WEEKLY THREAT BRIEF

TrapLayer Weekly Executive Threat Intelligence Brief

Scope: Last 7 days | Generated: 2026-09-14T09:35:07Z

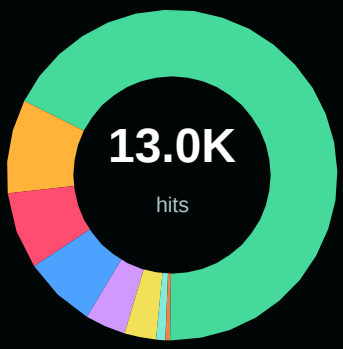
Executive Signal

TrapLayer observed 12969 public-safe high-signal events in the report window, including 437 high-risk events. The leading behavior category was secret_harvest, with cloud_reconnaissance 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
13.0K	437	7	80
report-window hits	risk >= 80	observed clusters	curated score

Attack Hit Circle

Distribution of report-window hits by attack surface.



Cloud metadata attacks	8767 hits	risk 92
MySQL attacks	1190 hits	risk 82
PostgreSQL attacks	977 hits	risk 79
Redis/data-store attacks	919 hits	risk 82
MS SQL attacks	515 hits	risk 64
SCADA/Modbus attacks	401 hits	risk 76
DevOps attacks	118 hits	risk 93
AI agent/MCP attacks	58 hits	risk 78
SMTP mail attacks	24 hits	risk 84
SSH shell attacks	0 hits	risk 0

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.

Trend Summary and Business Impact

Trend Summary

WINDOW SIGNAL

12,969 events are in the active report window.

12 weeks has 202,108 events.

TOP EXPOSURE

Cloud metadata attacks leads with 8,767 hits.

MySQL attacks follows at 1,190 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

12969 high-signal events met public reporting thresholds.

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

Average classifier confidence was 78.1 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 B4D08A

cloud probe

38 events | risk 68 | conf 88%

OBSERVED CLUSTER 2

Campaign 0658D3

cloud probe

1 events | risk 68 | conf 59%

OBSERVED CLUSTER 3

Campaign 2856D4

cloud probe

1 events | risk 68 | conf 59%

Common Attack Patterns

PATTERN	FAMILY	COUNT	MAX
cloud probe	cloud reconnaissance	8469	68
database probe	database reconnaiss...	3535	64
cloud secret harvest	cloud secret material	298	92
device identification probe	scada device identi...	229	76
function probe	scada read	161	76

MITRE and CVE Context

T1552 Unsecured Credentials	50 hits
T1651 Cloud Administration Command	41 hits
T1046 Network Service Discovery	8 hits

No CVE-specific indicators were observed. MITRE mapping is behavioral; CVE labels require explicit product exploit evidence.

AI Attack Intelligence

58 AI/prompt-adjacent events were observed: 32 tool/MCP probes. Avg classifier confidence: 81.3%. prompt/instruction probes and tool-use signals

agent_tool_discovery	32 hits
agent_probe	25 hits
agent_vector_search	1 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.