DIGIHUNT

Network Threat Detector

DIGINTRUDE

Introduction

A Network Threat Detection & Analysis is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms. Although Network Threat Detection & Analysis systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their Network Threat Detection & Analysis when they first install them. It means properly setting up the threat detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Overview

Digihunt is one of its kind Network Threat Detection and Analysis tool solution provides complete comprehensive visibility to your network traffic and malicious incidents occur on the network and normally stay undetected by perimeter devices. This solution gives an in-depth analytics view for all types of Inbound and Outbound traffic after identifying the intrusions successfully. On a successfully configured tapped network Digihunt signature needs to be fine-tuned by the IT team to reduced false-positives alerts.

Hardware Requirements

Architecture

Digihunt only supports x86-64 architecture (standard Intel/AMD 64-bit processors). Sorry, we do not support ARM or other processors!

Elastic Stack

If you are going to enable the Elastic Stack, please note that the MINIMUM requirements are 4 CPU cores and 12GB RAM. These requirements increase as you monitor more traffic and consume more logs.

We recommend placing all Elastic storage on SSD or fast spinning disk in a RAID10 configuration.

Standalone Deployments

In a standalone deployment, the master server components and the sensor components all run on a single box, your hardware requirements will reflect that. This deployment type is recommended for evaluation purposes, POC (proof-of-concept) and small to medium size single sensor deployment. Although you can deploy Digihunt in this manner, it is recommended that you separate the backend components and sensor components.

- CPU: Used to parse incoming events, index incoming events, search metadata, capture logs, analyze packets, and run the frontend components. As data and event consumption increases, a greater amount of CPU will be required.
- RAM: Used for Logstash, Elasticsearch, disk cache for Lucene, Suricata. The amount of available RAM will directly impact search speeds and reliability, as well as the ability to process and capture traffic.
- Disk: Used for storage of indexed metadata. A larger amount of storage allows for a longer retention period. It is typically recommended to retain no more than 30 days of hot ES indices.

Virtualization

We recommend dedicated physical hardware (especially if you are monitoring lots of traffic) to avoid competing for resources. Sensors can be virtualized, but you'll have to ensure that they are allocated sufficient resources.

CPU

Suricata is very CPU intensive. The more traffic you are monitoring, the more CPU cores you'll need. A very rough ballpark estimate would 100Mbps per Suricata instance. So, if you have a fully saturated 1 Gbps link and are running Suricata, then you'll want at least 10 Suricata instances which means you'll need at least 5 CPU cores for Suricata with additional CPU cores for other services.

RAM

RAM usage is highly dependent on several variables:

- The services that you enable
- The kinds of traffic you're monitoring (example: you may be monitoring a 1Gbps link but it's only using 200Mbps most of the time)
- The amount of packet loss that is "acceptable" to your organization

For best performance, over provision RAM so that you can fully disable swap.

Storage

Sensors that have full packet capture enabled need LOTS of storage. For example, suppose you are monitoring a link that averages 50Mbps, here are some quick calculations: 50Mb/s =6.25 MB/s= 375 MB/minute=22,500 MB/hour = 540,000 MB/day. So, you're going to need about 540GB for one day's worth of pcaps (multiply this by the number of days you want to keep on disk for investigative/forensic purpose). The more disk space you have, the more PCAP retention you'll have for doing investigations after the fact. The disk is cheap, get all you can!

NIC

You'll need at least two wired network interfaces: one for management (preferably connected to a dedicated management network) and then one or more of sniffing (connected to tap or span).

Use Cases

IP Packets

Security analysts can easily identify IP packet traffic like

a. the types of network traffic flowing over it,
b. who are flow talker & connectivity statistics
c. chart between devices connected to our network.

Anomaly Detection

Anomaly-based network intrusion detection plays a vital role in protecting networks against malicious activities. In recent years, data mining techniques have gained importance in addressing security issues in the network. Digihunt Intrusion Detection and Analysis System aim to identify intrusions with a low false alarm rate and a high detection rate.

Network behavior is the major parameter on which the anomaly detection systems rely upon. If the network behavior is within the predefined behavior, then the network transaction is accepted or else it triggers the alert in the anomaly detection systems. Acceptable network performance can be either predetermined or learned through specifications or conditions defined by the network administrator.

Signature Recognition

Network-level threats can be detected and category according to the different threat categories based on 29000 + signature by emerging threat.

Alert System and Reports

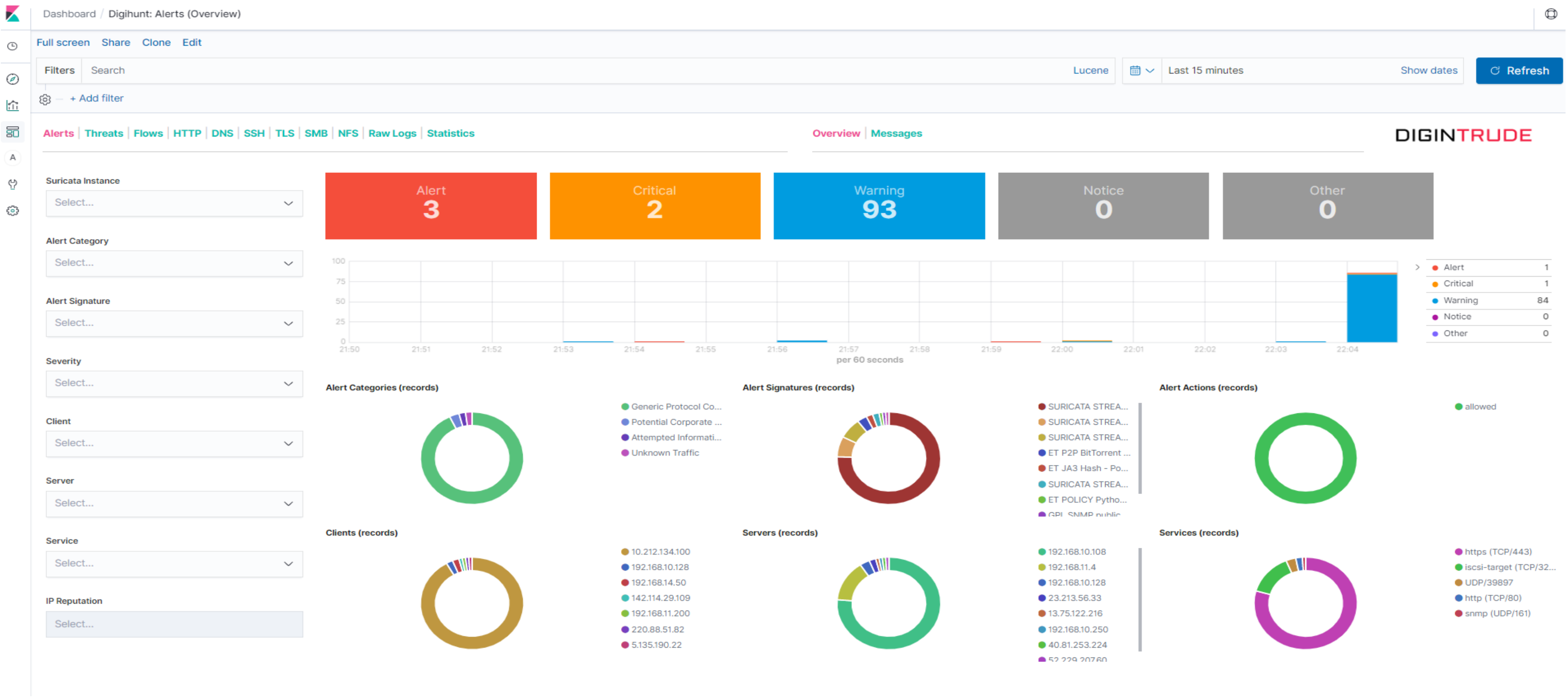
It has an alerting system to notify security analyst with various detection methods defined by the analyst to observe malicious traffic and take action according to corporate best practices, Standards & Controls. (Remove email-based notification & notify analyst regularly)

Dashboards

The following dashboards are provided.

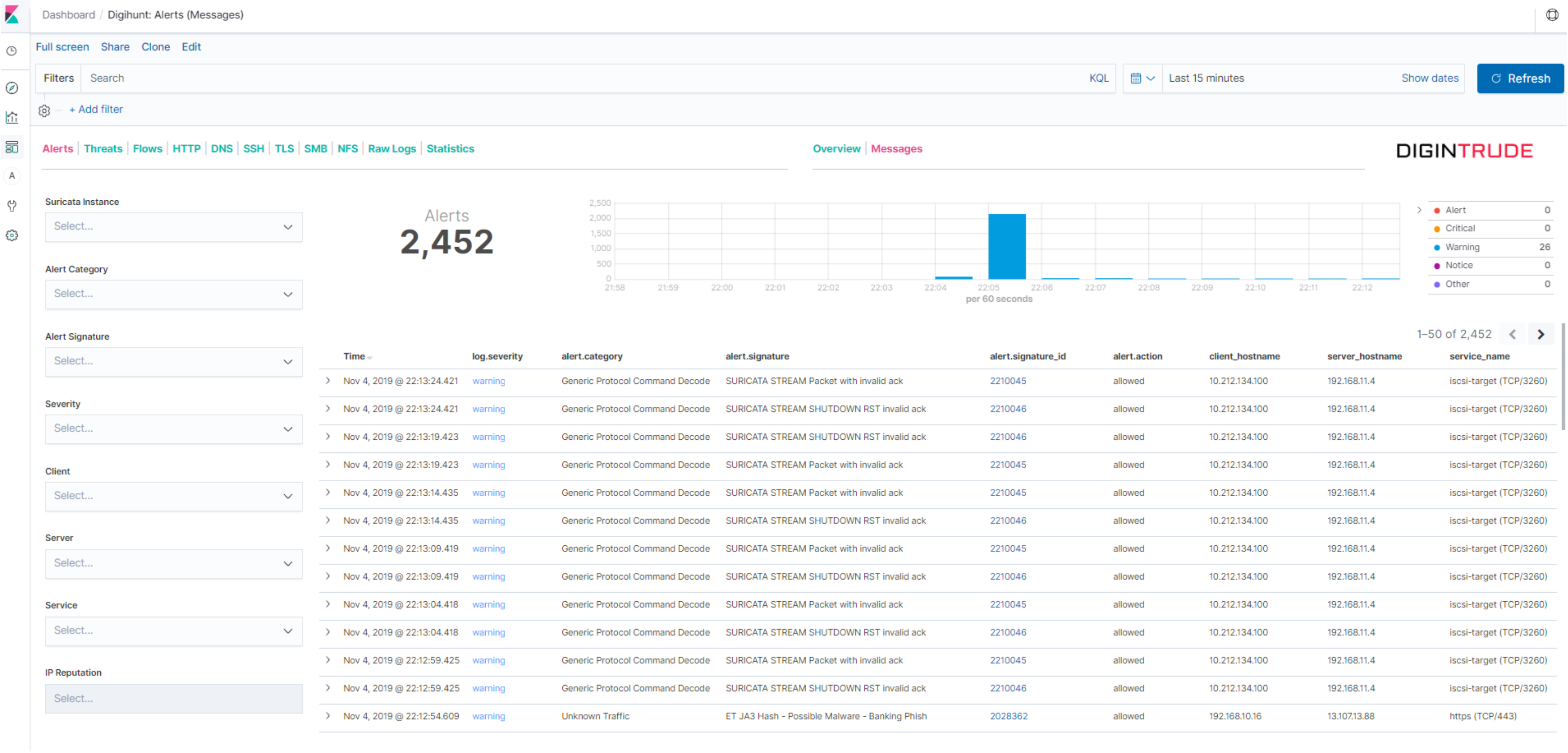
Suspicious Incidents - Overview

Complete visibility to the tapped network incidents been categorized on Priority of e.g. Alert, Critical, Warning, Notice, and Others. This Dashboard visualizes incident history as well as real-time analysis view of aggregated incidences detected by Digihunt.



Suspicious Incidents – Messages

This feature in the dashboard shows all the severities detected by Digihunt with a fine-tuned filtering system and timespan of the incident. A comprehensive analysis can be done to a particular type of suspicious activity using a messages tab.



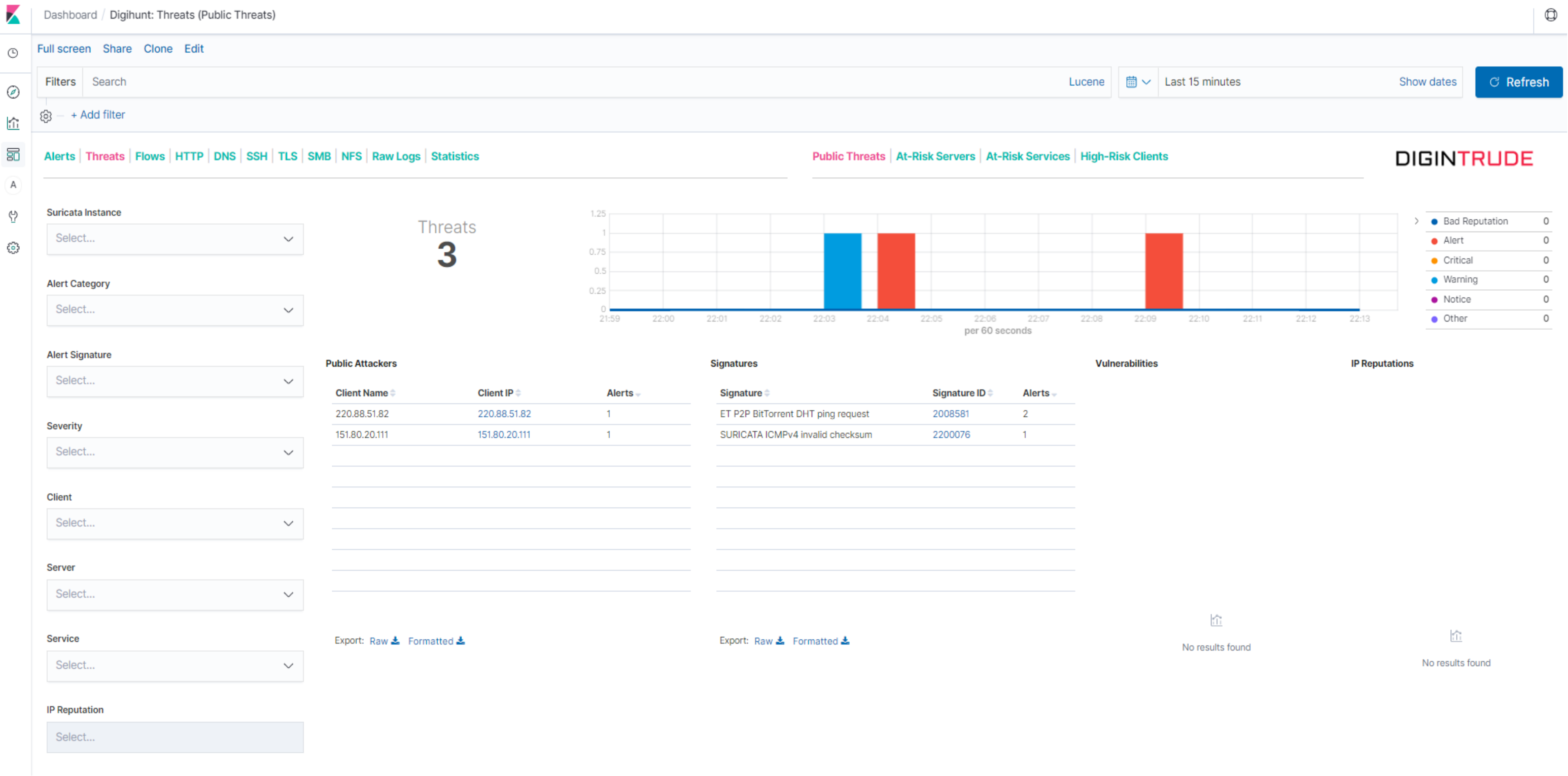
Alerts

2,452

Time	log.severity	alert.category	alert.signature	alert.signature_id	alert.action	client_hostname	server_hostname	service_name
Nov 4, 2019 @ 22:13:24.421	warning	Generic Protocol Command Decode	SURICATA STREAM Packet with invalid ack	2210045	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:13:24.421	warning	Generic Protocol Command Decode	SURICATA STREAM SHUTDOWN RST invalid ack	2210046	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:13:19.423	warning	Generic Protocol Command Decode	SURICATA STREAM SHUTDOWN RST invalid ack	2210046	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:13:19.423	warning	Generic Protocol Command Decode	SURICATA STREAM Packet with invalid ack	2210045	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:13:14.435	warning	Generic Protocol Command Decode	SURICATA STREAM Packet with invalid ack	2210045	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:13:14.435	warning	Generic Protocol Command Decode	SURICATA STREAM SHUTDOWN RST invalid ack	2210046	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:13:09.419	warning	Generic Protocol Command Decode	SURICATA STREAM Packet with invalid ack	2210045	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:13:09.419	warning	Generic Protocol Command Decode	SURICATA STREAM SHUTDOWN RST invalid ack	2210046	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:13:04.418	warning	Generic Protocol Command Decode	SURICATA STREAM Packet with invalid ack	2210045	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:13:04.418	warning	Generic Protocol Command Decode	SURICATA STREAM SHUTDOWN RST invalid ack	2210046	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:12:59.425	warning	Generic Protocol Command Decode	SURICATA STREAM Packet with invalid ack	2210045	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:12:59.425	warning	Generic Protocol Command Decode	SURICATA STREAM SHUTDOWN RST invalid ack	2210046	allowed	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)
Nov 4, 2019 @ 22:12:54.609	warning	Unknown Traffic	ET JA3 Hash - Possible Malware - Banking Phish	2028362	allowed	192.168.10.16	13.107.13.88	https (TCP/443)

Threats - Public Attackers

The public threat tab visualizes the incident detected by our Digihunt engine through signature and behavioral anomalies. It detects suspicious public IP talkers according to the severities. This also draws a statistical analysis view of history time span and real-time public IP traffics.



● Bad Reputation	0
● Alert	0
● Critical	0
● Warning	0
● Notice	0
● Other	0

Suricata Instance: Select...

Alert Category: Select...

Alert Signature: Select...

Severity: Select...

Client: Select...

Server: Select...

Service: Select...

IP Reputation: Select...

Public Attackers

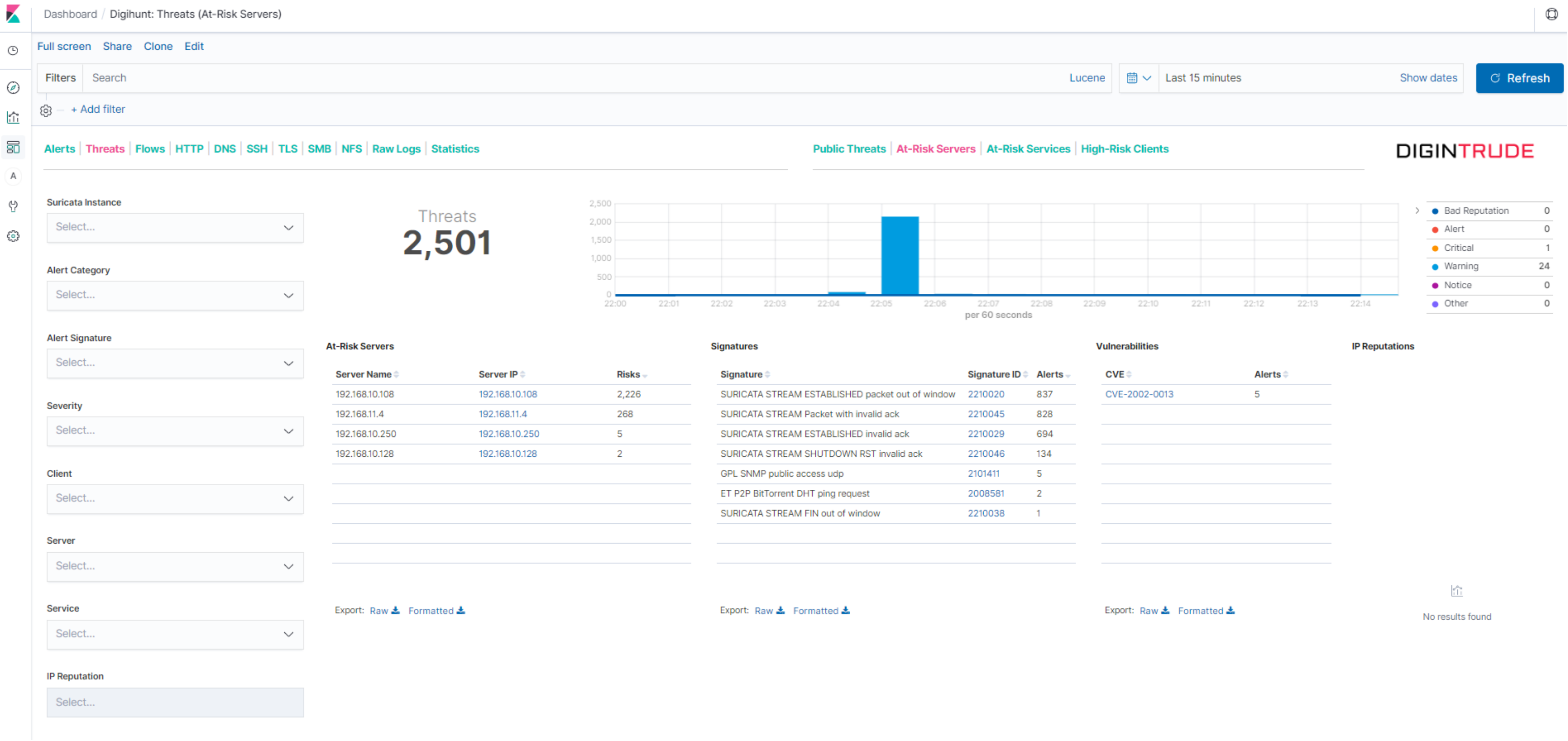
Client Name	Client IP	Alerts
220.88.51.82	220.88.51.82	1
151.80.20.111	151.80.20.111	1

Signatures

Signature	Signature ID	Alerts
ET P2P BitTorrent DHT ping request	2008581	2
SURICATA ICMPv4 invalid checksum	2200076	1

Threats - At-Risk Servers

At-Risk Servers tab visualize the incident detected by our Digihunt engine through signature and behavioral anomalies. It detects suspicious Internal IP talkers according to the severities and Risk Counts. This also draws a statistical analysis view of history time span and real-time Internal IP traffics.



● Bad Reputation	0
● Alert	0
● Critical	1
● Warning	24
● Notice	0
● Other	0

At-Risk Servers

Server Name	Server IP	Risks
192.168.10.108	192.168.10.108	2,226
192.168.11.4	192.168.11.4	268
192.168.10.250	192.168.10.250	5
192.168.10.128	192.168.10.128	2

Export: Raw Formatted

Signatures

Signature	Signature ID	Alerts
SURICATA STREAM ESTABLISHED packet out of window	2210020	837
SURICATA STREAM Packet with invalid ack	2210045	828
SURICATA STREAM ESTABLISHED invalid ack	2210029	694
SURICATA STREAM SHUTDOWN RST invalid ack	2210046	134
GPL SNMP public access udp	2101411	5
ET P2P BitTorrent DHT ping request	2008581	2
SURICATA STREAM FIN out of window	2210038	1

Export: Raw Formatted

Vulnerabilities

CVE	Alerts
CVE-2002-0013	5

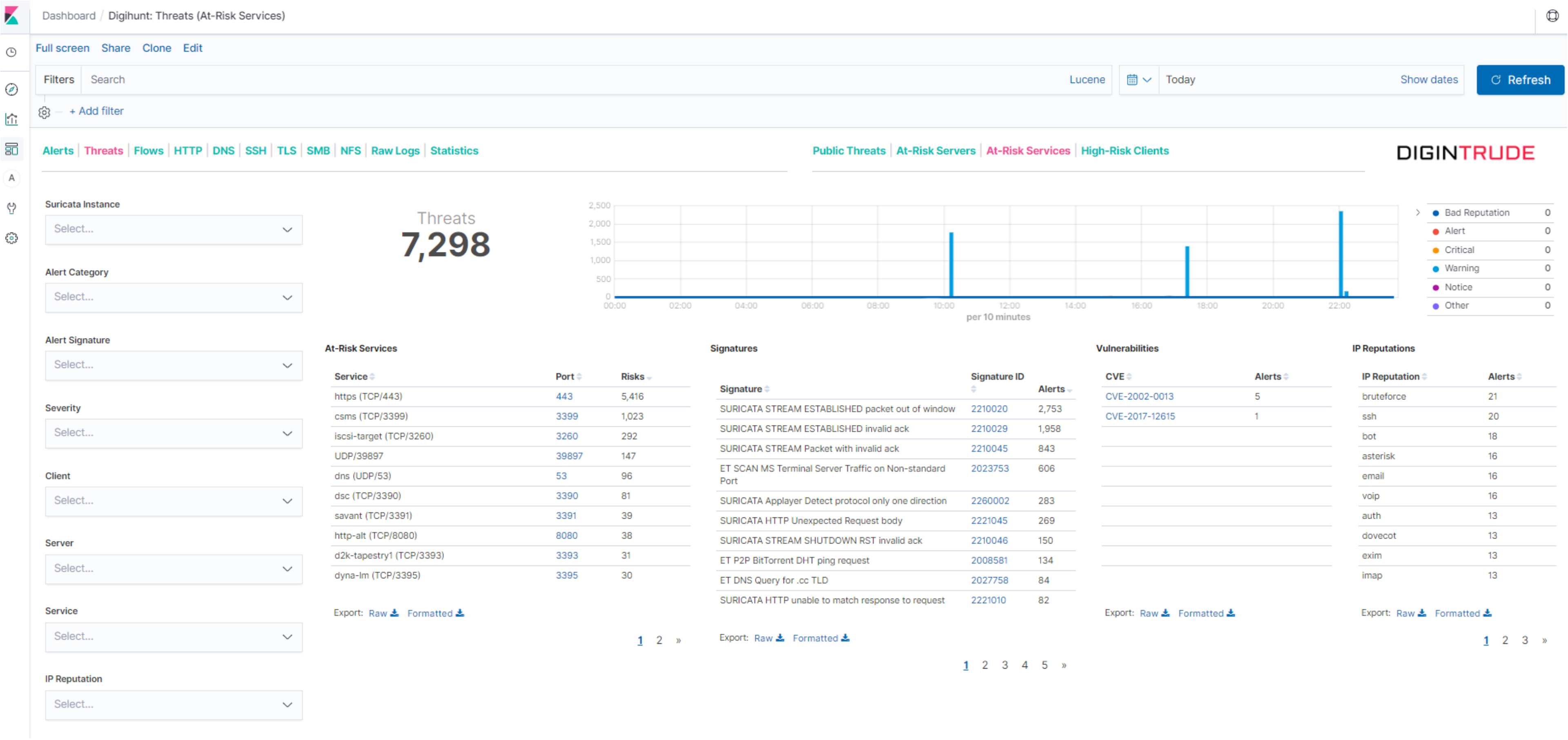
Export: Raw Formatted

IP Reputations

No results found

Threats - At-Risk Services

At-Risk Services tab visualizes the incident detected by our Digihunt engine through signature and behavioral anomalies. It detects suspicious Internal ports open on various end devices according to the severities and Risk Counts. This also draws a statistical analysis view of history time span and real-time Internal IP traffics.



At-Risk Services

Service	Port	Risks
https (TCP/443)	443	5,416
csms (TCP/3399)	3399	1,023
iscsi-target (TCP/3260)	3260	292
UDP/39897	39897	147
dns (UDP/53)	53	96
dsc (TCP/3390)	3390	81
savant (TCP/3391)	3391	39
http-alt (TCP/8080)	8080	38
d2k-tapestry1 (TCP/3393)	3393	31
dyna-lm (TCP/3395)	3395	30

Export: Raw Formatted

1 2 »

Signatures

Signature	Signature ID	Alerts
SURICATA STREAM ESTABLISHED packet out of window	2210020	2,753
SURICATA STREAM ESTABLISHED invalid ack	2210029	1,958
SURICATA STREAM Packet with invalid ack	2210045	843
ET SCAN MS Terminal Server Traffic on Non-standard Port	2023753	606
SURICATA Applayer Detect protocol only one direction	2260002	283
SURICATA HTTP Unexpected Request body	2221045	269
SURICATA STREAM SHUTDOWN RST invalid ack	2210046	150
ET P2P BitTorrent DHT ping request	2008581	134
ET DNS Query for .cc TLD	2027758	84
SURICATA HTTP unable to match response to request	2221010	82

Export: Raw Formatted

1 2 3 4 5 »

Vulnerabilities

CVE	Alerts
CVE-2002-0013	5
CVE-2017-12615	1

Export: Raw Formatted

IP Reputations

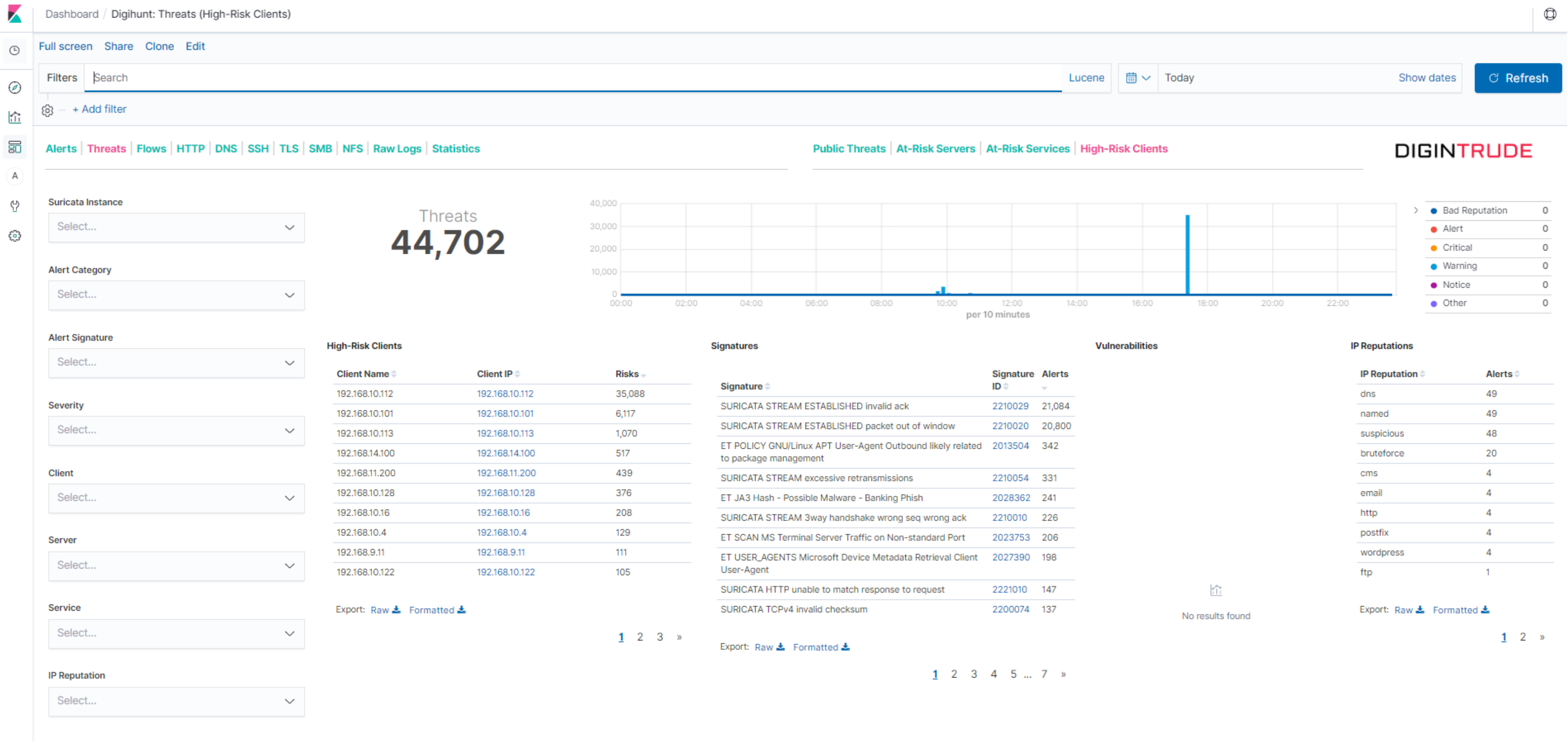
IP Reputation	Alerts
bruteforce	21
ssh	20
bot	18
asterisk	16
email	16
voip	16
auth	13
dovecot	13
exim	13
imap	13

Export: Raw Formatted

1 2 3 »

Threats - High-Risk Clients

High-Risk Clients tab visualize the incident detected by our Digihunt engine through signature and behavioral anomalies. It detects suspicious high-risk end devices according to risk counts and disclosed alerts. This also draws a statistical analysis view of history time span and real-time Internal IP traffics.



Dashboard / Digihunt: Threats (High-Risk Clients)
Full screen
Share
Clone
Edit
Filters
Search
Lucene
Today
Show dates
Refresh
+ Add filter
Alerts | Threats | Flows | HTTP | DNS | SSH | TLS | SMB | NFS | Raw Logs | Statistics
Public Threats | At-Risk Servers | At-Risk Services | High-Risk Clients
DIGINTRUDE
40,000
30,000
20,000
10,000
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
per 10 minutes

Suricata Instance: Select...

Alert Category: Select...

Alert Signature: Select...

Severity: Select...

Client: Select...

Server: Select...

Service: Select...

IP Reputation: Select...

Threats
44,702

● Bad Reputation	0
● Alert	0
● Critical	0
● Warning	0
● Notice	0
● Other	0

High-Risk Clients

Client Name	Client IP	Risks
192.168.10.112	192.168.10.112	35,088
192.168.10.101	192.168.10.101	6,117
192.168.10.113	192.168.10.113	1,070
192.168.14.100	192.168.14.100	517
192.168.11.200	192.168.11.200	439
192.168.10.128	192.168.10.128	376
192.168.10.16	192.168.10.16	208
192.168.10.4	192.168.10.4	129
192.168.9.11	192.168.9.11	111
192.168.10.122	192.168.10.122	105

Export: Raw Formatted

1 2 3 »

Signatures

Signature	Signature ID	Alerts
SURICATA STREAM ESTABLISHED invalid ack	2210029	21,084
SURICATA STREAM ESTABLISHED packet out of window	2210020	20,800
ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	2013504	342
SURICATA STREAM excessive retransmissions	2210054	331
ET JA3 Hash - Possible Malware - Banking Phish	2028362	241
SURICATA STREAM 3way handshake wrong seq wrong ack	2210010	226
ET SCAN MS Terminal Server Traffic on Non-standard Port	2023753	206
ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	2027390	198
SURICATA HTTP unable to match response to request	2221010	147
SURICATA TCPv4 invalid checksum	2200074	137

Export: Raw Formatted

1 2 3 4 5 ... 7 »

Vulnerabilities

No results found

IP Reputations

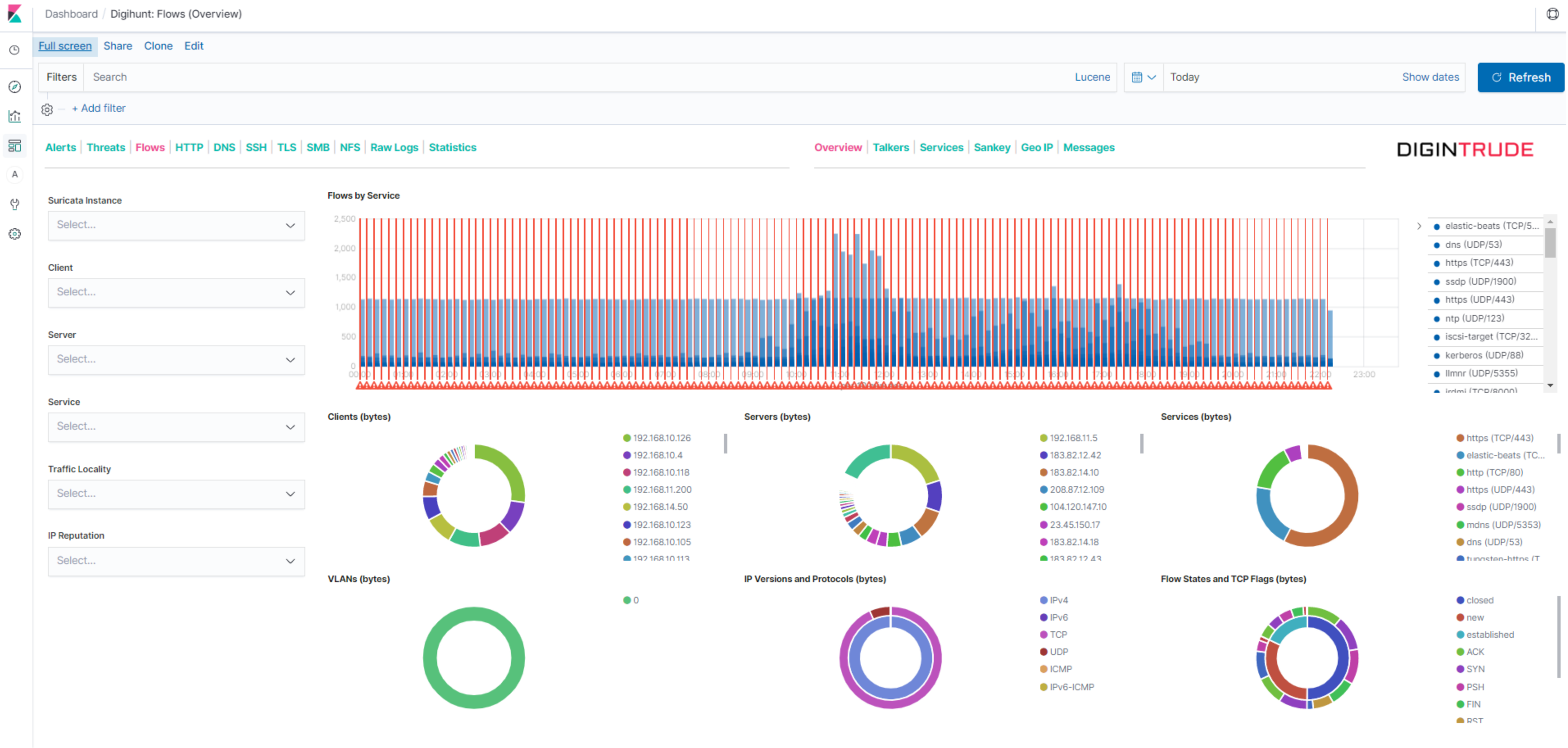
IP Reputation	Alerts
dns	49
named	49
suspicious	48
bruteforce	20
cms	4
email	4
http	4
postfix	4
wordpress	4
ftp	1

Export: Raw Formatted

1 2 »

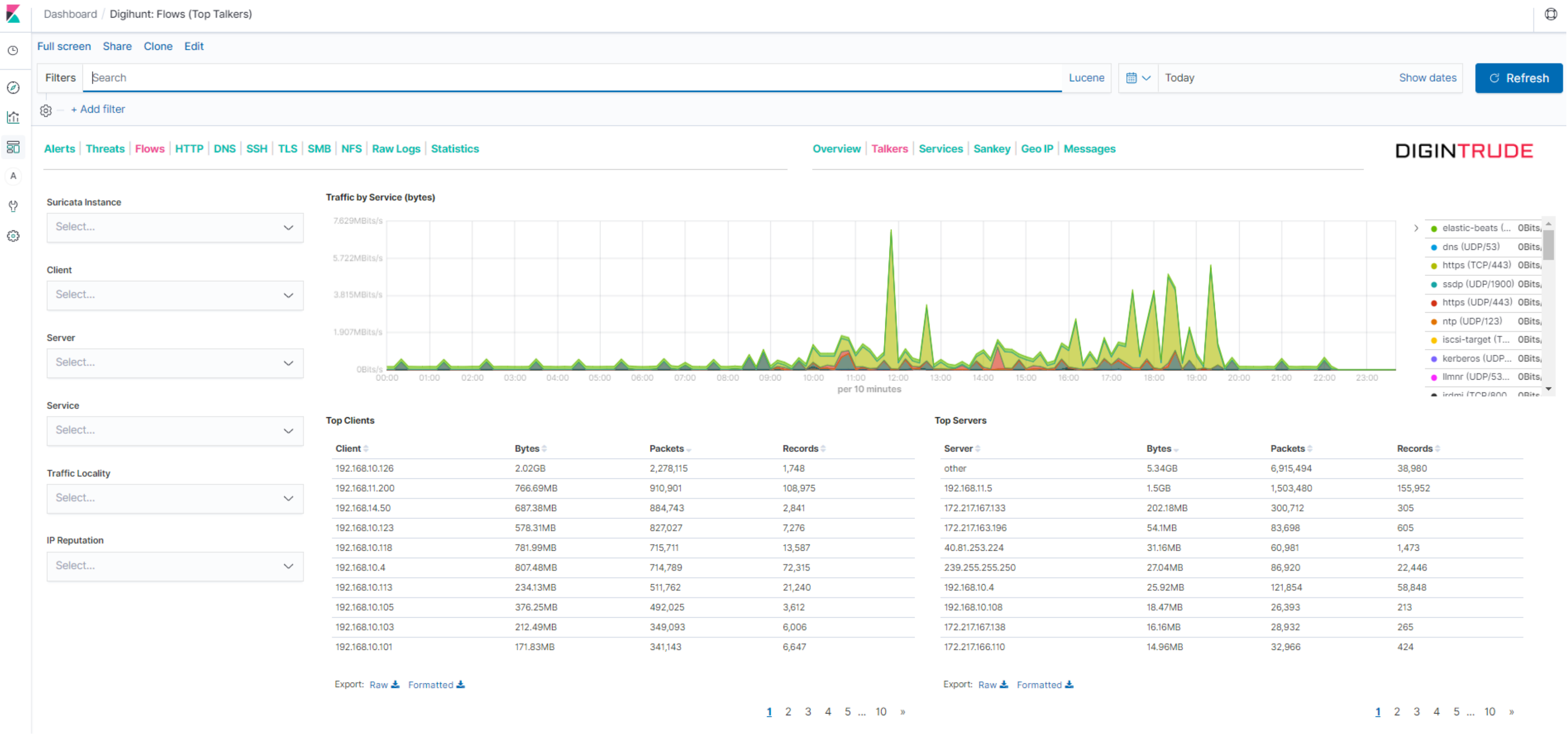
Flows – Overview

Overview tab visualizes network flow event detected by our Digihunt engine. It shows a visualization of Clients list, Servers, Services, VLANs, IP Versions & Protocols, Flow States & TCP Flags according to bytes. This also draws a statistical analysis view of history time span and real-time network flows overview.



Flows - Top Talkers

Talkers tab visualizes network flows on top bytes, packets, and records by our Digihunt engine. It shows visualization of Top Clients IP, Top Servers IP with a count of Packets and Records. This also draws a statistical analysis view of history time span and real-time network flows in Kbits/sec.



Dashboard / Digihunt: Flows (Top Talkers)

Full screen Share Clone Edit

Filters Search Lucene Today Show dates Refresh

+ Add filter

Alerts | Threats | Flows | HTTP | DNS | SSH | TLS | SMB | NFS | Raw Logs | Statistics

Overview | Talkers | Services | Sankey | Geo IP | Messages

DIGINTRUDE

Suricata Instance: Select...

Client: Select...

Server: Select...

Service: Select...

Traffic Locality: Select...

IP Reputation: Select...

Traffic by Service (bytes)

Top Clients

Client	Bytes	Packets	Records
192.168.10.126	2.02GB	2,278,115	1,748
192.168.11.200	766.69MB	910,901	108,975
192.168.14.50	687.38MB	884,743	2,841
192.168.10.123	578.31MB	827,027	7,276
192.168.10.118	781.99MB	715,711	13,587
192.168.10.4	807.48MB	714,789	72,315
192.168.10.113	234.13MB	511,762	21,240
192.168.10.105	376.25MB	492,025	3,612
192.168.10.103	212.49MB	349,093	6,006
192.168.10.101	171.83MB	341,143	6,647

Export: Raw Formatted

1 2 3 4 5 ... 10 »

Top Servers

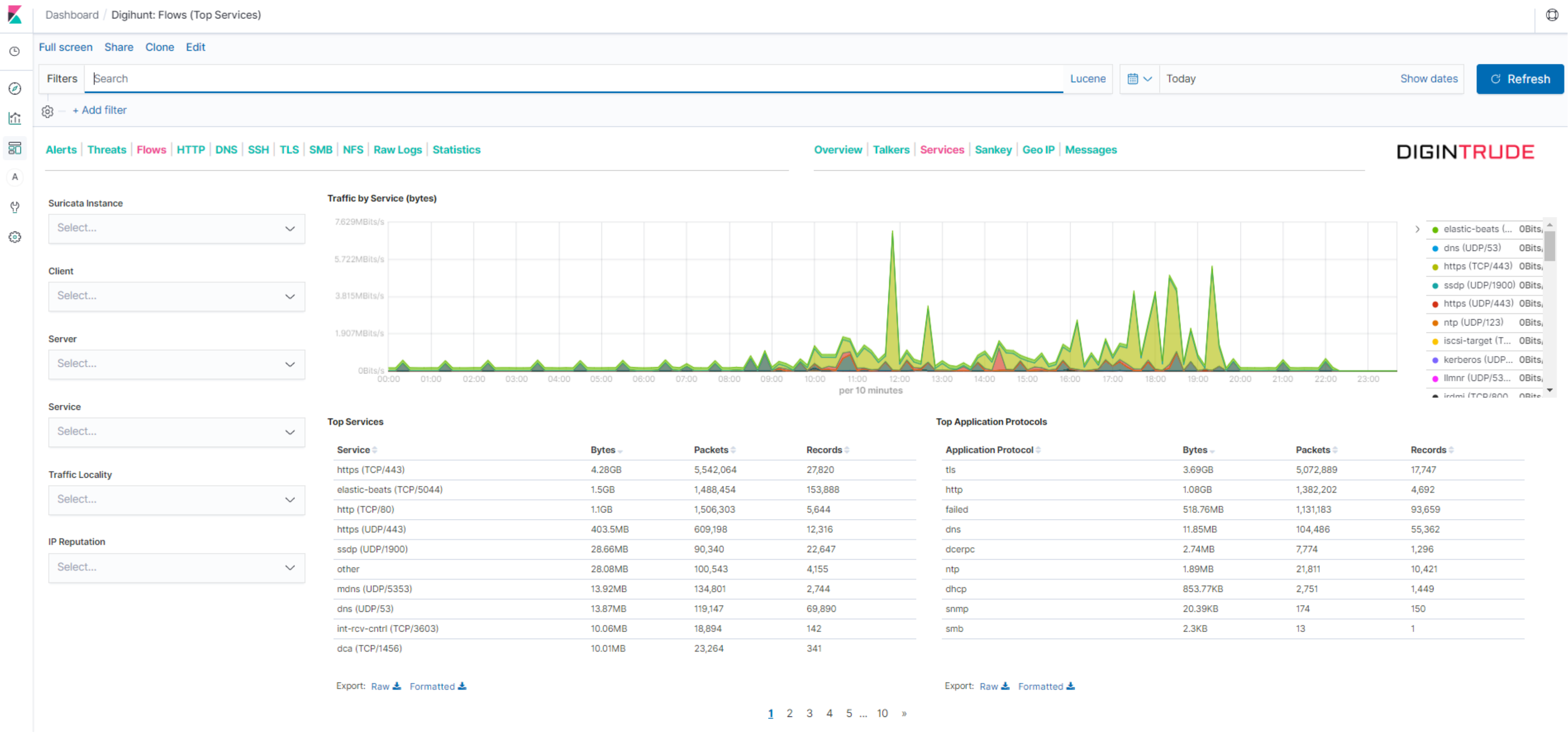
Server	Bytes	Packets	Records
other	5.34GB	6,915,494	38,980
192.168.11.5	1.5GB	1,503,480	155,952
172.217.167.133	202.18MB	300,712	305
172.217.163.196	54.1MB	83,698	605
40.81.253.224	31.16MB	60,981	1,473
239.255.255.250	27.04MB	86,920	22,446
192.168.10.4	25.92MB	121,854	58,848
192.168.10.108	18.47MB	26,393	213
172.217.167.138	16.16MB	28,932	265
172.217.166.110	14.96MB	32,966	424

Export: Raw Formatted

1 2 3 4 5 ... 10 »

Flows - Top Services

Services tab visualizes network flows on top bytes, packets, and records by our Digihunt engine. It shows a visualization of Top Services, Top Application Protocols with the count of Packets and Records. This also draws a statistical analysis view of history time span and real-time services and application protocol flows in Kbits/sec.



Top Services

Service	Bytes	Packets	Records
https (TCP/443)	4.28GB	5,542,064	27,820
elastic-beats (TCP/5044)	1.5GB	1,488,454	153,888
http (TCP/80)	1.1GB	1,506,303	5,644
https (UDP/443)	403.5MB	609,198	12,316
ssdp (UDP/1900)	28.66MB	90,340	22,647
other	28.08MB	100,543	4,155
mdns (UDP/5353)	13.92MB	134,801	2,744
dns (UDP/53)	13.87MB	119,147	69,890
int-rcv-cntrl (TCP/3603)	10.06MB	18,894	142
dca (TCP/1456)	10.01MB	23,264	341

Export: Raw Formatted

1 2 3 4 5 ... 10 »

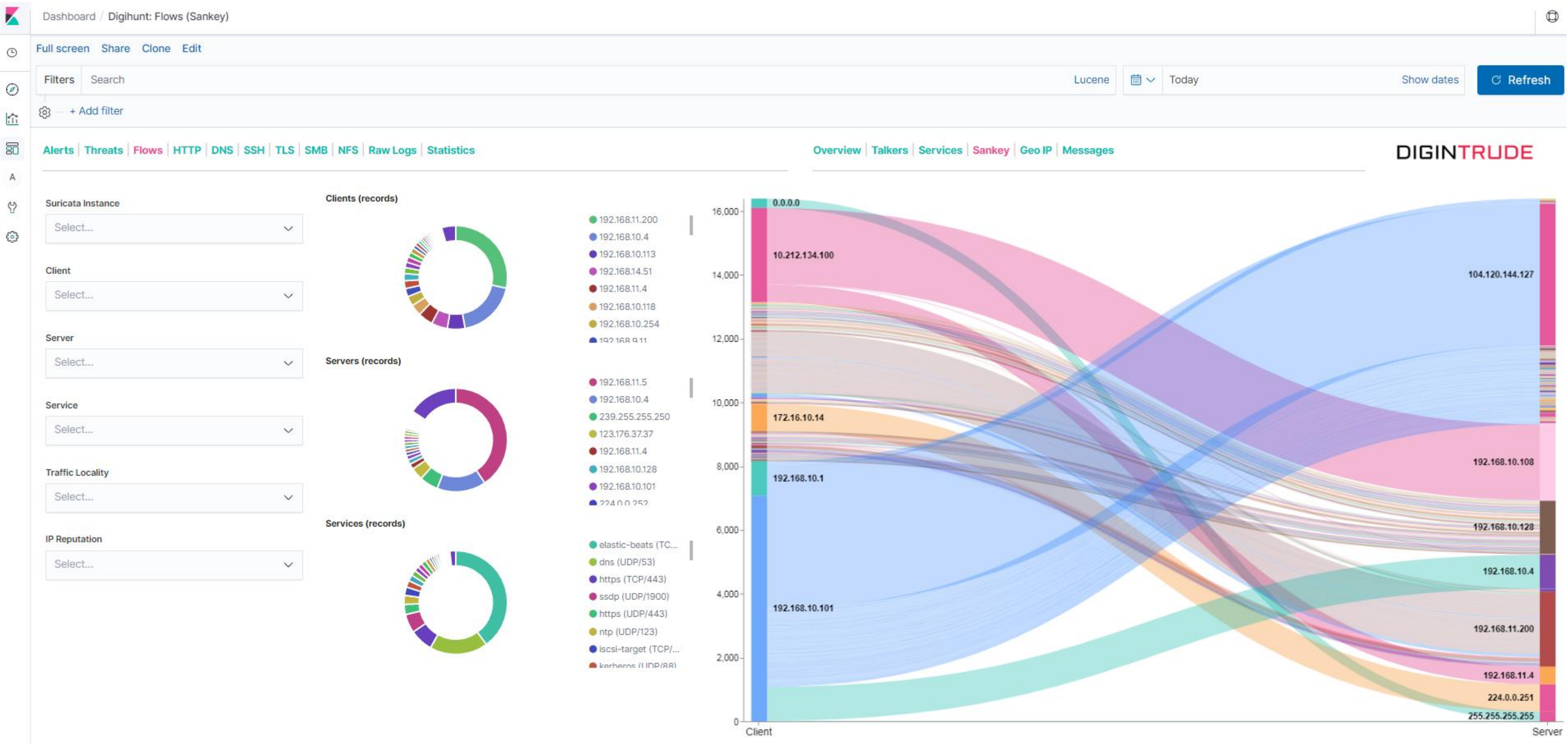
Top Application Protocols

Application Protocol	Bytes	Packets	Records
tls	3.69GB	5,072,889	17,747
http	1.08GB	1,382,202	4,692
failed	518.76MB	1,131,183	93,659
dns	11.85MB	104,486	55,362
dcerpc	2.74MB	7,774	1,296
ntp	1.89MB	21,811	10,421
dhcp	853.77KB	2,751	1,449
snmp	20.39KB	174	150
smb	2.3KB	13	1

Export: Raw Formatted

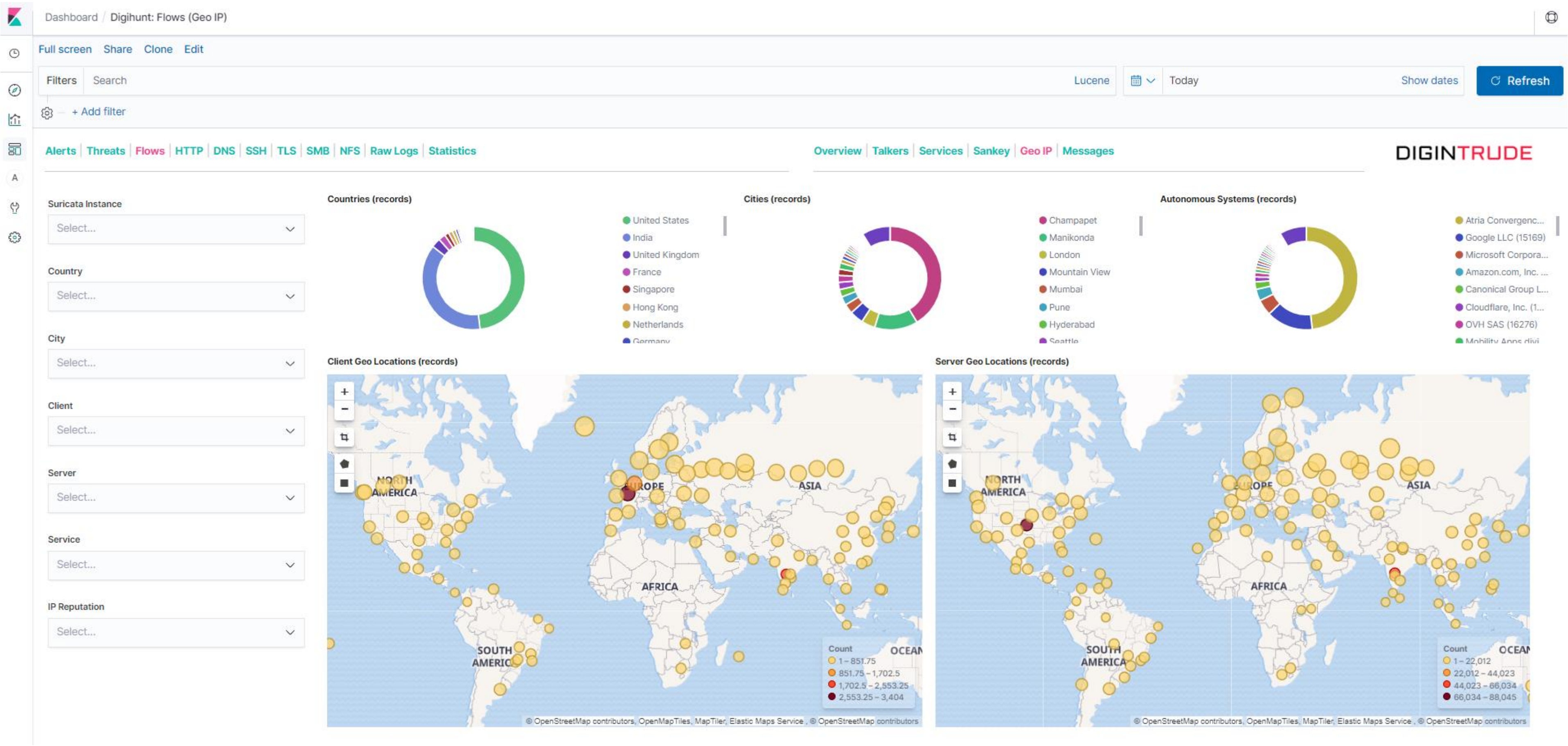
Flows – Sankey

Sankey tab visualizes network flows on top records by our Digihunt engine. It shows the visualization of Clients, Servers, and Services count of Records. This also draws Sankey's view of history time span and real-time source IP to destination IP.



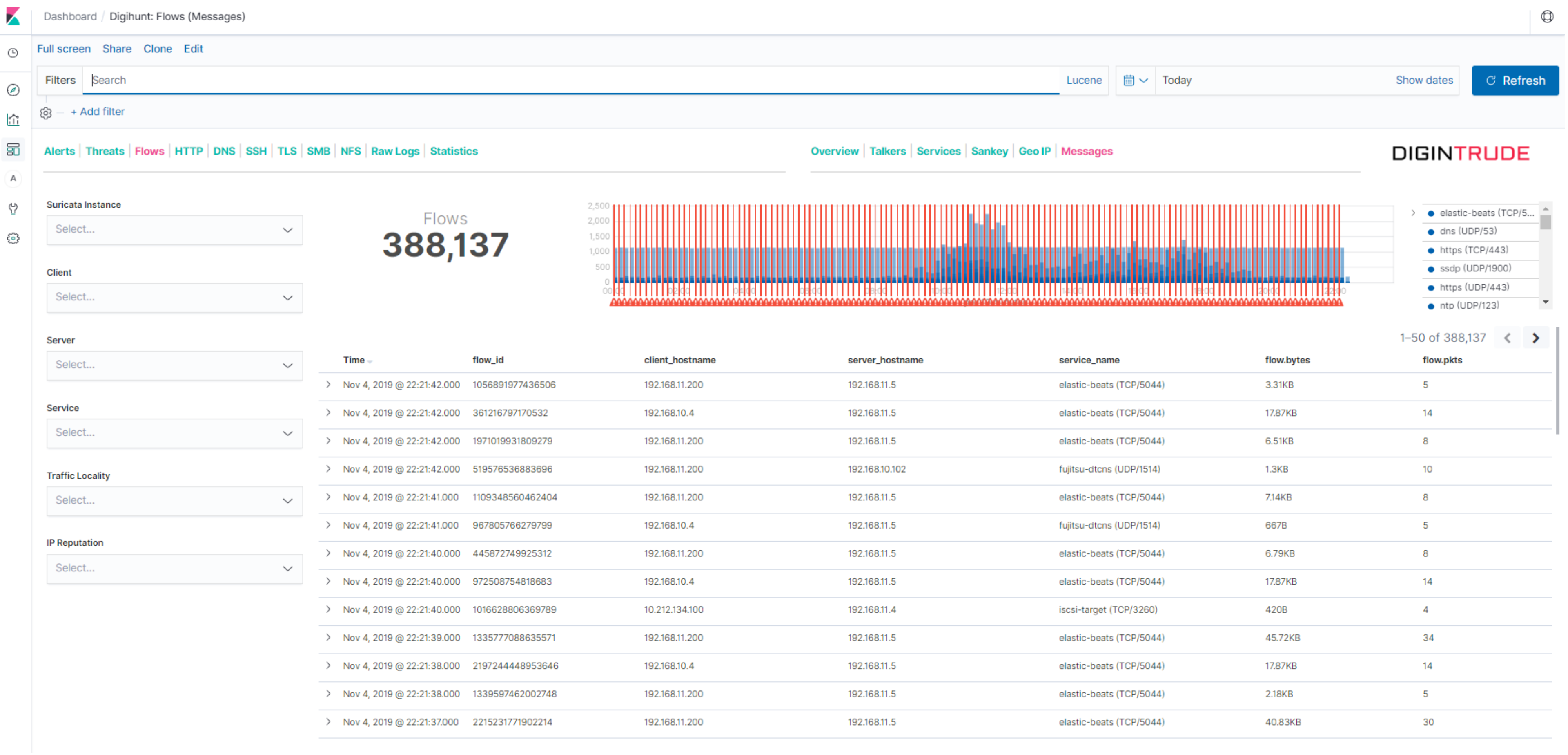
Flows - Geo IP

Geo IP tab visualizes network flows according to Geo Locations by our Digihunt engine. It shows the visualization of Countries, Cities and Autonomous Systems. This also draws the geo spots according to the network flow records initiated.



Flows – Messages

Messages tab visualize protocol traffics detailed information by our Digihunt engine. It shows the visualization of all active protocols event with Timestamp, flow_id, client_hostname, server_hostname, service_name, flow.bytes, flow.pkts fields. This also draws a statistical analysis graph according to the network flow services.



Suricata Instance: Select...

Client: Select...

Server: Select...

Service: Select...

Traffic Locality: Select...

IP Reputation: Select...

Flows

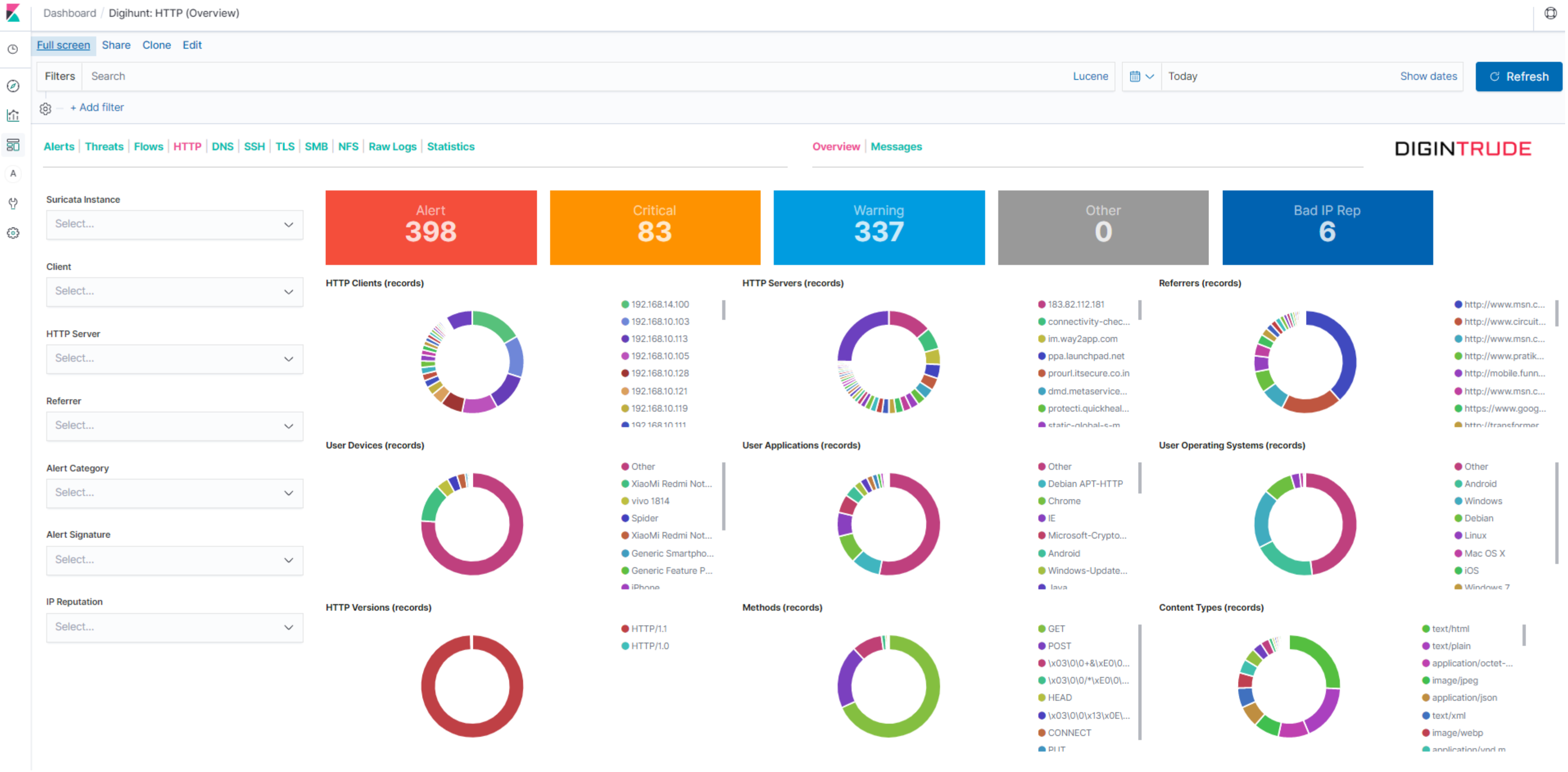
388,137

1–50 of 388,137

Time	flow_id	client_hostname	server_hostname	service_name	flow.bytes	flow.pkts
Nov 4, 2019 @ 22:21:42.000	1056891977436506	192.168.11.200	192.168.11.5	elastic-beats (TCP/5044)	3.31KB	5
Nov 4, 2019 @ 22:21:42.000	361216797170532	192.168.10.4	192.168.11.5	elastic-beats (TCP/5044)	17.87KB	14
Nov 4, 2019 @ 22:21:42.000	1971019931809279	192.168.11.200	192.168.11.5	elastic-beats (TCP/5044)	6.51KB	8
Nov 4, 2019 @ 22:21:42.000	519576536883696	192.168.11.200	192.168.10.102	fujitsu-dtcns (UDP/1514)	1.3KB	10
Nov 4, 2019 @ 22:21:41.000	1109348560462404	192.168.11.200	192.168.11.5	elastic-beats (TCP/5044)	7.14KB	8
Nov 4, 2019 @ 22:21:41.000	967805766279799	192.168.10.4	192.168.11.5	fujitsu-dtcns (UDP/1514)	667B	5
Nov 4, 2019 @ 22:21:40.000	445872749925312	192.168.11.200	192.168.11.5	elastic-beats (TCP/5044)	6.79KB	8
Nov 4, 2019 @ 22:21:40.000	972508754818683	192.168.10.4	192.168.11.5	elastic-beats (TCP/5044)	17.87KB	14
Nov 4, 2019 @ 22:21:40.000	1016628806369789	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)	420B	4
Nov 4, 2019 @ 22:21:39.000	1335777088635571	192.168.11.200	192.168.11.5	elastic-beats (TCP/5044)	45.72KB	34
Nov 4, 2019 @ 22:21:38.000	2197244448953646	192.168.10.4	192.168.11.5	elastic-beats (TCP/5044)	17.87KB	14
Nov 4, 2019 @ 22:21:38.000	1339597462002748	192.168.11.200	192.168.11.5	elastic-beats (TCP/5044)	2.18KB	5
Nov 4, 2019 @ 22:21:37.000	2215231771902214	192.168.11.200	192.168.11.5	elastic-beats (TCP/5044)	40.83KB	30

HTTP – Overview

Overview tab visualizes Http application services suspicious activity overview dashboard by our Digihunt engine. It shows the visualization of all suspicious activity on a priority of Alert, Critical, Warning, Other & Bad IP Reputations. This also shows all incident categories in real-time and timespan searches.



Alert 398

Critical 83

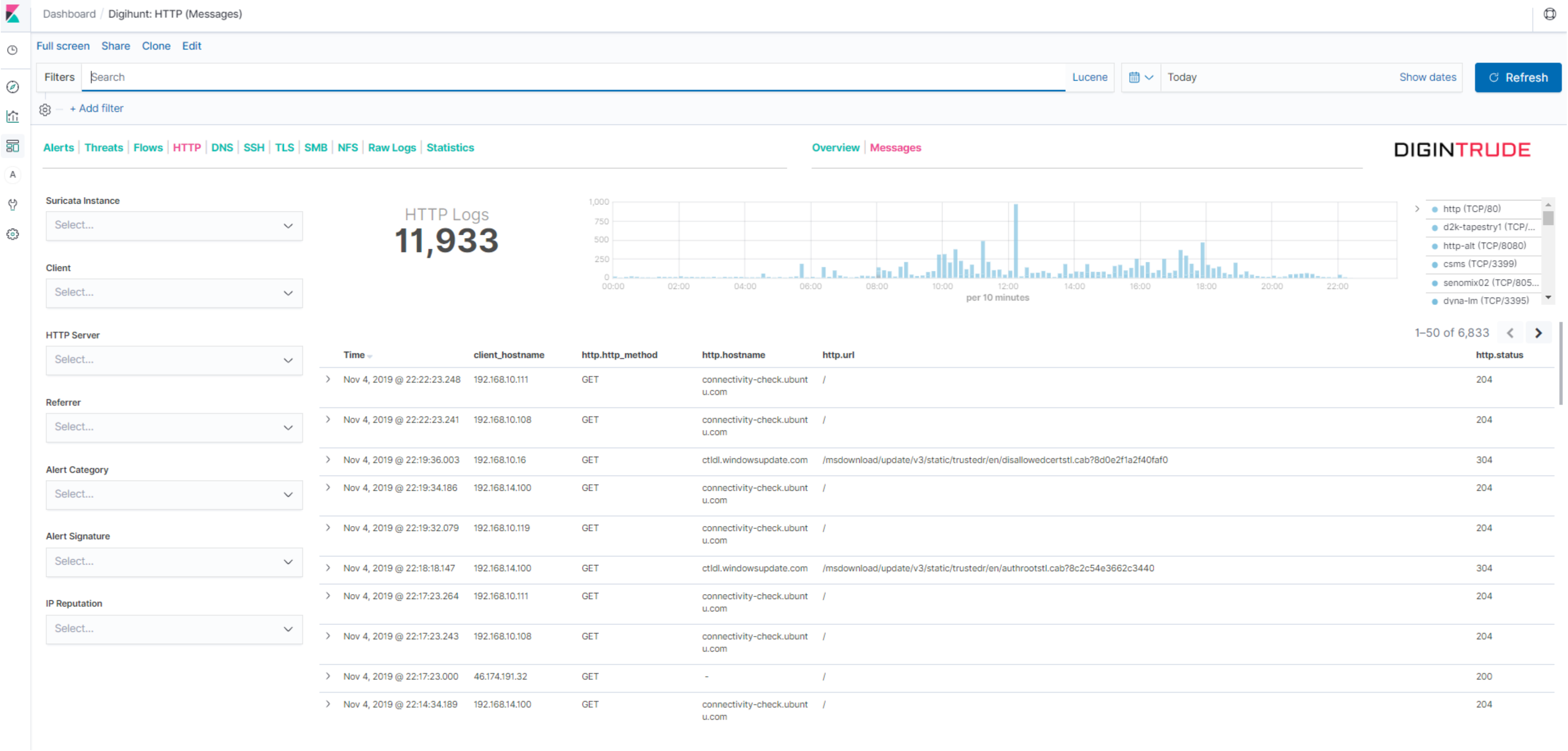
Warning 337

Other 0

Bad IP Rep 6

HTTP – Messages

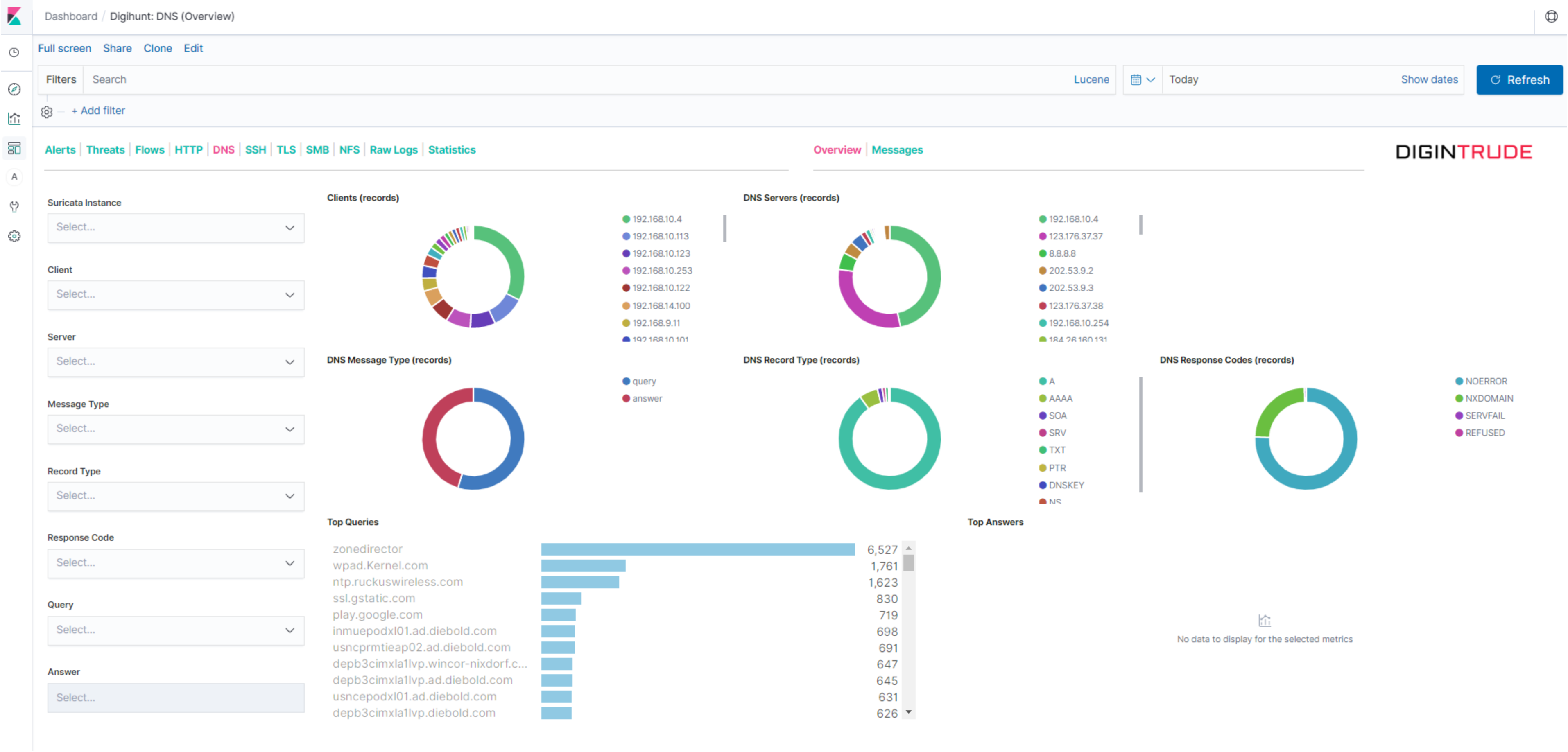
Messages tab visualize Http application services suspicious activity detailed information by our Digihunt engine. It shows the visualization of all suspicious activity on a priority of field like Time, Client_hostname, http.http_method, HTTP.hostname, http.url. This also draws a statistical analysis graph of applications according to real-time and timespan search.



Time	client_hostname	http.http_method	http.hostname	http.url	http.status
Nov 4, 2019 @ 22:22:23.248	192.168.10.111	GET	connectivity-check.ubuntu.com	/	204
Nov 4, 2019 @ 22:22:23.241	192.168.10.108	GET	connectivity-check.ubuntu.com	/	204
Nov 4, 2019 @ 22:19:36.003	192.168.10.16	GET	ctldl.windowsupdate.com	/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8d0e2f1a2f40faf0	304
Nov 4, 2019 @ 22:19:34.186	192.168.14.100	GET	connectivity-check.ubuntu.com	/	204
Nov 4, 2019 @ 22:19:32.079	192.168.10.119	GET	connectivity-check.ubuntu.com	/	204
Nov 4, 2019 @ 22:18:18.147	192.168.14.100	GET	ctldl.windowsupdate.com	/msdownload/update/v3/static/trustedr/en/authrootstl.cab?8c2c54e3662c3440	304
Nov 4, 2019 @ 22:17:23.264	192.168.10.111	GET	connectivity-check.ubuntu.com	/	204
Nov 4, 2019 @ 22:17:23.243	192.168.10.108	GET	connectivity-check.ubuntu.com	/	204
Nov 4, 2019 @ 22:17:23.000	46.174.191.32	GET	-	/	200
Nov 4, 2019 @ 22:14:34.189	192.168.14.100	GET	connectivity-check.ubuntu.com	/	204

DNS – Overview

Overview tab visualizes the DNS application services records overview dashboard by our Digihunt engine. It shows a visualization of all DNS related events in Clients, DNS Servers, DNS Messages, DNS Record Type, DNS Response Codes, Top Queries. This also shows all event categories in real-time and timespan searches.



Dashboard / Digihunt: DNS (Overview)
Full screen
Share
Clone
Edit
Filters
Search
Lucene
Today
Show dates
Refresh
+ Add filter
Alerts | Threats | Flows | HTTP | DNS | SSH | TLS | SMB | NFS | Raw Logs | Statistics
Overview | Messages
DIGINTRUDE

Suricata Instance: Select...

Client: Select...

Server: Select...

Message Type: Select...

Record Type: Select...

Response Code: Select...

Query: Select...

Answer: Select...

Clients (records)

DNS Servers (records)

DNS Message Type (records)

DNS Record Type (records)

DNS Response Codes (records)

Top Queries

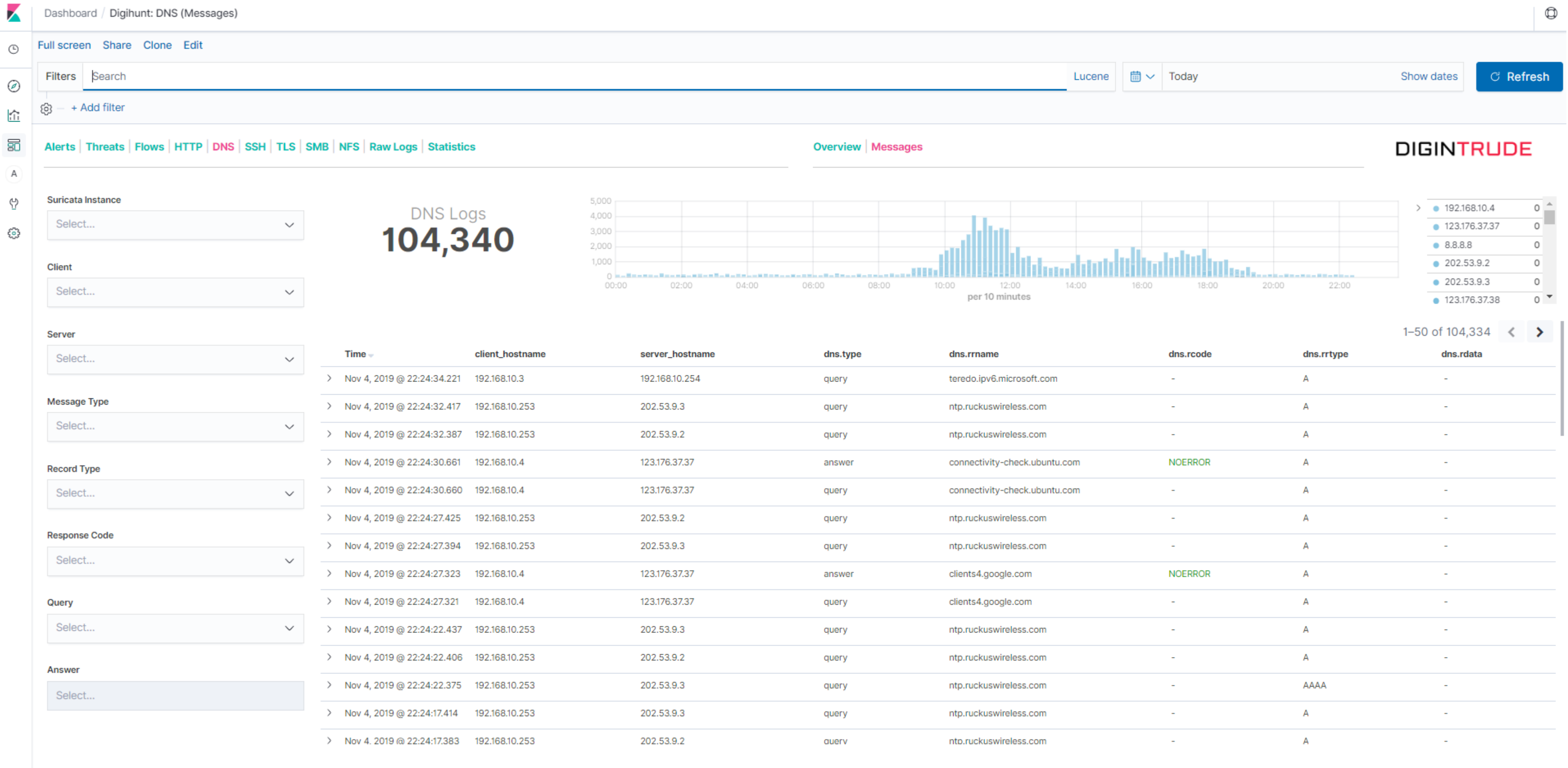
zonedirector	6,527
wpad.Kernel.com	1,761
ntp.ruckuswireless.com	1,623
ssl.gstatic.com	830
play.google.com	719
inmuepodxl01.ad.diebold.com	698
usncprmtieap02.ad.diebold.com	691
depb3cimxla1lvp.wincor-nixdorf.c...	647
depb3cimxla1lvp.ad.diebold.com	645
usncepodxl01.ad.diebold.com	631
depb3cimxla1lvp.diebold.com	626

Top Answers

No data to display for the selected metrics

DNS – Messages

Messages tab visualize DNS application services log detailed information by our Digihunt engine. It shows a visualization of all suspicious activity on a priority of field like Time, Client_hostname, Server_hostname, dns.type, dns.rrname, dns.rcode, dns.rrtype, dns.rdata. This also draws a statistical analysis graph of applications according to real-time and timespan searches.



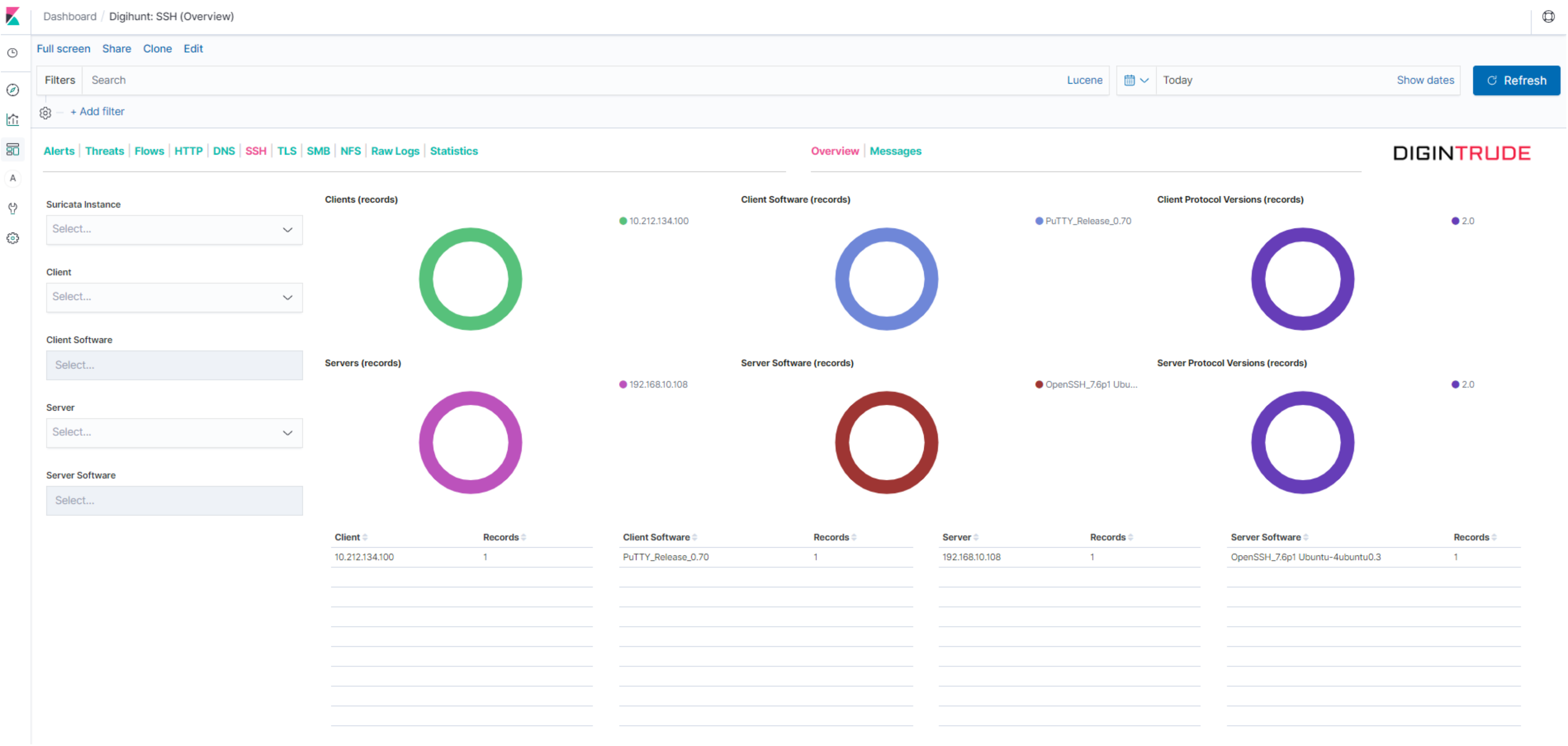
DNS Logs
104,340

1–50 of 104,334

Time	client_hostname	server_hostname	dns.type	dns.rrname	dns.rcode	dns.rrtype	dns.rdata
Nov 4, 2019 @ 22:24:34.221	192.168.10.3	192.168.10.254	query	teredo.ipv6.microsoft.com	-	A	-
Nov 4, 2019 @ 22:24:32.417	192.168.10.253	202.53.9.3	query	ntp.ruckuswireless.com	-	A	-
Nov 4, 2019 @ 22:24:32.387	192.168.10.253	202.53.9.2	query	ntp.ruckuswireless.com	-	A	-
Nov 4, 2019 @ 22:24:30.661	192.168.10.4	123.176.37.37	answer	connectivity-check.ubuntu.com	NOERROR	A	-
Nov 4, 2019 @ 22:24:30.660	192.168.10.4	123.176.37.37	query	connectivity-check.ubuntu.com	-	A	-
Nov 4, 2019 @ 22:24:27.425	192.168.10.253	202.53.9.2	query	ntp.ruckuswireless.com	-	A	-
Nov 4, 2019 @ 22:24:27.394	192.168.10.253	202.53.9.3	query	ntp.ruckuswireless.com	-	A	-
Nov 4, 2019 @ 22:24:27.323	192.168.10.4	123.176.37.37	answer	clients4.google.com	NOERROR	A	-
Nov 4, 2019 @ 22:24:27.321	192.168.10.4	123.176.37.37	query	clients4.google.com	-	A	-
Nov 4, 2019 @ 22:24:22.437	192.168.10.253	202.53.9.3	query	ntp.ruckuswireless.com	-	A	-
Nov 4, 2019 @ 22:24:22.406	192.168.10.253	202.53.9.2	query	ntp.ruckuswireless.com	-	A	-
Nov 4, 2019 @ 22:24:22.375	192.168.10.253	202.53.9.3	query	ntp.ruckuswireless.com	-	AAAA	-
Nov 4, 2019 @ 22:24:17.414	192.168.10.253	202.53.9.3	query	ntp.ruckuswireless.com	-	A	-
Nov 4. 2019 @ 22:24:17.383	192.168.10.253	202.53.9.2	query	ntp.ruckuswireless.com	-	A	-

SSH – Overview

Overview tab visualizes the ssh remote application services records overview dashboard by our Digihunt engine. It shows the visualization of all ssh related events in Clients, Client Software, Client Protocol Versions, Servers, Server Software, Server Protocol Versions. This also shows the record count of Client IPs, Client Software, Server & Server Software.



Client	Records
10.212.134.100	1

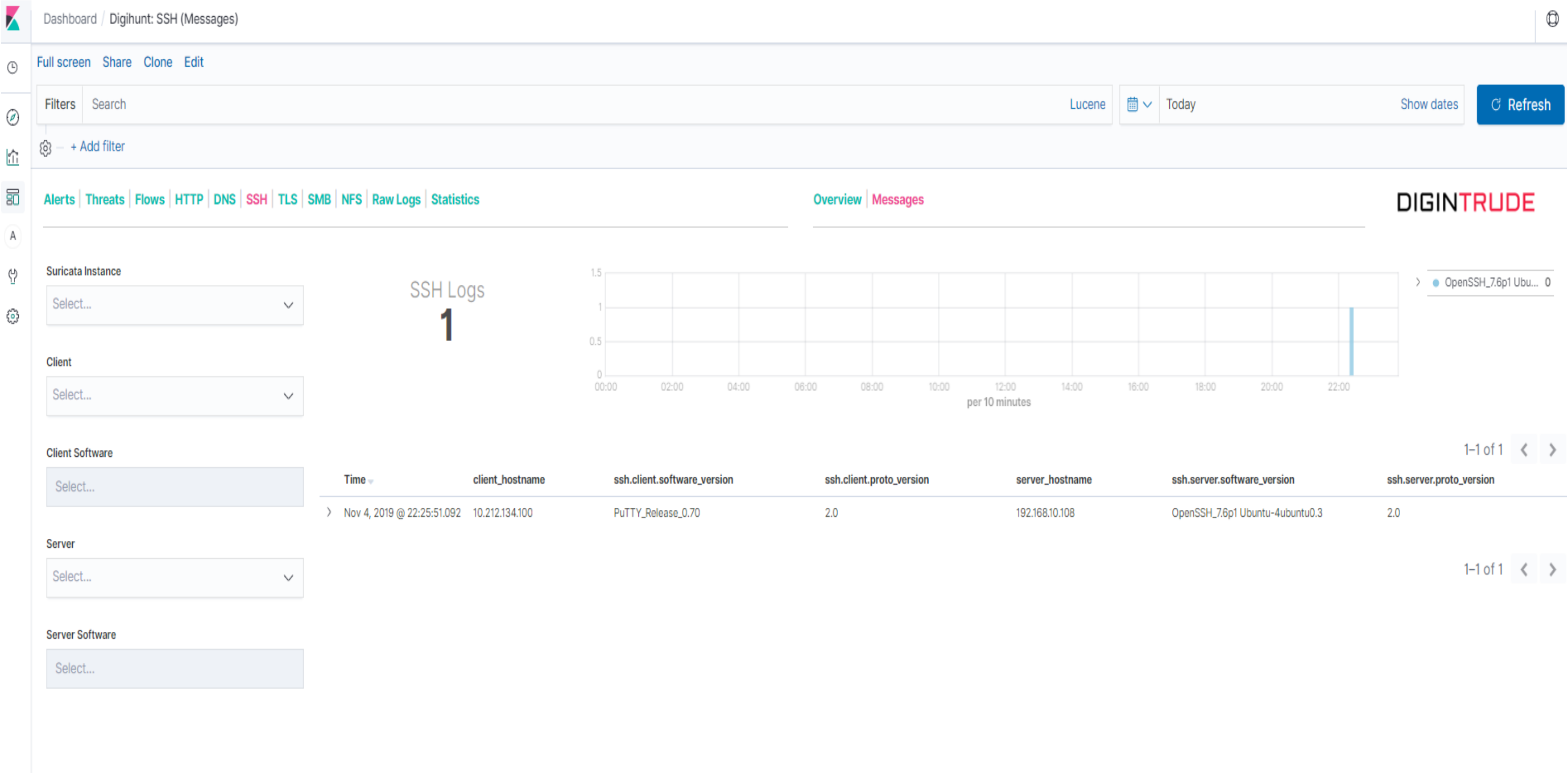
Client Software	Records
PuTTY_Release_0.70	1

Server	Records
192.168.10.108	1

Server Software	Records
OpenSSH_7.6p1 Ubuntu-4ubuntu0.3	1

SSH – Messages

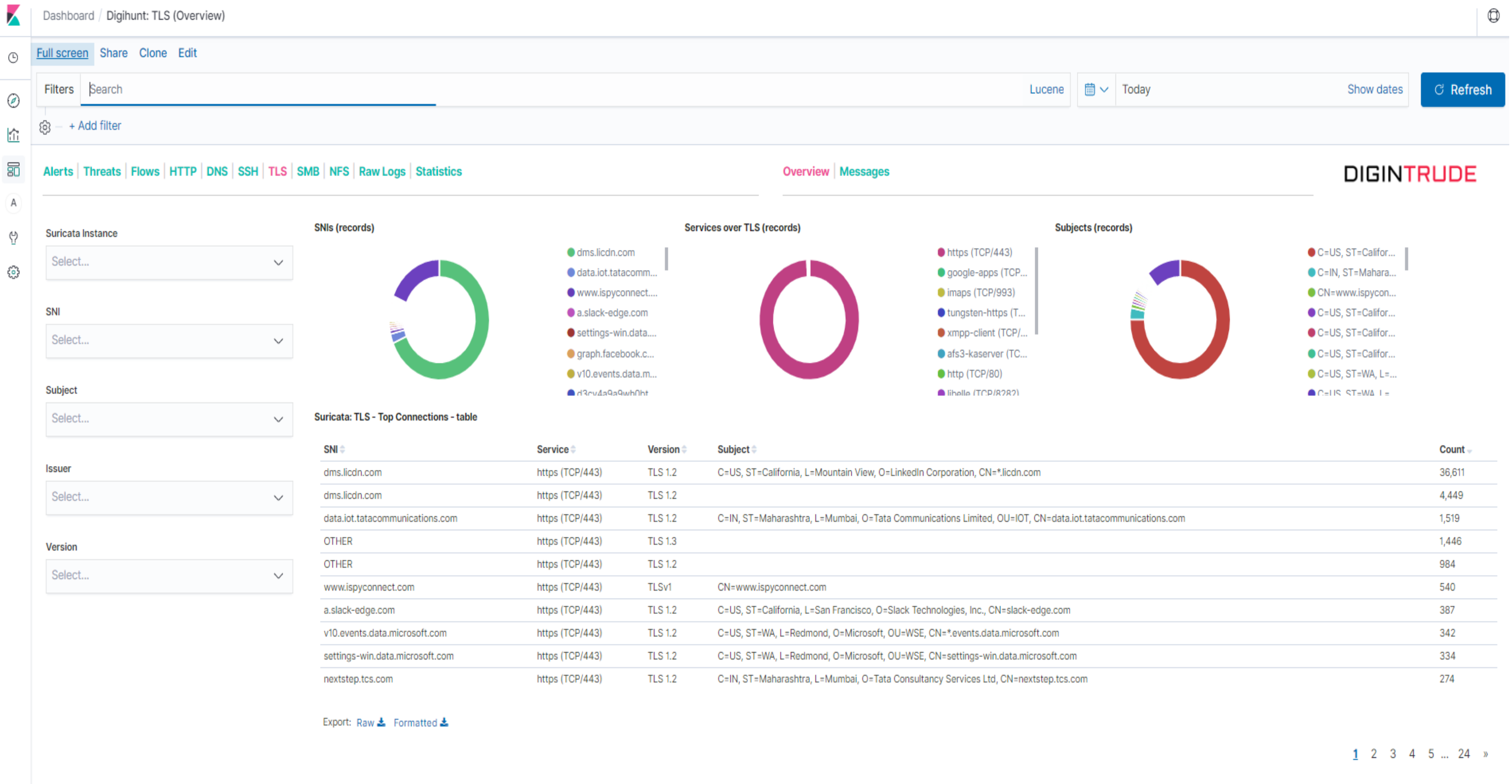
Message tab visualizes ssh remote application services records details by our Digihunt engine. It shows visualization of all ssh related records in Time, client_hostname, ssh.client_software_version, ssh.client_proto_version, server_hostname, sh.server.software_version, ssh.server.proto_version fields. This also filters according to Search Keyword & Show dates.



Time	client_hostname	ssh.client.software_version	ssh.client.proto_version	server_hostname	ssh.server.software_version	ssh.server.proto_version
Nov 4, 2019 @ 22:25:51.092	10.212.134.100	PuTTY_Release_0.70	2.0	192.168.10.108	OpenSSH_7.6p1 Ubuntu-4ubuntu0.3	2.0

TLS – Overview

Overview tab visualizes TLS remote application services records overview dashboard by our Digihunt engine. It shows the visualization of all TLS related events in SNIs, Services over TLS, Subjects, Suricata: TLS-Top Connections - Table. Add on the feature of filtering with show date and Search field.



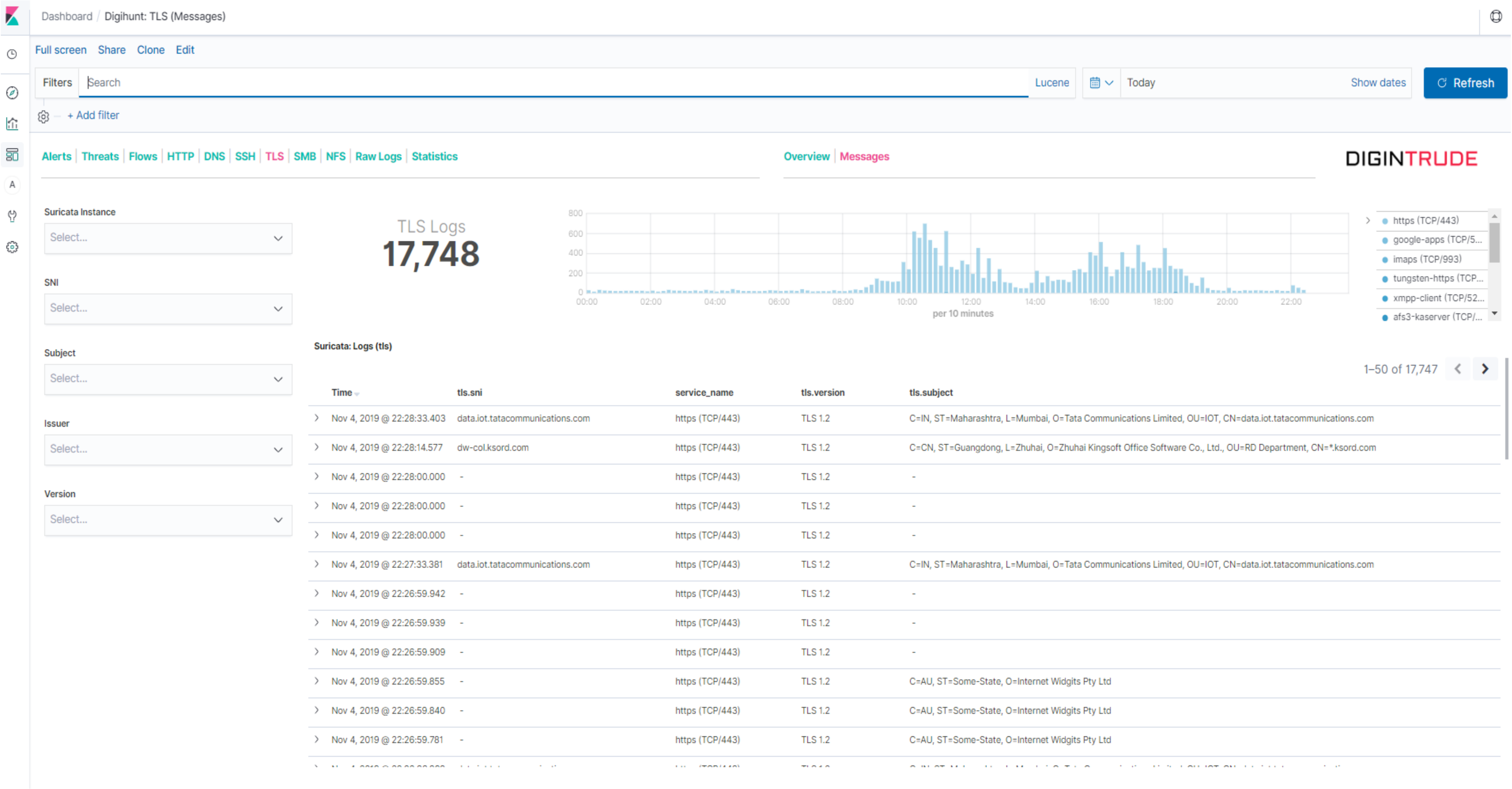
Suricata: TLS - Top Connections - table

SNI	Service	Version	Subject	Count
dms.licdn.com	https (TCP/443)	TLS 1.2	C=US, ST=California, L=Mountain View, O=LinkedIn Corporation, CN=*.licdn.com	36,611
dms.licdn.com	https (TCP/443)	TLS 1.2		4,449
data.iot.tatacommunications.com	https (TCP/443)	TLS 1.2	C=IN, ST=Maharashtra, L=Mumbai, O=Tata Communications Limited, OU=IOT, CN=data.iot.tatacommunications.com	1,519
OTHER	https (TCP/443)	TLS 1.3		1,446
OTHER	https (TCP/443)	TLS 1.2		984
www.ispyconnect.com	https (TCP/443)	TLSv1	CN=www.ispyconnect.com	540
a.slack-edge.com	https (TCP/443)	TLS 1.2	C=US, ST=California, L=San Francisco, O=Slack Technologies, Inc., CN=slack-edge.com	387
v10.events.data.microsoft.com	https (TCP/443)	TLS 1.2	C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE, CN=*.events.data.microsoft.com	342
settings-win.data.microsoft.com	https (TCP/443)	TLS 1.2	C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE, CN=settings-win.data.microsoft.com	334
nextstep.tcs.com	https (TCP/443)	TLS 1.2	C=IN, ST=Maharashtra, L=Mumbai, O=Tata Consultancy Services Ltd, CN=nextstep.tcs.com	274

Export: Raw Formatted

TLS – Messages

Message tab visualizes TLS remote application services records details by our Digihunt engine. It shows the visualization of all TLS related records in Time, tls.sni, service_name, tls.version, tls.subject fields. This also filters according to Search Keyword & Show dates.

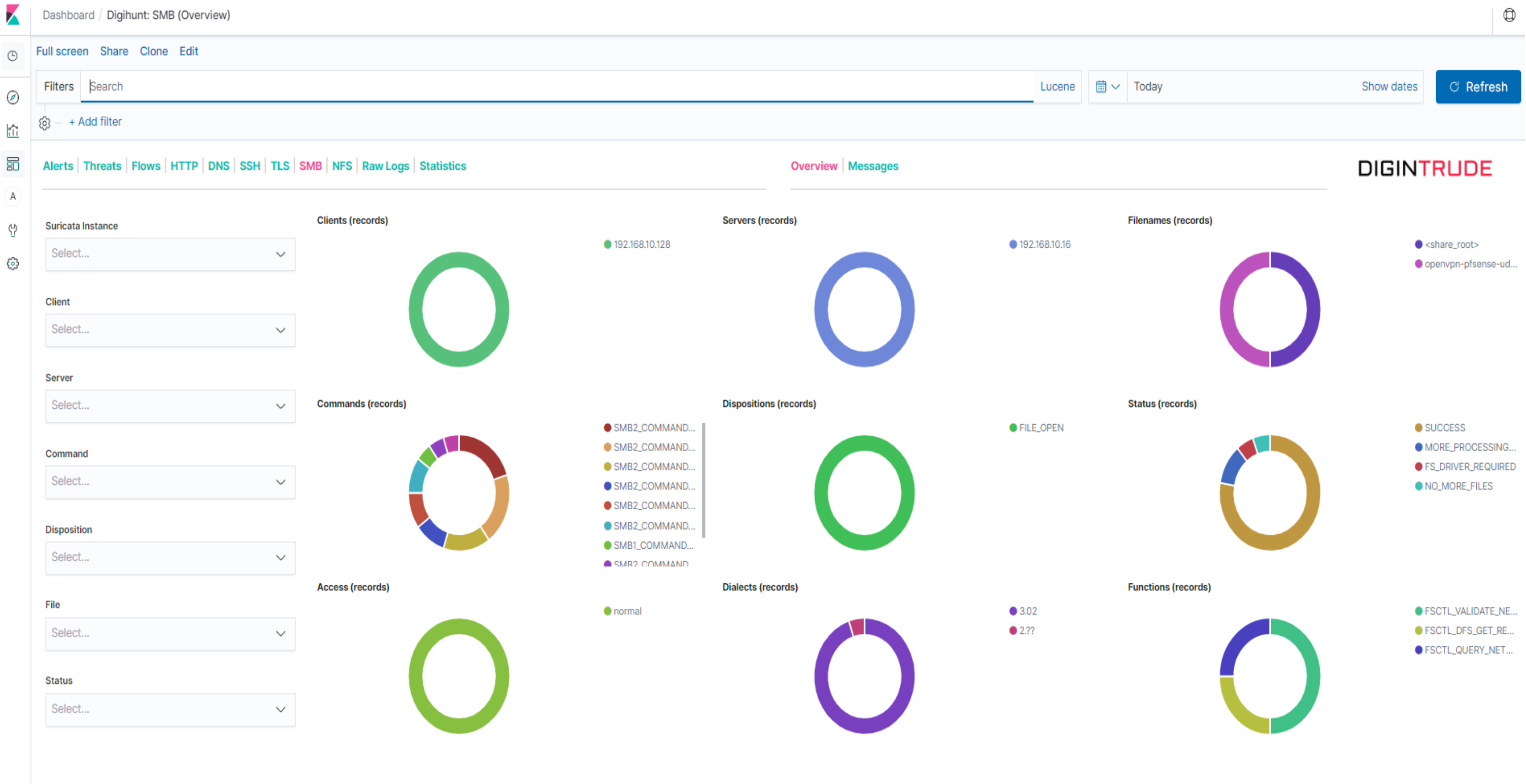


Suricata: Logs (tls)

Time	tls.sni	service_name	tls.version	tls.subject
Nov 4, 2019 @ 22:28:33.403	data.iot.tatacommunications.com	https (TCP/443)	TLS 1.2	C=IN, ST=Maharashtra, L=Mumbai, O=Tata Communications Limited, OU=IOT, CN=data.iot.tatacommunications.com
Nov 4, 2019 @ 22:28:14.577	dw-col.ksord.com	https (TCP/443)	TLS 1.2	C=CN, ST=Guangdong, L=Zhuhai, O=Zhuhai Kingsoft Office Software Co., Ltd., OU=RD Department, CN=*.ksord.com
Nov 4, 2019 @ 22:28:00.000	-	https (TCP/443)	TLS 1.2	-
Nov 4, 2019 @ 22:28:00.000	-	https (TCP/443)	TLS 1.2	-
Nov 4, 2019 @ 22:28:00.000	-	https (TCP/443)	TLS 1.2	-
Nov 4, 2019 @ 22:27:33.381	data.iot.tatacommunications.com	https (TCP/443)	TLS 1.2	C=IN, ST=Maharashtra, L=Mumbai, O=Tata Communications Limited, OU=IOT, CN=data.iot.tatacommunications.com
Nov 4, 2019 @ 22:26:59.942	-	https (TCP/443)	TLS 1.2	-
Nov 4, 2019 @ 22:26:59.939	-	https (TCP/443)	TLS 1.2	-
Nov 4, 2019 @ 22:26:59.909	-	https (TCP/443)	TLS 1.2	-
Nov 4, 2019 @ 22:26:59.855	-	https (TCP/443)	TLS 1.2	C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
Nov 4, 2019 @ 22:26:59.840	-	https (TCP/443)	TLS 1.2	C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
Nov 4, 2019 @ 22:26:59.781	-	https (TCP/443)	TLS 1.2	C=AU, ST=Some-State, O=Internet Widgits Pty Ltd

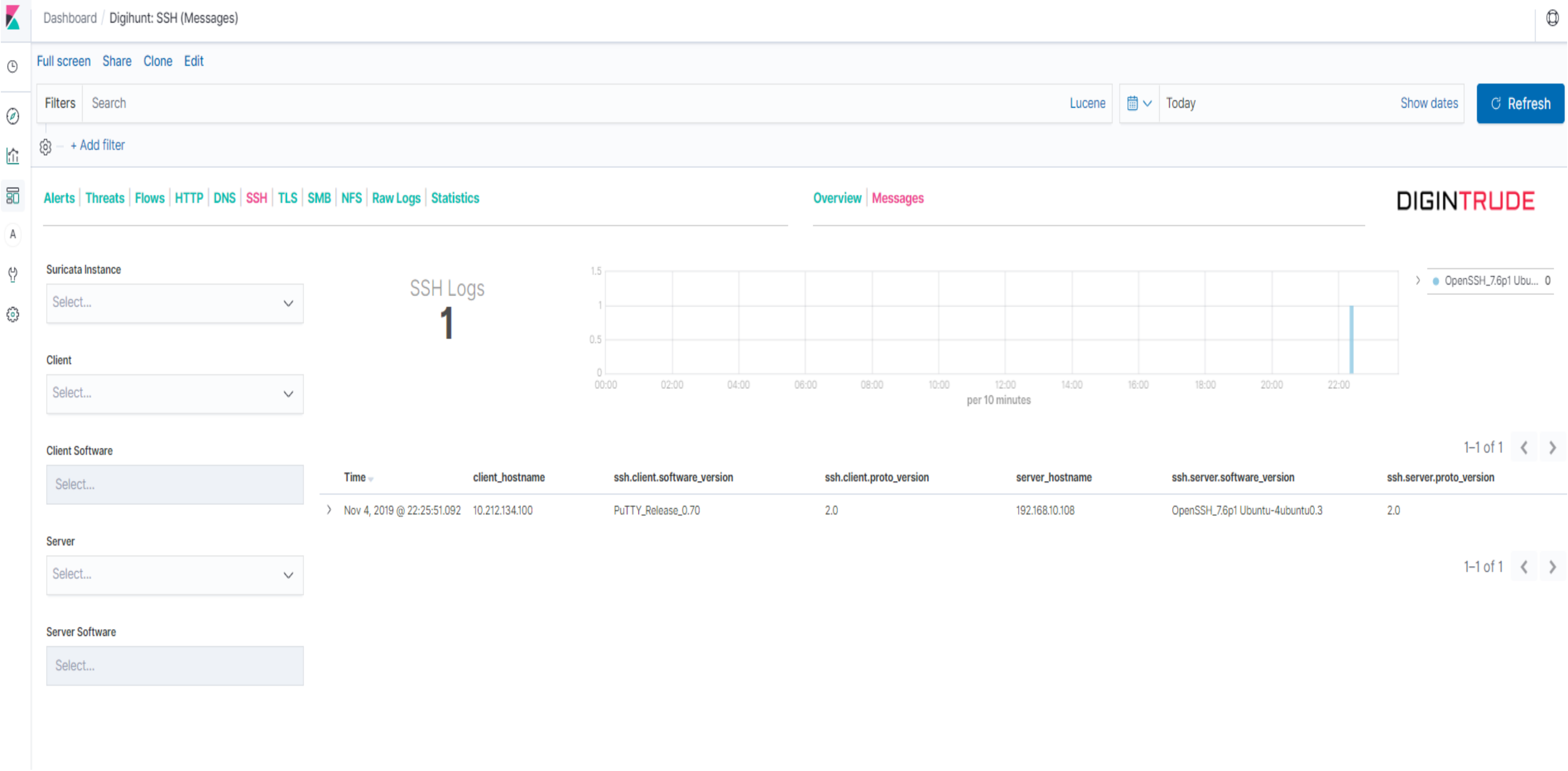
SMB – Overview

Overview tab visualizes SMB remote application services records overview dashboard by our Digihunt engine. It shows the visualization of all SMB related events in Clients, Servers, Filenames, Commands, Dispositions, Status, Access, Dialects, Functions. Add on the feature of filtering with show date and Search field.



SMB – Messages

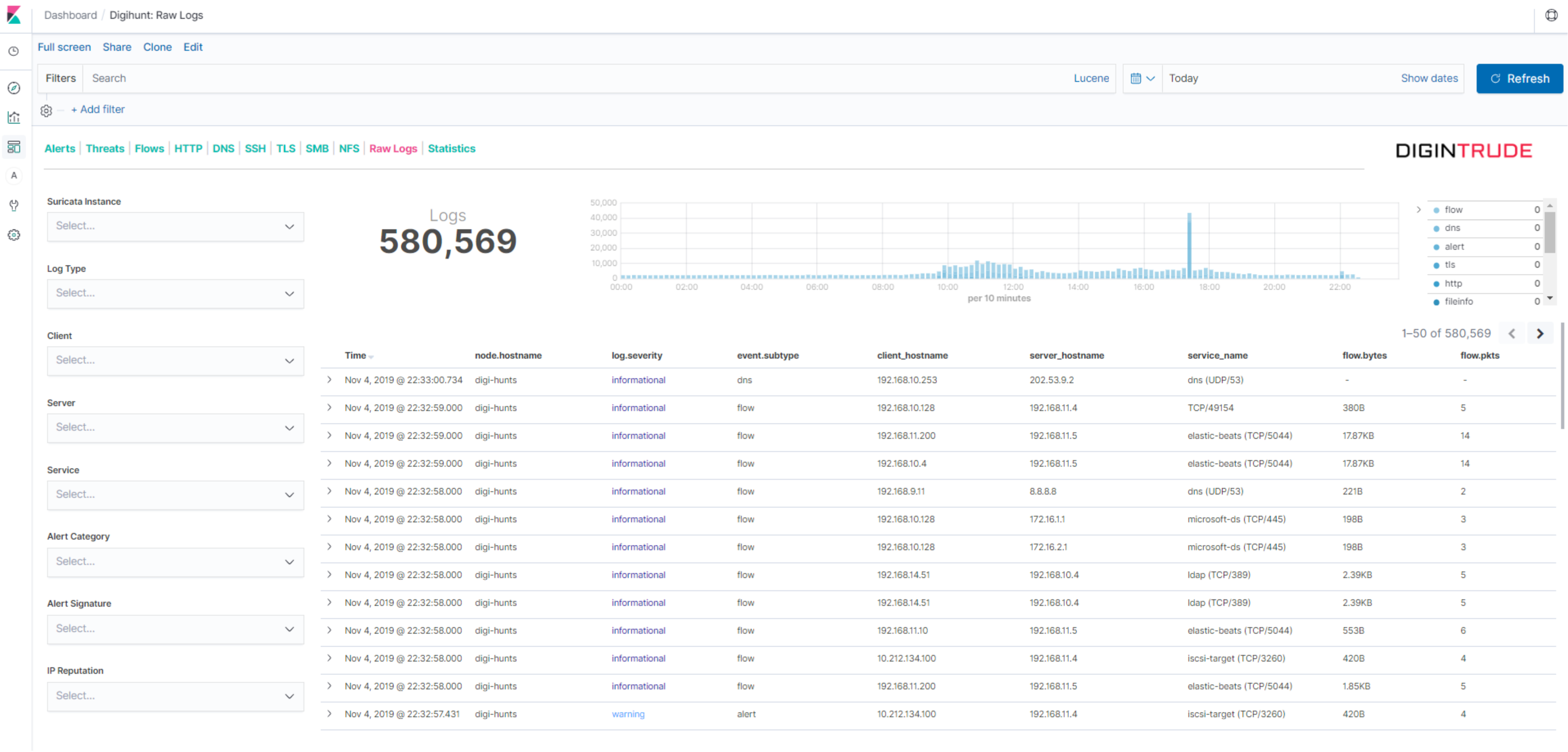
Message tab visualizes SMB remote application services records details by our Digihunt engine. It shows the visualization of all SMB related records in Time, client_hostname, ssh.client.software_version, ssh.client.proto_version, server_hostname, ssh.server.software_version, ssh.server.proto_version fields. This also draws a statistical analysis graph of applications according to real-time and timespan searches.



Time	client_hostname	ssh.client.software_version	ssh.client.proto_version	server_hostname	ssh.server.software_version	ssh.server.proto_version
Nov 4, 2019 @ 22:25:51.092	10.212.134.100	PuTTY_Release_0.70	2.0	192.168.10.108	OpenSSH_7.6p1 Ubuntu-4ubuntu0.3	2.0

Raw Logs

Raw Logs tab visualize logs application services records details by our Digihunt engine. It shows the visualization of all SMB related records in Time, node.hostname, log_severity, event.subtype, client_hostname, server_hostname, service_name, flow.bytes, flow pkts fields. This also draws a statistical analysis graph of applications according to real-time and timespan searches.



Time	node.hostname	log.severity	event.subtype	client_hostname	server_hostname	service_name	flow.bytes	flow.pkts
Nov 4, 2019 @ 22:33:00.734	digi-hunts	informational	dns	192.168.10.253	202.53.9.2	dns (UDP/53)	-	-
Nov 4, 2019 @ 22:32:59.000	digi-hunts	informational	flow	192.168.10.128	192.168.11.4	TCP/49154	380B	5
Nov 4, 2019 @ 22:32:59.000	digi-hunts	informational	flow	192.168.11.200	192.168.11.5	elastic-beats (TCP/5044)	17.87KB	14
Nov 4, 2019 @ 22:32:59.000	digi-hunts	informational	flow	192.168.10.4	192.168.11.5	elastic-beats (TCP/5044)	17.87KB	14
Nov 4, 2019 @ 22:32:58.000	digi-hunts	informational	flow	192.168.9.11	8.8.8.8	dns (UDP/53)	221B	2
Nov 4, 2019 @ 22:32:58.000	digi-hunts	informational	flow	192.168.10.128	172.16.1.1	microsoft-ds (TCP/445)	198B	3
Nov 4, 2019 @ 22:32:58.000	digi-hunts	informational	flow	192.168.10.128	172.16.2.1	microsoft-ds (TCP/445)	198B	3
Nov 4, 2019 @ 22:32:58.000	digi-hunts	informational	flow	192.168.14.51	192.168.10.4	ldap (TCP/389)	2.39KB	5
Nov 4, 2019 @ 22:32:58.000	digi-hunts	informational	flow	192.168.14.51	192.168.10.4	ldap (TCP/389)	2.39KB	5
Nov 4, 2019 @ 22:32:58.000	digi-hunts	informational	flow	192.168.11.10	192.168.11.5	elastic-beats (TCP/5044)	553B	6
Nov 4, 2019 @ 22:32:58.000	digi-hunts	informational	flow	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)	420B	4
Nov 4, 2019 @ 22:32:58.000	digi-hunts	informational	flow	192.168.11.200	192.168.11.5	elastic-beats (TCP/5044)	1.85KB	5
Nov 4, 2019 @ 22:32:57.431	digi-hunts	warning	alert	10.212.134.100	192.168.11.4	iscsi-target (TCP/3260)	420B	4

Digintrude Infosec Pvt Ltd.
611, Manjeera Majestic Commercial,
JNTU Road, Hyderabad - 500072,
Telangana, India.
Ph: +91 70935 28540
Email: sales@digintrude.com
Url: www.digintrude.com