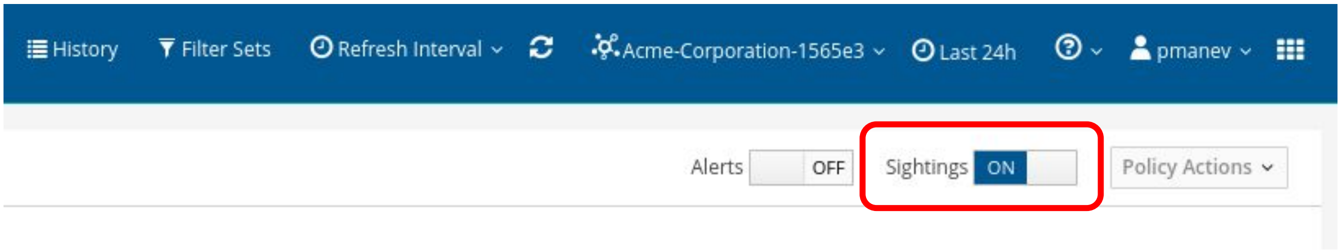
Clear NDR provides historical network protocol transaction and flow record logging that makes it easy for a security practitioner to discover if a questionable domain or IP address has previously been visited from within your organization.

Please follow the steps listed below in the Clear NDR, “Stamus Enriched Hunting” interface:

Finding First Occurrence via *Stamus Sightings*

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

You may identify any affected host – or “patient zero” – by searching the *Stamus Sightings* from the Stamus Enriched Hunting screen



Alerts OFF

Sightings ON

To Create a Filter:

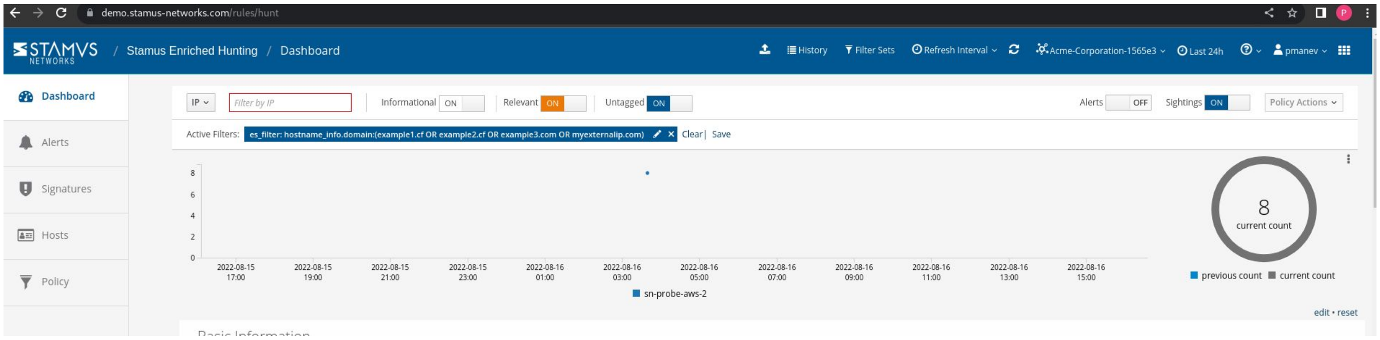
1. From the Stamus Enriched Hunting dashboard, click on the button labeled IP next to the query text field
2. In the pull down click ES Filter
3. In the query field copy and past the query below then press enter
4. Turn off alerts with the Alerts toggle switch (See picture above)
5. Make sure that the Sightings toggle is turned on (See picture above)
6. You are now ready to review the results and events in the Dashboard, Host Insights and Alert views

NOTE: These are malicious domains – do not click or visit directly !

The example screenshot below shows how to create a filter for a list of events:
hostname_info.domain:(example1.cf OR example2.cf OR example3.com OR example.com)

Query text:

```
hostname_info.domain:(cisco-help.cf OR cisco-helpdesk.cf OR ciscovpn1.com
OR ciscovpn2.com OR ciscovpn3.com OR devcisco.com OR devciscoprograms.com
OR helpzonecisco.com OR kazaboldu.net OR mycisco.cf OR mycisco.gq OR
mycisco-helpdesk.ml OR primecisco.com OR pwresetcisco.com)
```

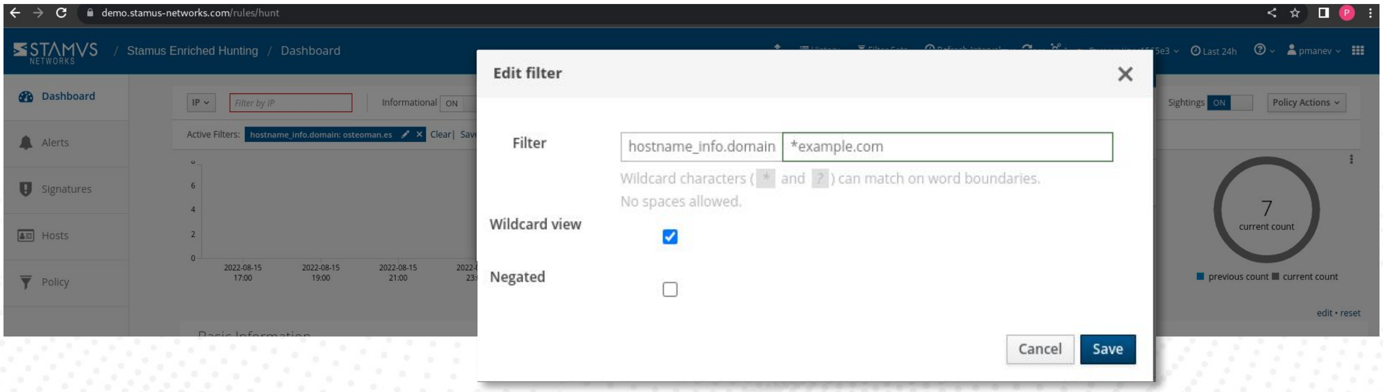


demo.stamus-networks.com/rules/hunt

Informational ON | Relevant ON | Untagged ON | Alerts OFF | Sightings ON

Active Filters: es_filter: hostname_info.domain:(example1.cf OR example2.cf OR example3.com OR myexternalip.com)

The example screenshot below illustrates how to create the query for a single domain name (regardless of whether it is a TLS or DNS record)



demo.stamus-networks.com/rules/hunt

Active Filters: hostname_info.domain: osteoman.es

Edit filter

Filter: hostname_info.domain | *example.com

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

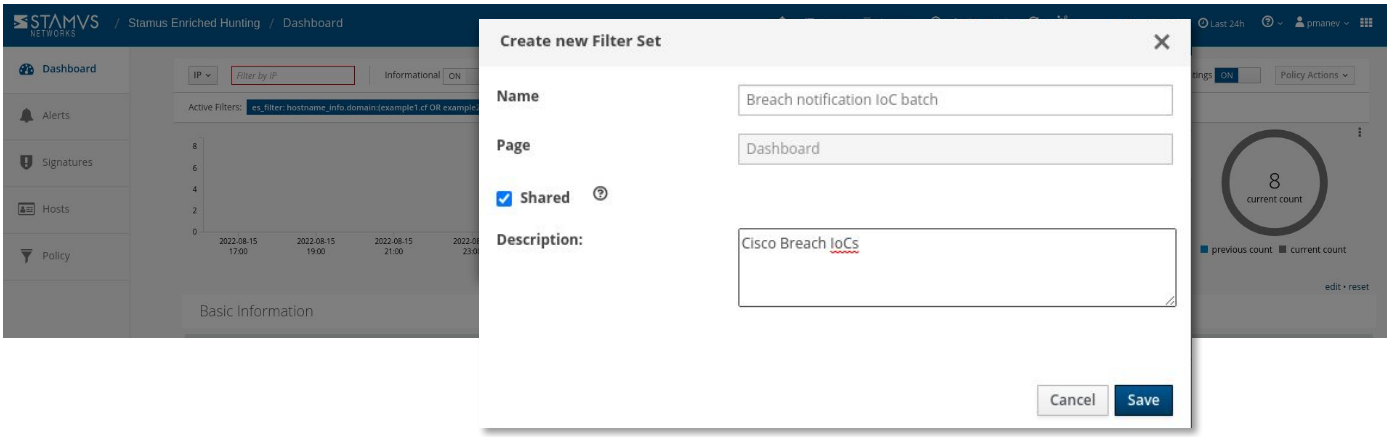
Wildcard view ☑

Negated ☐

Save the Stamus Enriched Hunting 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: es_filter: hostname_info.domain:(example1.cf OR example2

Create new Filter Set

Name: Breach notification IoC batch

Page: Dashboard

☑ Shared

Description: Cisco Breach IoCs

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

FROM THIRD PARTY SYSTEMS

All data generated by Clear NDR, such as alerts, protocol transactions, sightings events or Host Insights information, may be exported and shared with any SIEM or SOAR system.

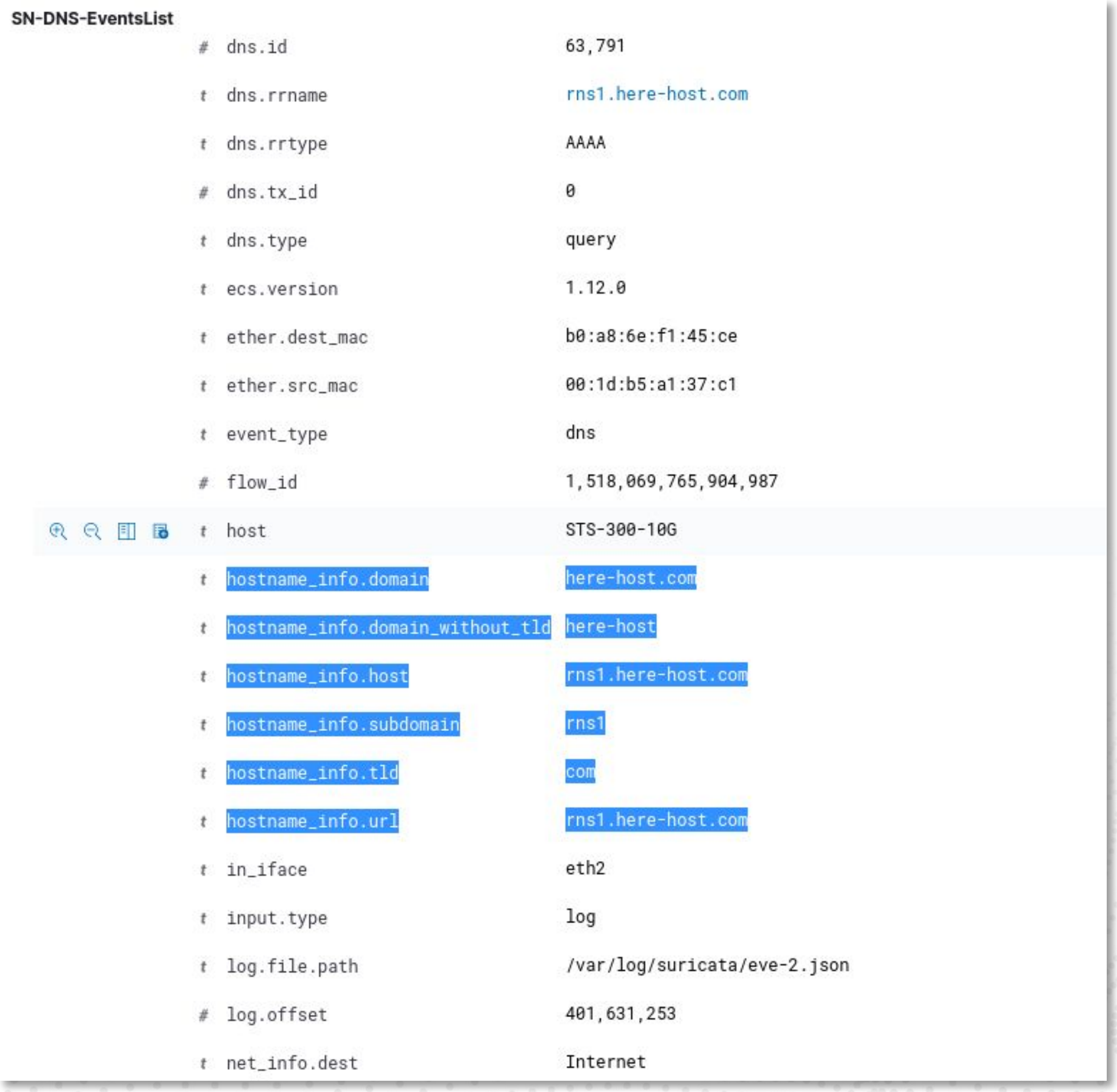
Over 4000 fields are available -- from domain requests, http user agents used, hostnames, usernames logged in -- to encrypted analysis including JA4/JA4S fingerprinting, TLS certificates and more.

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

As part of the Clear NDR event enrichment process, all TLS, HTTP or DNS events are enriched with a breakdown, mapping, and addition of the specific domain/url/tls sni event by the following fields:

hostname_info.domain_without_tld
hostname_info.host
hostname_info.subdomain
hostname_info.tld
hostname_info.url

Example:



SN-DNS-EventsList

#	dns.id	63,791
t	dns.rrname	rns1.here-host.com
t	dns.rrtype	AAAA
#	dns.tx_id	0
t	dns.type	query
t	ecs.version	1.12.0
t	ether.dest_mac	b0:a8:6e:f1:45:ce
t	ether.src_mac	00:1d:b5:a1:37:c1
t	event_type	dns
#	flow_id	1,518,069,765,904,987
t	host	STS-300-10G
t	hostname_info.domain	here-host.com
t	hostname_info.domain_without_tld	here-host
t	hostname_info.host	rns1.here-host.com
t	hostname_info.subdomain	rns1
t	hostname_info.tld	com
t	hostname_info.url	rns1.here-host.com
t	in_iface	eth2
t	input.type	log
t	log.file.path	/var/log/suricata/eve-2.json
#	log.offset	401,631,253
t	net_info.dest	Internet

This allows for simple, all inclusive, and accurate search in any SIEM or data lake.

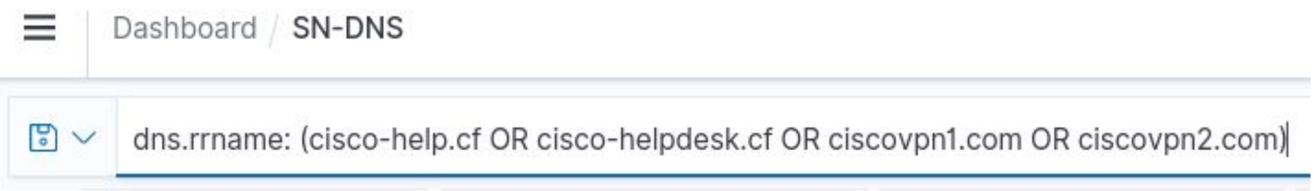
Kibana Queries of Elasticsearch Database and Data Export

In any of the SN-HTTP, SN-ALERT, SN-TLS, SN-DNS dashboards you can simply run the example query.

Dashboard query text:

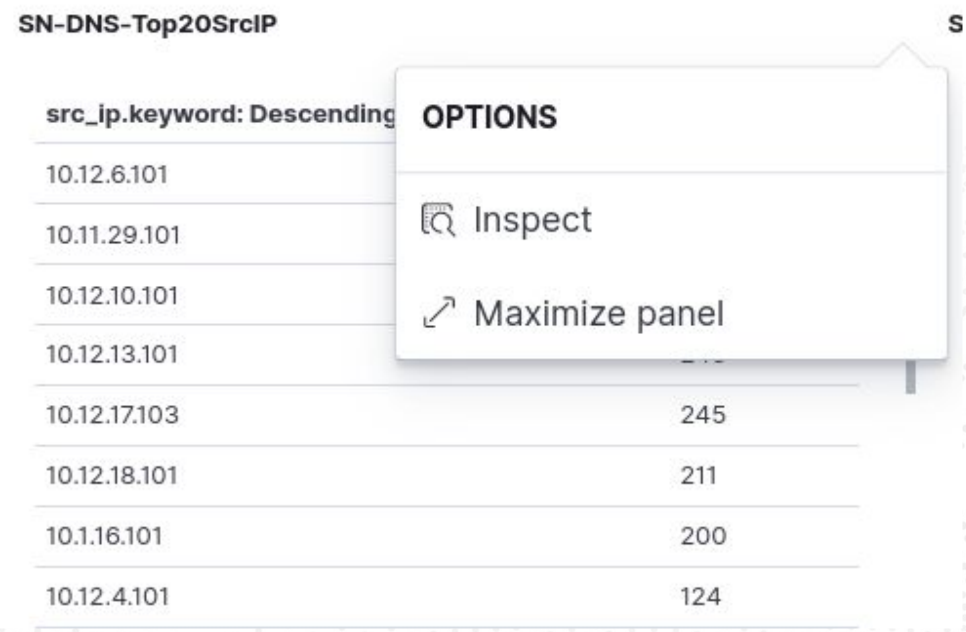
```
hostname_info.domain: (cisco-help.cf OR cisco-helpdesk.cf OR
ciscovpn1.com OR ciscovpn2.com OR ciscovpn3.com OR devcisco.com OR
devciscoprograms.com OR helpzonecisco.com OR kazaboldu.net OR
mycisco.cf OR mycisco.gq OR mycisco-helpdesk.ml OR primecisco.com OR
pwresetcisco.com)
```

See example screenshot below from the SN-DNS dashboard



```
dns.rrname: (cisco-help.cf OR cisco-helpdesk.cf OR ciscovpn1.com OR ciscovpn2.com)
```

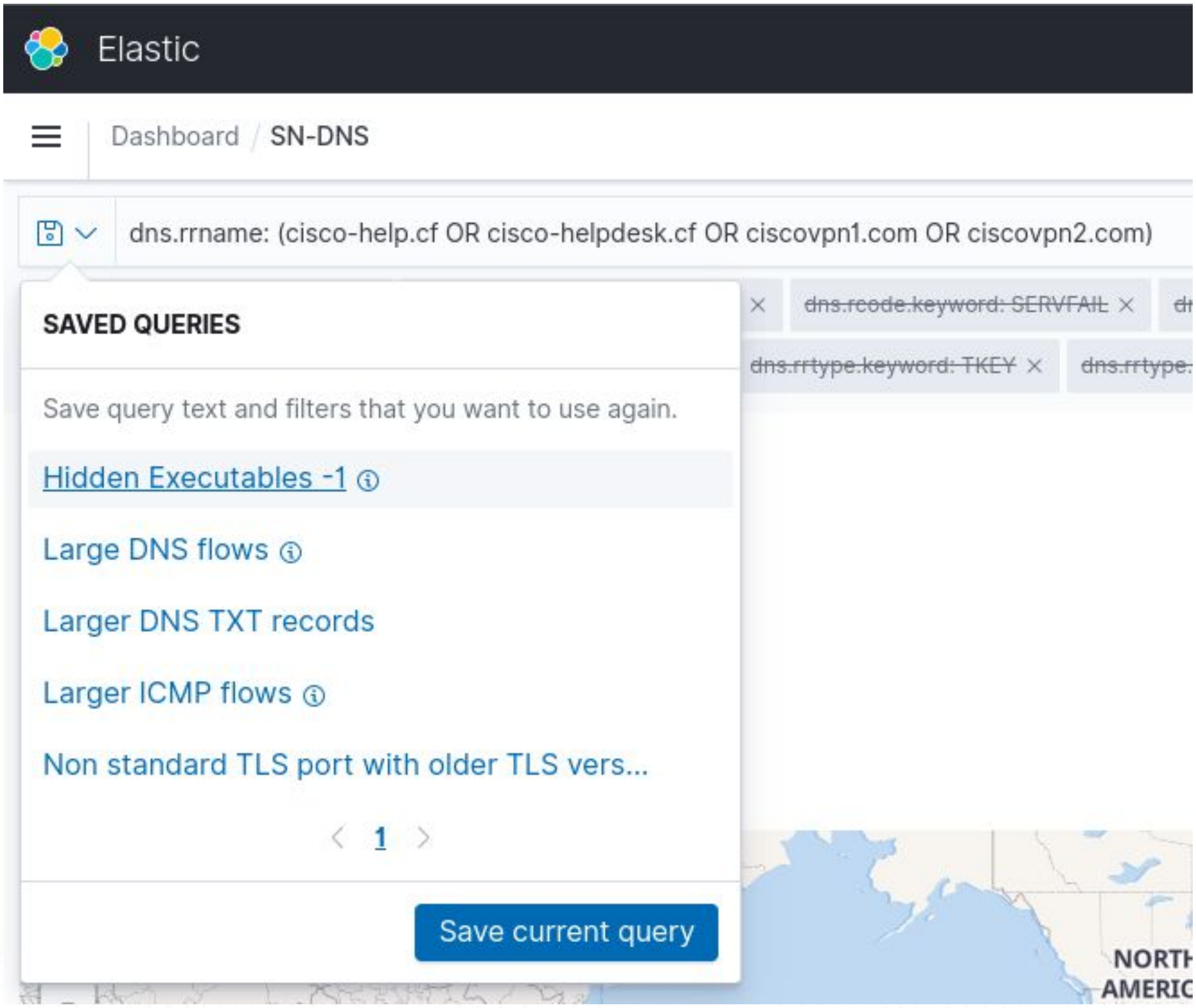
In order to export to CSV, click on the three dots in the upper right corner, and then select “Inspect” in any visualization.



SN-DNS-Top20SrcIP

src_ip.keyword: Descending	
10.12.6.101	
10.11.29.101	
10.12.10.101	
10.12.13.101	
10.12.17.103	245
10.12.18.101	211
10.1.16.101	200
10.12.4.101	124

You may save the query as follows:



dns.rrname: (cisco-help.cf OR cisco-helpdesk.cf OR ciscovpn1.com OR ciscovpn2.com)

Save query text and filters that you want to use again.

Splunk Queries and Data Export

Any query of the Clear NDR data (protocol transaction or alert logs) in Splunk may be exported via a regular Splunk query or visualization export.

Splunk users may access the enriched Clear NDR data via queries of four event types – Alerts, TLS, DNS and HTTP. Examples are shown below.

Splunk query on Alert events

```
`stamus_index` event_type="Alert" hostname_info.domain IN (cisco-help.cf,
cisco-helpdesk.cf, ciscovpn1.com, ciscovpn2.com, ciscovpn3.com, devcisco.com,
devciscoprograms.com, helpzonecisco.com, kazaboldu.net, mycisco.cf,
mycisco.gq, mycisco-helpdesk.ml, primecisco.com, pwresetcisco.com)
```

Splunk query on TLS events

```
`stamus_index` event_type="TLS" hostname_info.domain IN (cisco-help.cf,
cisco-helpdesk.cf, ciscovpn1.com, ciscovpn2.com, ciscovpn3.com, devcisco.com,
devciscoprograms.com, helpzonecisco.com, kazaboldu.net, mycisco.cf,
mycisco.gq, mycisco-helpdesk.ml, primecisco.com, pwresetcisco.com)
```

Splunk query on DNS events

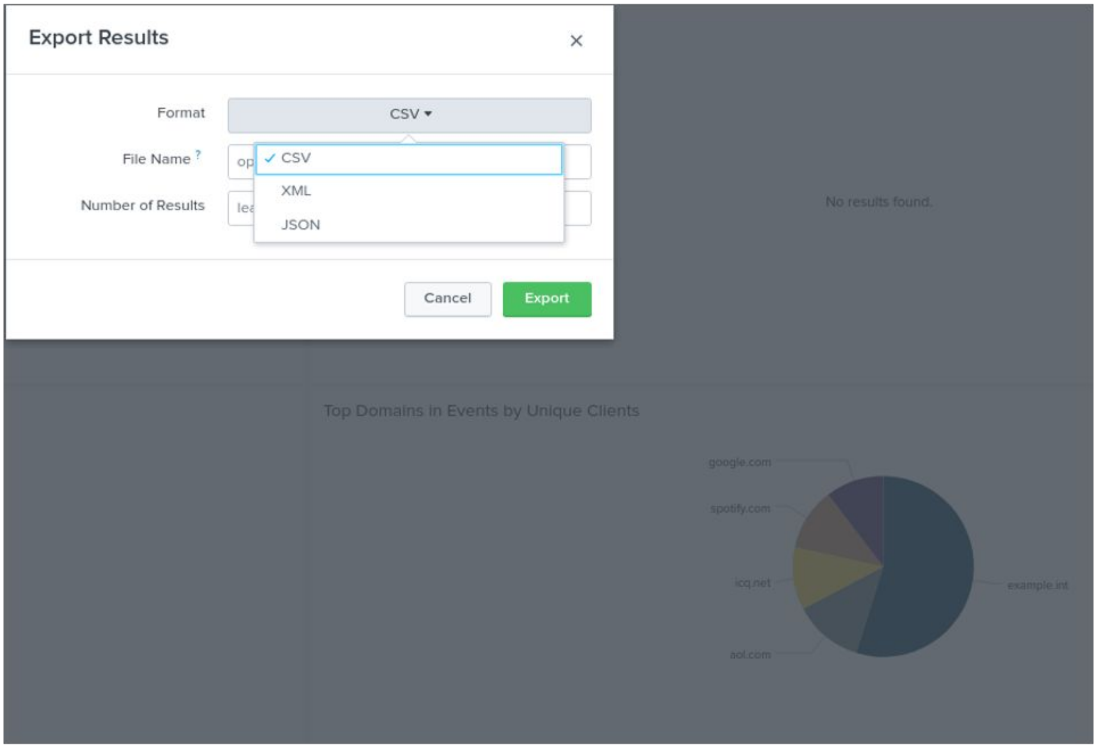
```
`stamus_index` event_type="DNS" hostname_info.domain IN (cisco-help.cf,
cisco-helpdesk.cf, ciscovpn1.com, ciscovpn2.com, ciscovpn3.com, devcisco.com,
devciscoprograms.com, helpzonecisco.com, kazaboldu.net, mycisco.cf,
mycisco.gq, mycisco-helpdesk.ml, primecisco.com, pwresetcisco.com)
```

Splunk query on HTTP events

```
`stamus_index` event_type="HTTP" hostname_info.domain IN (cisco-help.cf,
cisco-helpdesk.cf, ciscovpn1.com, ciscovpn2.com, ciscovpn3.com, devcisco.com,
devciscoprograms.com, helpzonecisco.com, kazaboldu.net, mycisco.cf,
mycisco.gq, mycisco-helpdesk.ml, primecisco.com, pwresetcisco.com)
```

Stamus Networks provides a free Splunk app https://splunkbase.splunk.com/app/5262 that may be used to do specific IoC searches among other use cases.

Additional Splunk visualizations queries that support for the IoC may be performed using the native Splunk export functionality shown below.



Export Results

Format: CSV

File Name

Number of Results

No results found.

Top Domains in Events by Unique Clients

REST API Commands

Security teams using third party tools such as a Security Orchestration, Automation and Response (SOAR) system may use REST API commands to directly query the Clear NDR database.

The example below is taken from our online documentation which may be found here https://docs.stamus-networks.com/developer-corner/soar-integration-examples.html

The examples use the “curl” linux utility for ease. The REST API queries may be developed in Python or any other programming/scripting language. The documentation provides extensive examples.

Example API Queries for Multiple Domains:

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilter\=dns.rrname:\(cisco-help.cf%20OR%20cisco-helpdesk.cf%20OR%20ciscovpn1.com%20OR%20ciscovpn2.com%20OR%20ciscovpn3.com%20OR%20devcisco.com%20OR%20devciscoprograms.com%20OR%20helpzonecisco.com%20OR%20kazaboldu.net%20OR%20mycisco.cf%20OR%20mycisco.gq%20OR%20mycisco-helpdesk.ml%20OR%20primecisco.com%20OR%20pwresetcisco.com\) -H 'Authorization: Token <token>' -H 'Content-Type:application/json' -X GET | jq -r
```

OR

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilter\=hostname_info.domain:\(cisco-help.cf%20OR%20cisco-helpdesk.cf%20OR%20ciscovpn1.com%20OR%20ciscovpn2.com%20OR%20ciscovpn3.com%20OR%20devcisco.com%20OR%20devciscoprograms.com%20OR%20helpzonecisco.com%20OR%20kazaboldu.net%20OR%20mycisco.cf%20OR%20mycisco.gq%20OR%20mycisco-helpdesk.ml%20OR%20primecisco.com%20OR%20pwresetcisco.com\) -H 'Authorization: Token <token>' -H 'Content-Type:application/json' -X GET | jq -r
```

Troubleshooting and Help

Please feel free to contact 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.

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