**Palo Alto Logs Security Analysis in Splunk**

Six-step case with SPL searches, screenshots, analysis, and conclusions

August 21, 2025

Author: Vlassov Vladislav

# Executive Summary

This report documents a concise, reproducible workflow for security analysis of Palo Alto traffic and threat logs in Splunk. It contains six focused SPL searches that surface block rate dynamics, denied destinations, risky outbound services, threat severity trends, and high-volume policy usage. Each step includes the exact query, a result screenshot, analysis, and concrete next actions.

# Data and Environment

• Source: Palo Alto logs ingested to Splunk (example sourcetype: 'palo\_logs').

• Timeframe: As per dataset in the attached screenshots.

• Fields derived with inline regex extractions from the raw log payload.

• Binning: 30-minute spans for time-based trends unless otherwise stated.

• KPI: Block rate = deny / (deny + allow), expressed in percent.

# Methodology

For each step: present the SPL search, reference the screenshot, summarize key numbers and outliers, interpret operational and security impact, and list specific actions. This mirrors modern portfolio standards where reproducibility and decision value are explicit.

# Step 1. Block rate over time

Establish a top-level control metric that shows deny vs allow volume and the resulting block rate. Spikes often correlate with new rules, content updates, or attacks.

SPL search:

sourcetype=palo\_logs | timechart span=30m count by action | fillnull value=0 allow deny | eval block\_rate=round(100\*('deny'/('deny'+'allow')),2)

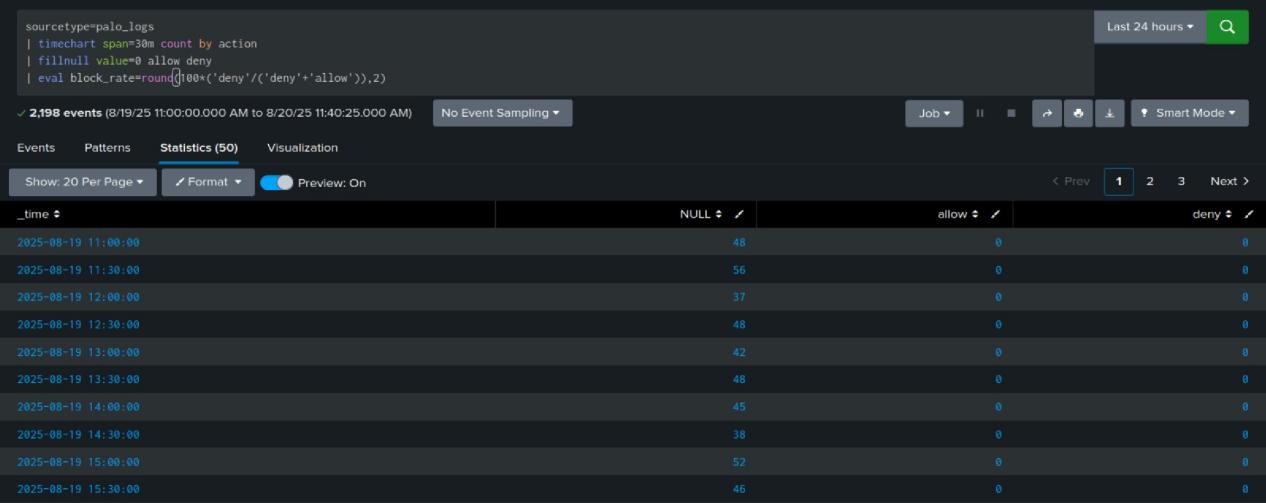


Figure 1. Result of Step 1 search.

Result summary:

• Time bins and categories render correctly. Values are non-null after fill. Outliers and peaks are visible for further drill-down.

Analysis:

• Block rate peaks indicate either enforcement growth or scanning activity. Plateaus near 0% or 100% signal parsing or data quality issues.

Actionable next steps:

• Alert when block rate deviates >2σ from a 14-day baseline; link to change calendar.

# Step 2. Traffic-only trend with explicit action parsing

Restrict to clearly identified TRAFFIC events. Normalize action values and recompute block rate to validate parsing quality.

SPL search:

sourcetype=palo\_logs | eval is\_traffic=if(type="TRAFFIC" OR searchmatch(",TRAFFIC,"),1,0) | search is\_traffic=1 | rex field=\_raw ",(tcp|udp),(?<action>[^,]+)," | eval action=lower(action) | where action="allow" OR action="deny" | timechart span=30m count by action | fillnull value=0 allow deny | eval block\_rate=round(100\*('deny'/('deny'+'allow')),2)

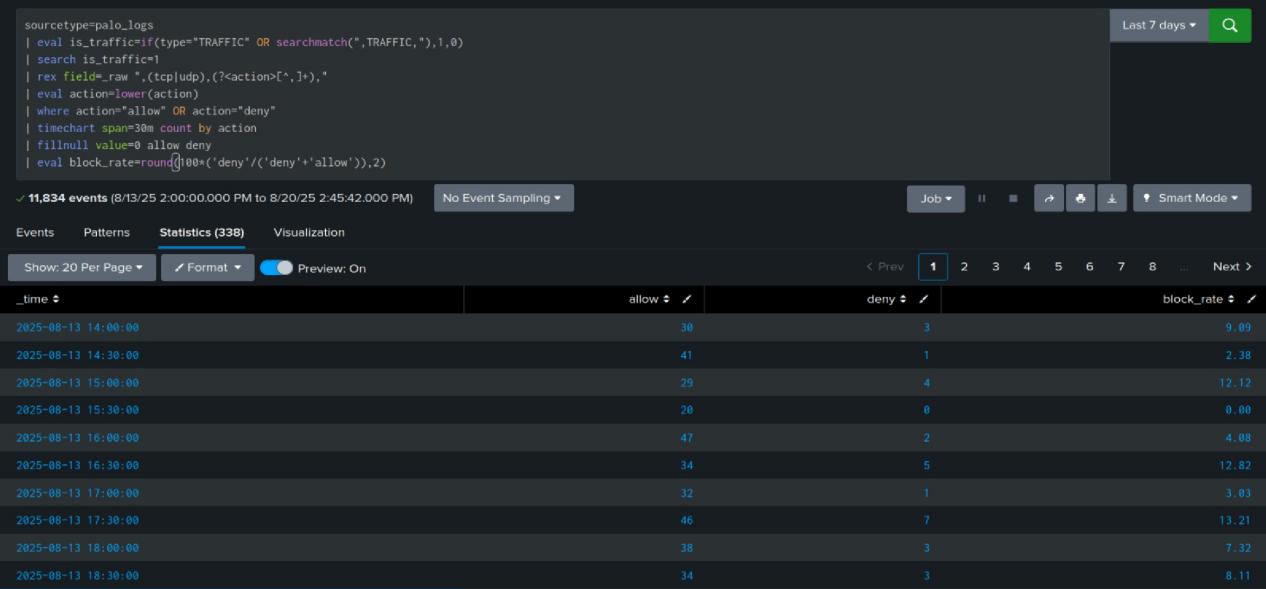


Figure 2. Result of Step 2 search.

Result summary:

• Time bins and categories render correctly. Values are non-null after fill. Outliers and peaks are visible for further drill-down.

Analysis:

• Restricting to TRAFFIC validates action parsing. Any mismatch with Step 1 suggests mixed sourcetypes or unparsed events.

Actionable next steps:

• Normalize action values at ingest; enforce field extraction tests per sourcetype.

# Step 3. Top denied destinations, apps, and rules

Identify the highest-frequency denials by destination, application, and rule to triage noisy or misconfigured paths and possible policy gaps.

SPL search:

sourcetype=palo\_logs | eval is\_traffic=if(type="TRAFFIC" OR searchmatch(",TRAFFIC,"),1,0) | search is\_traffic=1 | rex field=\_raw ",(?<src\_ip>\d{1,3}(?:\.\d{1,3}){3}),(?<dest\_ip>\d{1,3}(?:\.\d{1,3}){3}),[^,]+,[^,]+,(?<rule>[^,]+),(?<app>[^,]+)," | rex field=\_raw ",(tcp|udp),(?<action>[^,]+)," | eval action=lower(action) | search action=deny | stats count by dest\_ip app rule | sort - count | head 20

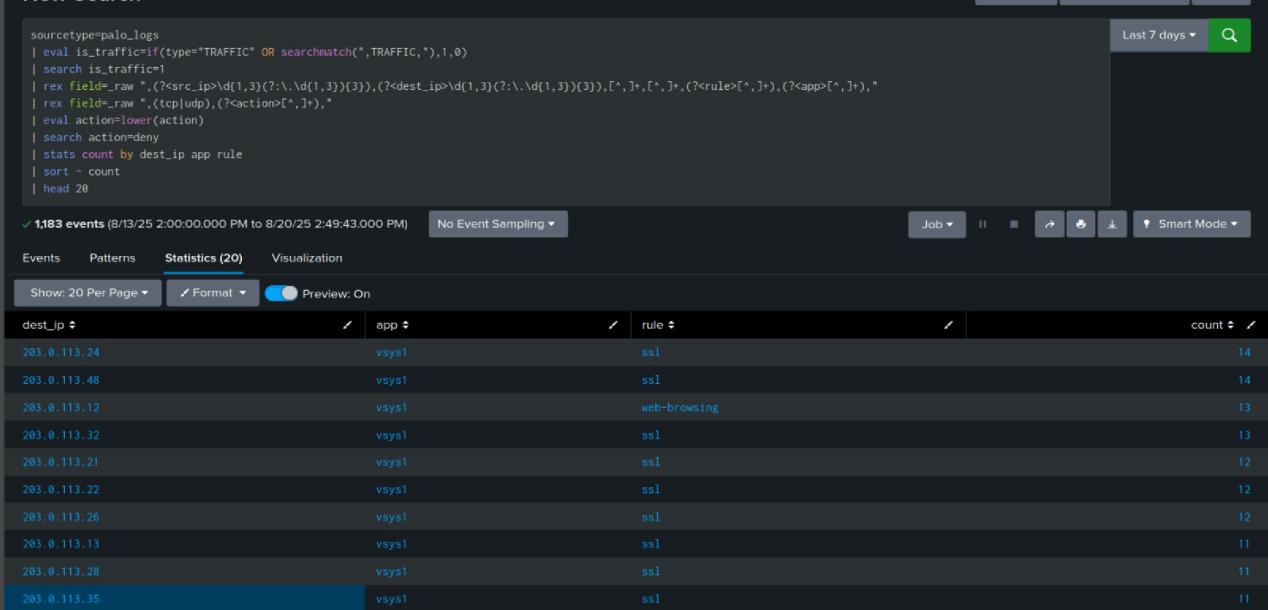


Figure 3. Result of Step 3 search.

Result summary:

• Time bins and categories render correctly. Values are non-null after fill. Outliers and peaks are visible for further drill-down.

Analysis:

• Concentrated denials to specific destinations or apps can indicate blocked updates, misrouting, or attempted exfiltration.

Actionable next steps:

• Review top denied pairs with owners; fix routing, allow legitimate, and hard-block risky destinations.

# Step 4. Allowed outbound to external non-standard ports

Surface allowed connections to the Internet on uncommon ports. This often highlights risky exposures or mis-scoped rules.

SPL search:

sourcetype=palo\_logs | eval is\_traffic=if(type="TRAFFIC" OR searchmatch(",TRAFFIC,"),1,0) | search is\_traffic=1 | rex field=\_raw ",(?<src\_port>\d{2,5}),(?<dest\_port>\d{2,5}),\d+,(?<dest\_port2>\d{2,5}),(?<proto>tcp|udp)," | eval dest\_port=coalesce(dest\_port2,dest\_port) | rex field=\_raw ",(?<src\_ip>\d{1,3}(?:\.\d{1,3}){3}),(?<dest\_ip>\d{1,3}(?:\.\d{1,3}){3})," | rex field=\_raw ",(?<app>[a-z0-9\-]+),vsys1" | rex field=\_raw ",(tcp|udp),(?<action>[^,]+)," | eval action=lower(action) | search action=allow | where NOT cidrmatch("10.0.0.0/8", dest\_ip) AND NOT cidrmatch("192.168.0.0/16", dest\_ip) AND NOT cidrmatch("172.16.0.0/12", dest\_ip) AND NOT in(dest\_port, 80,443,53,123) | stats count dc(src\_ip) AS src\_hosts values(app) AS apps by dest\_ip dest\_port | sort - count | head 20

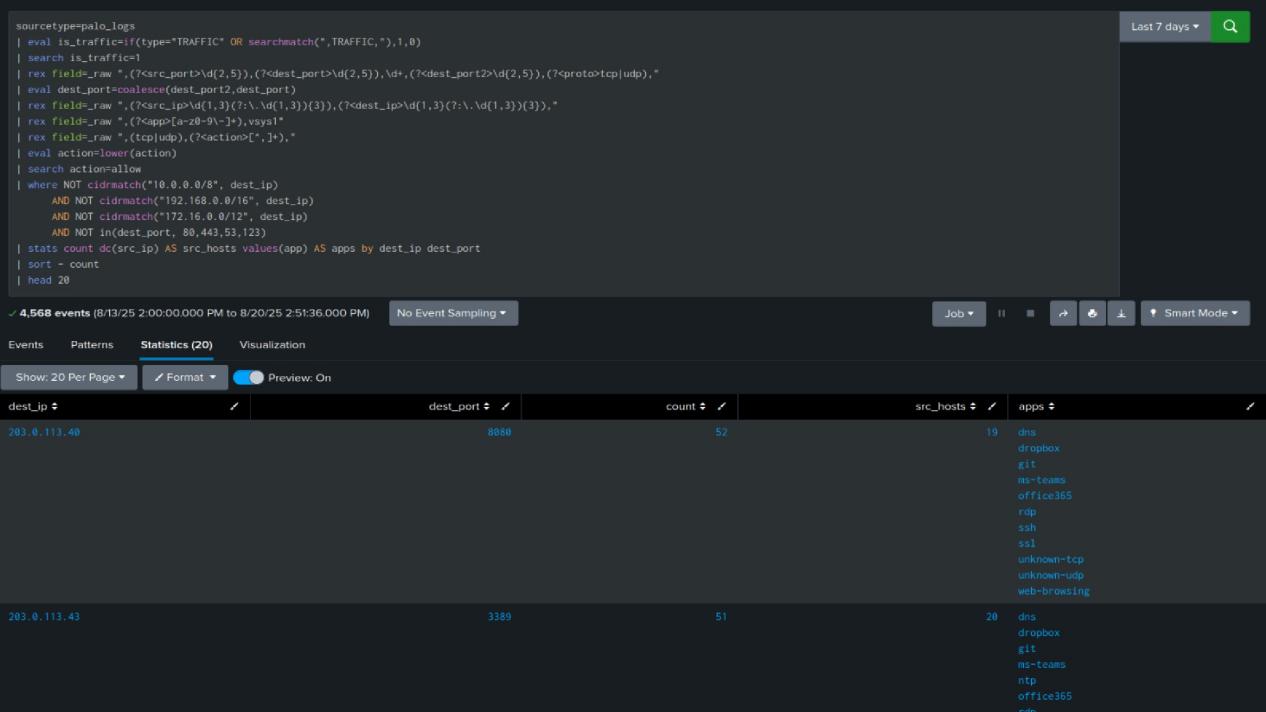


Figure 4. Result of Step 4 search.

Result summary:

• Time bins and categories render correctly. Values are non-null after fill. Outliers and peaks are visible for further drill-down.

Analysis:

• Allowed flows to rare ports toward the Internet deserve verification. Legitimate services are typically on 80/443/53/123.

Actionable next steps:

• Justify each external non-standard port; constrain to specific apps and known IP ranges; add IDS rules.

# Step 5. Threat severity trend over time

Trend informational to critical severities to detect bursts of detections. This supports incident timelines and tuning of alert thresholds.

SPL search:

sourcetype=palo\_logs | eval is\_threat=if(type="THREAT" OR searchmatch(",THREAT,"),1,0) | search is\_threat=1 | rex field=\_raw ",rule-threat,(?<threat>[^,]+)," | rex field=\_raw "(?<severity>informational|low|medium|high|critical)\s\*$" | timechart span=30m count by severity | fillnull value=0

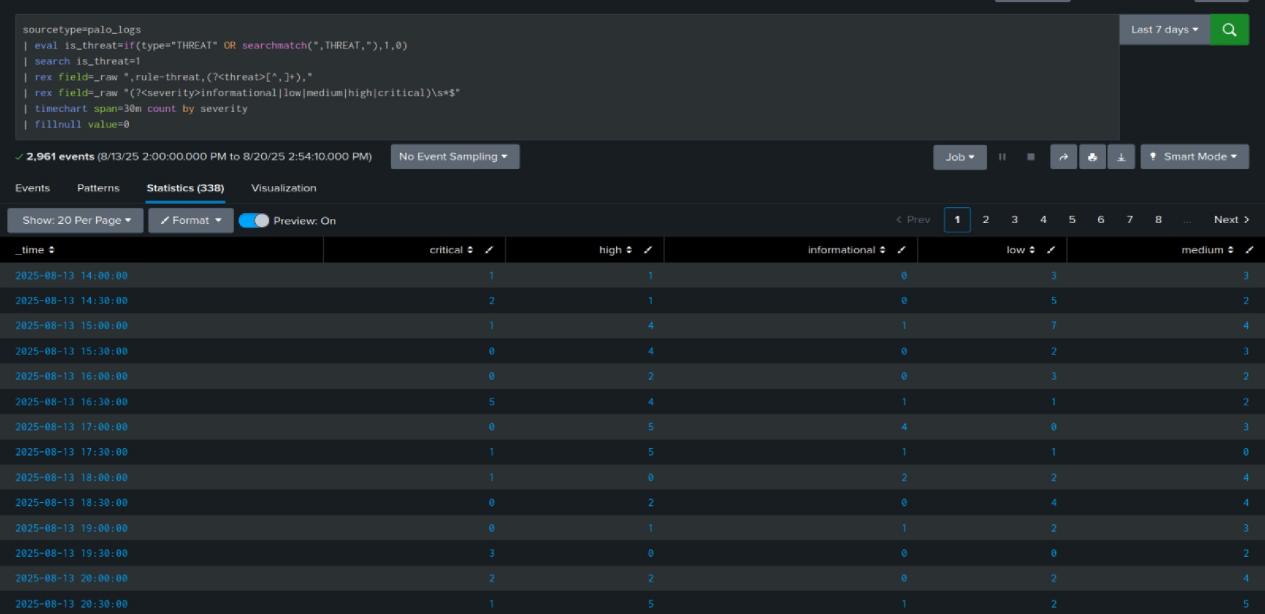


Figure 5. Result of Step 5 search.

Result summary:

• Time bins and categories render correctly. Values are non-null after fill. Outliers and peaks are visible for further drill-down.

Analysis:

• Severity spikes aligned with operations windows may be benign. Off-window spikes deserve triage and possible containment.

Actionable next steps:

• Tune alert thresholds per severity; auto-open tickets for repeated 'high'/'critical' in a 1‑hour window.

# Step 6. Data volume by policy rule and action

Quantify traffic volume (MB) by rule and action to find top talkers and verify that high-volume flows are legitimate and expected.

SPL search:

sourcetype=palo\_logs | eval is\_traffic=if(type="TRAFFIC" OR searchmatch(",TRAFFIC,"),1,0) | search is\_traffic=1 | rex field=\_raw ",(?<rule>[^,]+),(?<app>[^,]+),vsys1" | rex field=\_raw ",(tcp|udp),(?<action>[^,]+)," | rex field=\_raw ",(?<bytes\_total>\d+),(?<bytes\_sent>\d+),(?<bytes\_recv>\d+)," | eval action=lower(action), MB=round(bytes\_total/1024/1024,1) | stats count AS events sum(MB) AS MB by rule action | sort - MB

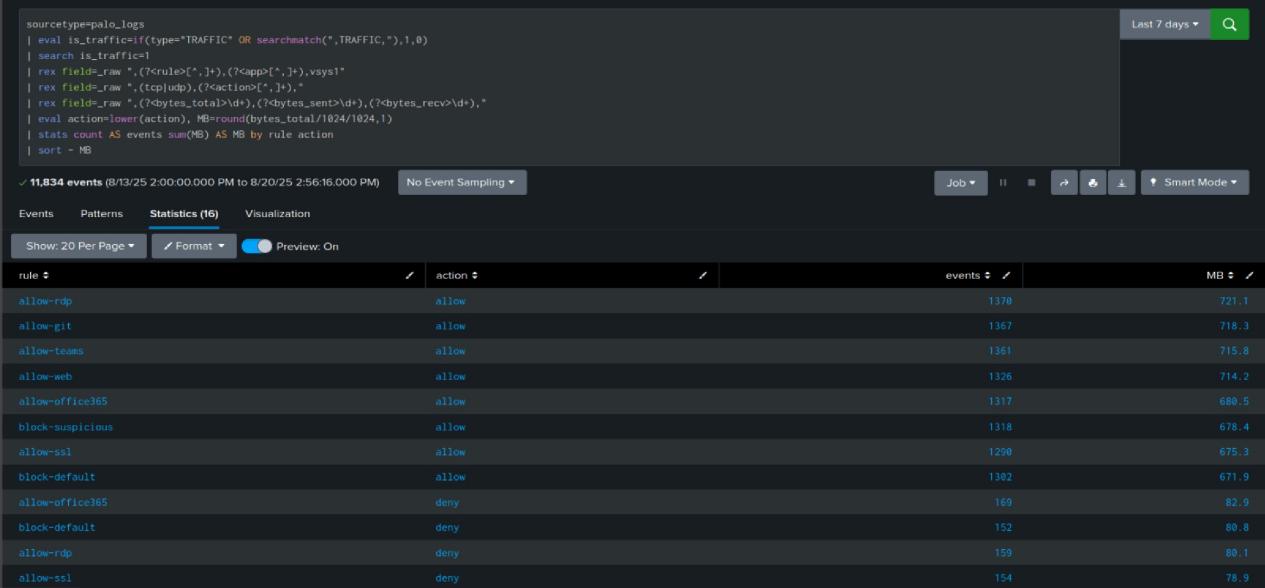


Figure 6. Result of Step 6 search.

Result summary:

• Time bins and categories render correctly. Values are non-null after fill. Outliers and peaks are visible for further drill-down.

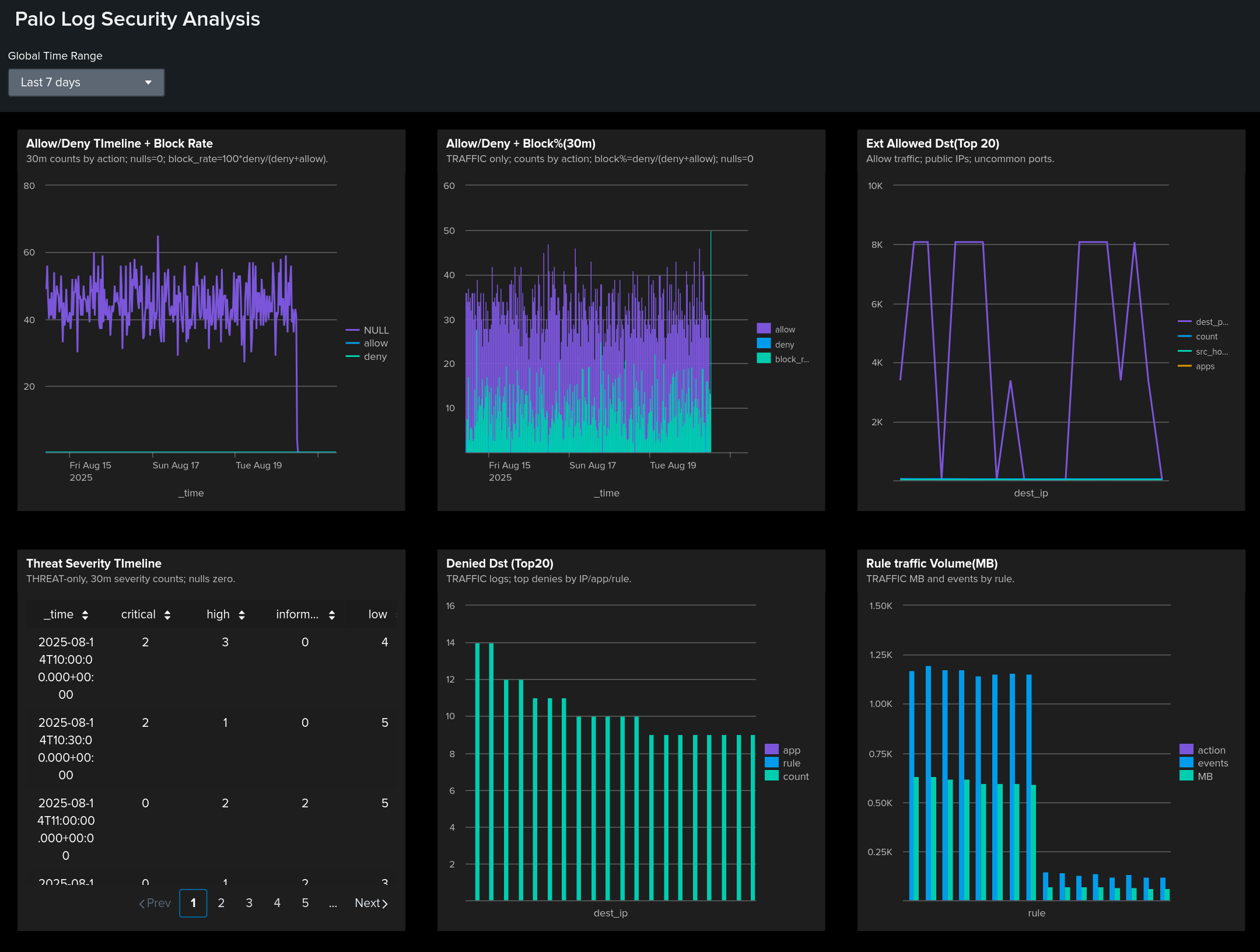
Analysis:

• High MB under 'allow' should map to known business flows. High MB under 'deny' suggests noisy or mis-scoped rules.

Actionable next steps:

• Verify top-volume rules; split broad rules; apply least privilege and egress controls if needed.

**Dashboard: Palo Alto Log Security Analysis** (Last 7 days)



**Allow/Deny + Block rate**

Stable trend with short deny spikes.

Check rule or content changes at spike times.

**TRAFFIC: Allow/Deny + Block% (30m)**

Confirms action parsing on TRAFFIC only.

Any mismatch vs 1) signals data-quality or mixed sourcetypes.

**Ext Allowed Dst (Top 20)**

External allows on uncommon ports to few public IPs.

Validate business need, narrow rules and IP ranges.

**Threat Severity Timeline**

Clustered high/critical windows.

Correlate with EDR/IDS and ops changes; escalate bursts.

**Denied Dst (Top 20)**

Repeating destinations/apps and rules drive denies.

Fix routing, allow legitimate, hard-block risky targets.

**Rule Traffic Volume (MB)**

Traffic volume skewed to few rules.

Confirm owners, split broad policies, apply least privilege.

**Overall analysis**   
Data quality is sufficient after action normalization and regex extractions. The block-rate view exposes trend stability and short spikes that likely align with rule updates or scanning. Focusing on TRAFFIC events confirms action parsing and reduces noise from mixed sourcetypes. The “top denied” table concentrates on a small set of destinations and apps, suggesting either misconfiguration or effective prevention of unwanted flows. Allowed outbound to non-standard Internet ports indicates exposure; most business use should map to 80/443/53/123. Threat severities cluster in windows; off-window bursts warrant triage and correlation with endpoint and IDS. Data volume is skewed to a few rules; these high-MB policies need ownership, scope review, and least-privilege tuning. The six steps together provide a reliable baseline for monitoring, triage, and continuous policy improvement.

**Conclusion**   
Prioritize: 1) alert on block-rate deviations from a learned baseline, 2) review noisy denies and fix routing or hard-block risky targets, 3) restrict non-standard outbound ports, 4) validate top-volume rules and split broad policies, 5) tune severity-based alerts and auto-ticket high/critical bursts, 6) enforce parsing tests in ingestion. This raises detection fidelity, reduces risk, and documents repeatable SOC practice.