OPENSSH ANALYSIS REPORT

PREPARED BY GROUP 4

SOC ACADEMY

13TH JUNE, 2025

GROUP MEMBERS

Adebisi Mololuwa
Aderinola Kehinde
Comfort Ukangwobia
Odunayo Balogun
Oghenetejiri Love Brume
Aleka Moses ogamodey
Victoria Simon
Nwobodo Chigozie
Gyekye Micaiah Ampofo

EXECUTIVE SUMMARY

Our organization recently experience few suspicious incidence and our team was tasked with analyzing an OpenSSH Log file to help identify potential security threat to the organization, main objectives include the identification and monitoring of suspicious activities such as unusual IP addresses, multiple failed login attempts, and other indicators of potential security issues. Splunk Cloud was deployed and Log file uploaded with a suspicious pattern identified, through the analyses we found several Authentication failures, Invalid user access attempts, repeated login failures (e.g., from 183.62.140.253), Disconnect messages (e.g., Bye Bye [preauth]) with multiple IP addresses with high event counts from different geolocations. The behavior of this log file confirms a brute-force attempts via automated scanning botnet or unauthorized probes. A dashboard and an ALERT system was created with certain conditions to visualize, detects and trigger any potential brute-force or unauthorized access attempts. In addition, user roles were created and reviewed in line with the principle of least privilege.

OBJECTIVES

Create user account for the team

Analyze the provided OpenSSH logs for suspicious behavior

Detect any unusual IP addresses

Detect multiple failed login attempts

Create a dashboard for real-time monitoring

Set up automated alerts for critical events.

As well as extracting a field.

USER CREATION AND ROLE MANAGEMENT

Users account were created within the Splunk Cloud environment showing the roles and access capabilities of members, 2 users have Admin privilege, 7 users with power role and 1 with user's role.

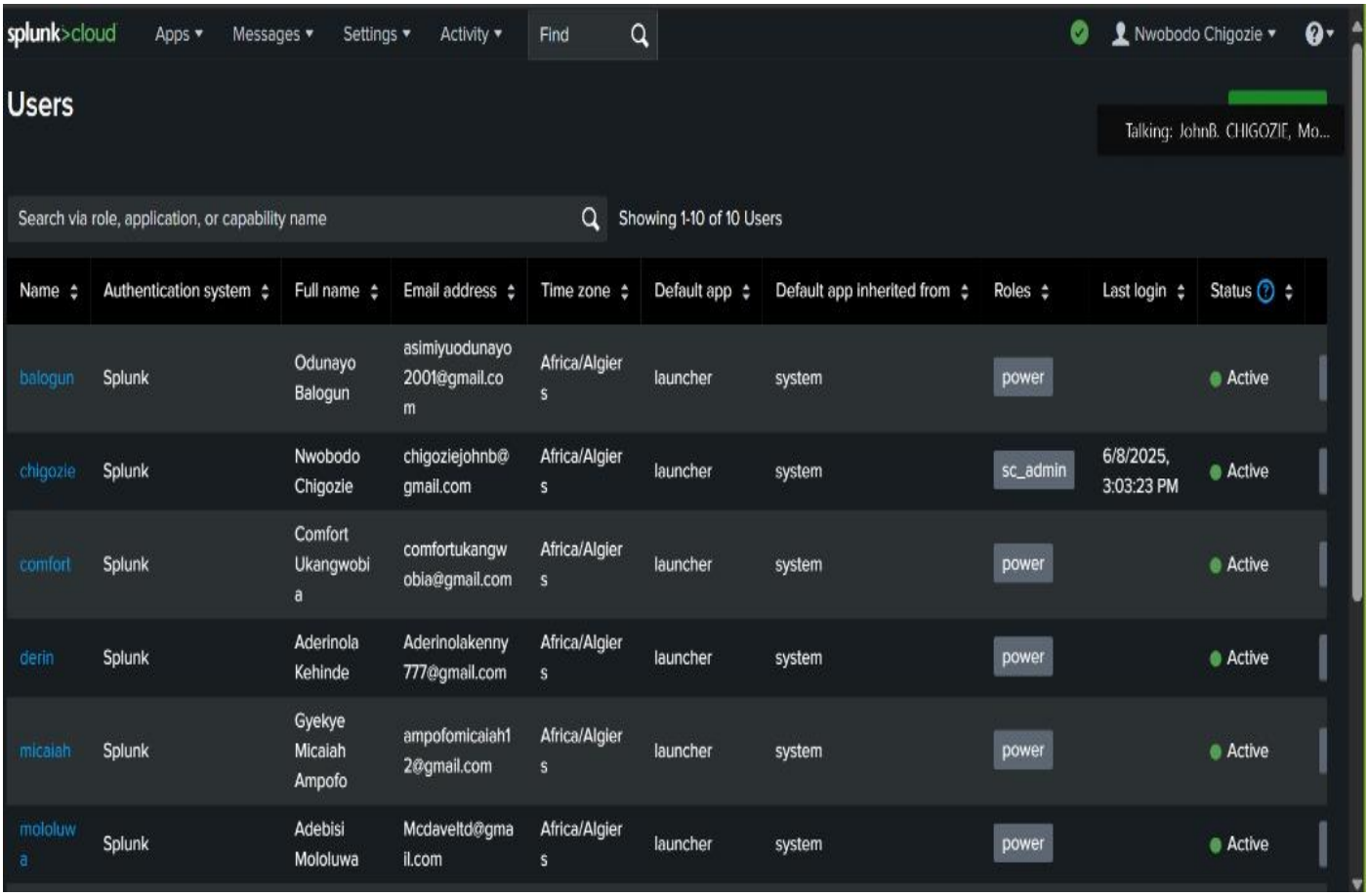
The aim is to ensure proper access control, validate role assignments, and support internal audits or compliance efforts.

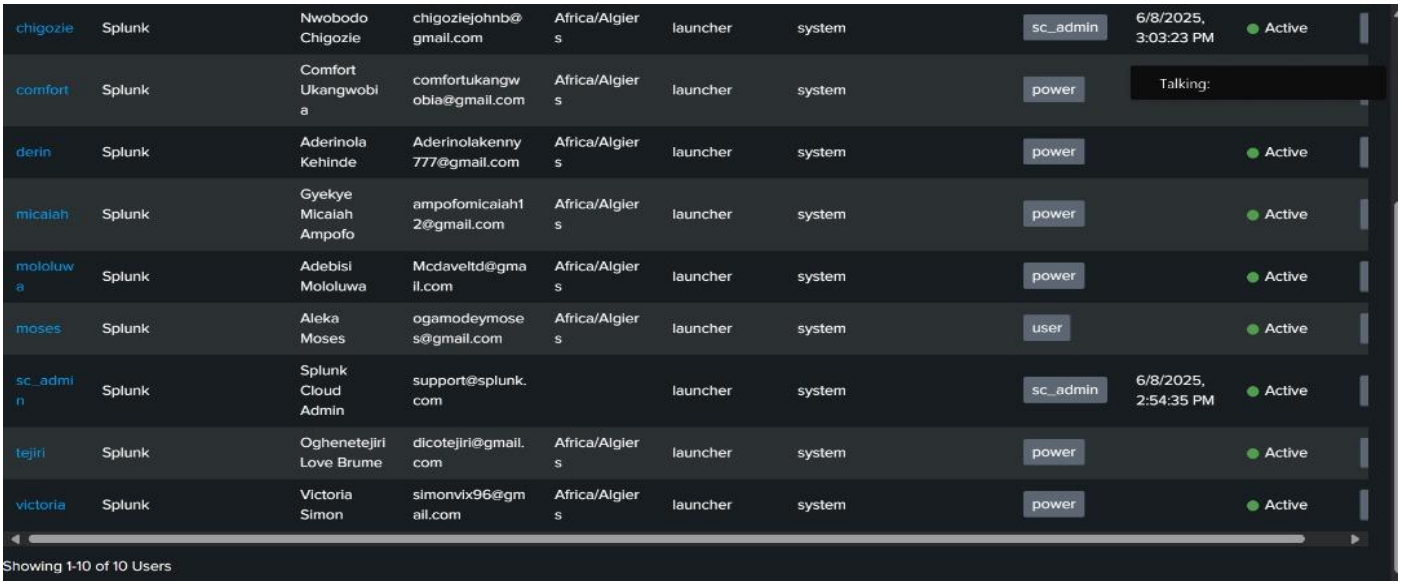
During account setup:

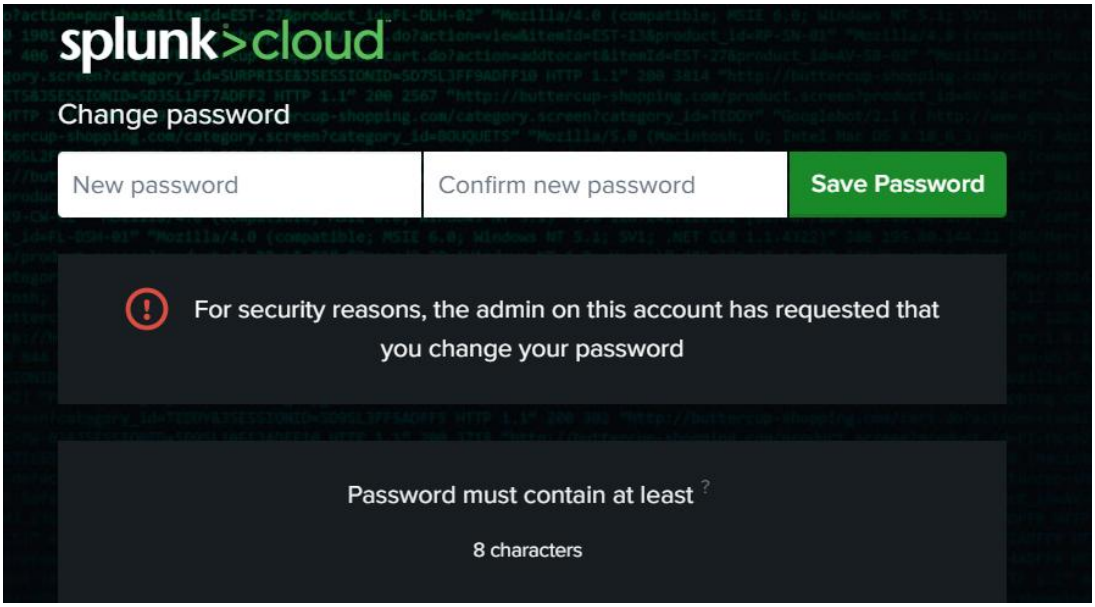
The Time Zone for each user was configured to **West Africa Time (WAT)** to maintain consistency in event timestamps.

The default application was set to Launcher (Home) for a uniform user interface experience upon login.

Password Policy was enforced to mandate password changes upon first login, enhancing account security.

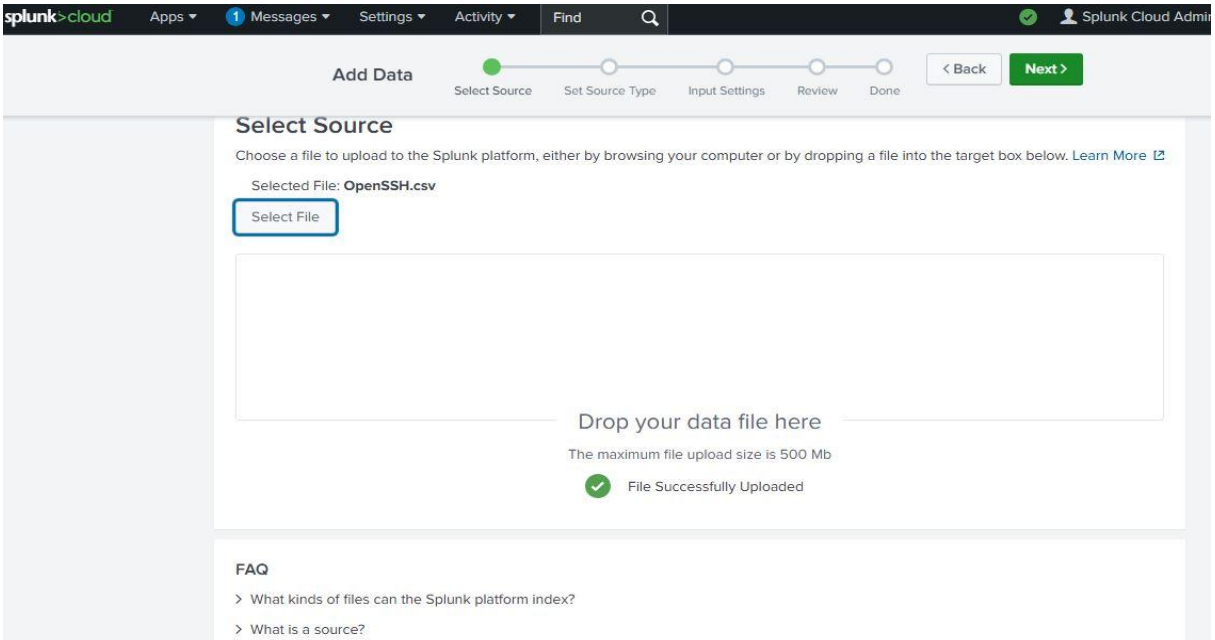




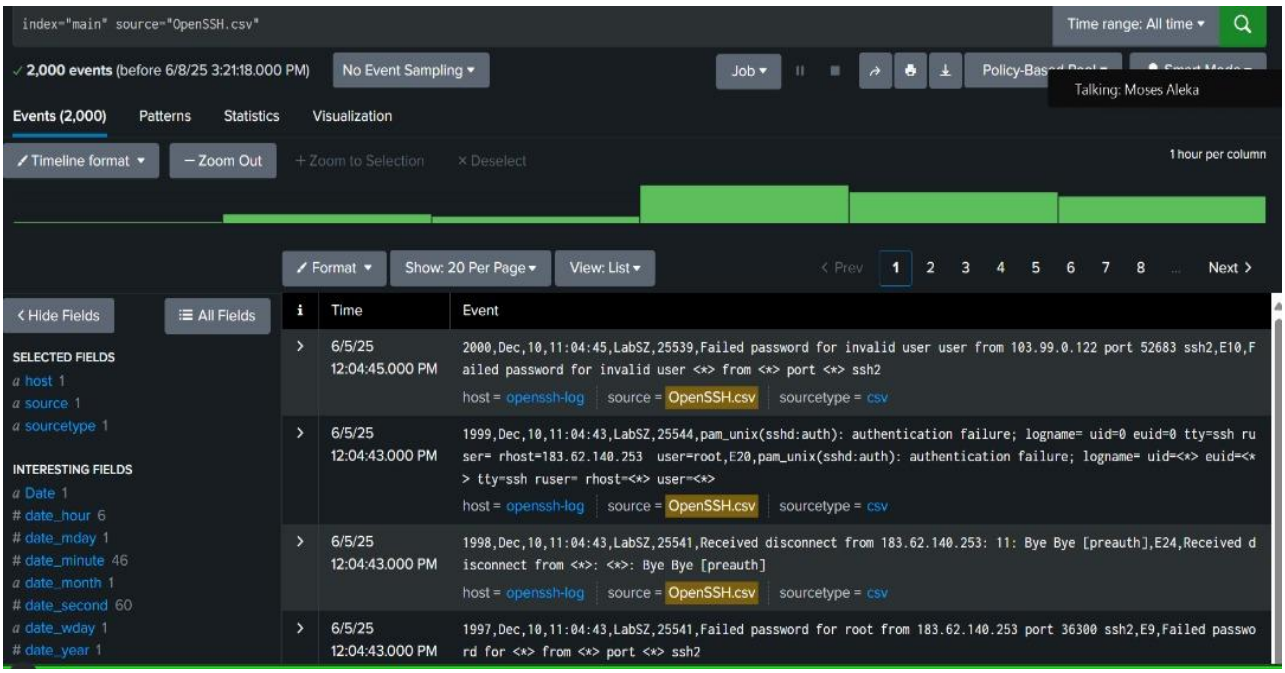


ANALYSIS OF OPENSSH LOG FILE

The OpenSSH file was manually uploaded to Splunk Cloud which is crucial for managing and searching data effectively with the following parameters
Source= OpenSSH.csv (the origin or where splunk gets it data from either a file or directory)
Sourcetype = csv (the format, structure or how splunk data is parse or understood in this case, comma separated value was used)
Index = main (where Splunk *stores* the data like a database or folder)



The analysis contains 2,000 event with key observation features like Failed Logins Attempts, Disconnection event, external IP, Timestamp and IP Locations.



ANALYSIS BY MULTIPLE FAILED ATTEMPTS

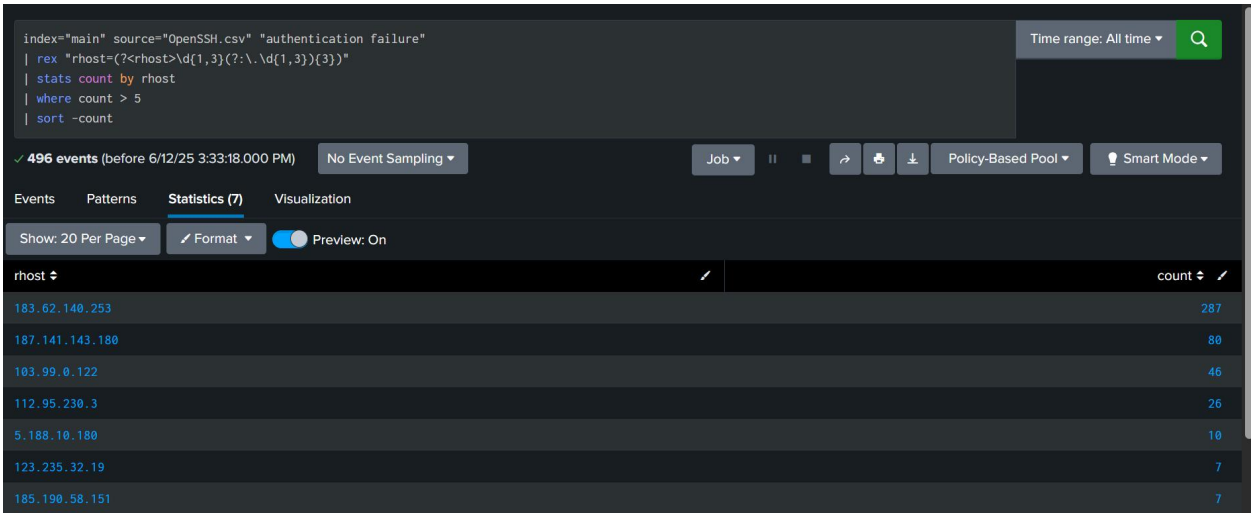
To identify the IP addresses (rhost) responsible for the highest number of failed SSH login attempts and assess potential brute-force or reconnaissance behavior.

The following command was ran and the interpretation given below;

```
index="main" source="OpenSSH.csv" "authentication failure"
| rex "rhost=(?<rhost>\d{1,3}(?:\.\d{1,3}){3})"
| stats count by rhost
| where count > 5
| sort –count
```

183.62.140.253 is the most active attacker, accounting for 57.8% of the total 496 failed attempts

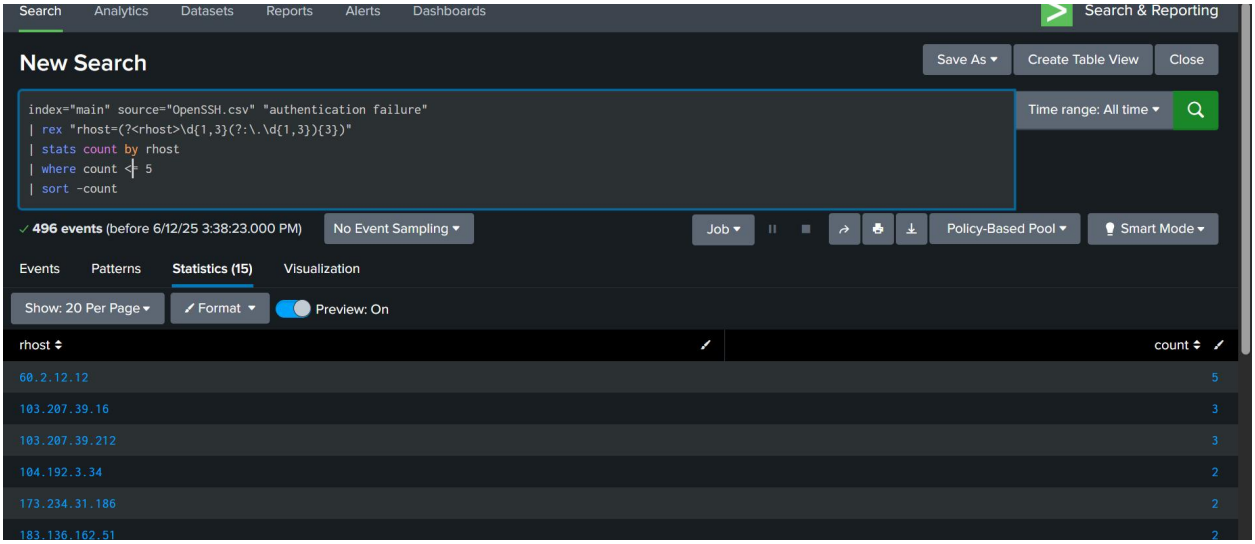
All the IPs from the 183.62.140.x subnet collectively contributed 431 attempts which suggest a coordinated scanning or attack from a botnet or single actor using multiple IPs, Repeated IPs and consistent failure rates point to brute-force activity



UNUSUAL IP ADDRESS DETECTION

To identify suspicious or unusual IP addresses attempting to access our infrastructure, we used the following Splunk SPL query:

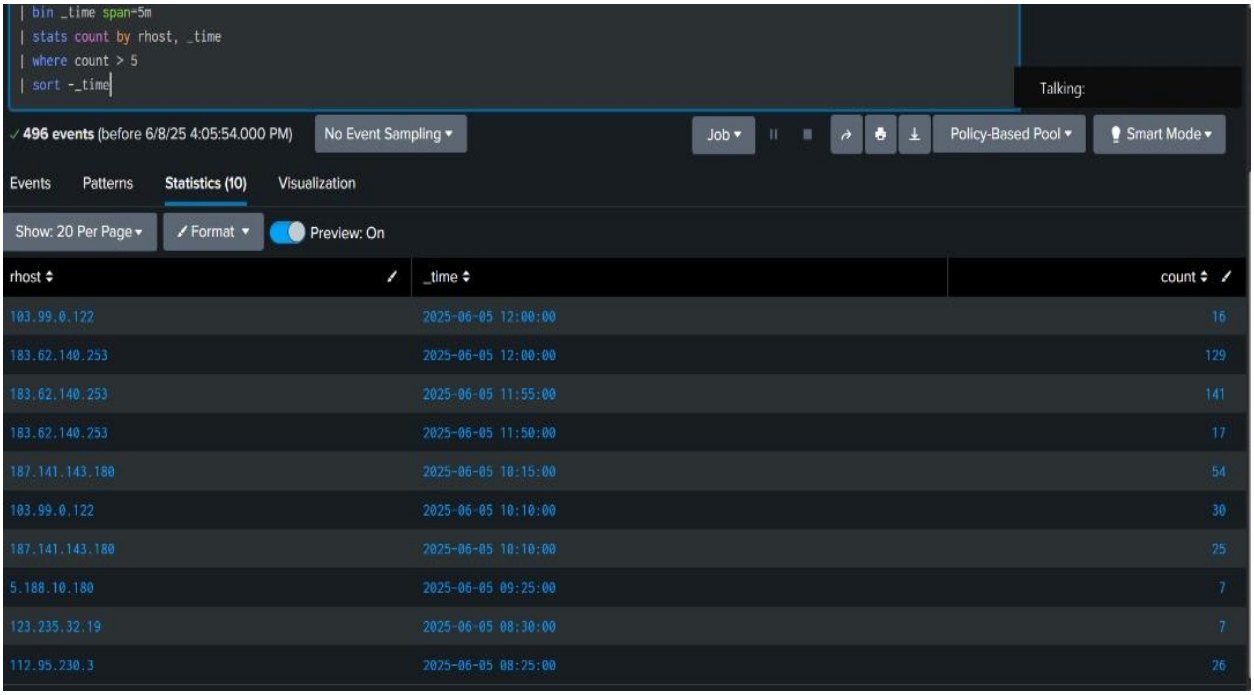
```
index="main" source="OpenSSH.csv" "authentication failure"
| rex "rhost=(?<rhost>\d{1,3}(?:\.\d{1,3}){3})"
| stats count by rhost
| where count <= 5
| sort -count
```



This query allowed us to aggregate and rank the number of connection attempts by remote hosts (rhost). Based on the results, we identified approximately 15 unusual IP addresses exhibiting abnormal behavior or access patterns, indicating potential unauthorized access attempts or brute-force activities. These findings were further analyzed to support alert configurations and dashboard visualizations for proactive monitoring.

ANALYSIS BY TIMESTAMP

Further analysis done breaks the event by timestamps into 5-minute and group the events that occurred within the same 5-minute window, counts how many events like failed login attempts each remote host (rhost) generated per 5-minute window and filters only those IPs that attempted access more than 5 times in any 5-minute window then sorts the output in descending order by time (latest attempts first).



rhost	_time	count
103.99.0.122	2025-06-05 12:00:00	16
183.62.140.253	2025-06-05 12:00:00	129
183.62.140.253	2025-06-05 11:55:00	141
183.62.140.253	2025-06-05 11:50:00	17
187.141.143.180	2025-06-05 10:15:00	54
103.99.0.122	2025-06-05 10:10:00	30
187.141.143.180	2025-06-05 10:10:00	25
5.188.10.180	2025-06-05 09:25:00	7
123.235.32.19	2025-06-05 08:30:00	7
112.95.230.3	2025-06-05 08:25:00	26

Clearer insights into the activities of the above image shows IP 183.62.140.253 is highly aggressive showing 129-141 login attempts within just 5-minute intervals. IPs like 103.99.0.122, 187.141.143.180, and 112.195.230.3 are also showing repeated attempts which is possibly a brute-force or scanning activity.

These are not normal user behaviors and suggest potential malicious actors attempting SSH login brute-force attacks.

ANALYSIS BY GEOLOCATION

A total of 496 failed SSH authentication attempts were identified from non-Nigerian IP addresses with source IPs mapped to countries known for botnet or brute-force activity. These attempts represent a potential external brute-force attack pattern targeting our infrastructure.

China is the top source country with over 300 combined attempts from multiple cities (Beijing, Shenzhen, Weifang, Langfang).

Mexico and Vietnam also show a substantial volume of attempts. The data was filtered to exclude internal/Nigerian IPs suggesting these are likely unauthorized foreign entities.

(See image below)

```
index="main" source="OpenSSH.csv" "authentication failure"
| rex "rhost=(?<rhost>\d{1,3}(?:\.\d{1,3}){3})"
| iplocation rhost
| search NOT Country="Nigeria"
| stats count by rhost Country City
| sort - count
```

Time range: All time

✓ **496 events** (before 6/10/25 1:06:51.000 AM)

Job | Policy-Based Pool | Smart Mode | No Event Sampling

Events | Patterns | **Statistics (22)** | Visualization

Show: 20 Per Page | Format | Preview: On | Prev | 1 | 2 | Next

rhost	Country	City	count
183.62.140.253	China	Beijing	287
187.141.143.180	Mexico	Mexico City (Miguel Hidalgo Villa Olimpica)	80
103.99.0.122	Vietnam	Hanoi	46
112.95.230.3	China	Shenzhen	26
5.188.10.180	Russia	St Petersburg	10
123.235.32.19	China	Weifang	7
185.190.58.151	United States	Los Angeles (Central LA)	7
60.2.12.12	China	Langfang	5
103.207.39.16	Vietnam	Hanoi	3

ANALYSIS BY USERS

Analyses was done for failed SSH login attempts in the OpenSSH logs to identify the most frequently targeted usernames. The report states **root** was the primary target accounting for 74.3% of all failed attempts. Other usernames like uucp, ftp, mysql, and git are common service accounts. The heavy targeting of `root` suggests an active brute-force attack aiming for administrative access. Attempts on service accounts indicate automated scans or credential stuffing using known usernames. These patterns are typical of external threat actors probing for vulnerable systems.

```
index="main" source="OpenSSH.csv" "authentication failure"
| rex "user=(?<user>\w+)"
| stats count by user
| sort -count
```

Time range: All time

✓ **496 events** (before 6/10/25 1:23:42.000 AM)

Job | Policy-Based Pool | Smart Mode | No Event Sampling

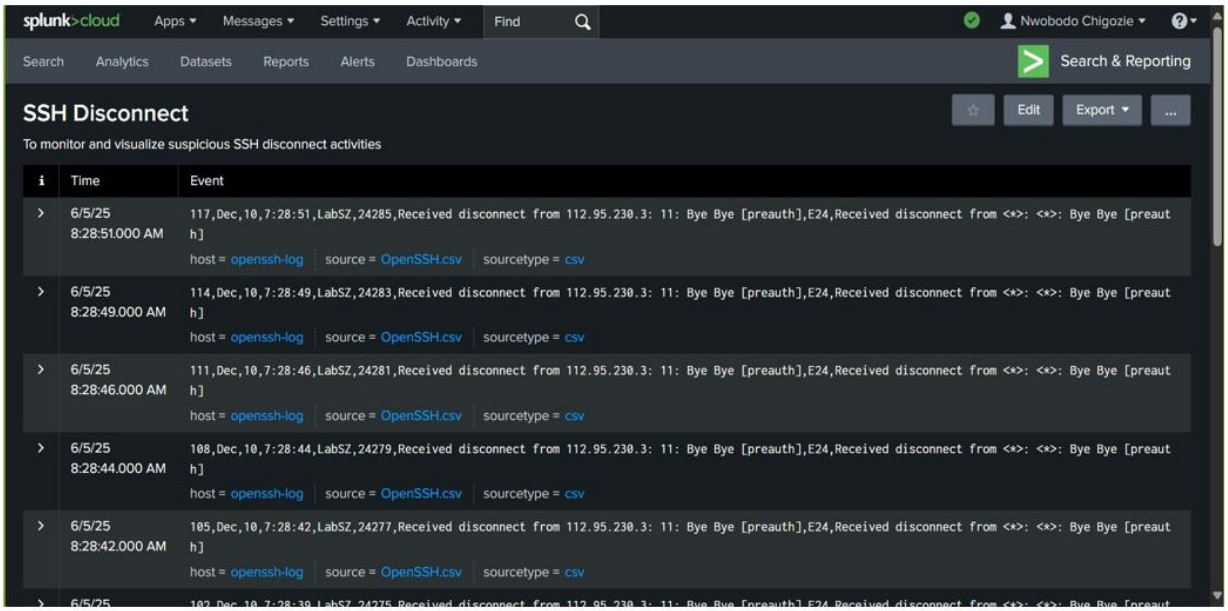
Events | Patterns | **Statistics (6)** | Visualization

Show: 20 Per Page | Format | Preview: On

user	count
root	369
uucp	5
ftp	3
git	3
mysql	2
sshd	2

DASHBOARD CONFIGURATION

A Dashboard was created to monitor and give early warning sign to a high frequency logs of disconnects initiated from the IP address 112.95.230.3 The repetitive pattern and timing suggest that a system likely external is attempting to establish SSH connections and being disconnected repeatedly before authentication ([preauth]). The disconnection messages are consistent, indicating potential scanning or brute-force attack behavior.

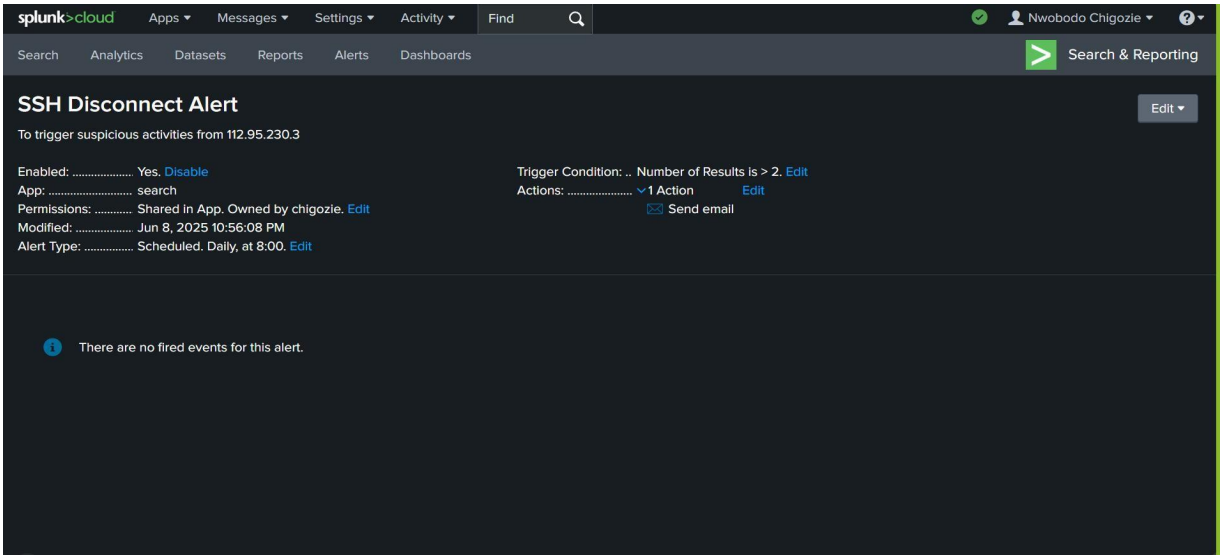


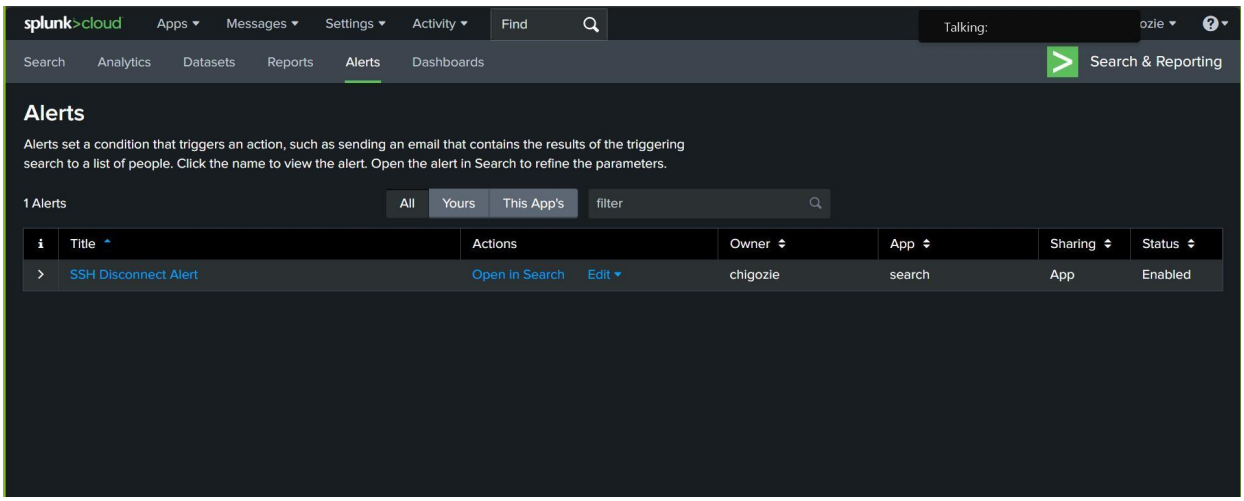
ALERT CONFIGURATION

To complement the dashboard, an automated alert system was configured with the following settings:

a) Schedule: Runs daily at 8:00 AM (WAT).
b) Alert Expiration: Set to expire after 24 hours.
c) Trigger Condition: Fires when the number of matching results is greater than 2.
d) Notification Type: Sent via plain text email.
e) Recipients: All Group 4 members were added as recipients to ensure collective visibility.
f) Domain Restriction: Splunk was configured to only allow emails to be sent to a specific domain (e.g., gmail.com) to enhance security and limit alert delivery to approved users.

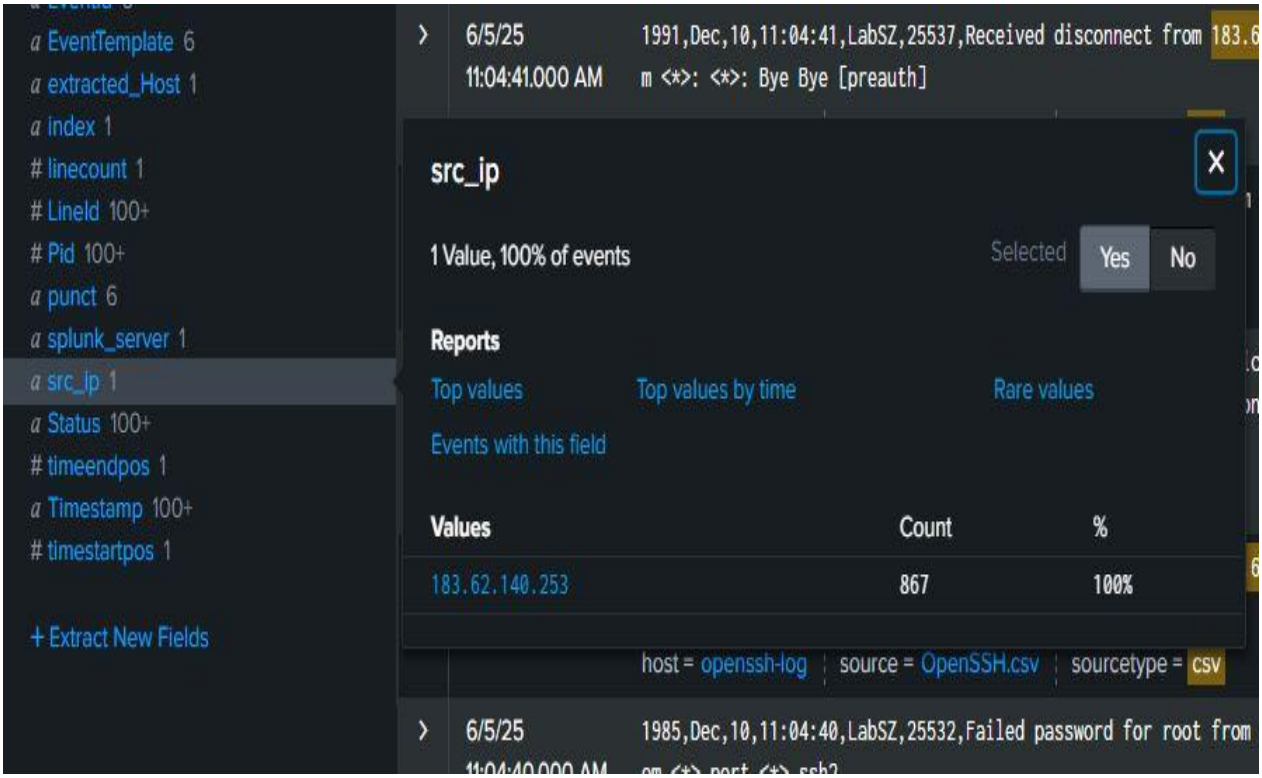
This alert is designed to monitor and automatically detect suspicious SSH disconnect events which could indicate Brute-force attack attempts (automated login failures), Network scanning or reconnaissance activity Abuse from malicious IP addresses (bots or unauthorized users), Unexpected session terminations on critical servers.





FIELD EXTRACTION CONFIGURATION

A custom field (src_ip) was created and extracted to store the IP 183.62.140.253. The src_ip field is crucial for tracking source hosts in SSH disconnect events and ensure the IP is constantly tagged for correlation, reporting and alerting, it provides actionable intelligence about suspicious SSH activity and inform automated defenses, blacklists, and SIEM correlation rules. Splunk identified 867 events generated by this this IP, covering 99.95% of all events in the dataset



RECOMMENDATIONS

To enhance the security of your SSH service and prevent unauthorized access, this should be implemented

1. Immediate Mitigation
   Block/Blacklist Malicious IPs using firewall rules to block high-risk IPs like 183.62.140.253
   Disable Root Login In
2. Access Hardening
   Enable Rate Limiting: Deploy fail2ban or sshguard to automatically block IPs with multiple failed attempts.
   Restrict Access via Geo-IP: Implement IP filtering to block SSH access from high-risk countries unless necessary for operations.
   Use SSH Keys Instead of Passwords: Enforce public key authentication for all users to eliminate password-based attacks.
3. Account Security
   Enforce Strong Password Policies: Require complex passwords and change them periodically.
   Limit SSH Access to Specific Users: Use AllowUsers or AllowGroups in SSH configuration.

CONCLUSION

The analysis of the OpenSSH.csv logs through Splunk has revealed a high number of failed SSH authentication attempts primarily from a concentrated group of external IP addresses like 183.62.140.253 from Beijing China as the top offender with 287 login failures, several other IPs from the same subnet were also active suggesting automated or coordinated attack attempts likely brute-force in nature. Attempts were mainly directed at privileged accounts like root accounting for 74% of the total failed logins 369 out of 496, The source of attacks includes countries such as China, Mexico, Vietnam, Russia, and the United States, indicating global threat vectors targeting the system.

These patterns are typical of credential stuffing, dictionary attacks, or brute force login attempts, and if not mitigated could lead to unauthorized system access and compromise of critical infrastructure.