📡 DHCP Log Analysis Using Splunk SIEM

📌 Project Overview

This project demonstrates how a Security Operations Center (SOC) analyst can analyze DHCP logs using Splunk SIEM to monitor IP address assignments, detect anomalous network behavior, and identify unauthorized or suspicious clients.

The project follows a SOC workflow:

Log Ingestion → Field Extraction → Traffic Analysis → Anomaly Detection → IP Monitoring → Alerting

---

🎯 Project Objectives

- Monitor DHCP IP address assignments in real-time
- Identify unauthorized or rogue devices requesting IP addresses
- Detect anomalies in lease durations, IP renewals, or repeated requests
- Build SOC-ready detections for network security

🔹 Step-by-Step DHCP Analysis

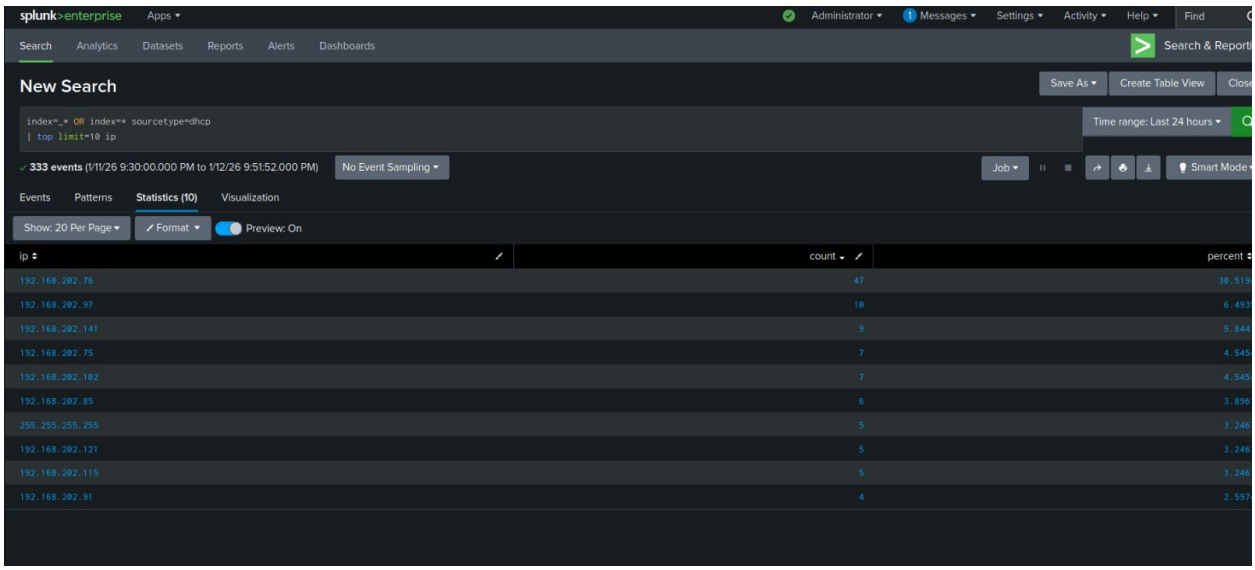
Step 1: Search for DHCP Events

Confirm that DHCP logs are ingested successfully:

index=main sourcetype=dhcp

✅ Check for:

- Correct timestamps



- Client IP addresses and MAC addresses
- Lease durations and server IP

Step 2: Extract Relevant Fields

Key fields to extract from DHCP logs:

- client_identifier / MAC address
- leased_ip / assigned IP
- lease_duration
- lease_renewal / status
- timestamp

Step 3: Analyze DHCP Traffic Patterns

Top Leased Ips:-

```
index=main sourcetype=dhcp
| top limit=10 leased_ip
```

IP Distribution Count:-

```
index=main sourcetype=dhcp
| stats count by leased_ip
```

These searches help understand network usage patterns and frequently assigned IPs.

Step 4: Detect Anomalies

DHCP Requests Over Time:-

```
index=main sourcetype=dhcp
| timechart span=1h count by _time
```

Unauthorized Client Requests:-

```
index=main sourcetype=dhcp
| search NOT client_identifier="authorized_identifier"
```

Multiple Lease Renewals:-

```
index=main sourcetype=dhcp
| stats count by leased_ip, lease_renewal
| where count > 1 AND lease_renewal="true"
```

🚨 **Alerts can be triggered when:**

- Unauthorized MAC addresses request IPs
- IPs are leased more than expected
- Lease durations deviate from normal

Step 5: Monitor IP Usage Patterns

Analyze DHCP traffic over longer periods to identify network deviations:-

```
index=main sourcetype=dhcp
| timechart span=1d count by leased_ip
```

This helps detect:

- Rogue devices
- Network misconfigurations
- Abnormal client behavior

📌 Conclusion

Analyzing DHCP logs with Splunk SIEM provides valuable insights into IP address management, helps detect rogue devices, and improves overall network security.