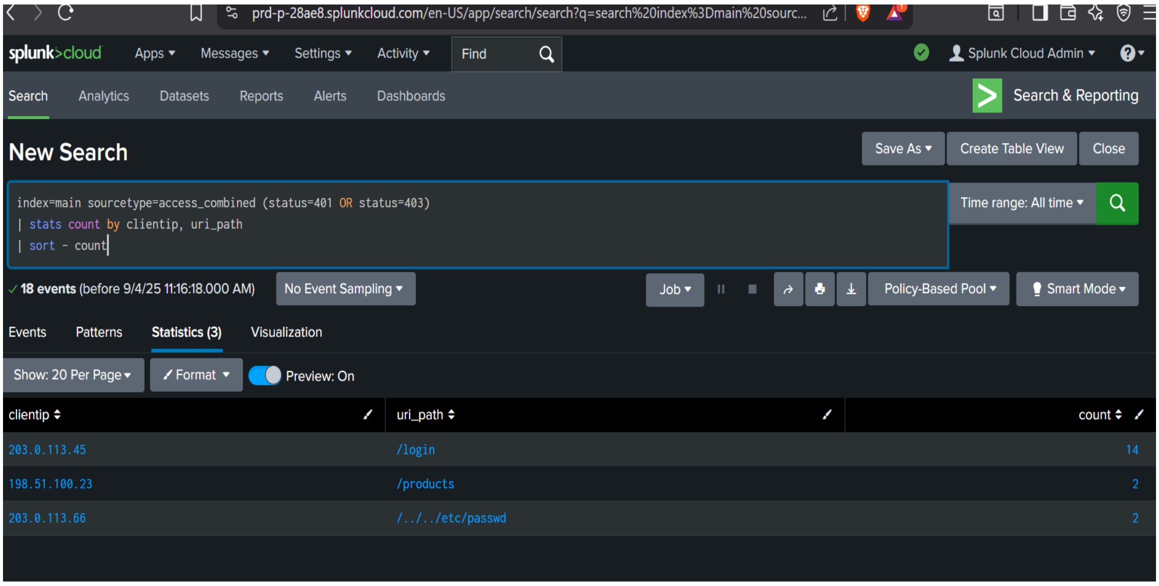
Incident Response Report - Task 2 (SIEM with Splunk)

This report presents findings from Task 2 of the Cybersecurity Internship Project using Splunk as a SIEM tool. Sample web access logs were analyzed to detect potential security incidents such as unauthorized access attempts, brute-force login attempts, and SQL injection probes.

1. Unauthorized Access Attempts

We filtered HTTP status codes **401 (Unauthorized)** and **403 (Forbidden)**. This revealed repeated access attempts to sensitive endpoints.



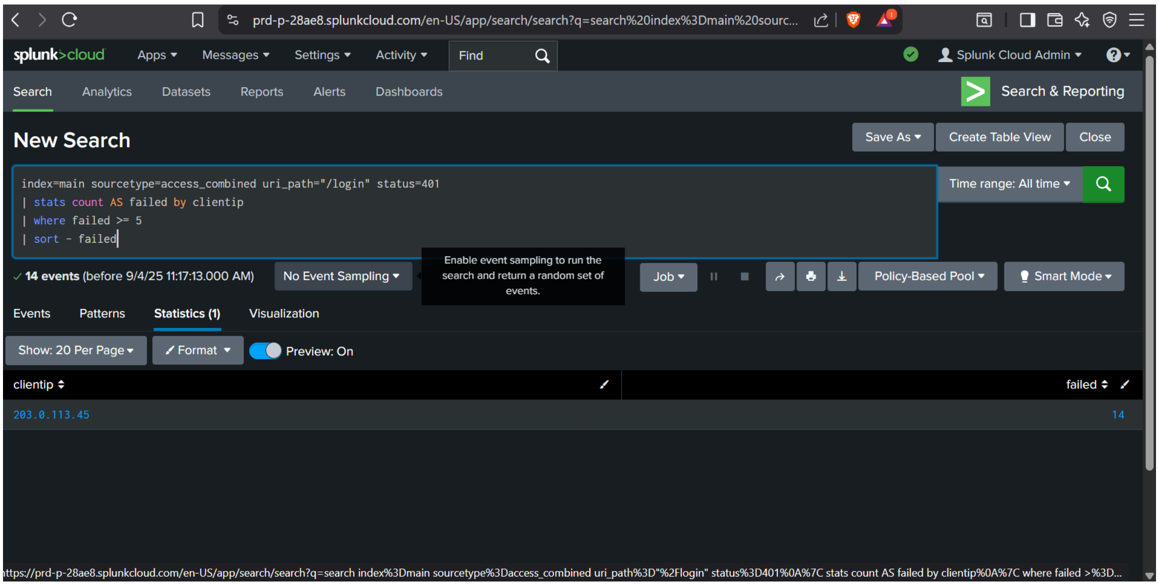
```
index=main sourcetype=access_combined (status=401 OR status=403)
| stats count by clientip, uri_path
| sort - count
```

✓ **18 events** (before 9/4/25 11:16:18.000 AM)

clientip	uri_path	count
203.0.113.45	/login	14
198.51.100.23	/products	2
203.0.113.66	/../../etc/passwd	2

2. Brute-Force Login Attempts

A search was performed for multiple failed login attempts (HTTP 401 errors on /login). We flagged IP addresses with 5 or more failures as possible brute-force attackers.



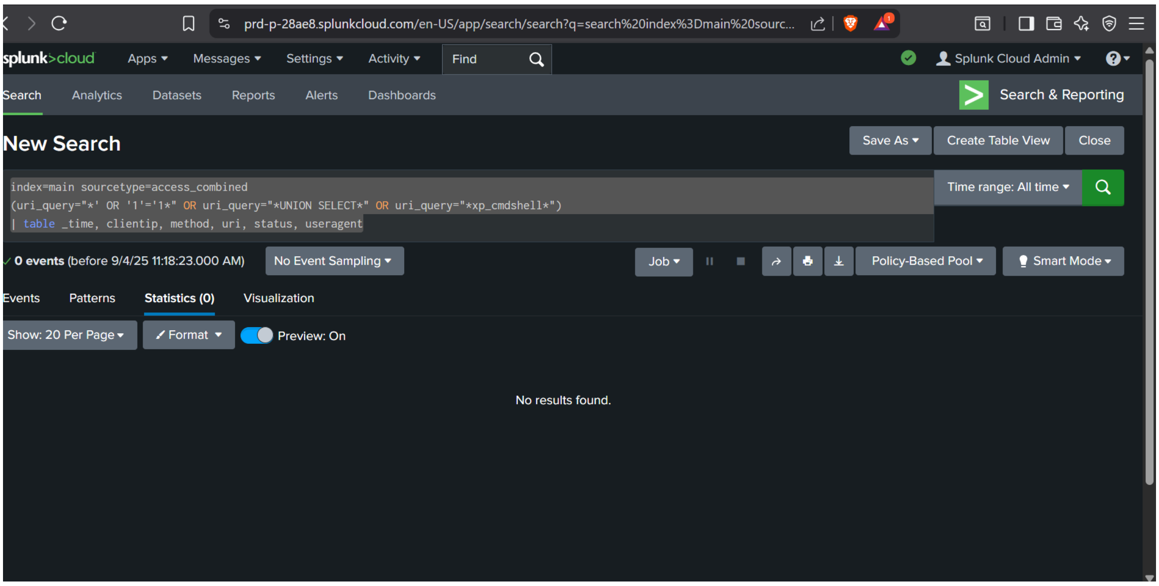
```
index=main sourcetype=access_combined uri_path="/login" status=401
| stats count AS failed by clientip
| where failed >= 5
| sort - failed
```

✓ 14 events (before 9/4/25 11:17:13.000 AM)

clientip	failed
203.0.113.45	14

3. SQL Injection Probes

Search queries were run for suspicious patterns such as ' OR '1'='1, UNION SELECT, and xp_cmdshell. No SQL injection probes were detected in the dataset.



```
index=main sourcetype=access_combined
(uri_query="*' OR '1'='1*" OR uri_query="*UNION SELECT*" OR uri_query="*xp_cmdshell*")
| table _time, clientip, method, uri, status, useragent
```

✓ 0 events (before 9/4/25 11:18:23.000 AM)

No results found.

Conclusion:
The Splunk analysis identified multiple unauthorized access attempts and brute-force login behavior. Although no SQL injection attempts were found, the presence of repeated login failures and forbidden access attempts indicates potential malicious activity. Recommended actions include blocking suspicious IPs, enforcing strong password policies, and enabling multi-factor authentication (MFA).