Analyzing DNS Log Files Using Splunk SIEM

Project Overview

This project demonstrates **SOC-style DNS monitoring and threat hunting** using **Splunk SIEM** and **Wireshark**. The objective is to analyze DNS log data to identify anomalies, suspicious domains, and potential DNS-based Command-and-Control (C2) or data exfiltration techniques, while mapping detections to the **MITRE ATT&CK framework**.

Project Objectives

- Ingest and analyze DNS logs in Splunk
- Perform statistical and behavioral DNS analysis
- Detect anomalies related to DNS tunneling and C2
- Validate findings using Wireshark
- Map detections to MITRE ATT&CK
- Document findings in a SOC-style report

Tools & Technologies Used

- **Splunk Enterprise** (SIEM)
- **Wireshark** (Packet analysis)
- **Sample DNS Logs**
- **MITRE ATT&CK Framework**

Project Architecture

DNS Log Files
↓
Splunk SIEM (Indexing & Analysis)
↓
SOC Analysis & MITRE Mapping
↓
Wireshark (Packet Validation)

🗃️ Dataset Used

- **Source:** DNS Logs
- **Fields Exctrated:**
  - Source IP → src_ip
  - Destination IP → dst_ip
  - Domain Name →domain_name
  - Query Type → query
  - Response Code → response_code

🚀 Step-by-Step Roadmap (What I Did)

◇ Step 1: Prepare DNS Log Files

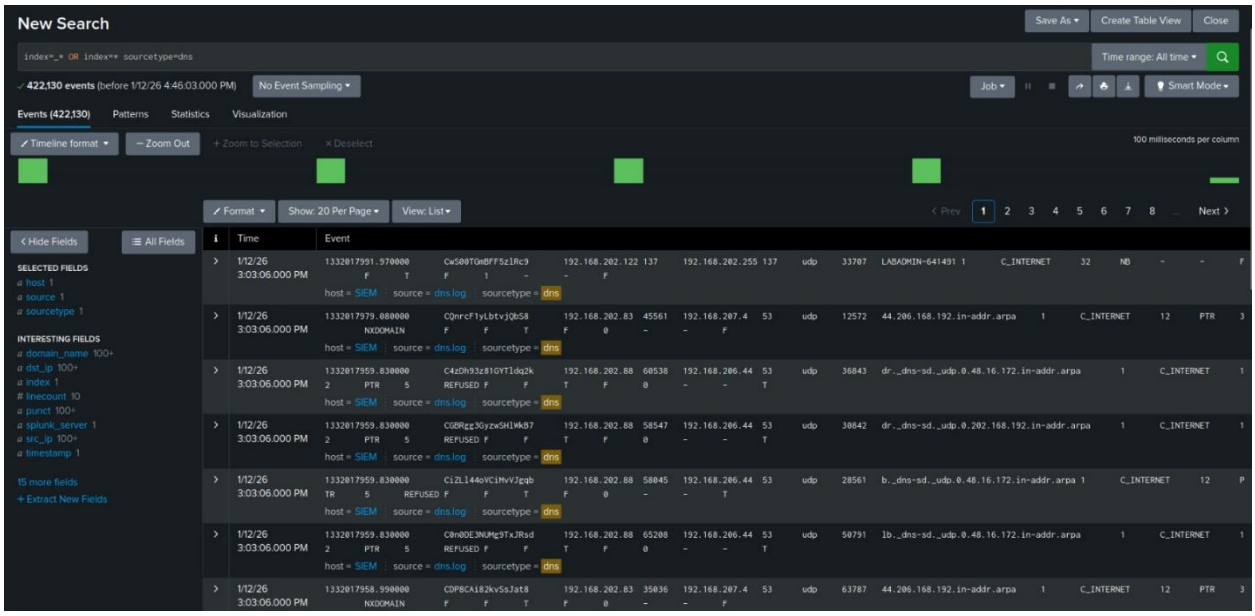
- Downloaded DNS logs from public repository
- Extracted and stored logs locally
- Ensured logs contained valid DNS events

◇ Step 2: Upload Logs into Splunk

- Navigated to **Settings → Add Data → Upload**
- Selected DNS log file
- Assigned:
  - **Sourcetype:** dns
- Completed ingestion and verified indexing

Verification SPL:

```
index=_* OR index=* sourcetype=dns
```



◇ Step 3: Initial DNS Event Exploration

Retrieved all DNS events to understand data structure.

index=_* OR index=* sourcetype=dns

◇ Step 4: Identify DNS-Related Events

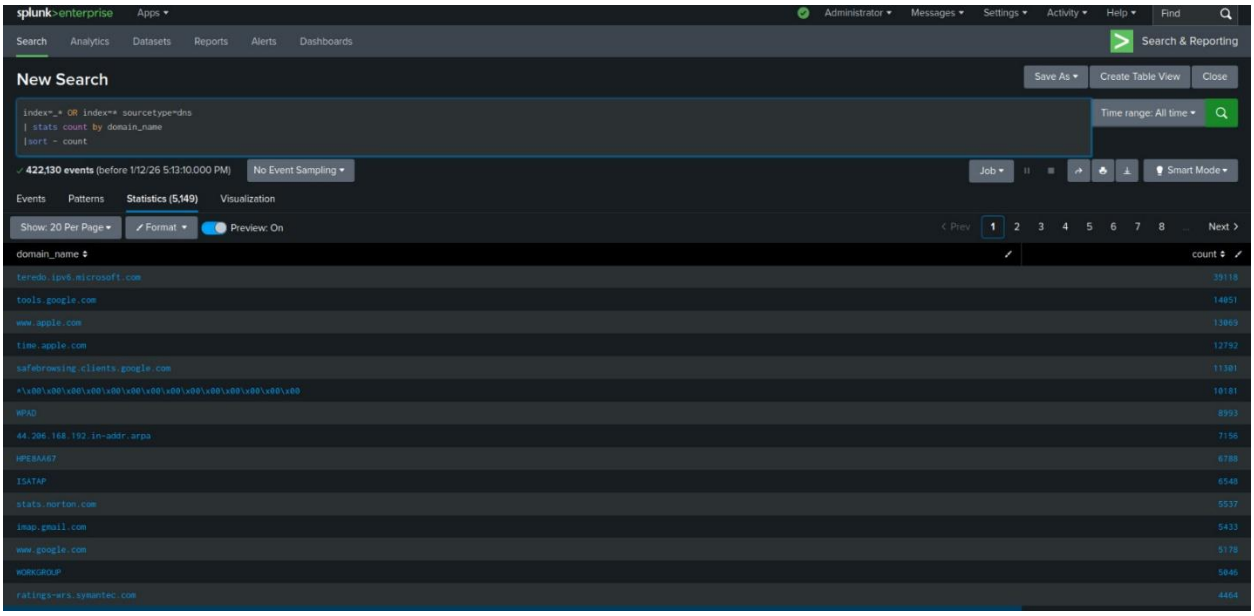
Filtered events using DNS-related keywords.

index=_* OR index=* sourcetype=dns
| regex _raw="(?i)\b(dns|domain|query|response|port 53)\b"

◇ Step 5: DNS Frequency & Statistical Analysis

Identified frequently queried domains.

index=_* OR index=* sourcetype=dns
| stats count by domain_name
| sort -count



◇ Step 6: Identify Top DNS Sources

Detected hosts generating the most DNS traffic.

```
index=_* OR index=* sourcetype=dns
| top domain_name, src_ip
```

◇ Step 7: Detect DNS Anomalies (Tunneling Indicators)

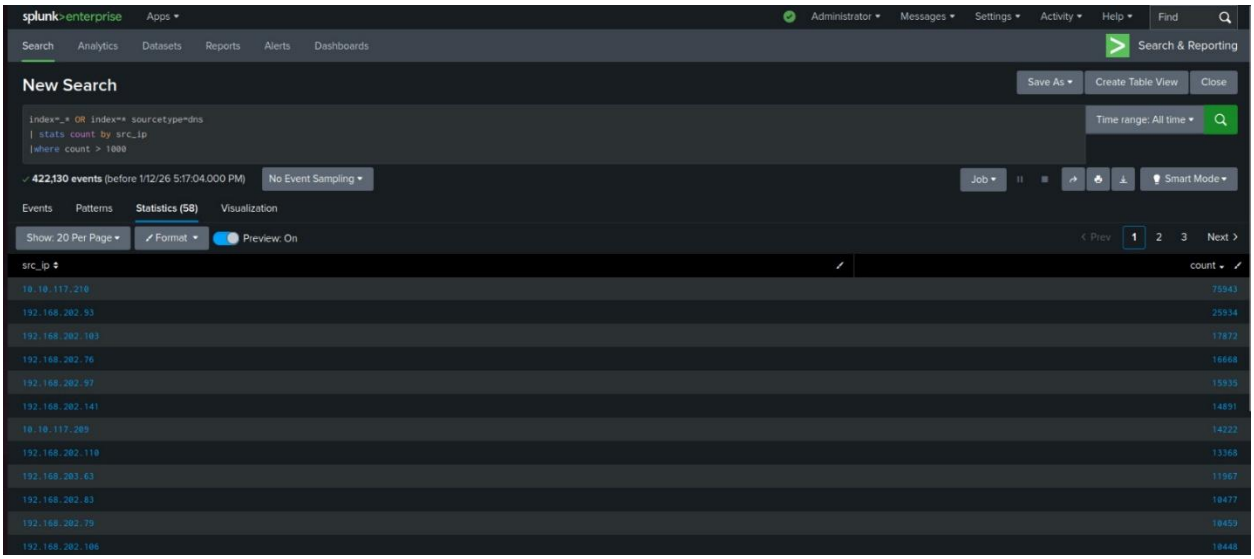
Checked for unusually long DNS queries (possible encoded data).

```
index=_* OR index=* sourcetype=dns
| eval domain_len=len(domain_name)
| where domain_len > 50
```

◇ Step 8: Detect High-Volume DNS Activity

Identified potential DNS beaconing behavior.

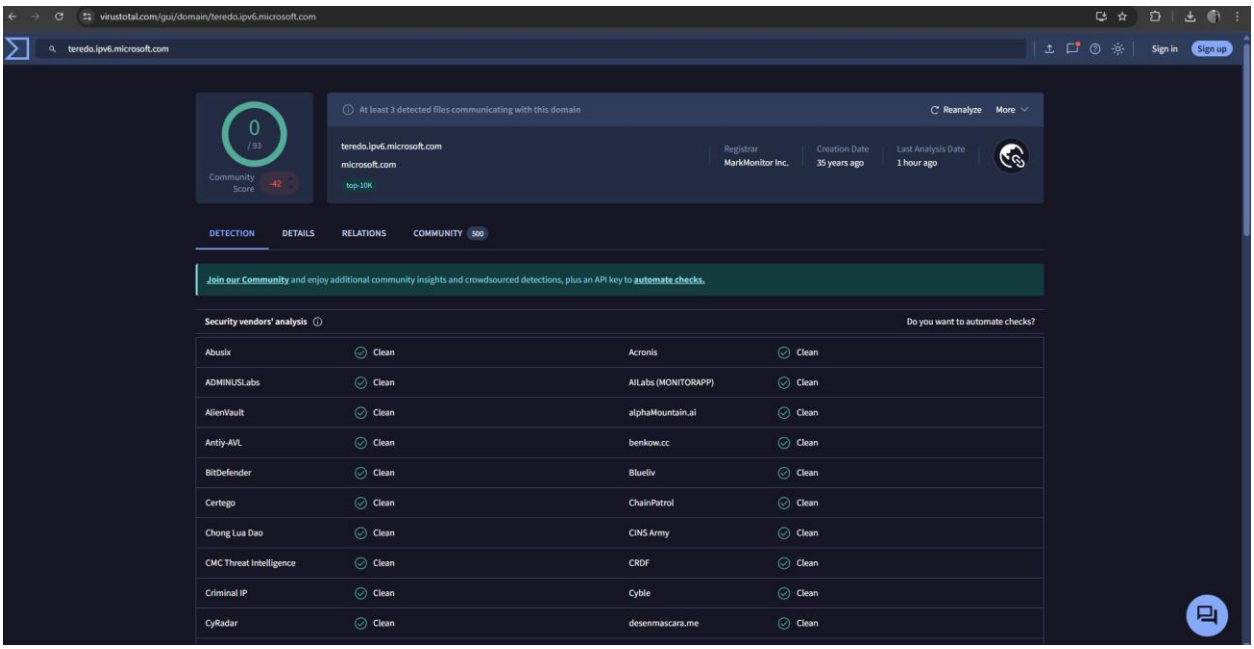
```
index=_* OR index=* sourcetype=dns
| stats count by src_ip
| where count > 1000
```



◇ Step 9: Suspicious Domain Investigation

Manually checked suspicious domains using threat intelligence sources (VirusTotal).

index=_* OR index=* sourcetype=dns domain_name="maliciousdomain.com"



◇ Step 10: Wireshark Packet Analysis

Used Wireshark to validate DNS behavior at packet level.

Wireshark Filters Used:

```
dns
dns && strlen(dns.qry.name) > 50
!mdns
```

Analyzed: - DNS query length - Subdomain patterns - Request frequency - Known tunneling patterns (dnscat, dns2tcp)

MITRE ATT&CK Mapping - https://attack.mitre.org/

Observed Behavior	Tactic	Technique	ID
Long DNS queries	Command & Control	DNS C2	T1071.004
High DNS frequency	Command & Control	Beaconing	T1071.004
Encoded subdomains	Exfiltration	Alt Protocol	T1048
DNS tunneling	Exfiltration	Alt Protocol	T1048

SOC Response & Investigation Steps (If Detected)

This section documents **what actions a SOC analyst would take** if the following DNS threats were detected. Even though no malicious activity was found in this project, defining response steps demonstrates **real-world SOC readiness**.

---

1. Long DNS Queries Detected

MITRE: T1071.004 – DNS-based Command & Control

Detection Indicator: - Abnormally long domain name- Possible encoded payloads in subdomains

SOC Response Steps: 1. Identify affected source host (src_ip) 2. Validate query length using Splunk and Wireshark 3. Check domain reputation using threat intelligence (VirusTotal) 4. Correlate with endpoint logs (Sysmon, Windows Event Logs) 5. Isolate the endpoint if suspicious behavior is confirmed 6. Block the domain at DNS firewall / proxy level 7. Escalate to Tier-2 SOC for malware investigation

---

2. High DNS Frequency (Beaconing)

MITRE: T1071.004 – Command & Control

Detection Indicator: - Repeated DNS queries to same domain - Regular time intervals (beaconing behavior)

SOC Response Steps:

1. Identify source IP generating excessive DNS traffic
2. Analyze query intervals for periodic patterns
3. Validate traffic in Wireshark (timestamp analysis)
4. Check endpoint for suspicious processes or persistence
5. Apply temporary network containment if required
6. Block C2 domain/IP
7. Document incident and update detection rules

---

3. Encoded Subdomains Detected

MITRE: T1048 – Exfiltration Over Alternative Protocol

Detection Indicator: - Random-looking, high-entropy subdomains - Base64 / hex-like patterns in DNS queries

SOC Response Steps:

1. Extract and analyze suspicious subdomain strings
2. Calculate entropy to confirm encoding
3. Inspect DNS packet payloads in Wireshark
4. Search for data exfiltration indicators
5. Isolate affected system
6. Preserve logs for forensic investigation
7. Notify incident response team

---

4. DNS Tunneling Detected

MITRE: T1048 – Exfiltration Over Alternative Protocol

Detection Indicator: - Large volume of long DNS queries - Known tunneling tool patterns (dnscat, dns2tcp)

SOC Response Steps:

1. Confirm tunneling behavior using Splunk + Wireshark
2. Identify tunneling tool signatures
3. Immediately block DNS communication for affected host
4. Capture memory and disk artifacts (forensics)
5. Reset credentials if data exposure is suspected
6. Perform root cause analysis
7. Update SOC playbooks and alerts

Findings

- No malicious domains detected
- DNS query lengths within normal limits
- No evidence of DNS tunneling or C2 activity
- DNS traffic behavior observed was normal

Conclusion

This project successfully demonstrates **SOC-level DNS monitoring and analysis** using Splunk SIEM and Wireshark. Although no malicious activity was identified, the project validates effective threat-hunting techniques and aligns detections with the MITRE ATT&CK framework.

SOC Incident Summary

- **Incident Status:** False Positive
- **Risk Level:** Low
- **Confidence:** High
