VIT®

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE ENGINEERING AND
INFORMATION
SYSTEMS

CSE3502 – INFORMATION SECURITY MANAGEMENT

ASSESSMENT - 1

NAME : MOHAMMED TAHA HASAN K

REG.NO : 20MIS0015

FACULTY : PROF. SIVA RAMA KRISHNAN S

QUESTION :

As a security analyst, formulate a report to detect abnormal system behaviours by applying behavioural analytics to network traffic data using any NDR tool.

NDR Tool – Corelight

Introduction:

Traditional security solutions struggle with modern threats. Network Detection and Response (NDR) tools empower us to move beyond reaction and actively hunt for suspicious activity using advanced network traffic analysis.

This report explores how Corelight, a powerful NDR platform, leverages behavioral analytics to identify abnormal system behaviors indicative of potential security breaches.

Methodology:

1. **Gathering Network Intelligence:** Corelight sensors strategically placed throughout the network capture traffic data from various sources.
2. **Unveiling Hidden Threats:** Corelight's advanced behavioral analytics algorithms dissect network traffic patterns, extracting valuable insights and uncovering anomalies that might signal security threats.
3. **Spotting the Unusual:** Deviations from established network behavior trigger alerts within Corelight's anomaly detection engine, prompting investigation of potential security incidents.
4. **Rapid Response:** Upon detecting abnormal behaviors, Corelight provides real-time alerts with contextual information to facilitate swift incident response and mitigation.

Findings:

1. **Seeing the Bigger Picture:** Corelight grants security analysts complete visibility into network traffic, enabling them to effectively monitor and analyze network activity.
2. **Beyond the Obvious:** Corelight's behavioral analytics capabilities go beyond traditional threat detection, uncovering insider threats, malware infections, and other suspicious network activity.

3. **Understanding User Behavior:** Corelight facilitates the creation of behavioral profiles for users, devices, and applications. This allows for more precise anomaly detection and accurate threat identification.
4. **Enhancing Threat Detection:** Corelight integrates with external threat intelligence feeds. This enriches network traffic data with information about known malicious actors and activities, further improving the accuracy of anomaly detection.

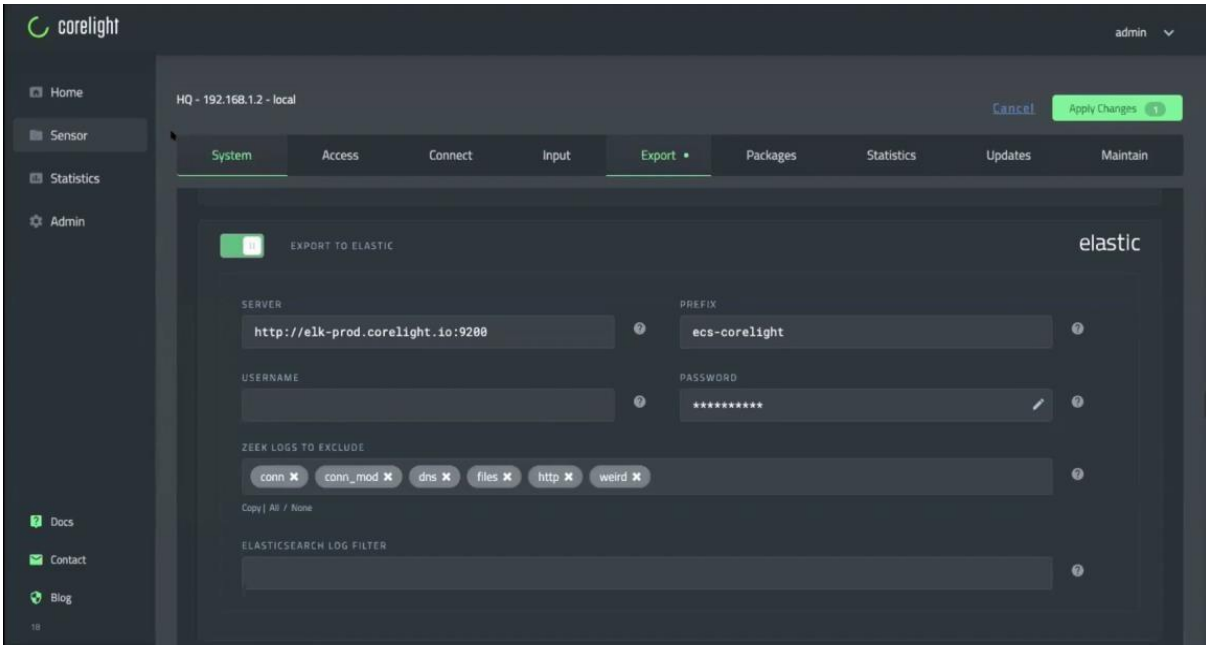
Recommendations:

1. **Constant Vigilance:** Implement continuous network traffic monitoring with Corelight for real-time detection and response to abnormal system behaviors.
2. **Proactive Threat Hunting:** Leverage Corelight's capabilities to proactively hunt for potential security threats that might bypass traditional security measures.
3. **Empowering Your Team:** Provide training and education to security personnel on utilizing Corelight and best practices for analyzing and responding to detected threats.
4. **Staying Ahead of the Curve:** Regularly update Corelight sensors with the latest threat intelligence and software patches to maintain effectiveness against ever-evolving threats.

Conclusion:

By leveraging Corelight's behavioral analytics on network traffic data, organizations can shift towards a proactive security posture. This allows for the identification of abnormal system behaviors indicative of potential security incidents, ultimately enhancing the protection of sensitive data and critical assets from cyberattacks.

SNIPS (DEMO)



EXPORT TO ELASTIC

SERVER: http://elk-prod.corelight.io:9200

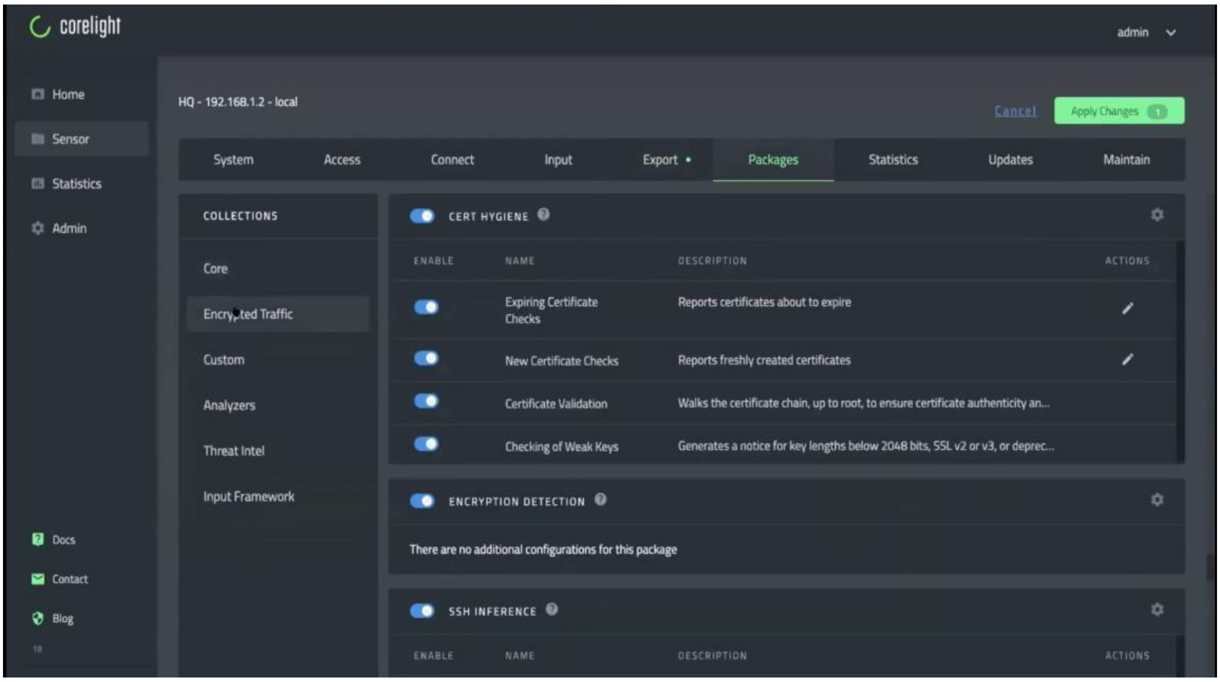
PREFIX: ecs-corelight

USERNAME:

PASSWORD: **********

ZEEK LOGS TO EXCLUDE: conn, conn_mod, dns, files, http, weird

ELASTICSEARCH LOG FILTER:



CERT HYGIENE

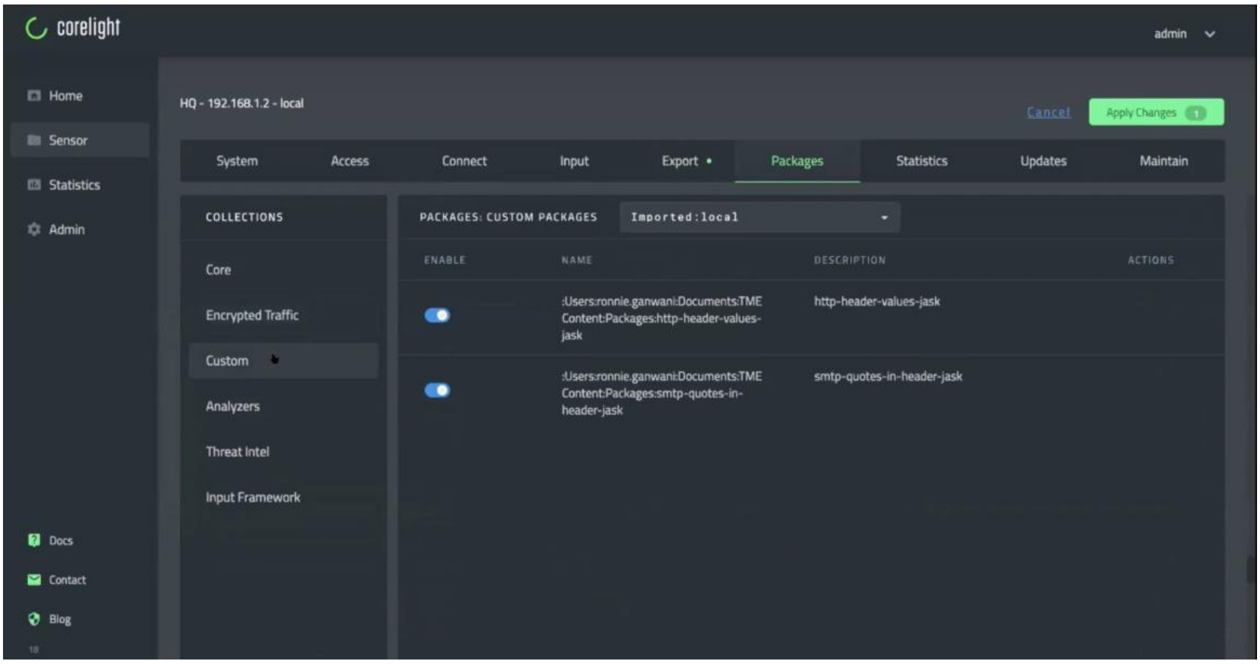
ENABLE	NAME	DESCRIPTION	ACTIONS
●	Expiring Certificate Checks	Reports certificates about to expire	✎
●	New Certificate Checks	Reports freshly created certificates	✎
●	Certificate Validation	Walks the certificate chain, up to root, to ensure certificate authenticity an...	
●	Checking of Weak Keys	Generates a notice for key lengths below 2048 bits, SSL v2 or v3, or deprec...	

ENCRYPTION DETECTION

There are no additional configurations for this package

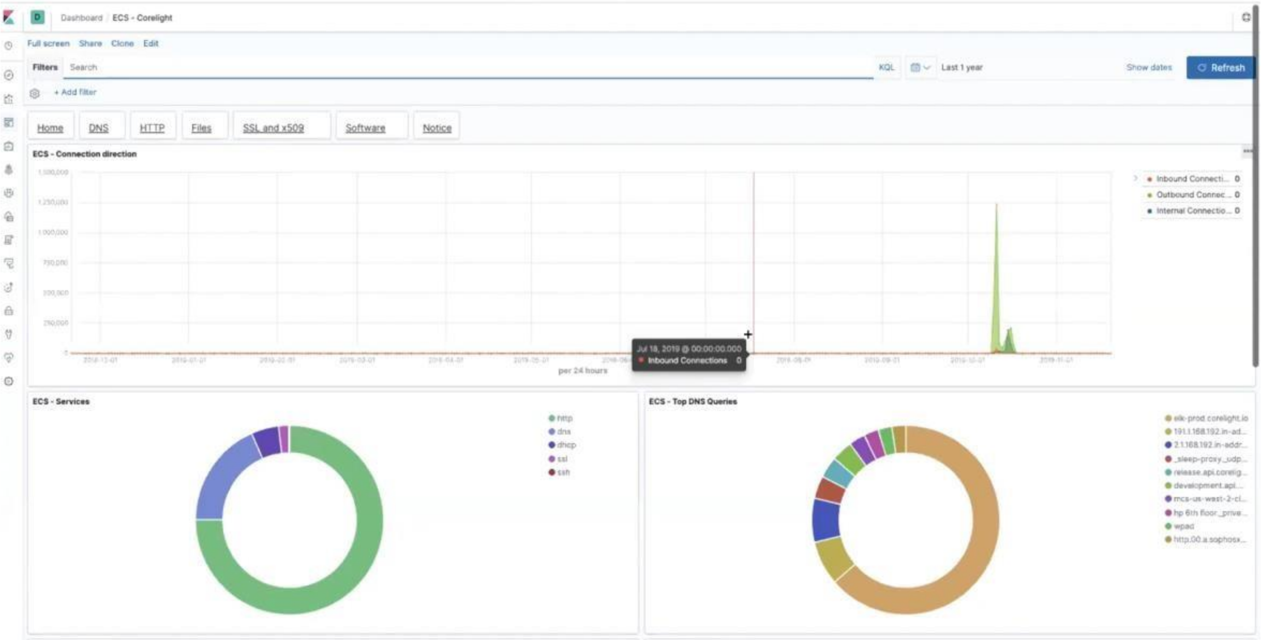
SSH INFERENCE

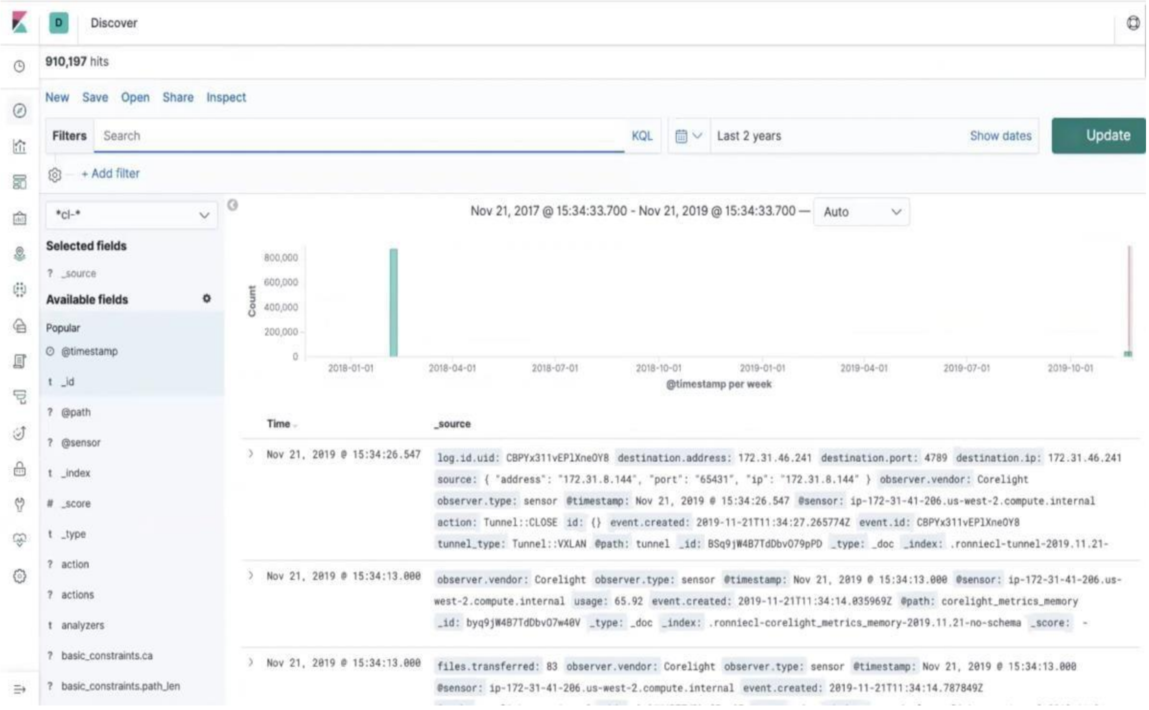
ENABLE	NAME	DESCRIPTION	ACTIONS



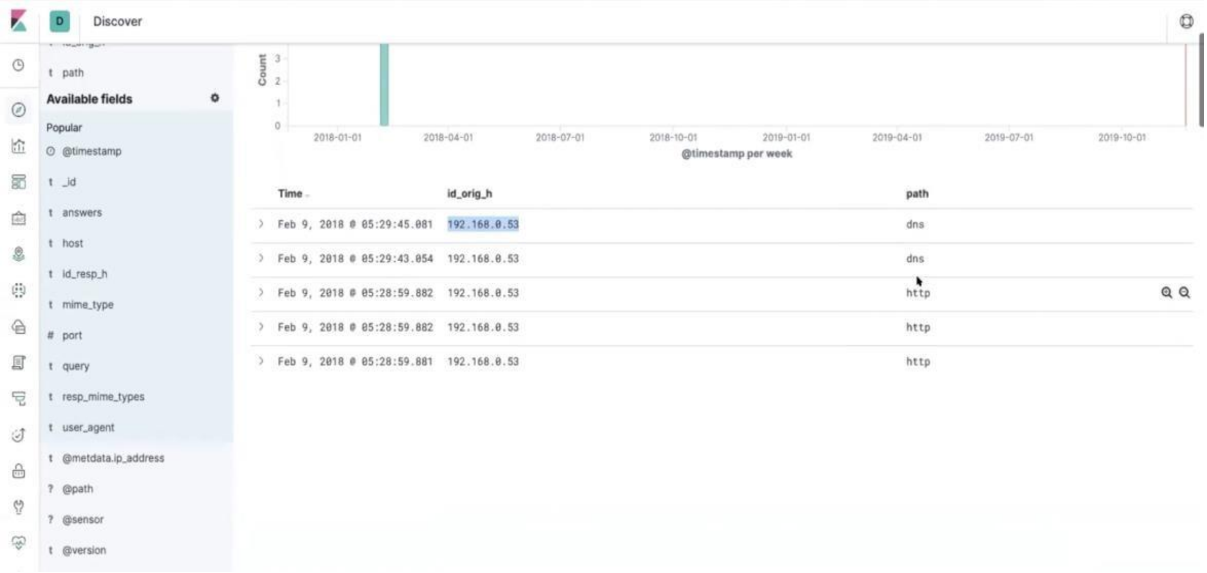
PACKAGES: CUSTOM PACKAGES Imported:local

ENABLE	NAME	DESCRIPTION	ACTIONS
●	:Users:ronnie.ganwani:Documents:TME Content:Packages:http-header-values-jask	http-header-values-jask	
●	:Users:ronnie.ganwani:Documents:TME Content:Packages:smtp-quotes-in-header-jask	smtp-quotes-in-header-jask	

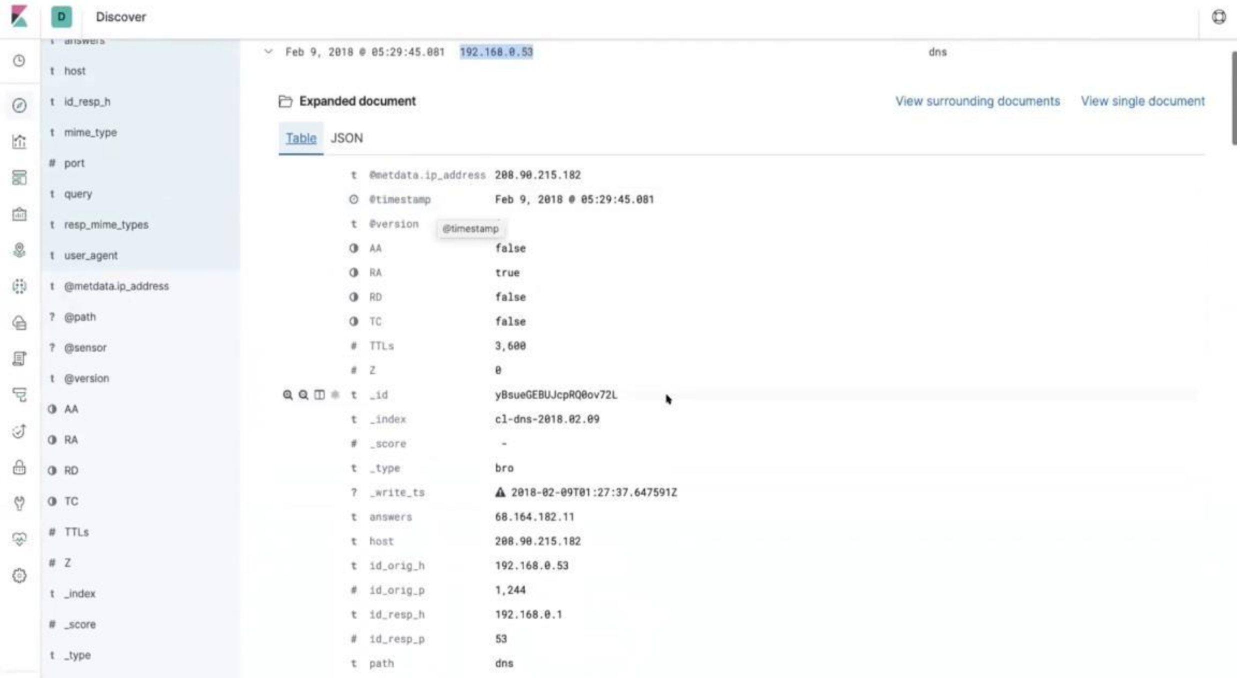




```
Time        _source
Nov 21, 2019 @ 15:34:26.547   log.id.uid: CBPYx311vEPlXneOY8 destination.address: 172.31.46.241 destination.port: 4789 destination.ip: 172.31.46.241
                              source: { "address": "172.31.8.144", "port": "65431", "ip": "172.31.8.144" } observer.vendor: Corelight
                              observer.type: sensor @timestamp: Nov 21, 2019 @ 15:34:26.547 @sensor: ip-172-31-41-206.us-west-2.compute.internal
                              action: Tunnel::CLOSE id: {} event.created: 2019-11-21T11:34:27.265774Z event.id: CBPYx311vEPlXneOY8
                              tunnel_type: Tunnel::VXLAN @path: tunnel _id: BSq9jW4B7TdDbvO79pPD _type: _doc _index: .ronniecl-tunnel-2019.11.21-
Nov 21, 2019 @ 15:34:13.000   observer.vendor: Corelight observer.type: sensor @timestamp: Nov 21, 2019 @ 15:34:13.000 @sensor: ip-172-31-41-206.us-
                              west-2.compute.internal usage: 65.92 event.created: 2019-11-21T11:34:14.035969Z @path: corelight_metrics_memory
                              _id: byq9jW4B7TdDbvO7w40V _type: _doc _index: .ronniecl-corelight_metrics_memory-2019.11.21-no-schema _score: -
Nov 21, 2019 @ 15:34:13.000   files.transferred: 83 observer.vendor: Corelight observer.type: sensor @timestamp: Nov 21, 2019 @ 15:34:13.000
                              @sensor: ip-172-31-41-206.us-west-2.compute.internal event.created: 2019-11-21T11:34:14.787849Z
```



```
Time                          id_orig_h       path
Feb 9, 2018 @ 05:29:45.081    192.168.0.53    dns
Feb 9, 2018 @ 05:29:43.054    192.168.0.53    dns
Feb 9, 2018 @ 05:28:59.882    192.168.0.53    http
Feb 9, 2018 @ 05:28:59.882    192.168.0.53    http
Feb 9, 2018 @ 05:28:59.881    192.168.0.53    http
```



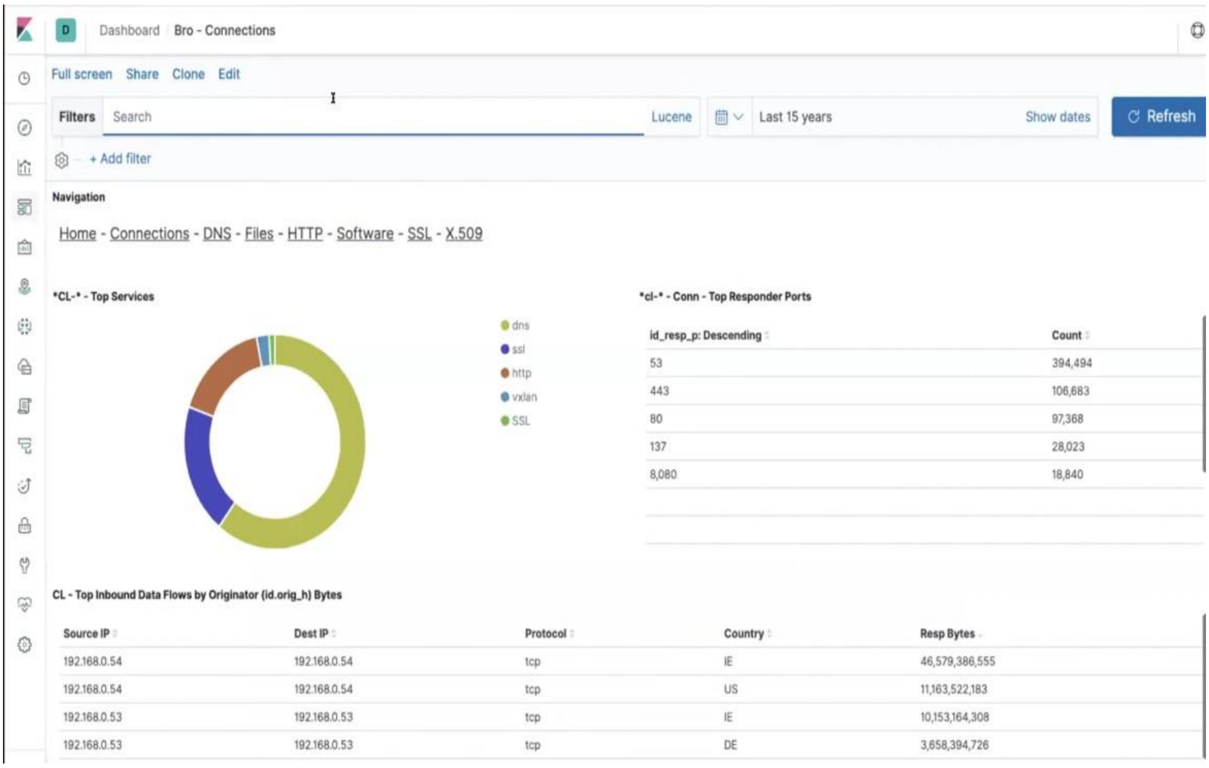
```
Feb 9, 2018 @ 05:29:45.081   192.168.0.53                                    dns
```

Expanded document

View surrounding documents   View single document

Table   JSON

	Field	Value
t	@metdata.ip_address	208.90.215.182
⊙	@timestamp	Feb 9, 2018 @ 05:29:45.081
t	@version	
◑	AA	false
◑	RA	true
◑	RD	false
◑	TC	false
#	TTLs	3,600
#	Z	0
t	_id	yBsueGEBUJcpRQ0ov72L
t	_index	cl-dns-2018.02.09
#	_score	-
t	_type	bro
?	_write_ts	⚠ 2018-02-09T01:27:37.647591Z
t	answers	68.164.182.11
t	host	208.90.215.182
t	id_orig_h	192.168.0.53
#	id_orig_p	1,244
t	id_resp_h	192.168.0.1
#	id_resp_p	53
t	path	dns



Navigation

Home - Connections - DNS - Files - HTTP - Software - SSL - X.509

CL- - Top Services

cl- - Conn - Top Responder Ports

id_resp_p: Descending	Count
53	394,494
443	106,683
80	97,368
137	28,023
8,080	18,840

CL - Top Inbound Data Flows by Originator (id.orig_h) Bytes

Source IP	Dest IP	Protocol	Country	Resp Bytes
192.168.0.54	192.168.0.54	tcp	IE	46,579,386,555
192.168.0.54	192.168.0.54	tcp	US	11,163,522,183
192.168.0.53	192.168.0.53	tcp	IE	10,153,164,308
192.168.0.53	192.168.0.53	tcp	DE	3,658,394,726