Splunk Security Analysis

**Data domain: Okta Identity**Author: Vlassov Vladislav  
**Date:** 2025-08-19

# Executive Summary

This case demonstrates a six-step security analytics workflow in Splunk. Each step introduces a query, presents the evidence, and provides analysis and conclusions.

# Data and Environment

Data source: Authentication events ingested to Splunk. Fields parsed via spath and sourcetype knowledge. Key fields include user identifiers, client IPs, result status, geography, and ASN enrichment.

# Methodology

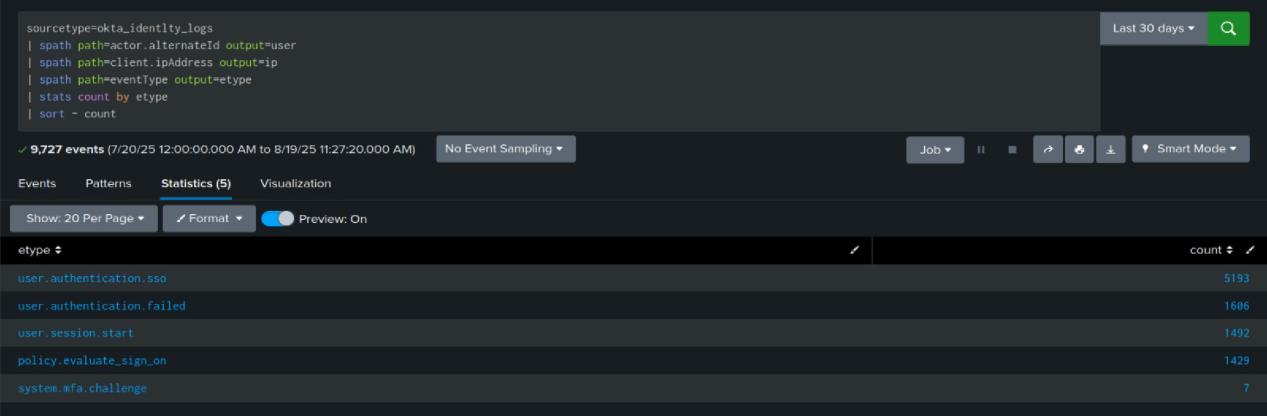
For each step: run the SPL, review results, interpret security implications, and record conclusions. Screenshots of Splunk results are embedded.

## 1. Event Type Distribution

Search Processing Language (SPL):

sourcetype=okta\_identlty\_logs | spath path=actor.alternateId output=user | spath path=client.ipAddress output=ip | spath path=eventType output=etype | stats count by etype | sort - count

Result evidence:



Analysis:

Identify dominant event categories to set a baseline. Spikes in specific event types may indicate probing or configuration drift.

Conclusion:

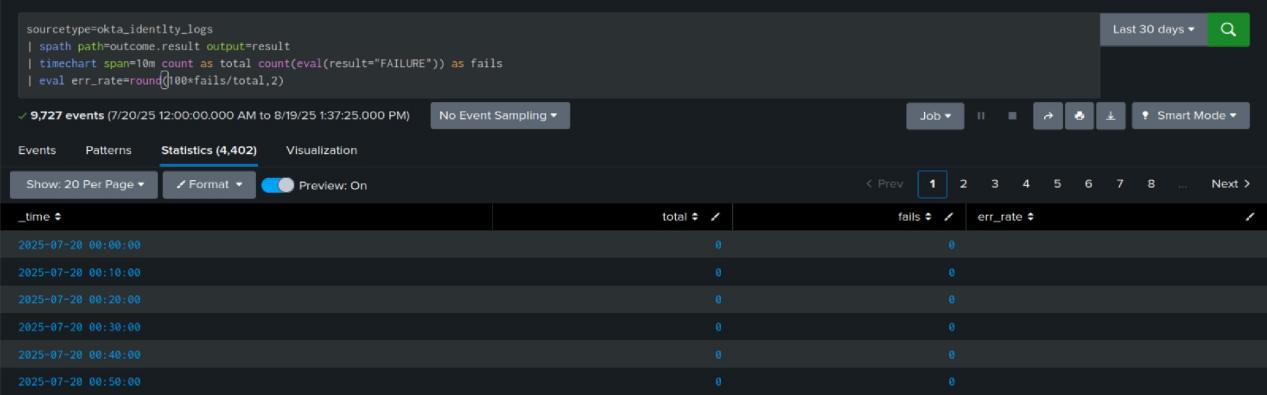
Noisy sources and suspicious patterns are identified for further triage. Convert this search into a saved alert or correlation rule as needed.

## 2. Error Rate Over Time

Search Processing Language (SPL):

sourcetype=okta\_identlty\_logs | spath path=outcome.result output=result | timechart span=10m count as total count(eval(result="FAILURE")) as fails | eval err\_rate=round(100\*fails/total,2)

Result evidence:



Analysis:

Track aggregate error rate. Sustained elevation suggests broad authentication or availability issues; sudden spikes suggest attacks.

Conclusion:

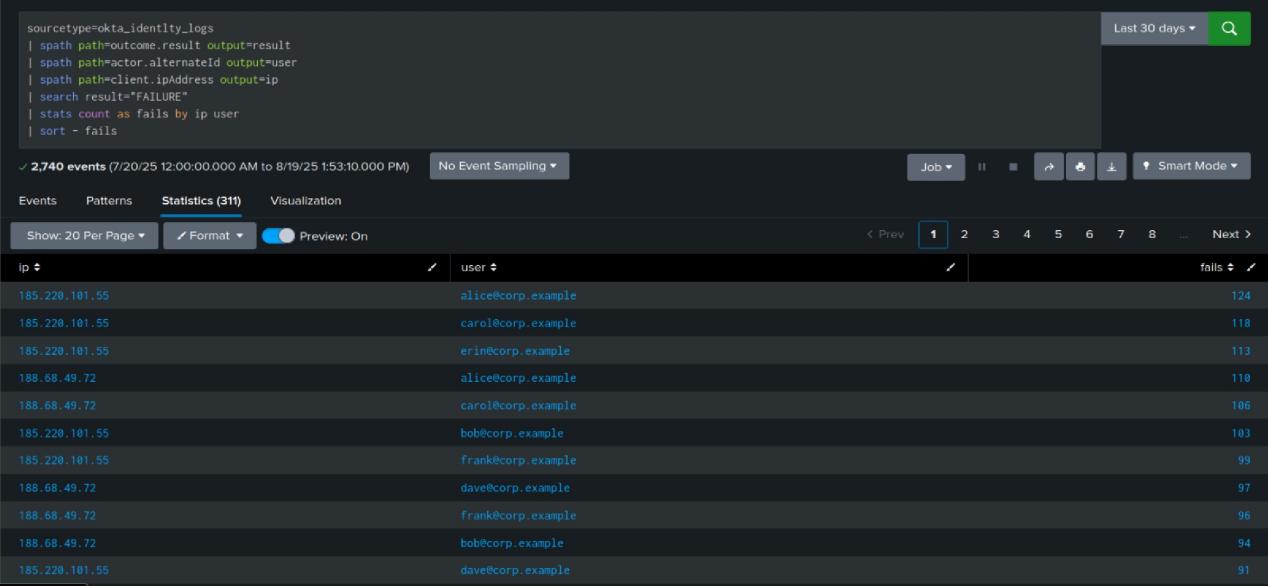
Noisy sources and suspicious patterns are identified for further triage. Convert this search into a saved alert or correlation rule as needed.

## 3. Failure Sources by IP and User

Search Processing Language (SPL):

sourcetype=okta\_identlty\_logs | spath path=outcome.result output=result | spath path=actor.alternateId output=user | spath path=client.ipAddress output=ip | search result="FAILURE" | stats count as fails by ip user | sort - fails

Result evidence:



Analysis:

Rank failure volume by IP and user to isolate targeted accounts or noisy sources.

Conclusion:

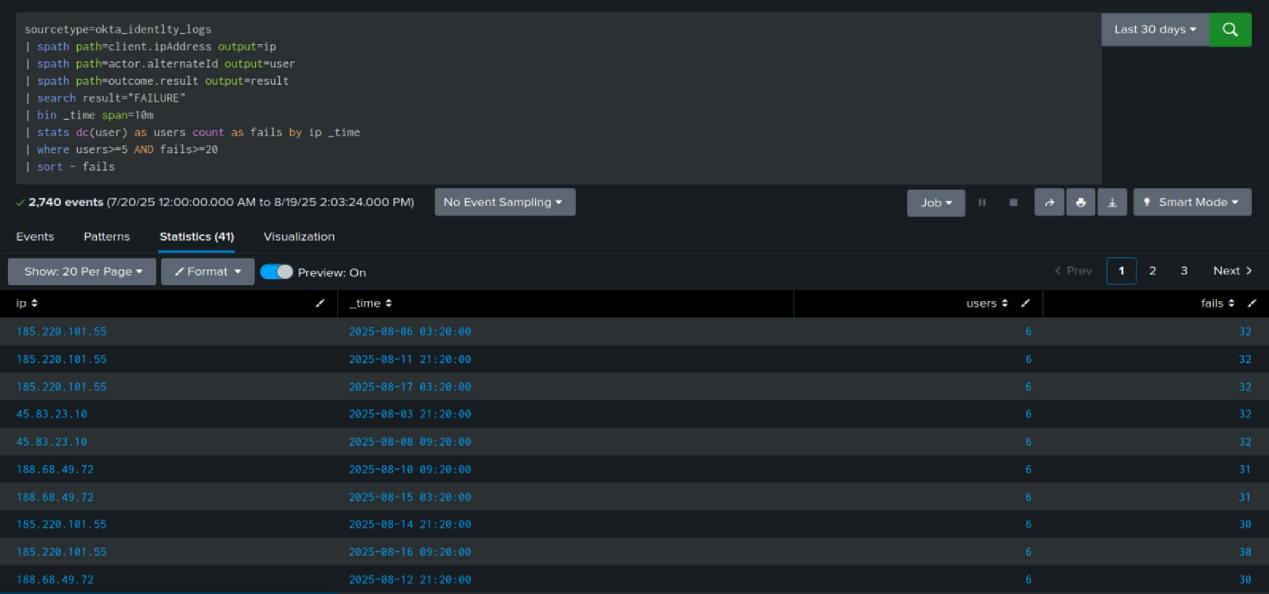
Noisy sources and suspicious patterns are identified for further triage. Convert this search into a saved alert or correlation rule as needed.

## 4. Brute-force Pattern Over 10-Minute Windows

Search Processing Language (SPL):

sourcetype=okta\_identlty\_logs | spath path=client.ipAddress output=ip | spath path=actor.alternateId output=user | spath path=outcome.result output=result | search result="FAILURE" | bin \_time span=10m | stats dc(user) as users count as fails by ip \_time | where users>=5 AND fails>=20 | sort - fails

Result evidence:



Analysis:

Detect coordinated brute-force behavior using distinct-user counts and failure thresholds.

Conclusion:

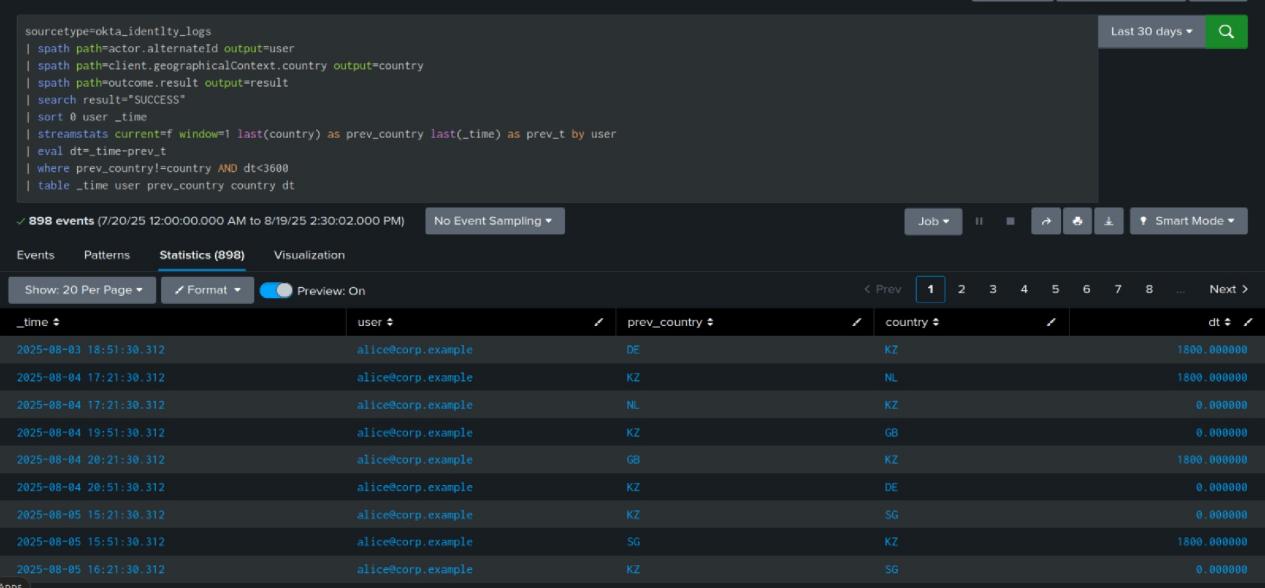
Noisy sources and suspicious patterns are identified for further triage. Convert this search into a saved alert or correlation rule as needed.

## 5. Geographical Anomalies (Rapid Country Change)

Search Processing Language (SPL):

sourcetype=okta\_identlty\_logs | spath path=actor.alternateId output=user | spath path=client.geographicalContext.country output=country | spath path=outcome.result output=result | search result="SUCCESS" | sort 0 user \_time | streamstats current=f window=1 last(country) as prev\_country last(\_time) as prev\_t by user | eval dt=\_time-prev\_t | where prev\_country!=country AND dt<3600 | table \_time user prev\_country country dt

Result evidence:



Analysis:

Flag impossible travel or geo anomalies that may indicate account takeover or VPN misuse.

Conclusion:

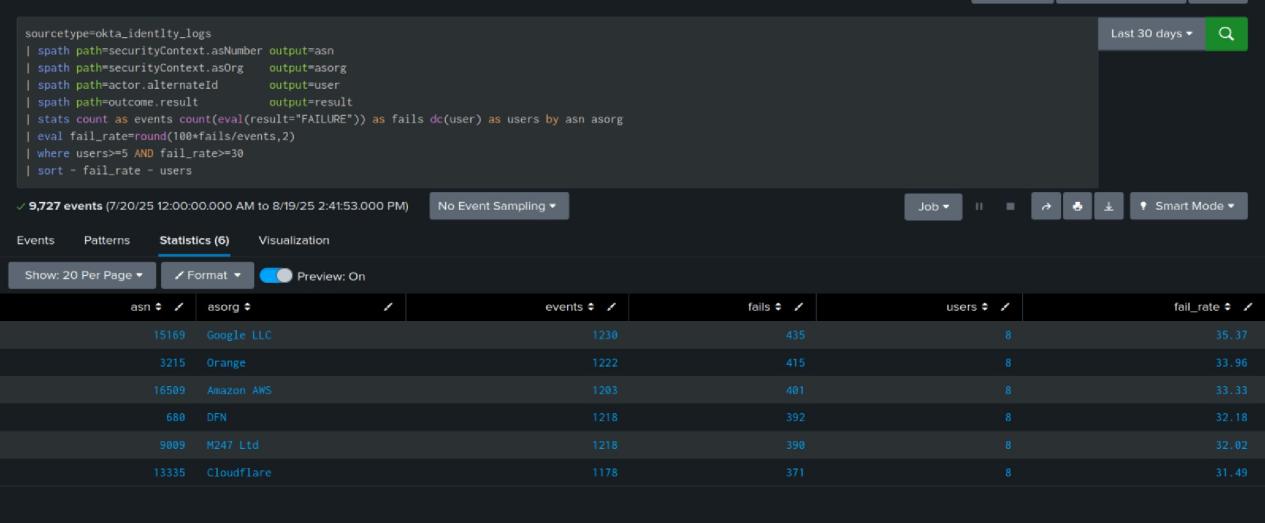
Noisy sources and suspicious patterns are identified for further triage. Convert this search into a saved alert or correlation rule as needed.

## 6. High-Risk ASNs by Failure Rate and User Impact

Search Processing Language (SPL):

sourcetype=okta\_identlty\_logs | spath path=securityContext.asNumber output=asn | spath path=securityContext.asOrg output=asorg | spath path=actor.alternateId output=user | spath path=outcome.result output=result | stats count as events count(eval(result="FAILURE")) as fails dc(user) as users by asn asorg | eval fail\_rate=round(100\*fails/events,2) | where users>=5 AND fail\_rate>=30 | sort - fail\_rate - users

Result evidence:



Analysis:

Surface network providers with disproportionate failure rates and many affected users.

Conclusion:

Noisy sources and suspicious patterns are identified for further triage. Convert this search into a saved alert or correlation rule as needed.

**Summary:** Baseline is steady, with focused credential attacks against specific hosts and accounts.

**Findings**

Event mix: user.authentication.sso dominates; notable user.authentication.failed; almost no mfa.challenge - weak step-up coverage.

Source: internal 10.66.10.10 shows failures across many users - shared gateway/proxy or misconfiguration.

10-min bursts: 185.220.101.55 and 45.83.23.10 drive multi-user failure series - automated guessing.

Geo: rapid country switches for a single user (e.g., DE-KZ-NL within ≤30 min) - impossible travel.

Networks: ≥30% fail rate from DFN, Orange, M247, Cloudflare, Google, AWS - proxy/hosting, higher risk.

**Risks**  
Account takeover, password reuse, MFA fatigue, lockout DoS, lateral movement.

**Actions**  
Enforce step-up/MFA and rate-limits; block noisy IPs/ASNs; alert on bursts, “one IP - many users,” and fast geo switches; rotate passwords/sessions for impacted users; review 10.66.10.10 config; run weekly trend reviews.

### Overall Analysis

Baseline is stable. Error spikes are short and sharp, consistent with automated guessing. Failures concentrate on a few IPs and accounts. Ten minute windows show clustered attempts, a brute force signal. Rapid country switches for a single identity indicate impossible travel. A small set of ASNs drives disproportionate failures, typical for proxies and hosting. Risks: account takeover, password reuse, MFA fatigue, lockout DoS, lateral movement, data exfiltration.

### Conclusion

Baseline is normal with focused credential attacks present. Actions: promote searches to alerts, enforce step up and MFA, block and rate limit noisy IPs and ASNs, rotate passwords for impacted users, monitor geo anomalies, tune thresholds to the observed baseline, run a weekly trend review.