WEEKLY THREAT BRIEF

TrapLayer Weekly Executive Threat Intelligence Brief

Scope: Last 7 days | Generated: 2026-09-21T09:23:27Z

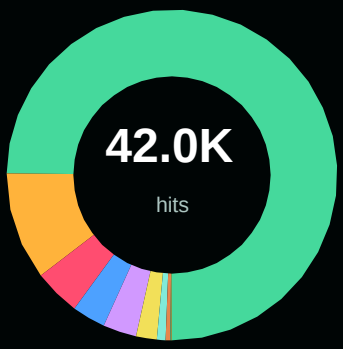
Executive Signal

TrapLayer observed 41979 public-safe high-signal events in the report window, including 1636 high-risk events. The leading behavior category was protocol_attacks, with ssh_session as the most common payload family. The most-attacked vertical was energy; week-over-week change is not yet available.

EVENTS	HIGH RISK	FINGERPRINTS	AVG RISK
42.0K	1,636	10	80
report-window hits	risk >= 80	observed clusters	curated score

Attack Hit Circle

Distribution of report-window hits by attack surface.



SSH shell attacks	31418 hits	risk 93
Cloud metadata attacks	4434 hits	risk 92
PostgreSQL attacks	1910 hits	risk 79
Redis/data-store attacks	1377 hits	risk 82
MySQL attacks	1371 hits	risk 82
MS SQL attacks	851 hits	risk 79
SCADA/Modbus attacks	359 hits	risk 95
DevOps attacks	199 hits	risk 93
AI agent/MCP attacks	37 hits	risk 82
SMTP mail attacks	23 hits	risk 61

What This Report Includes

Public-safe intelligence summary for open web publication.

- Report-window metrics, attack surface distribution, and trend baselines.
- Actor hypotheses, common attack patterns, and MITRE/CVE context.
- AI attack intelligence when prompt or agent-like telemetry is observed.
- Public-safe handling with sensitive raw telemetry excluded from the PDF.

TrapLayer

TREND READOUT

Trend Summary and Business Impact

Trend Summary

WINDOW SIGNAL

41,979 events are in the active report window.

12 weeks has 244,084 events.

TOP EXPOSURE

SSH shell attacks leads with 31,418 hits.

Cloud metadata attacks follows at 4,434 hits.

ANALYST READOUT

Observed cluster 1 is the leading behavior cluster.

Public copy excludes raw identifiers and customer-

Comparative Windows

Counts are server-generated cache values for comparable report windows.

Targeting and Exposure Notes

energy	50 hits

Briefing Notes

41979 high-signal events met public reporting thresholds.

1636 events reached high-risk scoring at or above 80.

Average classifier confidence was 81.3 across reportable events.

TrapLayer

ANALYST VIEW

Patterns, Clusters, and Defensive Readout

Top Observed Actor Hypotheses

Hypotheses are behavior clusters only. TrapLayer does not claim real-world identity from this report.

OBSERVED CLUSTER 1

Campaign 48D827

cloud secret harvest

3 events | risk 92 | conf 66%

OBSERVED CLUSTER 2

Campaign 79AD09

cloud probe

3 events | risk 68 | conf 61%

OBSERVED CLUSTER 3

Campaign 2856D4

cloud probe

1 events | risk 68 | conf 59%

Common Attack Patterns

PATTERN	FAMILY	COUNT	MAX
ssh session probe	ssh session	12690	65
ssh client fingerprint	ssh client fingerprint	11969	64
ssh auth probe	ssh authentication	5566	78
database probe	database reconnaiss...	5440	64
cloud probe	cloud reconnaissance	4224	68

MITRE and CVE Context

T1552 Unsecured Credentials	50 hits
T1046 Network Service Discovery	41 hits
T1651 Cloud Administration Command	9 hits
T1110 Brute Force	3 hits

No CVE-specific indicators were observed.
MITRE mapping is behavioral; CVE labels

AI Attack Intelligence

37 AI/prompt-adjacent events were observed: 24 tool/MCP probes. Avg classifier confidence: 82.8%.
prompt/instruction probes and tool-use signals

agent_tool_discovery	22 hits
agent_probe	9 hits
agent_tool_invocation	2 hits

Public-safe handling

This report is classified GREEN. It contains public-safe intelligence and excludes raw ip, ip hash, headers, payload, session id, full user agent, canary token.

Use actor hypotheses as triage leads only; confirm with customer telemetry before attribution or enforcement.