# SOC Analysis Report

DHCP Log Analysis in Splunk

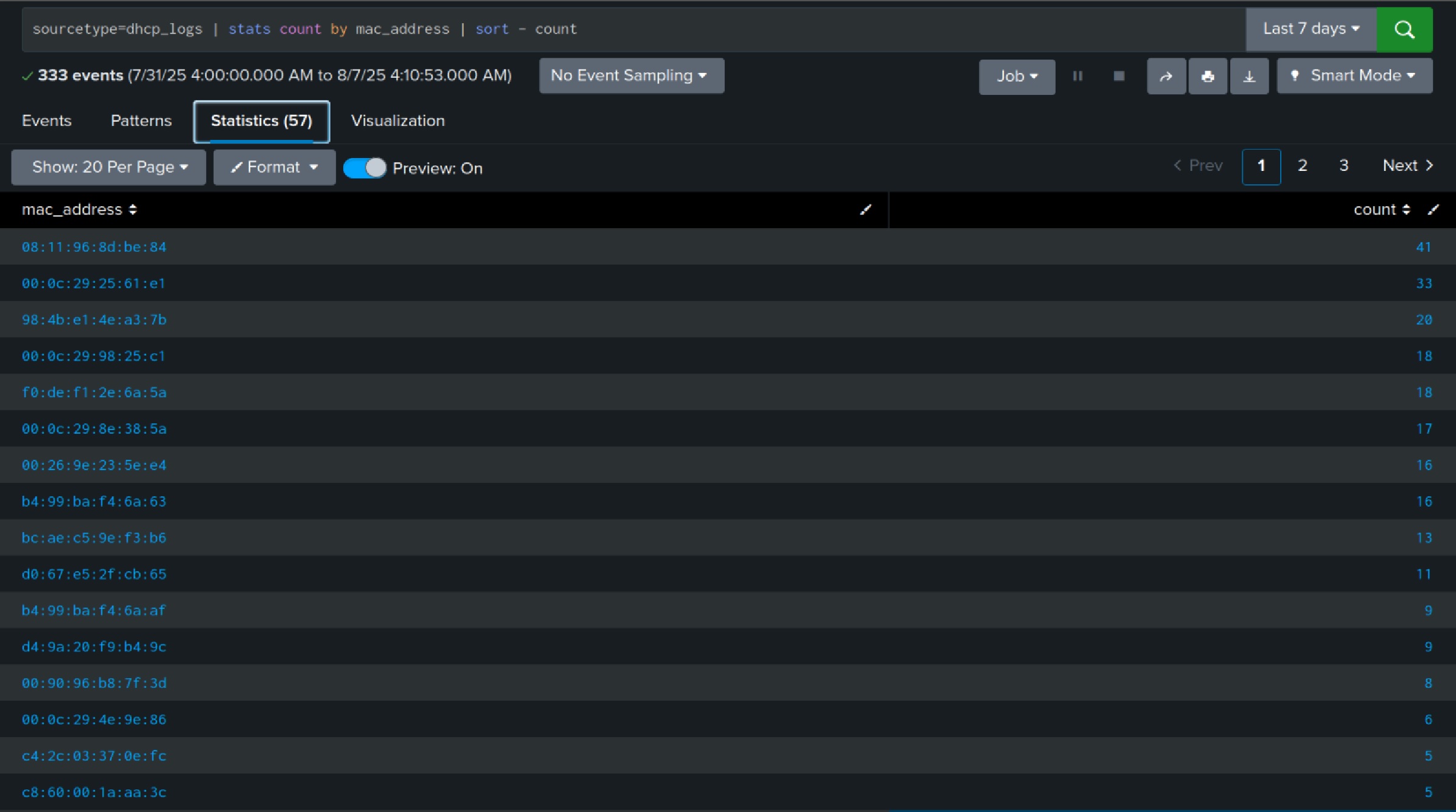
Author: Vlassov Vladislav

## Introduction

This SOC-style report presents the analysis of DHCP logs ingested into Splunk,   
performed using SPL queries to detect anomalies, configuration issues, and possible security incidents.  
The project demonstrates practical SOC analyst skills including log analysis, anomaly detection, and visualization.

## 1. Top MAC Addresses by Request Count

SPL Query: sourcetype=dhcp\_logs | stats count by mac\_address | sort - count

Result: Identified the most active devices in the network. Top devices generated 41 and 33 requests respectively, indicating high activity levels.

## viz

## 2. IP Addresses Assigned to Multiple MACs (Conflicts)

SPL Query: sourcetype=dhcp\_logs | stats dc(mac\_address) as unique\_macs by client\_ip | where unique\_macs > 1

Result: Found IP addresses used by more than one device, suggesting possible IP conflicts or spoofing.

## unique_macs3. MAC Addresses with Zero Lease Time

SPL Query: sourcetype=dhcp\_logs | where lease\_time = 0 | stats count by mac\_address | sort - count

Result: 28 events with zero lease time were detected, indicating potential DHCP issues or misconfigurations.

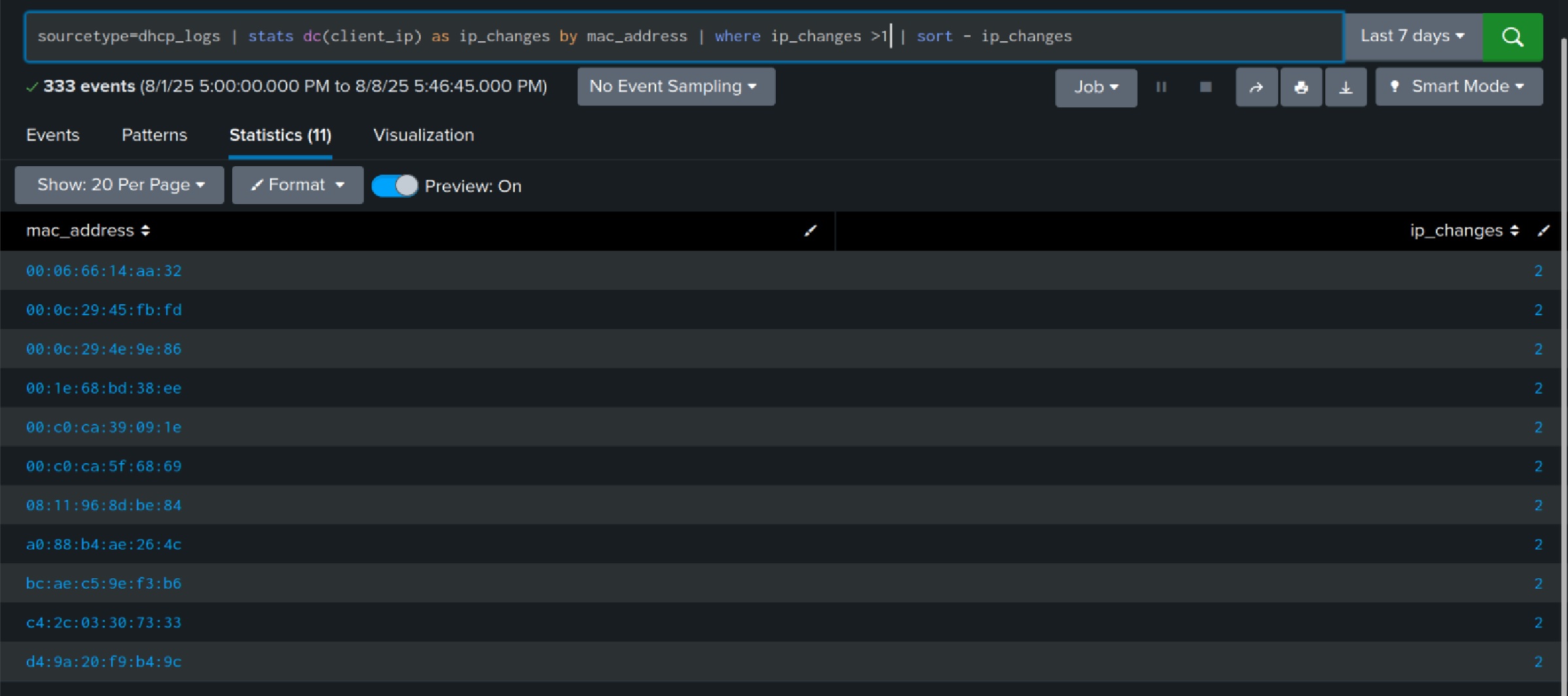
## stats

## viz

## 4. MAC Addresses Frequently Changing IP

SPL Query: sourcetype=dhcp\_logs | stats dc(client\_ip) as ip\_changes by mac\_address | where ip\_changes > 1 | sort - ip\_changes

Result: Identified devices changing IP addresses frequently, which may be normal for mobile devices but suspicious for stationary assets.



## 5. Frequently Requesting MAC Addresses

SPL Query: sourcetype=dhcp\_logs | stats count by mac\_address | where count > 100 | sort - count

Result: Detected devices sending excessive DHCP requests, which could indicate misconfigurations or DoS attempts.

## often_,mac_stats

## viz

## 6. DHCP Requests Outside Business Hours

SPL Query: sourcetype=dhcp\_logs | eval hour = tonumber(strftime(\_time, '%H')) | where hour < 6 OR hour > 20 | stats count by mac\_address | sort - count

Result: Observed active DHCP requests during nighttime, potentially indicating automated systems or compromised devices.

## stats night

## viz_night

## 7. MAC Addresses Inactive for Over 24 Hours

SPL Query: sourcetype=dhcp\_logs | stats latest(\_time) as last\_seen by mac\_address | where last\_seen < relative\_time(now(), '-1d')

Result: 13 devices did not renew their lease for over a day, possibly indicating they left the network.

## faSummary and Recommendations

Findings:  
1. Several devices showed unusually high DHCP request rates.  
2. Detected IP conflicts possibly indicating network misconfiguration or malicious actions.  
3. Suspicious activity outside business hours warrants investigation.  
4. Devices with zero lease time could signal service or configuration issues.  
5. Some devices were inactive for more than 24 hours.  
  
Recommendations:  
- Configure Splunk alerts for excessive DHCP requests.  
- Investigate and resolve IP conflicts promptly.  
- Monitor nighttime DHCP activity.  
- Audit and fix DHCP configurations causing zero lease time.  
- Keep an updated inventory of active devices.