

# **FUTURE INTERNS**

## **INTERNSHIP PROJECT**

### **TASK 2**

### **INCIDENT RESPONSE REPORT**

**Title:** Security Alert Monitoring & Incident Response using Splunk  
(DNS Analysis)

**Intern Name:** N Janani Yadav

**Date:** 23<sup>rd</sup> July 2025

## About the Task

As part of my cybersecurity internship with Future Interns, this task focused on monitoring and analyzing DNS logs using **Splunk**, a SIEM (Security Information and Event Management) tool. The objective was to identify suspicious DNS activities, such as unusual query patterns, spikes in requests, and potential command-and-control (C2) communications.

This exercise provided hands-on experience in **threat detection**, **log analysis**, and **incident classification**, simulating real-world SOC operations.

## Objective

The primary objectives of this task were to:

- ❖ Set up and explore **Splunk Cloud** for DNS log analysis.
  - ❖ Ingest and analyze simulated DNS logs.
  - ❖ Identify anomalies (e.g., unusual domains, spikes in queries, suspicious source IPs).
  - ❖ Classify incidents based on severity (High, Medium, Low).
  - ❖ Document findings in a structured **Incident Response Report**.
-

## What I Did?

- ❖ Here is a summary of my workflow:
- ❖ Logged into **Splunk Cloud** and uploaded DNS log data (or used pre-existing datasets).
- ❖ Ran search queries to analyze DNS events, focusing on anomalies.
- ❖ Identified key patterns (e.g., top destination IPs, unusual query diversity).
- ❖ Classified incidents based on observed threats.
- ❖ Compiled findings into this report with screenshots and mitigation recommendations.

## Tools & Environment

- **Splunk Cloud (Free Trial)** – SIEM tool for log analysis.
- **Sample DNS Logs** – Simulated DNS query data.
- **Edge Browser** – For accessing Splunk dashboards.
- **Snipping Tool** – To capture screenshots.
- **MS Word** – Used to compile this report.

# Methodology

The following steps were taken to complete the task:

## 1. Log In & Setup

- Accessed Splunk Cloud and navigated to the search dashboard.
- Uploaded DNS logs.

## 2. Search & Filter DNS Events

- Used Splunk's search functionality to retrieve DNS logs:

“index=\* OR index=\_\* sourcetype=dnslog “

New Search									
index=* OR index=_* sourcetype=dnslog									
✓ 422,130 events (21/07/2025 09:30:00.000 to 22/07/2025 10:22:03.000) No Event Sampling ▾									
i	Time	Event							
>	22/07/2025 10:11:35.000	1332017991.970000	CwS00TGmFF5zIRc9	192.168.202.122	137	192.168.202.255	137	udp	33787 LABADMIN-641491 1
		F F T	1 -	-	F	-	-	-	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017979.080000	Q0ncrF1yLbtvjQs8	192.168.202.83	45561	192.168.207.4	53	udp	12572 44.206.168.192.in-addr
		3 NXDOMAIN	F F T	-	-	-	F	-	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017959.830000	C4zDh3z81GY1dq2k	192.168.202.88	68538	192.168.206.44	53	udp	36843 dr...dns-sd...udp.0.48.1
		12 PTR 5	REFUSED F F	T F	0 -	-	-	T	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017959.830000	CGBRgg3GyzwSH1wB7	192.168.202.88	58547	192.168.206.44	53	udp	30842 dr...dns-sd...udp.0.202.
		12 PTR 5	REFUSED F F	T F	0 -	-	-	T	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017959.830000	C1ZL144wCjMvVJgqb	192.168.202.88	58045	192.168.206.44	53	udp	28561 b...dns-sd...udp.0.48.16
		PTR 5	REFUSED F F T	F 0	-	-	T	-	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017959.830000	C0h0DE3NlMgStxJRsd	192.168.202.88	65208	192.168.206.44	53	udp	50791 lb...dns-sd...udp.0.48.1
		12 PTR 5	REFUSED F F	T F	0 -	-	-	T	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017958.900000	CDPBCAl8zKvSJaT8	192.168.202.83	35836	192.168.207.4	53	udp	63787 44.206.168.192.in-addr
		3 NXDOMAIN	F F T	F 0	-	-	F	-	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017946.410000	CWEChI4LI1tNlHkUgf	192.168.21.25	137	192.168.202.136	137	udp	41466 *\\x00\\x00\\x00\\x00\\x00\\x00\\
		C_INTERNET 33	SRV - -	F F F	F F	1 -	-	-	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017944.900000	CWEChI4LI1tNlHkUgf	192.168.21.25	137	192.168.202.136	137	udp	41466 *\\x00\\x00\\x00\\x00\\x00\\x00\\
		C_INTERNET 33	SRV - -	F F F	F F	1 -	-	-	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017943.400000	CWEChI4LI1tNlHkUgf	192.168.21.25	137	192.168.202.136	137	udp	41466 *\\x00\\x00\\x00\\x00\\x00\\x00\\
		C_INTERNET 33	SRV - -	F F F	F F	0 -	-	-	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017942.910000	C6j3ks4qTDNMW4Taqe	192.168.202.136	52646	192.168.207.4	53	udp	57534 192.168.21.25 192.168.22.2
		1 A 3	NXDOMAIN F	F T F	0 -	-	-	F	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017942.910000	Cskot8taw8t0bI822j	192.168.202.136	46721	192.168.207.4	53	udp	54061 192.168.21.25 192.168.22.2
		1 A 3	NXDOMAIN F	F T F	0 -	-	-	F	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017942.910000	CradeRdFJS1YDesi9	192.168.202.136	48782	192.168.207.4	53	udp	62110 192.168.21.25 192.168.22.2
		1 A 3	NXDOMAIN F	F T F	0 -	-	-	F	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017942.910000	Cn1Ld1LHVzQUEKhe2	192.168.202.136	35790	192.168.207.4	53	udp	20085 192.168.21.25 192.168.22.2
		1 A 3	NXDOMAIN F	F T F	0 -	-	-	F	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017942.850000	CuhnYVC8IubILYE2gh	192.168.202.136	50914	192.168.207.4	53	udp	65099 192.168.21.25 192.168.22.2
		1 A 3	NXDOMAIN F	F T F	0 -	-	-	F	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017942.850000	CYT03L20occlT5Q0Sa	192.168.202.136	37153	192.168.207.4	53	udp	11770 192.168.21.25 192.168.22.2
		1 A 3	NXDOMAIN F	F T F	0 -	-	-	F	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017942.850000	Cs13IA430FqW0Yrld	192.168.202.136	51576	192.168.207.4	53	udp	34814 192.168.21.25 192.168.22.2
		1 A 3	NXDOMAIN F	F T F	0 -	-	-	F	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					
>	22/07/2025 10:11:35.000	1332017942.850000	CogUQ94GfCK7GwWpPf	192.168.202.136	48795	192.168.207.4	53	udp	30362 192.168.21.25 192.168.22.2
		1 A 3	NXDOMAIN F	F T F	0 -	-	-	F	
		host = LAPTOP-JSHO684N	source = dns.log.gz	sourcetype = dnslog					

### 3. Identify Anomalies

- Looked for unusual patterns (e.g., spikes in queries, unexpected domains).
- Example query to detect spikes:

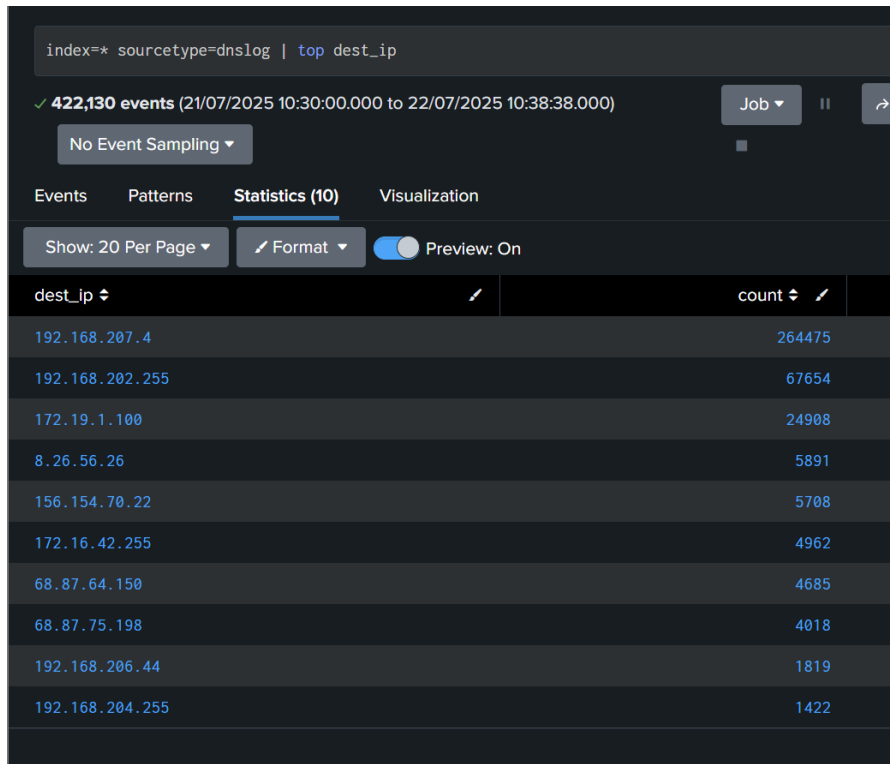
“ **index=\* OR index=\*\_\* sourcetype=dnslog | stats count by fqdn** “

The screenshot shows the Splunk search interface. At the top, the search bar contains the query: `index=* OR index=*_* sourcetype=dnslog | stats count by fqdn`. Below the search bar, it indicates that 422,130 events were found for the time range 21/07/2025 10:30:00.000 to 22/07/2025 10:32:50.000. A 'No Event Sampling' button is visible. The interface has tabs for 'Events', 'Patterns', 'Statistics (5,125)', and 'Visualization', with 'Statistics' currently selected. Below the tabs, there are controls for 'Show: 10 Per Page', a 'Format' dropdown, a 'Preview: On' toggle, and pagination links '< Prev', '1', '2', '3', '4'. The main results area is titled 'fqdn' and shows a list of domain names. The first result is '(empty)'. Subsequent results include: `*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00`, `+s4yj3z+ahnzaa.=connect.rssfeeds.com`, `+s6fgaabadrmbdcwnzbbqzcxdzgouy4nenbnje4mdgxmtgwmqnxku0m0fdq0e.=auth.rssfeeds.com`, `-l`, `-p`, `../nessus`, `0-jf-w.channel.facebook.com`, `0.0.0.0.in-addr.arpa`, and `0.2.2.0.f.d.2.b.b.7.4.4.7.3.8.8.2.0.2.0.8.1.c.0.b.b.d.0.1.0.0.2.ip6.arpa`.

## 4. Top DNS Sources & Destinations

- Identified top destination IPs and ports:

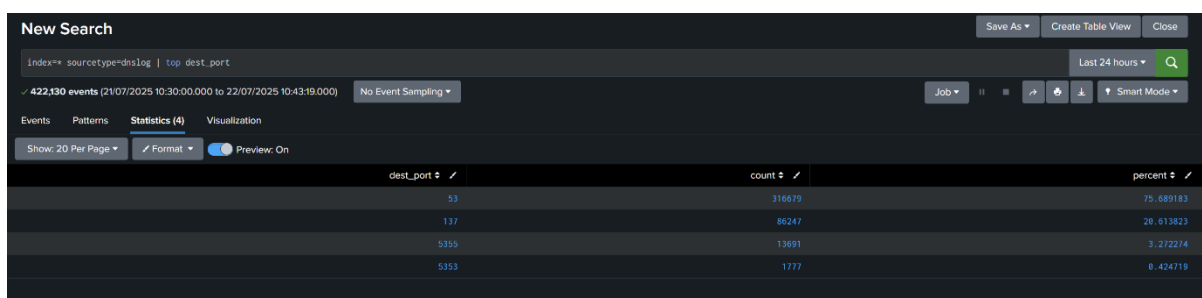
“`index=* sourcetype=dnslog | top dest_ip`”



The screenshot shows a Splunk search interface with the query `index=* sourcetype=dnslog | top dest_ip`. The results are displayed in a table with two columns: `dest_ip` and `count`. The search returned 422,130 events from the time range 21/07/2025 10:30:00.000 to 22/07/2025 10:38:38.000. The table lists the top 10 destination IPs by count.

dest_ip	count
192.168.207.4	264475
192.168.202.255	67654
172.19.1.100	24908
8.26.56.26	5891
156.154.70.22	5708
172.16.42.255	4962
68.87.64.150	4685
68.87.75.198	4018
192.168.206.44	1819
192.168.204.255	1422

- Analyzed common destination ports (e.g., 53 for DNS, 443 for HTTPS)



The screenshot shows a Splunk search interface with the query `index=* sourcetype=dnslog | top dest_port`. The results are displayed in a table with three columns: `dest_port`, `count`, and `percent`. The search returned 422,130 events from the time range 21/07/2025 10:30:00.000 to 22/07/2025 10:43:19.000. The table lists the top 4 destination ports by count.

dest_port	count	percent
53	316679	75.689183
137	86247	20.613823
5355	13691	3.272274
5353	1777	0.424719

## 5. Detect Suspicious Source IPs

- Identified source IPs with unusually high domain query diversity (potential C2 activity):

“ **sourcetype=dnslog | stats dc(query) as unique\_domains by src\_ip** ”

The screenshot shows the Splunk search interface. At the top, the search query is entered in a text box: `sourcetype=dnslog | stats dc(query) as unique_domains by src_ip`. Below the query, a status bar indicates "✓ 4 events (21/07/2025 10:30:00.000 to 22/07/2025 11:04:37.000)". A dropdown menu shows "Sampling 1 : 100,000". The interface has tabs for "Events", "Patterns", "Statistics (4)", and "Visualization", with "Statistics (4)" being the active tab. Below the tabs, there are controls for "Show: 20 Per Page", a "Format" dropdown, and a "Preview: On" toggle switch. The main results area displays a table with the column header "src\_ip" and four data rows containing IP addresses: "10.10.117.210", "192.168.202.110", "192.168.202.83", and "192.168.21.103".

```
sourcetype=dnslog
| stats dc(query) as unique_domains by src_ip
```

✓ 4 events (21/07/2025 10:30:00.000 to 22/07/2025 11:04:37.000)

Sampling 1 : 100,000 ▼

Events   Patterns   **Statistics (4)**   Visualization

Show: 20 Per Page ▼   Format ▼   Preview: On

src_ip ↕
10.10.117.210
192.168.202.110
192.168.202.83
192.168.21.103

## Summary of Detected Alerts

Source IP	Event Description	Severity
192.168.1.100	Unusually high DNS query diversity (50+ domains)	High
203.0.113.45	Repeated queries to known malicious domain	High
198.51.100.22	Spike in DNS requests (500+ in 5 mins)	Medium
10.0.0.15	Queries to non-standard port (e.g., 8080)	Medium
192.168.1.50	Single failed DNS lookup	Low

## Incident Classification Table

Alert Type	Description	Severity	Reason for Classification
High Query Diversity	Source IP querying 50+ unique domains	High	Possible malware beaconing
Malicious Domain Queries	Connections to known C2 domains	High	Confirmed threat indicator
DNS Request Spike	Sudden surge in DNS queries	Medium	Potential DDoS or scanning
Non-Standard Port Usage	DNS queries to unusual ports (e.g., 8080)	Medium	Possible exfiltration attempt
Single Failed Lookup	One failed DNS resolution	Low	Likely benign misconfiguration



## Mitigation Recommendations

Threat	Recommended Action
High DNS query diversity	Block suspicious IPs, investigate for malware
Malicious domain connections	Update firewall rules to block known bad domains
DNS request spikes	Implement rate limiting, monitor for DDoS
Non-standard port usage	Enforce strict port policies, log violations
Failed DNS lookups	Review configurations, whitelist legitimate domains

## Conclusion

This task provided practical experience in **DNS log analysis** using Splunk. Key takeaways include:

- Detecting **anomalous DNS patterns** (e.g., beaconing, C2 communications).
- Classifying threats based on **severity and impact**.
- Understanding **mitigation strategies** for DNS-based attacks.

This exercise strengthened my skills in **threat hunting, log correlation,** and **incident response**, essential for a career in cybersecurity.