Corelight integration for Splunk Enterprise Security

Introduction

Corelight Sensors are built on Zeek, the powerful and widely used open source network analysis platform that generates actionable insights from network data for thousands of SOCs worldwide. Corelight data drives faster incident response times and significantly improves threat hunt capabilities.

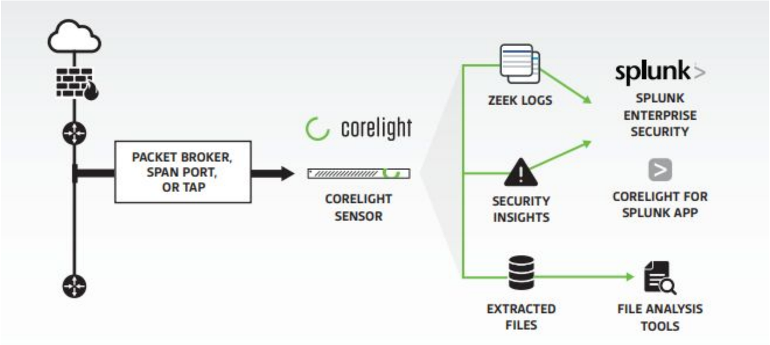
The power of Corelight data is easily experienced when used in Splunk Enterprise and Splunk Enterprise Security (ES). Out of the box, Corelight data feeds the most prevalent Splunk data models including:

- Network Traffic, Network Resolutions (DNS)
- Network Sessions
- Certificates
- Intrusion Detection
- Web
- Email

Further, Corelight has a native integration with Splunk, meaning the data is Common Information Model (CIM) compliant without any additional administrator effort. After reading this document you will learn how easily Corelight data fits into Splunk data models, and how to maximize Splunk ES with Corelight.

Corelight data to Splunk

Corelight Sensors monitor network traffic through packet brokers, taps, or spans and extract security rich metadata into log files. The log files are then exported to Splunk indexers via the integrated Splunk universal forwarder.

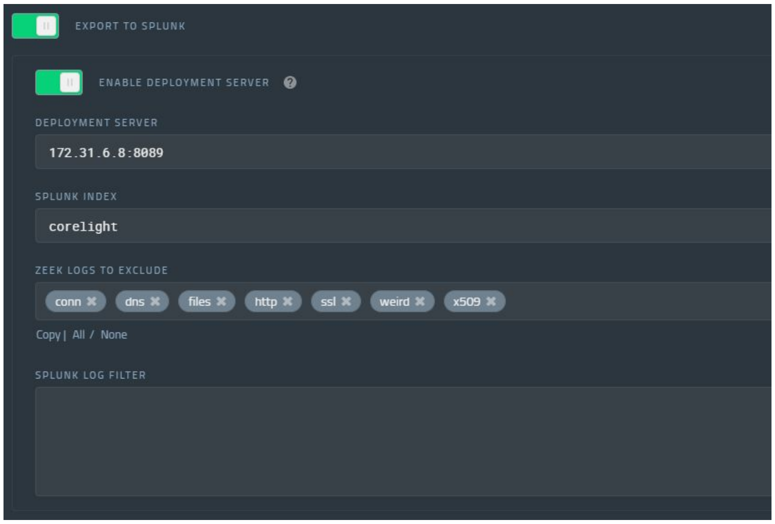


Follow these simple steps to ingest CIM compliant Corelight data into Splunk:

1. Install the Corelight App for Splunk and/or TA for Corelight on the Splunk server(s). The Corelight App typically is installed on search heads and standalone instances. The TA should be installed on indexers and heavy forwarders. The App and TA should never be installed on the same Splunk instance.

Corelight App for Splunk	https://splunkbase.splunk.com/app/3884/
TA for Corelight	https://splunkbase.splunk.com/app/3885/

2. Configure the Corelight Sensor to export data to Splunk. Corelight Sensors have native Splunk export configurable through the Web UI or the Corelight command line client. This export uses the Splunk Universal Forwarder on the sensor and supports management by a Splunk Deployment Server.



EXPORT TO SPLUNK

ENABLE DEPLOYMENT SERVER

DEPLOYMENT SERVER

172.31.6.8:8089

SPLUNK INDEX

corelight

ZEEK LOGS TO EXCLUDE

conn ✖ dns ✖ files ✖ http ✖ ssl ✖ weird ✖ x509 ✖

Copy | All / None

SPLUNK LOG FILTER

As an alternative, an app can be uploaded using the corelight-client command line utility:

```
corelight-client splunk list

splunk delete    Removes a previously uploaded Splunk App.
splunk download  Retrieves a previously installed Splunk App as a ZIP file.
splunk list      Returns a list of all installed custom Splunk Apps.
splunk upload    Uploads a new Splunk App from a ZIP file.
```

3. If you are concerned about the volume of data being ingested from Corelight you can optionally enable the Corelight data reduction package. This package reduces the data volume of common log types by suppressing typically low-value log entries and duplicate ones. This could result in a log volume reduction of 30-40%.

4. Filter logs that overlap with the reduced log formats. The conn, dns, files, http, ssl, weird, and x509 logs should be filtered using the "ZEEKS LOGS TO EXCLUDE" option (shown in graphic above).

5. Validate logs are arriving in Splunk using search or the Corelight App for Splunk.

Corelight data and Splunk data models

Corelight data automatically populates important fields in the most prevalent Splunk data models including Network Traffic, Network Resolutions (DNS), Network Sessions, Certificates, Web, and Email. Now that Corelight has integrated the leading open source IDS Suricata, the Intrusion Detection data model can also be populated.

Corelight published a blog that encourages the addition of fields to the DNS data model and a few tweaks to correlation searches that significantly increases Splunk efficiency. It is important to note that before a data model is modified, Splunk customers read and understand the short-term impacts required for the long-term benefit. Please see this Splunk page for details.

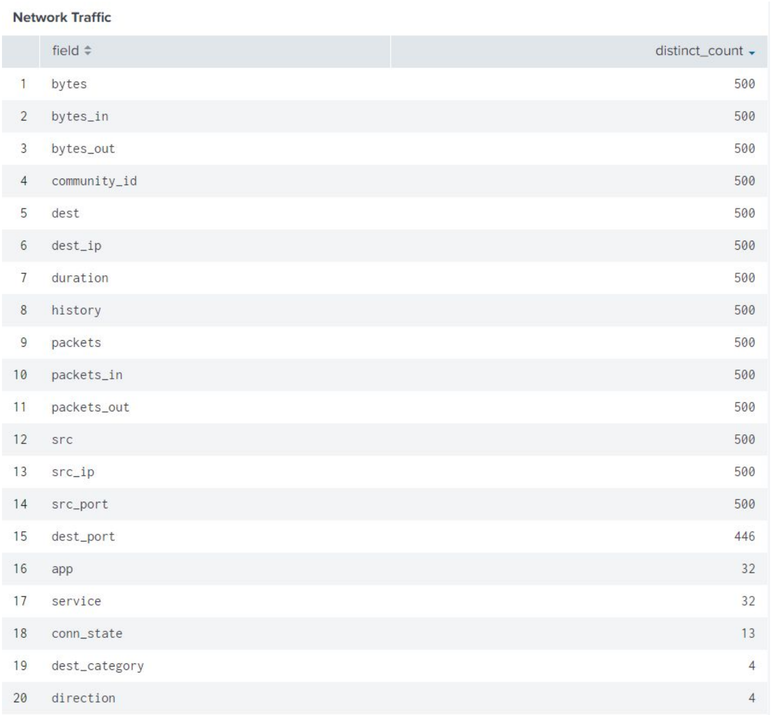
Sourcetype to data model mapping

corelight_conn	Network_Sessions
corelight_conn	Network_Traffic
corelight_dhcp	Network_Sessions
corelight_dns	Network_Resolution
corelight_http	Web
corelight_smtp	Email
corelight_ssl	Certificates
corelight_x509	Certificates
corelight_suricata	Intrusion_Detecion

Corelight data model field coverage is exceptional

In each of the following sections, graphics illustrate the depth of the Corelight data (as depicted by the distinct counts for each field).

Network Traffic: Corelight data populates the most commonly used fields in correlation searches based on the Network Traffic data model.



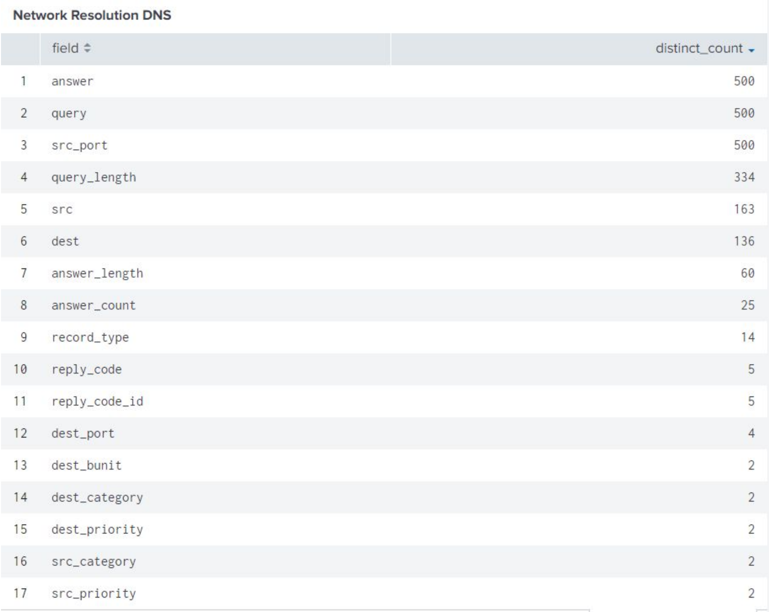
Network Traffic

	field	distinct_count
1	bytes	500
2	bytes_in	500
3	bytes_out	500
4	community_id	500
5	dest	500
6	dest_ip	500
7	duration	500
8	history	500
9	packets	500
10	packets_in	500
11	packets_out	500
12	src	500
13	src_ip	500
14	src_port	500
15	dest_port	446
16	app	32
17	service	32
18	conn_state	13
19	dest_category	4
20	direction	4

The Network Traffic data model can be extended with these data fields:

- **`community_id`:** Is an open source capability developed by Corelight that generates a hash to represent each network flow (akin to a database foreign key). The hash can be used to quickly pivot between the data from multiple security tools with a quick single search.
- **`uid`:** Unique identifier of connection linking the connection summary log to the protocol specific log(s)
- **`history`:** TCP/UDP history between hosts in a connection
- **`conn_state`:** A summarized history state for each connection
- **`local_orig`:** True if connection originated locally
- **`local_resp`:** True if connection responded locally

Network Resolutions (DNS): Corelight data populates all of the most commonly used fields in the Network Resolution Data Model. You won't find a better data set for Splunk Enterprise Security DNS correlation searches.



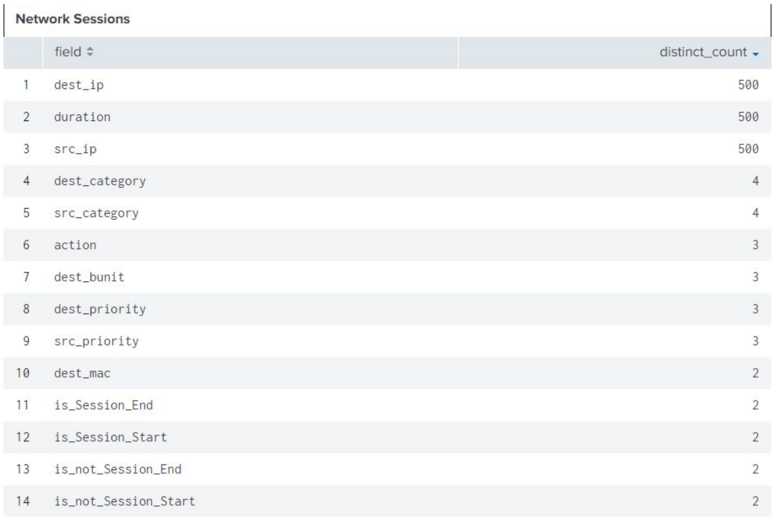
Network Resolution DNS

	field ⇕	distinct_count ▾
1	answer	500
2	query	500
3	src_port	500
4	query_length	334
5	src	163
6	dest	136
7	answer_length	60
8	answer_count	25
9	record_type	14
10	reply_code	5
11	reply_code_id	5
12	dest_port	4
13	dest_bunit	2
14	dest_category	2
15	dest_priority	2
16	src_category	2
17	src_priority	2

The Network Resolution data model can be extended with these data fields:

- **`answer_count:`** The number of answers returned by the DNS server. Note that multiple answers being returned is a common feature of modern DNS load-balancing schemes.
- **`answer_length:`** Size in characters of the string representation of the DNS answer (i.e. "8.8.8.8" = 7, "s0-2mdn-net.l.google.com" = 24). Only available when answer_count = 1.
- **`query_count:`** The number of queries sent in the DNS request by the client. Note that it is rare for clients to send multiple queries in a single packet on the modern Internet.
- **`dns_any:`** A flag set to true if a DNS client requests all record types for a domain at once. This is uncommon behavior similar to a zone transfer, that often indicates reconnaissance against a target.

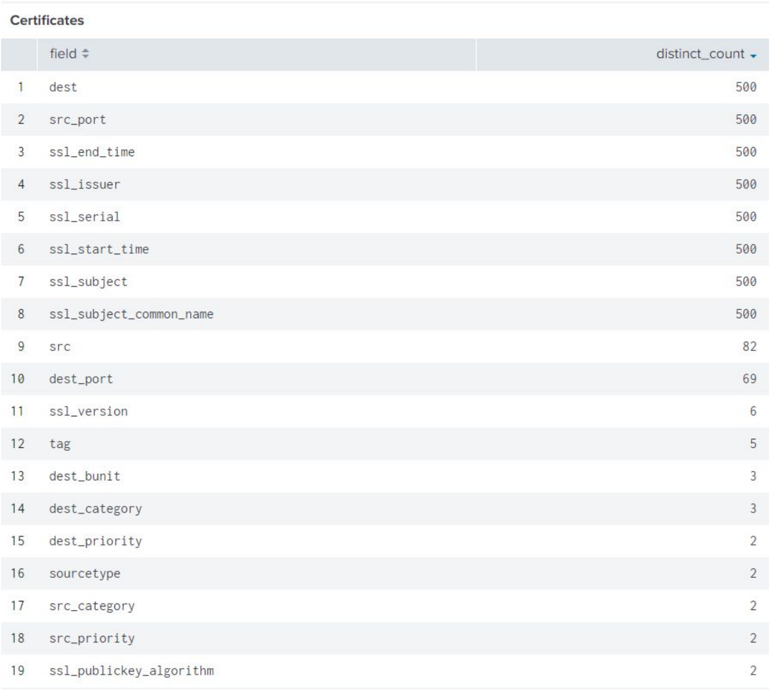
Network Sessions: Corelight data populates the commonly used fields in correlation searches based on the Network Sessions model.



Network Sessions

	field	distinct_count
1	dest_ip	500
2	duration	500
3	src_ip	500
4	dest_category	4
5	src_category	4
6	action	3
7	dest_bunit	3
8	dest_priority	3
9	src_priority	3
10	dest_mac	2
11	is_Session_End	2
12	is_Session_Start	2
13	is_not_Session_End	2
14	is_not_Session_Start	2

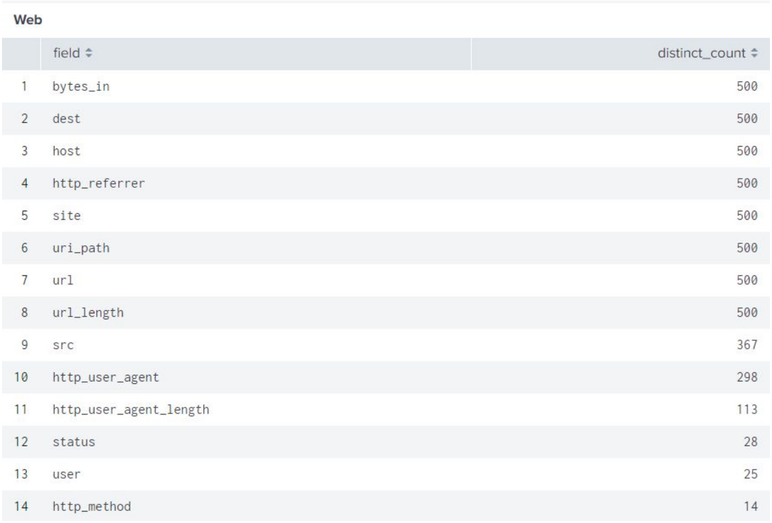
Certificates: Corelight data populates the most commonly used fields in correlation searches based on the Certificates data model.



Certificates

	field	distinct_count
1	dest	500
2	src_port	500
3	ssl_end_time	500
4	ssl_issuer	500
5	ssl_serial	500
6	ssl_start_time	500
7	ssl_subject	500
8	ssl_subject_common_name	500
9	src	82
10	dest_port	69
11	ssl_version	6
12	tag	5
13	dest_bunit	3
14	dest_category	3
15	dest_priority	2
16	sourcetype	2
17	src_category	2
18	src_priority	2
19	ssl_publickey_algorithm	2

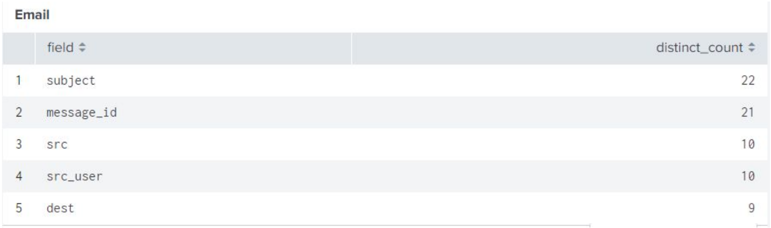
Web: Corelight data populates the most commonly used fields in correlation searches based on the Web data model.



Web

	field ≑	distinct_count ≑
1	bytes_in	500
2	dest	500
3	host	500
4	http_referrer	500
5	site	500
6	uri_path	500
7	url	500
8	url_length	500
9	src	367
10	http_user_agent	298
11	http_user_agent_length	113
12	status	28
13	user	25
14	http_method	14

Email: Corelight data populates the some commonly used fields in correlation searches based on the Email data model.



Email

	field ≑	distinct_count ≑
1	subject	22
2	message_id	21
3	src	10
4	src_user	10
5	dest	9

Get the most from Splunk ES using Corelight

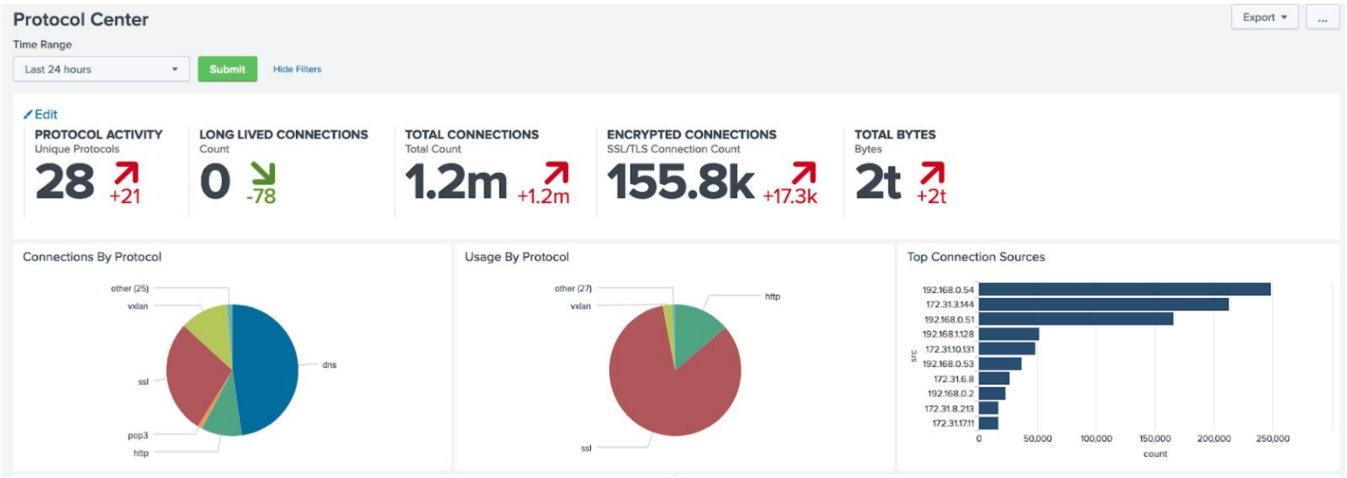
Data from Corelight Sensors illuminates all things communicating on the enterprise network. This data immediately improves the Splunk ES dashboards through easy to enable Correlation searches. The following sections highlight the data available.

Dashboards

Security intelligence dashboards sections for Protocol Intelligence, Threat Intelligence, and Web Intelligence will populate out of the box based on Corelight data. Most of the dashboards in Security Domains for Networks will also populate out of the box.

Security Intelligence

Protocol Center

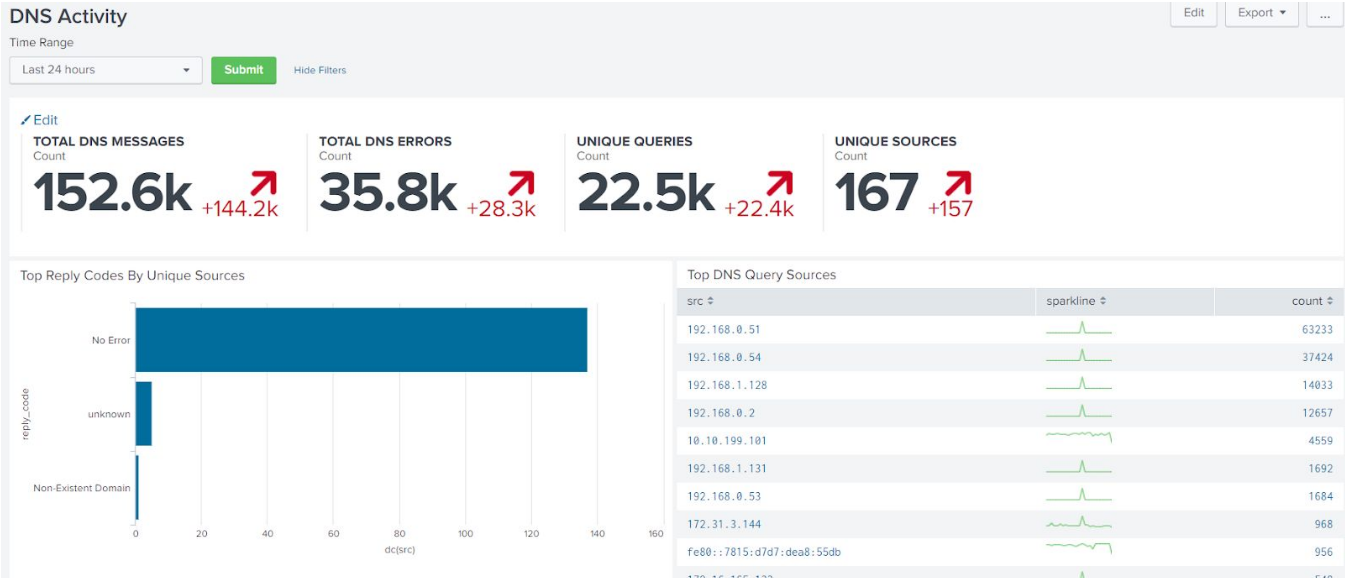


Protocol Center

Time Range: Last 24 hours

PROTOCOL ACTIVITY	LONG LIVED CONNECTIONS	TOTAL CONNECTIONS	ENCRYPTED CONNECTIONS	TOTAL BYTES
Unique Protocols	Count	Total Count	SSL/TLS Connection Count	Bytes
28 ↗ +21	0 ↘ -78	1.2m ↗ +1.2m	155.8k ↗ +17.3k	2t ↗ +2t

Protocol > DNS Activity



DNS Activity

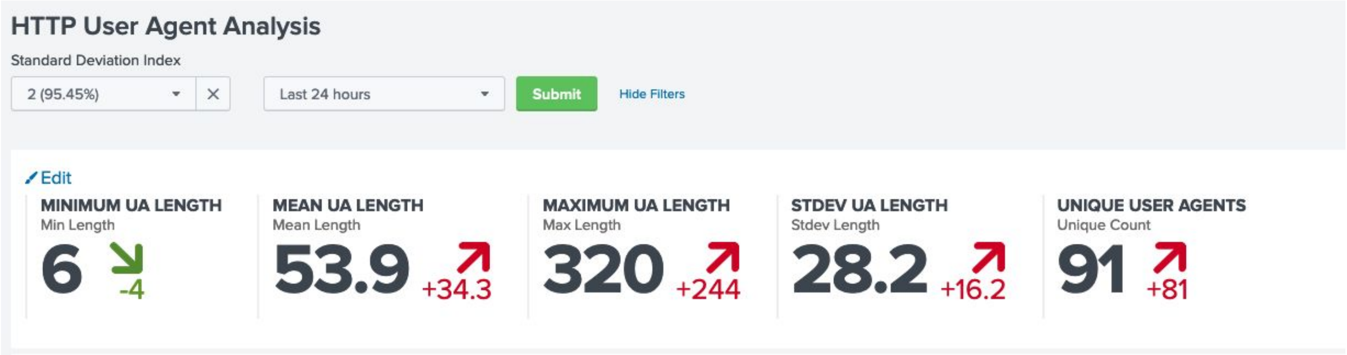
Time Range: Last 24 hours

TOTAL DNS MESSAGES	TOTAL DNS ERRORS	UNIQUE QUERIES	UNIQUE SOURCES
Count	Count	Count	Count
152.6k ↗ +144.2k	35.8k ↗ +28.3k	22.5k ↗ +22.4k	167 ↗ +157

Top DNS Query Sources

src	sparkline	count
192.168.0.51		63233
192.168.0.54		37424
192.168.1.128		14033
192.168.0.2		12657
10.10.199.101		4559
192.168.1.131		1692
192.168.0.53		1684
172.31.3.144		968
fe80::7815:d7d7:dea8:55db		956

Web Intelligence > HTTP User Agent Analysis



HTTP User Agent Analysis

Standard Deviation Index: 2 (95.45%)

Last 24 hours

MINIMUM UA LENGTH
Min Length
6 -4

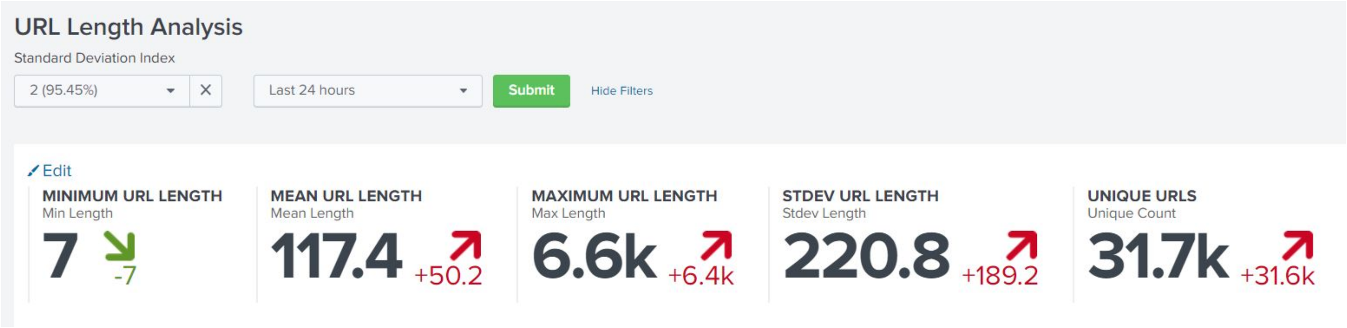
MEAN UA LENGTH
Mean Length
53.9 +34.3

MAXIMUM UA LENGTH
Max Length
320 +244

STDEV UA LENGTH
Stdev Length
28.2 +16.2

UNIQUE USER AGENTS
Unique Count
91 +81

Web Intelligence > URL Length Analysis



URL Length Analysis

Standard Deviation Index: 2 (95.45%)

Last 24 hours

MINIMUM URL LENGTH
Min Length
7 -7

MEAN URL LENGTH
Mean Length
117.4 +50.2

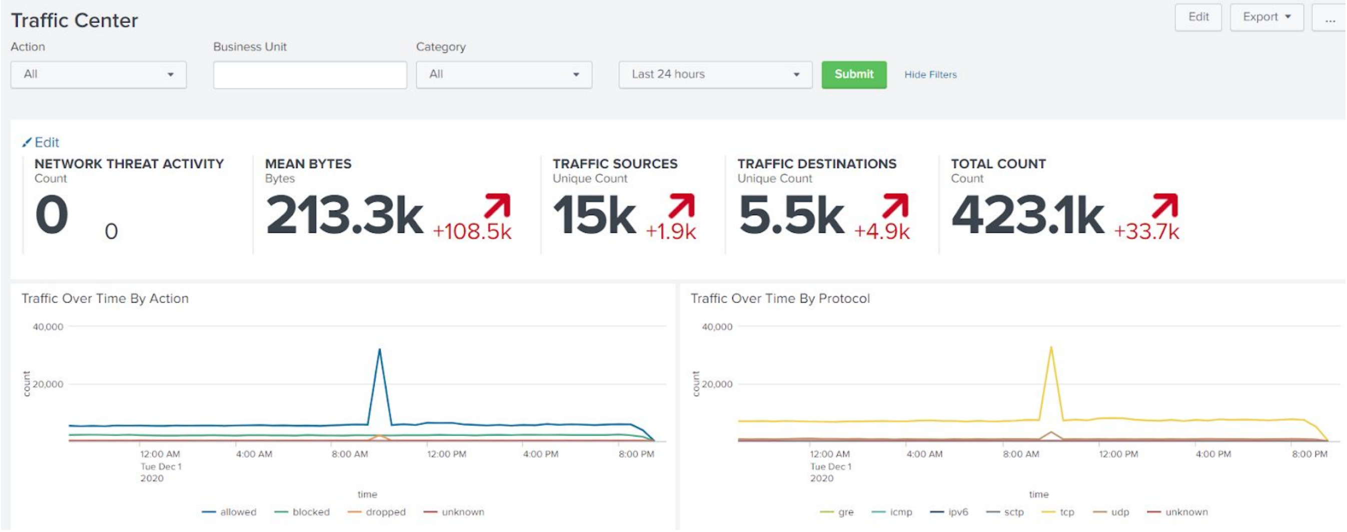
MAXIMUM URL LENGTH
Max Length
6.6k +6.4k

STDEV URL LENGTH
Stdev Length
220.8 +189.2

UNIQUE URLS
Unique Count
31.7k +31.6k

Security Domains

Network > Traffic Center



Traffic Center

Action: All

Business Unit:

Category: All

Last 24 hours

NETWORK THREAT ACTIVITY
Count
0 0

MEAN BYTES
Bytes
213.3k +108.5k

TRAFFIC SOURCES
Unique Count
15k +1.9k

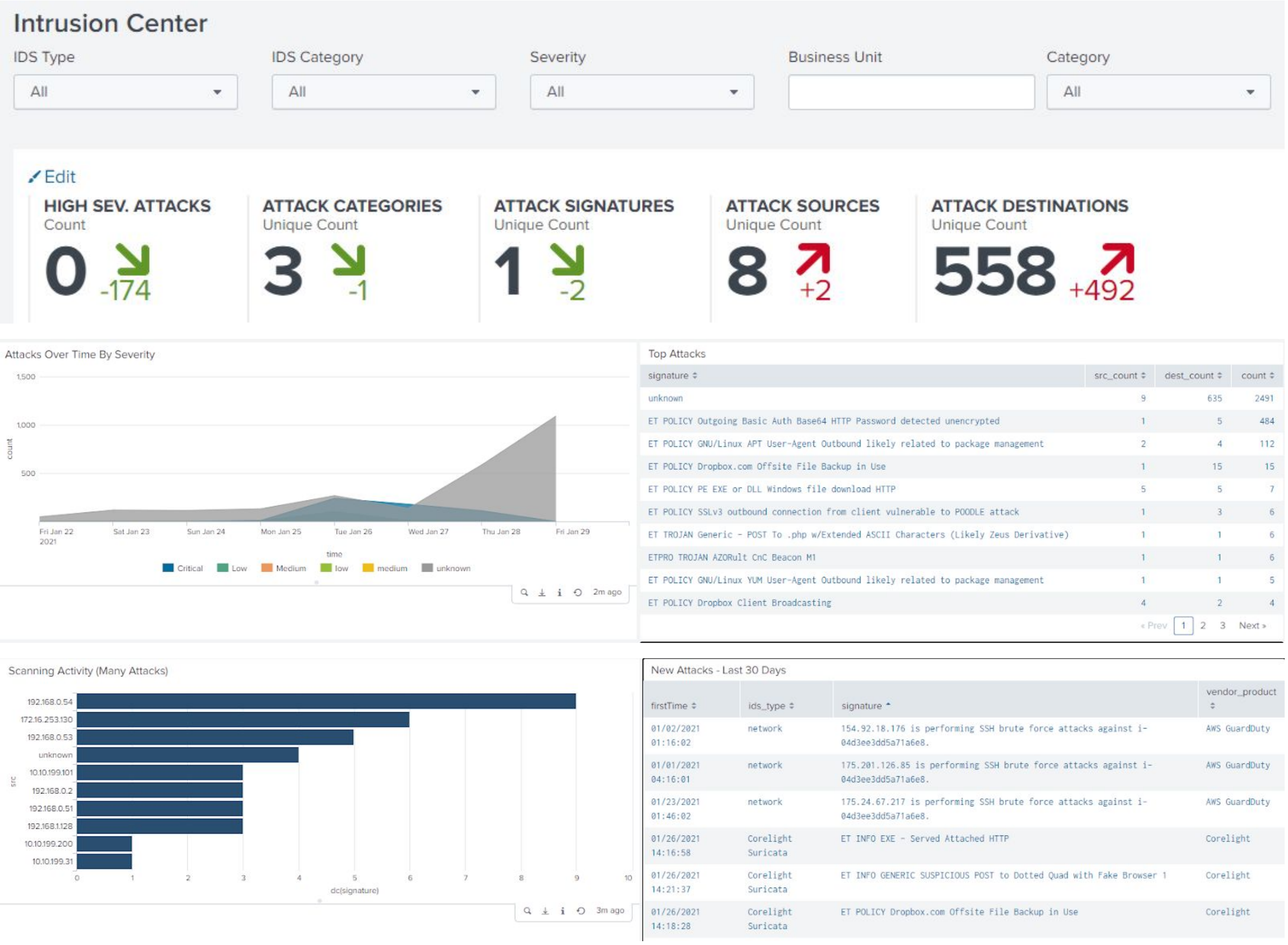
TRAFFIC DESTINATIONS
Unique Count
5.5k +4.9k

TOTAL COUNT
Count
423.1k +33.7k

Traffic Over Time By Action

Traffic Over Time By Protocol

Intrusion Center



IDS Type: All

IDS Category: All

Severity: All

Business Unit:

Category: All

HIGH SEV. ATTACKS Count	ATTACK CATEGORIES Unique Count	ATTACK SIGNATURES Unique Count	ATTACK SOURCES Unique Count	ATTACK DESTINATIONS Unique Count
0 ↘ -174	3 ↘ -1	1 ↘ -2	8 ↗ +2	558 ↗ +492

Top Attacks

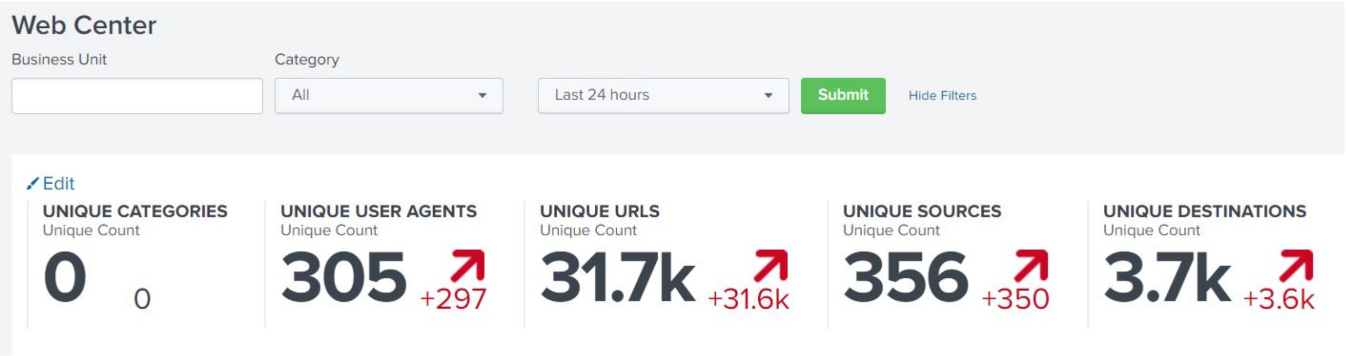
signature ⇕	src_count ⇕	dest_count ⇕	count ⇕
unknown	9	635	2491
ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	1	5	484
ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	2	4	112
ET POLICY Dropbox.com Offsite File Backup in Use	1	15	15
ET POLICY PE EXE or DLL Windows file download HTTP	5	5	7
ET POLICY SSLv3 outbound connection from client vulnerable to POODLE attack	1	3	6
ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)	1	1	6
ETPRO TROJAN AZORult CnC Beacon M1	1	1	6
ET POLICY GNU/Linux YUM User-Agent Outbound likely related to package management	1	1	5
ET POLICY Dropbox Client Broadcasting	4	2	4

« Prev 1 2 3 Next »

New Attacks - Last 30 Days

firstTime ⇕	ids_type ⇕	signature ▲	vendor_product ⇕
01/02/2021 01:16:02	network	154.92.18.176 is performing SSH brute force attacks against i-04d3ee3dd5a71a6e8.	AWS GuardDuty
01/01/2021 04:16:01	network	175.201.126.85 is performing SSH brute force attacks against i-04d3ee3dd5a71a6e8.	AWS GuardDuty
01/23/2021 01:46:02	network	175.24.67.217 is performing SSH brute force attacks against i-04d3ee3dd5a71a6e8.	AWS GuardDuty
01/26/2021 14:16:58	Corelight Suricata	ET INFO EXE - Served Attached HTTP	Corelight
01/26/2021 14:21:37	Corelight Suricata	ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1	Corelight
01/26/2021 14:18:28	Corelight Suricata	ET POLICY Dropbox.com Offsite File Backup in Use	Corelight

Network > Web Center



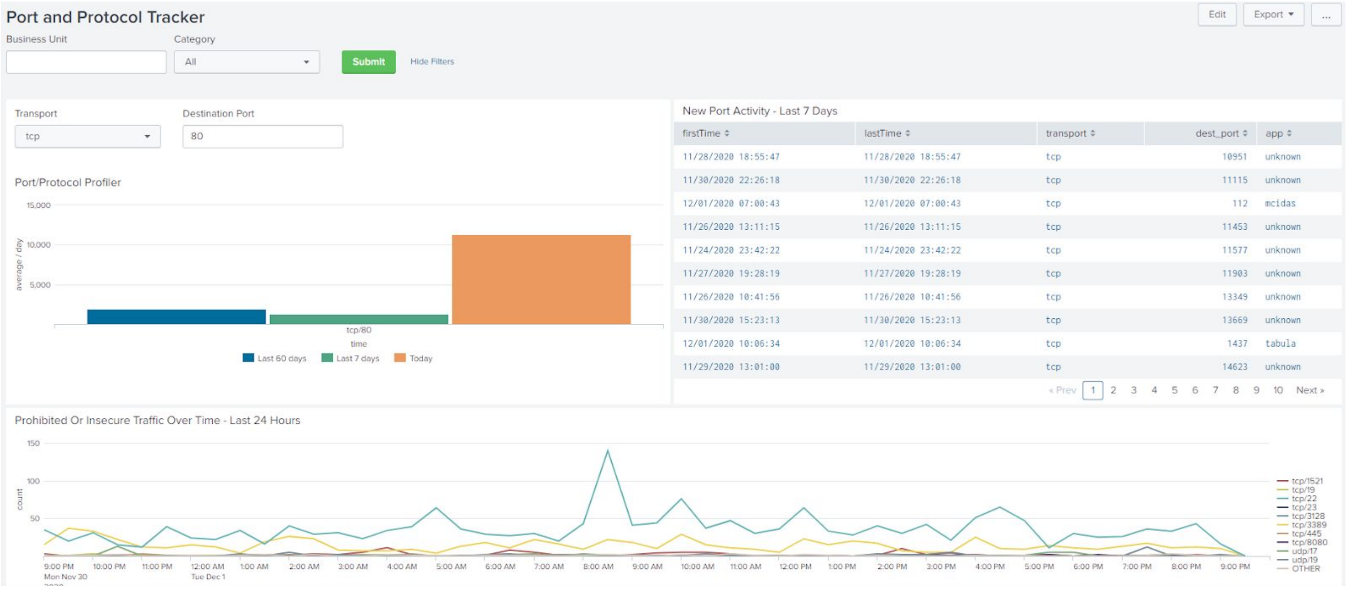
Business Unit:

Category: All

Last 24 hours

UNIQUE CATEGORIES Unique Count	UNIQUE USER AGENTS Unique Count	UNIQUE URLS Unique Count	UNIQUE SOURCES Unique Count	UNIQUE DESTINATIONS Unique Count
0 0	305 ↗ +297	31.7k ↗ +31.6k	356 ↗ +350	3.7k ↗ +3.6k

Network > Port and Protocol Tracker



Port and Protocol Tracker

Business Unit:

Category: All

Transport: tcp

Destination Port: 80

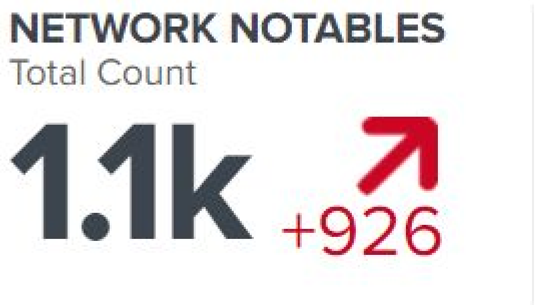
Port/Protocol Profiler

New Port Activity - Last 7 Days

firstTime ⇕	lastTime ⇕	transport ⇕	dest_port ⇕	app ⇕
11/28/2020 18:55:47	11/28/2020 18:55:47	tcp	10951	unknown
11/30/2020 22:26:18	11/30/2020 22:26:18	tcp	11115	unknown
12/01/2020 07:00:43	12/01/2020 07:00:43	tcp	112	mcidas
11/26/2020 13:11:15	11/26/2020 13:11:15	tcp	11453	unknown
11/24/2020 23:42:22	11/24/2020 23:42:22	tcp	11577	unknown
11/27/2020 19:28:19	11/27/2020 19:28:19	tcp	11903	unknown
11/26/2020 10:41:56	11/26/2020 10:41:56	tcp	13349	unknown
11/30/2020 15:23:13	11/30/2020 15:23:13	tcp	13669	unknown
12/01/2020 10:06:34	12/01/2020 10:06:34	tcp	1437	tabula
11/29/2020 13:01:00	11/29/2020 13:01:00	tcp	14623	unknown

Prohibited Or Insecure Traffic Over Time - Last 24 Hours

Because of the security rich metadata contained in the Corelight data, Splunk ES administrators will immediately see NETWORK NOTABLES of the Security Posture dashboard start to grow as soon as Correlation Searches are enabled.



NETWORK NOTABLES

Total Count

1.1k +926

Correlation Searches

Network, web, certificates, and other correlation searches can be enabled and tuned out of the box using Corelight data. Corelight data feeds advanced and unique correlation searches, increasing Splunk network detection capabilities. The Corelight metadata and insights when paired with Splunk data models are excellent for Machine Learning and UEBA workflows.

Security domain	Title
endpoint	Endpoint - Host Sending Excessive Email - Rule
network	ESCU - Clients Connecting to Multiple DNS Servers - Rule
network	ESCU - Detect DNS requests to Phishing Sites leveraging EvilGinx2 - Rule
network	ESCU - Detect hosts connecting to dynamic domain providers - Rule
network	ESCU - Detect Long DNS TXT Record Response - Rule
network	ESCU - Detection of DNS Tunnels - Rule
network	ESCU - DNS Query Length Outliers - MLTK - Rule
network	ESCU - DNS Query Length With High Standard Deviation - Rule
network	ESCU - DNS Query Requests Resolved by Unauthorized DNS Servers - Rule
network	ESCU - DNS record changed - Rule
network	ESCU - Email servers sending high volume traffic to hosts - Rule
network	ESCU - Excessive DNS Failures - Rule
network	ESCU - Hosts receiving high volume of network traffic from email server - Rule
network	ESCU - Large Volume of DNS ANY Queries - Rule
network	ESCU - Monitor DNS For Brand Abuse - Rule
network	ESCU - Prohibited Network Traffic Allowed - Rule
network	ESCU - Protocol or Port Mismatch - Rule
network	ESCU - Protocols passing authentication in cleartext - Rule
network	ESCU - Remote Desktop Network Bruteforce - Rule
network	ESCU - Remote Desktop Network Traffic - Rule
network	ESCU - Suspicious Email Attachment Extensions - Rule
identity	Identity - High Volume Email Activity with Non-corporate Domains - Rule
network	Network - Detect DNS connections to external DNS devices - Rule
network	Network - Detect DNS on non-standard port - Rule
network	Network - Excessive DNS Failures - Rule

network	Network - Excessive DNS Queries - Rule
network	Network - Excessive HTTP Failure Responses - Rule
network	Network - Substantial Increase in Port Activity (By Destination) - Rule
network	Network - Unapproved Port Activity Detected - Rule
network	Network - Unroutable Host Activity - Rule
network	Web - Abnormally High Number of HTTP Method Events By Src - Rule