**Splunk Security Analysis: Windows Authentication and Kerberos Events**

*Case • 2025-08-20*

# **Author : Vlassov Vladislav**

# Executive Summary

Six-step threat-hunting workflow in Splunk using Windows Security events. Each step includes the SPL query, a result screenshot placeholder, analysis, conclusion, and alert recommendation.

# Data and Environment

• Logs: Windows Security (sourcetype=winsec\_logs).

• Fields: EventCode, TargetUserName, IpAddress, LogonType; XML parsed via spath.

• Assumption: The six screenshots in the source doc map to sections 1–6 in order.

# 1. Authentication Failure Rate Over Time

SPL:

sourcetype=winsec\_logs   
| eval result=case(EventCode=4624,"SUCCESS", EventCode=4625,"FAIL", true(), null())   
| timechart span=30m count as total count(eval(result="FAIL")) as fails   
| eval err\_rate=round(100\*fails/total,2)

Result:

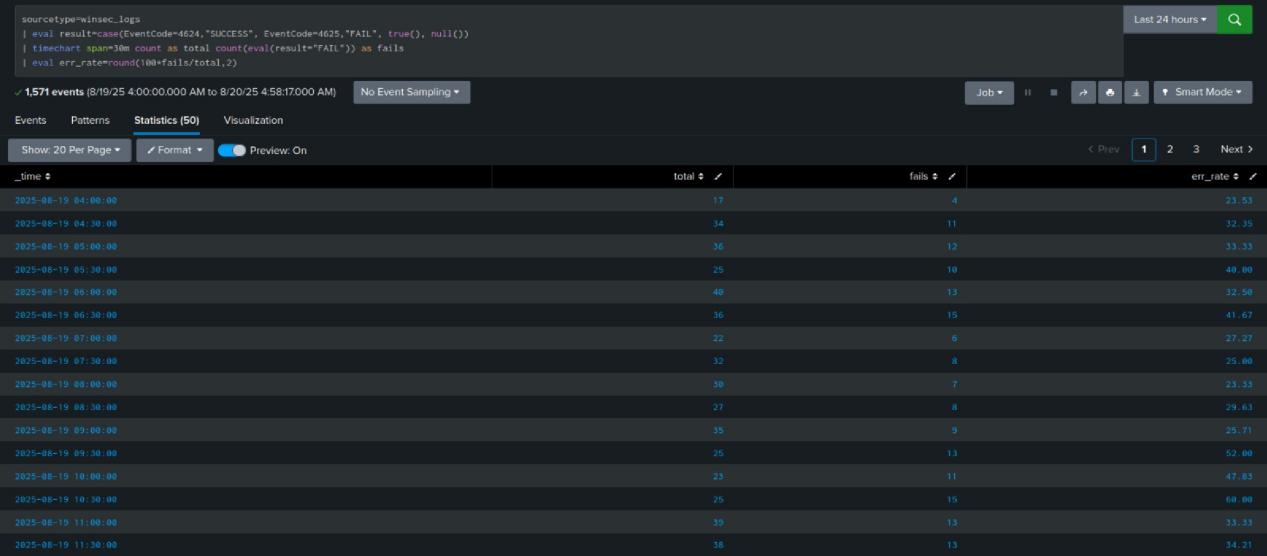


Figure 1. Result screenshot.

Analysis:

• Error-rate spikes may indicate brute force or credential issues.

• Correlate peaks with change windows to reduce false positives.

Conclusion:

Alert on err\_rate deviations above baseline.

# 2. Top Source IPs for Failed Logons

SPL:

sourcetype=winsec\_logs EventCode=4625 earliest=-14d   
| spath   
| eval user=coalesce('TargetUserName','EventData.TargetUserName')   
| eval ip=coalesce('IpAddress','EventData.IpAddress','Source\_Network\_Address')   
| where isnotnull(user) AND isnotnull(ip) AND ip!="-"   
| bin \_time span=10m   
| stats dc(user) as users count as fails by ip \_time   
| sort - fails   
| head 20

Result:

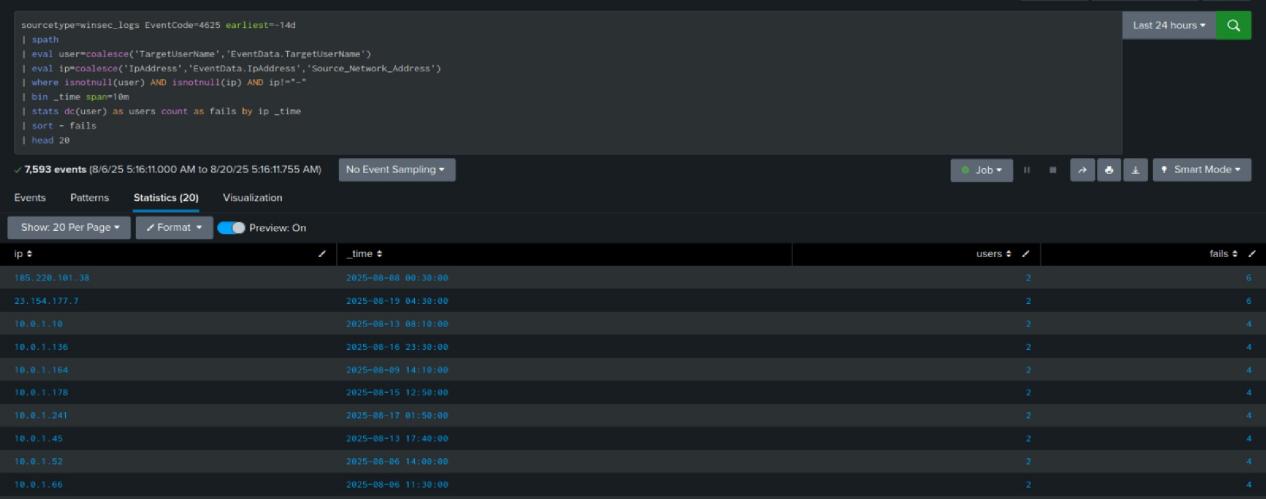


Figure 2. Result screenshot.

Analysis:

• Many fails across many users from one IP suggests password spraying.

• Public IPs are higher risk than RFC1918 sources.

Conclusion:

Alert when a source IP fails many accounts within short windows.

# 3. After-hours RDP Logons

SPL:

sourcetype=winsec\_logs EventCode=4624 LogonType=10   
| eval hour=tonumber(strftime(\_time,"%H"))   
| where hour<6 OR hour>=23   
| stats count by TargetUserName IpAddress   
| sort - count

Result:

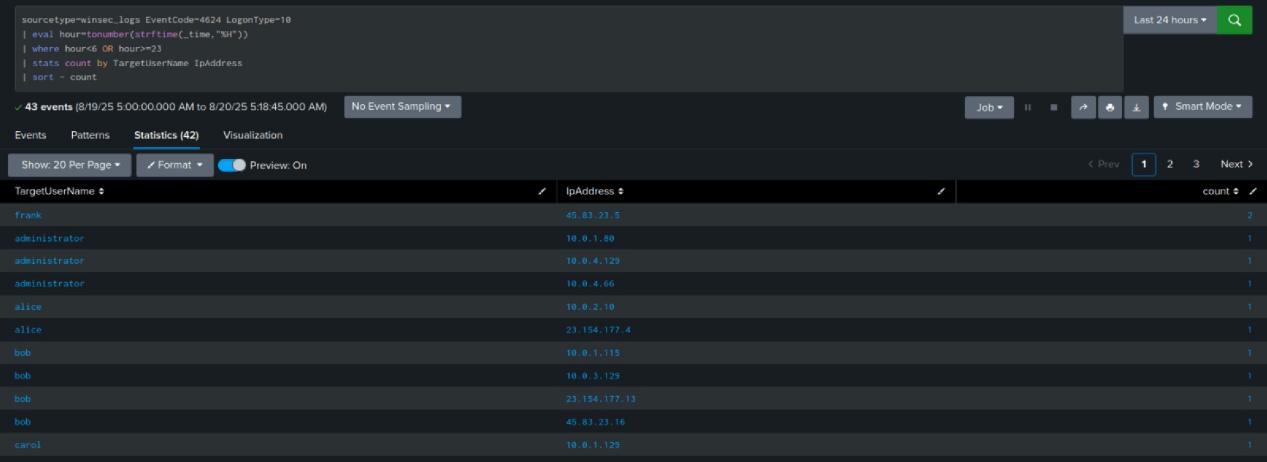


Figure 3. Result screenshot.

Analysis:

• Off-hours RDP successes require justification and MFA policy checks.

• Unknown user-IP pairs with high counts are suspicious.

Conclusion:

Alert on off-hours RDP successes excluding approved bastions.

# 4. Privileged Activity After Special Privilege Assignment

SPL:

sourcetype=winsec\_logs (EventCode=4672 OR EventCode=4648)   
| eval user=coalesce(SubjectUserName,TargetUserName)   
| sort 0 user Computer \_time   
| streamstats current=f window=1 last(eval(if(EventCode=4672,\_time,null()))) as t4672 by user Computer   
| eval delta=\_time - t4672   
| where EventCode=4648 AND t4672>0 AND delta<=900   
| table \_time Computer user delta ProcessName IpAddress TargetServerName

Result:

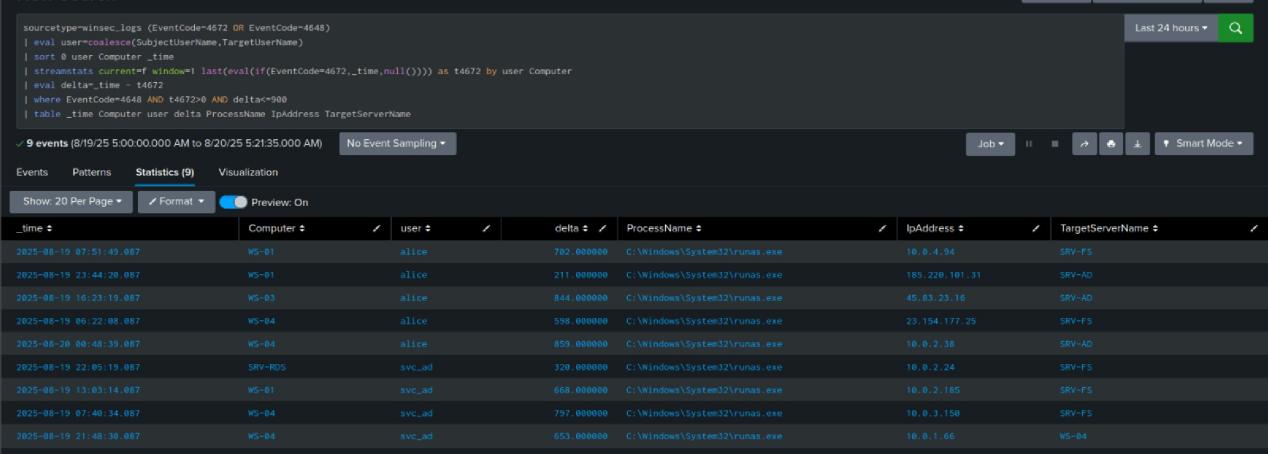


Figure 4. Result screenshot.

Analysis:

• Short deltas between 4672 and 4648 can indicate privilege escalation.

• Unusual processes or targets increase risk.

Conclusion:

Alert when 4672 is followed by 4648 within 15 minutes per user-host.

# 5. Kerberos Service Tickets: RC4 and External Access

SPL:

sourcetype=winsec\_logs EventCode=4769   
| spath   
| eval enc=tonumber(coalesce('TicketEncryptionType','EventData.TicketEncryptionType'))   
| eval ip=coalesce(IpAddress,'EventData.IpAddress')   
| eval svc=coalesce(ServiceName,'EventData.ServiceName')   
| eval is\_rc4=if(enc==23,1,0)   
| eval is\_ext=if(cidrmatch("10.0.0.0/8",ip) OR cidrmatch("192.168.0.0/16",ip) OR cidrmatch("172.16.0.0/12",ip),0,1)   
| stats count as events sum(is\_rc4) as rc4 sum(is\_ext) as ext by svc   
| eval rc4\_rate=round(100\*rc4/events,1), ext\_rate=round(100\*ext/events,1)   
| where rc4\_rate>=50 OR ext\_rate>=50   
| sort - rc4\_rate - ext\_rate

Result:

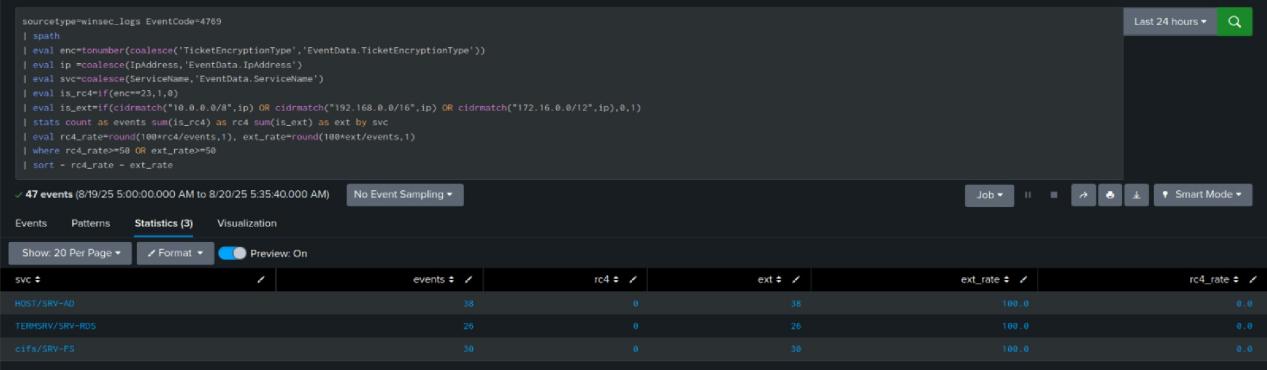


Figure 5. Result screenshot.

Analysis:

• High RC4 usage shows legacy crypto; external sources indicate exposure.

• Prioritize services with rc4\_rate or ext\_rate ≥50% for remediation.

Conclusion:

Audit RC4 services and restrict external access paths.

# 6. New Accounts and Domain Admin Additions

SPL:

sourcetype=winsec\_logs EventCode IN (4720,4728)   
| eval action=case(EventCode=4720,"UserCreated", EventCode=4728,"AddedToDomainAdmins")   
| timechart span=1d count by action

Result:

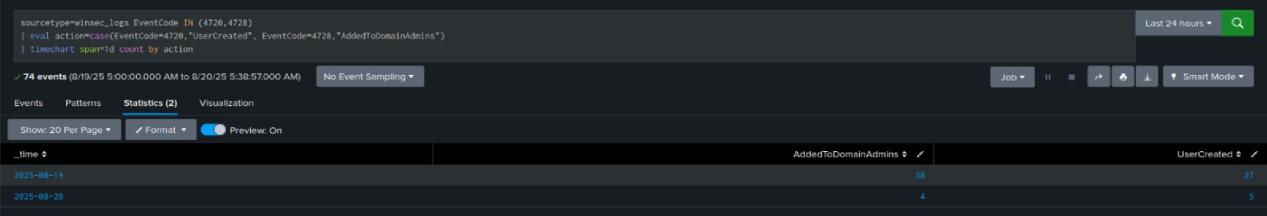


Figure 6. Result screenshot.

Analysis:

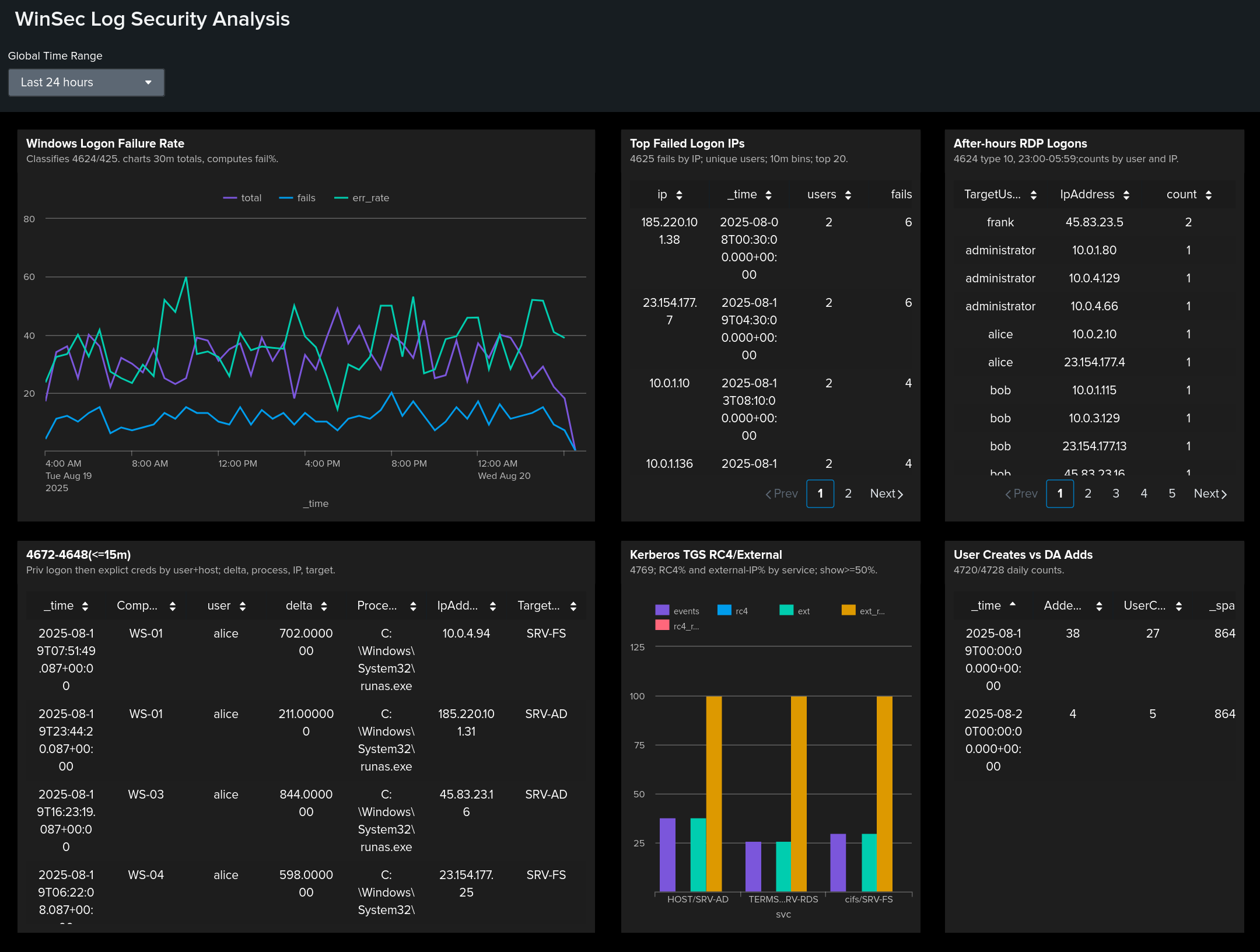
• Spikes in account creation and admin additions outside change windows are critical.

• Require tickets and approvals for admin group changes.

Conclusion:

Alert on account creations and Domain Admin additions.

# Dashboard: WinSec Log Security Analysis

****

**Purpose:** One-page view of auth risk.  
**Scope:** WinSec 4624, 4625, 4648, 4672, 4720, 4728, 4769. Default: last 24h.

## Panels

**Windows Logon Failure Rate** - 30m totals/fails/err\_rate. Action: investigate spikes vs change windows; pivot to IPs and users.

**Top Failed Logon IPs** - rank IP by fails and distinct users. Action: enrich, geolocate, block per policy.

**After-hours RDP Logons** - LogonType=10 at 23:00–06:00. Action: verify business need, MFA, jump-host use.

**4672→4648 (≤15m)** - explicit creds soon after special privileges on same host/user. Action: review process and target.

**Kerberos TGS RC4/External** - per service totals, RC4%, external%. Action: migrate crypto, restrict exposure.

**User Creates vs DA Adds** - daily 4720/4728. Action: require tickets; escalate spikes

## KPIs

Err\_rate > baseline +3σ for ≥60m.

Spraying: IP ≥N fails across ≥M users in ≤15m.

After-hours RDP: any success 23:00–06:00 (allowlist bastions/service accounts).

4672→4648 within 15m per user-host.

RC4% ≥50% or external% ≥50% per service.

Any DA addition; user-creates above daily baseline.

## MITRE

1: T1110 · 2: T1110,T1078 · 3: T1021.001,T1078 · 4: T1548,T1550 · 5: T1558 · 6: T1136,T1098

# Final Conclusion

These six searches provide a practical Windows authentication hunting pack: brute-force visibility, risky RDP access, privilege-escalation indicators, Kerberos weaknesses, and critical account lifecycle events.