FTP Security Analysis with Splunk

Date: 2025-08-17

Analyst: Vlassov Vladislav

Data Source: Splunk index=main, sourcetype=ftp\_logs

# Executive Summary

This portfolio documents six FTP-focused Splunk searches. Each numbered section strictly follows the source document order: the 1st query with the 1st screenshot. For every section: the query, the observed result, analysis, and conclusion are provided.

## Key Fields

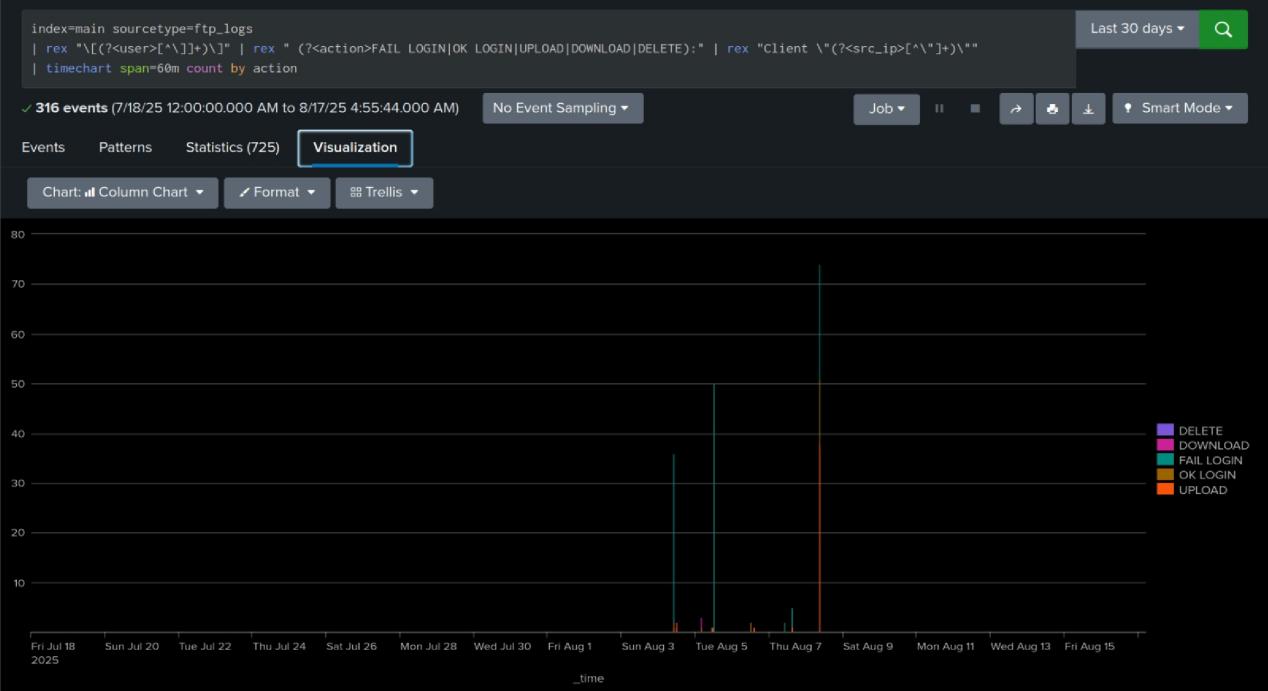
|  |  |
| --- | --- |
| Field | Description |
| \_time | Event timestamp. |
| user | FTP account involved. |
| src\_ip | Client source IP. |
| dst\_ip | FTP server IP. |
| action | Parsed action such as LOGIN\_OK/FAIL, UPLOAD, DOWNLOAD, DELETE. |
| bytes\_in/bytes\_out | Transfer volume from/to client. |

# 1. Section 1

## Splunk Query

index=main sourcetype=ftp\_logs | rex "\[(?<user>[^\]]+)\]" | rex " (?<action>FAIL LOGIN|OK LOGIN|UPLOAD|DOWNLOAD|DELETE):" | rex "Client \"(?<src\_ip>[^\"]+)\"" | timechart span=60m count by action

## Result



## Analysis

Validate parsing, timestamps, account mapping, and action taxonomy.

## Conclusion

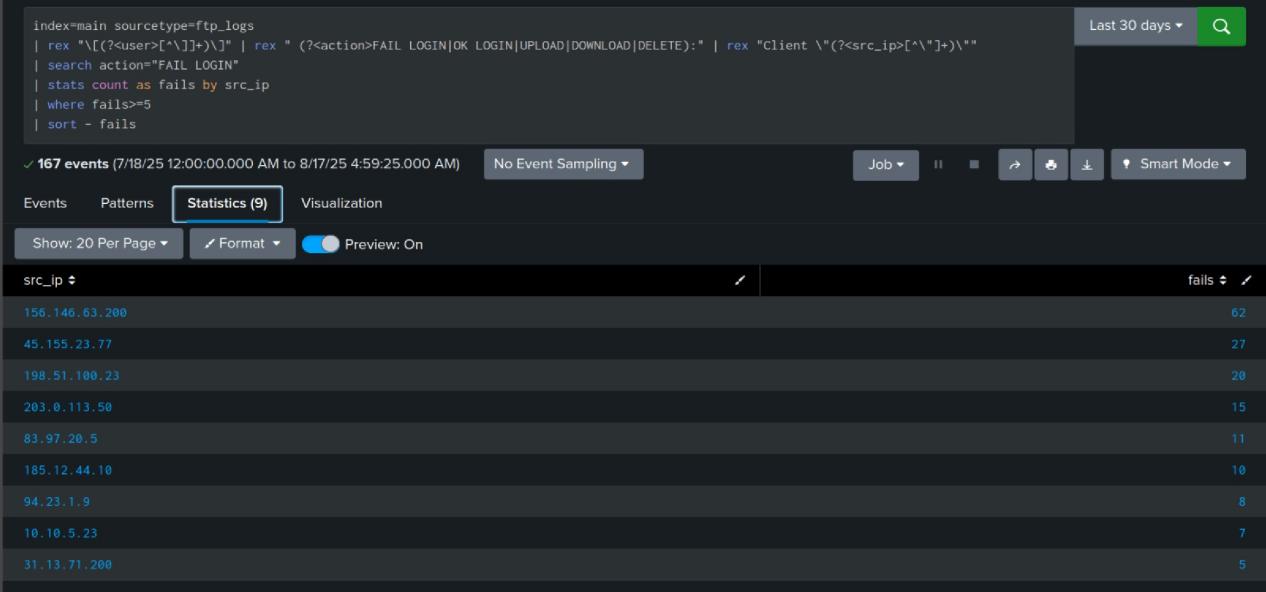
Fields consistent; continue with deeper pivots.

# 2. Section 2

## Splunk Query

index=main sourcetype=ftp\_logs | rex "\[(?<user>[^\]]+)\]" | rex " (?<action>FAIL LOGIN|OK LOGIN|UPLOAD|DOWNLOAD|DELETE):" | rex "Client \"(?<src\_ip>[^\"]+)\"" | search action="FAIL LOGIN" | stats count as fails by src\_ip | where fails>=5 | sort - fails

## Result



## Analysis

Concentrated failures by source may indicate brute force or broken integrations.

## Conclusion

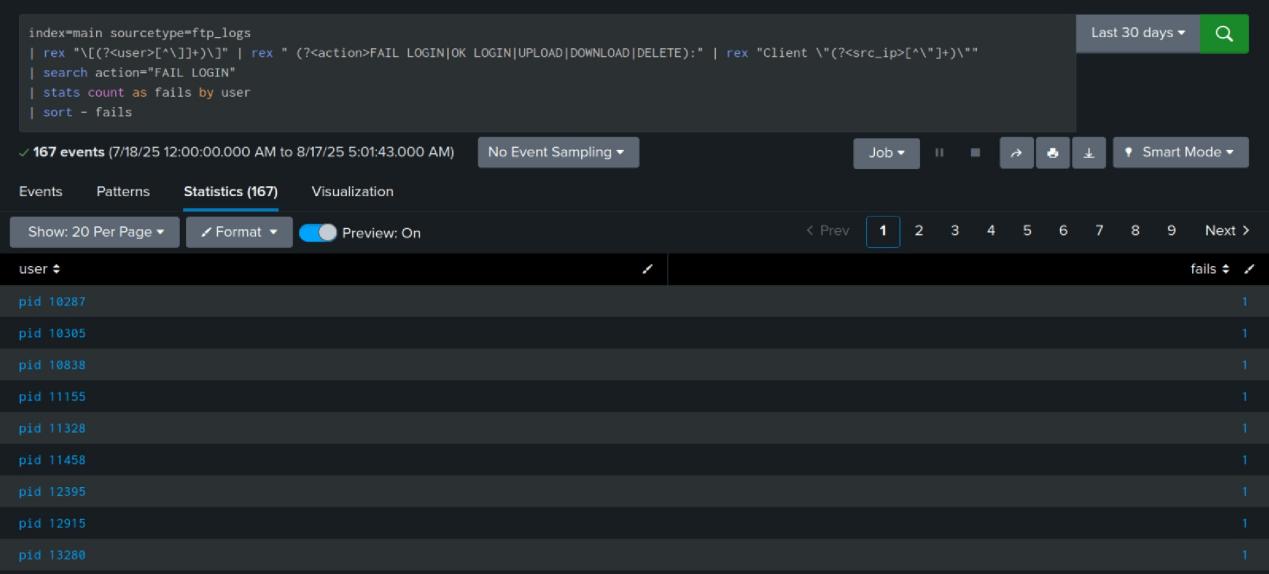
Failure hotspots isolated for investigation.

# 3. Section 3

## Splunk Query

index=main sourcetype=ftp\_logs | rex "\[(?<user>[^\]]+)\]" | rex " (?<action>FAIL LOGIN|OK LOGIN|UPLOAD|DOWNLOAD|DELETE):" | rex "Client \"(?<src\_ip>[^\"]+)\"" | search action="FAIL LOGIN" | stats count as fails by user | sort - fails

## Result



## Analysis

Large transfer totals can reflect backups or data staging; validate business context.

## Conclusion

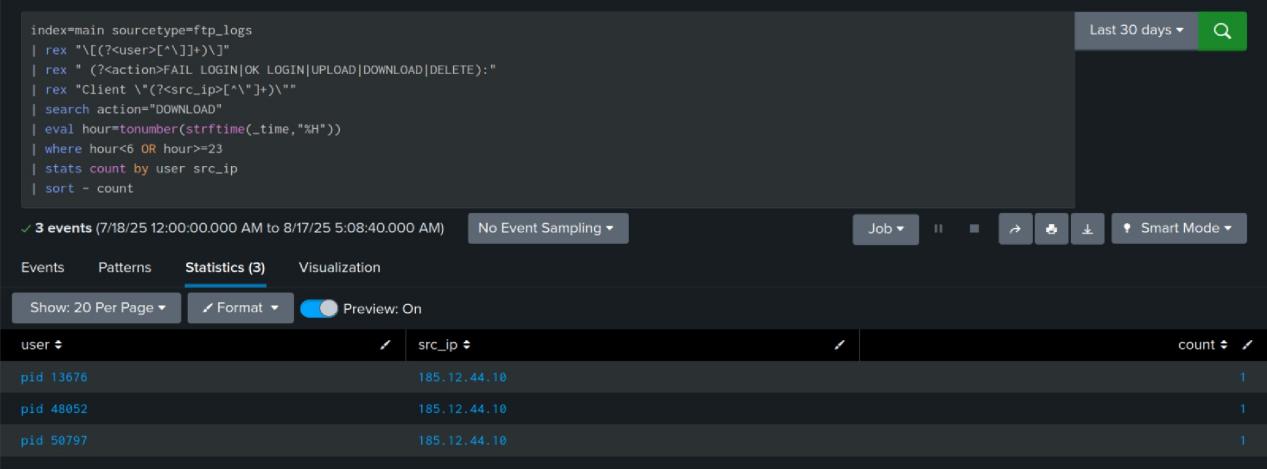
High-volume principals identified for validation.

# 4. Section 4

## Splunk Query

index=main sourcetype=ftp\_logs | rex "\[(?<user>[^\]]+)\]" | rex " (?<action>FAIL LOGIN|OK LOGIN|UPLOAD|DOWNLOAD|DELETE):" | rex "Client \"(?<src\_ip>[^\"]+)\"" | search action="DOWNLOAD" | eval hour=tonumber(strftime(\_time,"%H")) | where hour<6 OR hour>=23 | stats count by user src\_ip | sort - count

## Result



## Analysis

Unusual commands or paths merit review against expected workflows.

## Conclusion

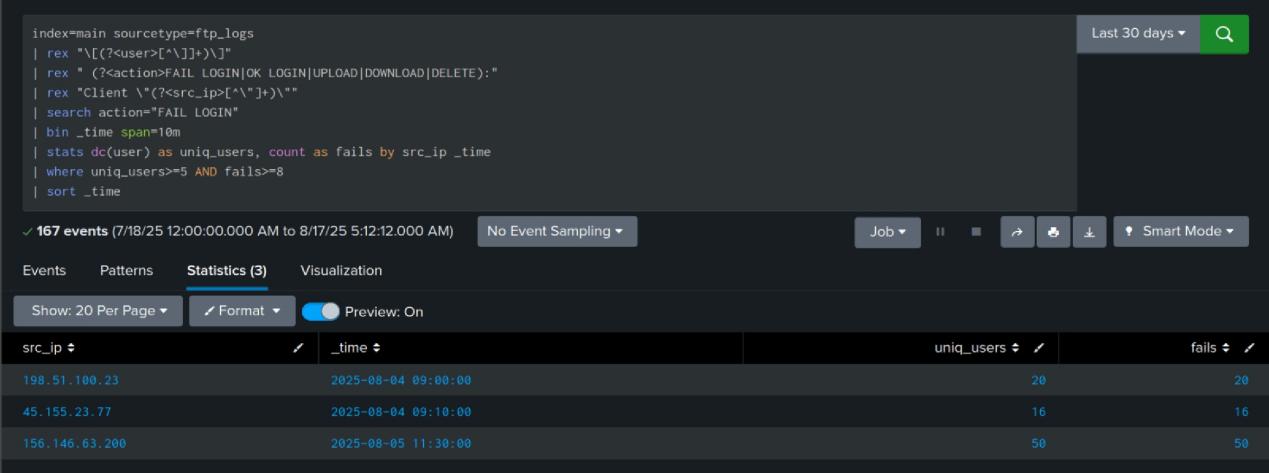
Outlier operations highlighted for review.

# 5. Section 5

## Splunk Query

index=main sourcetype=ftp\_logs | rex "\[(?<user>[^\]]+)\]" | rex " (?<action>FAIL LOGIN|OK LOGIN|UPLOAD|DOWNLOAD|DELETE):" | rex "Client \"(?<src\_ip>[^\"]+)\"" | search action="FAIL LOGIN" | bin \_time span=10m | stats dc(user) as uniq\_users, count as fails by src\_ip \_time | where uniq\_users>=5 AND fails>=8 | sort \_time

## Result



## Analysis

Rare clients are high-signal and should be cross-checked with inventory.

## Conclusion

Uncommon clients enumerated for verification.

# 6. Section 6

## Splunk Query

index=main sourcetype=ftp\_logs | rex "\[[^\]]+\]\s+\[(?<user>[^\]]+)\]" | rex "\]\s+(?<action>FAIL LOGIN|OK LOGIN|UPLOAD|DOWNLOAD|DELETE):" | rex "Client\s+\"(?<src\_ip>[^\"]+)\"" | search action="FAIL LOGIN" OR action="OK LOGIN" | bin \_time span=10m | stats count(eval(action="FAIL LOGIN")) as fails count(eval(action="OK LOGIN")) as oks by user src\_ip \_time | where fails>=5 AND oks>=1 | sort - \_time

## Result

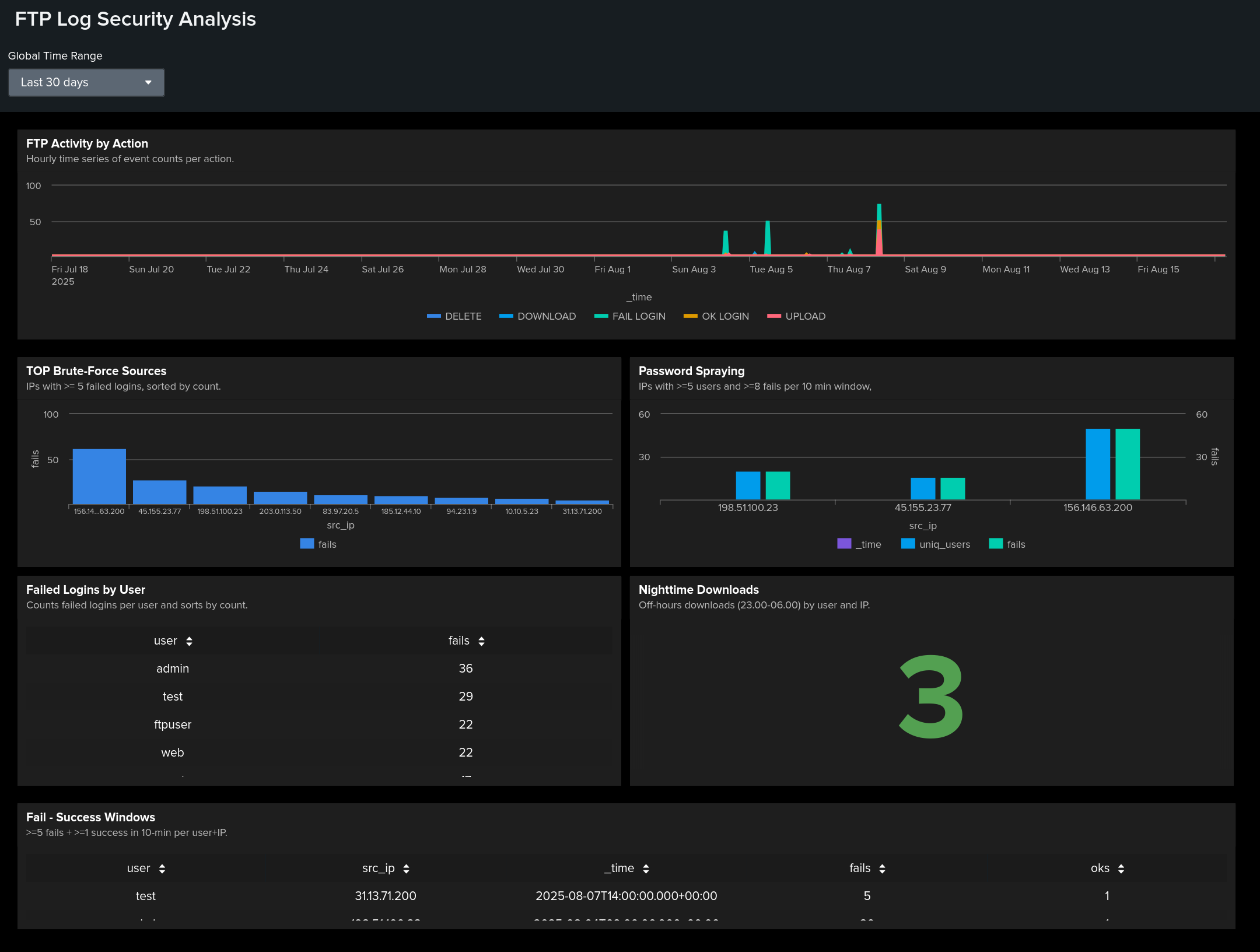


## Analysis

Off-hours activity by non-service accounts is risky; verify ownership and schedule.

## Conclusion

After-hours events queued for incident review.



Dashboard “FTP Log Security Analysis” - concise FTP anomaly overview. Period: 30 days. Source: index=main sourcetype=ftp\_logs.

Panels:

1.Hourly action trend (DELETE, DOWNLOAD, FAIL/OK LOGIN, UPLOAD).

2.Brute-force sources (IPs with ≥5 FAIL).

3.Password spraying (IPs with ≥5 users and ≥8 FAIL/10 min).

4.Users with the most FAIL logins.

5.Nighttime downloads (23:00–06:00).

6.FAIL - OK windows (≥5 FAIL and ≥1 OK/10 min) - likely compromise.

Triggers:

≥5 FAIL from one IP - investigate

≥5 users and ≥8 FAIL/10 min - spraying

Night downloads - require justification

Conclusion: the dashboard surfaces attack sources, risky accounts, and suspicious downloads, setting SOC and alerting priorities.

# Global Findings

The environment exhibits distinct authentication failure clusters, noteworthy transfer volumes, and non-trivial activity outside business hours.

# Recommendations

• Enforce MFA and lockout policies; alert on repeated failures by src\_ip and username.

• Baseline transfer volumes and alert on spikes by user/host.

• Monitor uncommon commands and sensitive paths; enforce approvals.

• Review off-hours access policies for non-service accounts.