2026

State of SIEM REPORT

Buying signals, ranked threats, and practical guidance for lean security teams

graylog

Table of Contents

Executive Summary

Lean security teams at mid-sized enterprises enter 2026 with compressed intrusion timelines, identity-led compromise, and higher financial impact per incident. Attacker speed keeps improving while many SIEM programs still rely on human-driven correlation across too many tools and too much data. For teams of one to ten people, that gap shows up as slower scoping, inconsistent responses, and increased time spent on reporting rather than containment.

This report targets mid-market realities: hybrid environments, SaaS-heavy stacks, limited tuning time, and no dedicated SIEM engineering bench. It combines established industry research with patterns surfaced in evaluation cycles with CISOs, CIOs, SOC leads, and analysts, then validates the Top 10 issues against how teams operationalize security data in Graylog deployments.

The ranking reflects a consistent operating reality: identity drives access, ransomware drives disruption, and third parties widen blast radius. Credential abuse extends dwell time, supply chain exposure turns isolated incidents into downstream impact, and financial consequences remain high across insider events and public cloud breaches. Across Graylog environments, early adoption clusters around high-signal telemetry for fast scoping and repeatable response: Windows Security logs, Linux system logs, and perimeter controls such as firewalls, often across Fortinet, Palo Alto, Cisco, and Check Point ecosystems. Coverage typically expands to web server telemetry like Apache HTTPD, then email, SaaS, and cloud audit logging while keeping retention predictable. **In 2026, SIEM value is defined by speed, analyst execution, and cost control.**

Three takeaways for SIEM buyers in 2026

- **Speed comes from execution, not volume.** Lean teams prioritize the telemetry sources most environments share: OS logs, web logs, and firewall activity, then expand coverage based on risk.
- **Identity context reduces alert fatigue.** Asset synchronization and entity risk scoring help analysts focus on the few events that represent real exposure, with context available at triage and investigation.
- **Retention must be predictable.** The goal is usable history for investigations and audits, supported by a cost model that stays stable as data grows.

Who This Report Is For

This report targets **mid-market organizations (250 to 5,000 employees)** operating **lean security teams (1-10 dedicated staff)** that rely on a small number of analysts and shared IT responsibilities.

Common constraints assumed throughout:

- Limited time for rule tuning and content engineering
- Hybrid environments and SaaS-heavy stacks
- Budget sensitivity to ingest and retention volatility
- Partial coverage hours with frequent on-call burden

Methodology

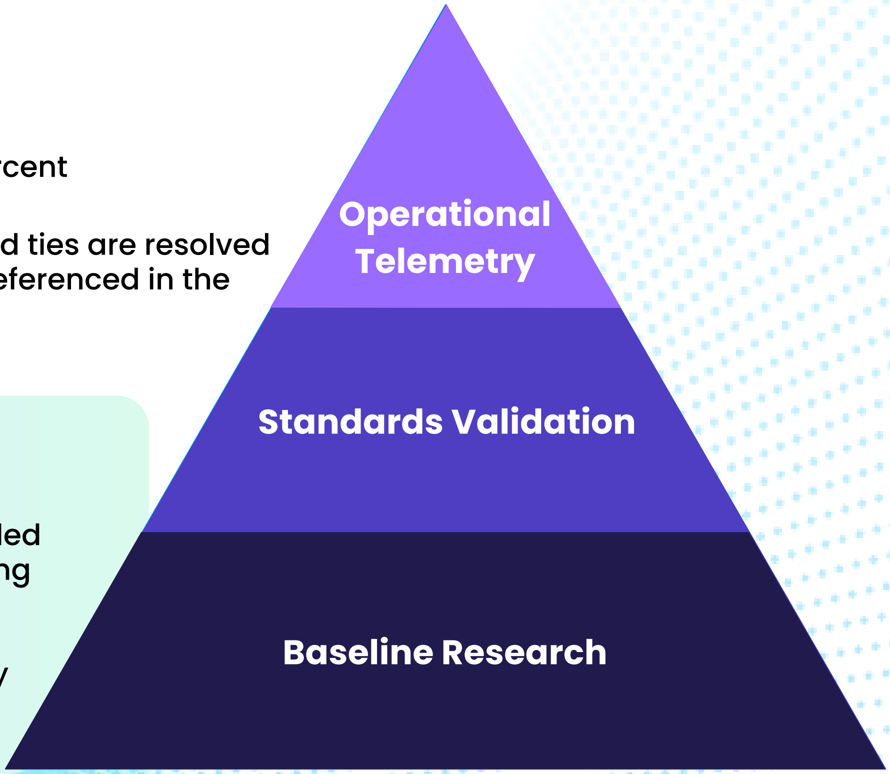
Threats are prioritized using a weighted scoring model across four criteria:

- Prevalence: 35 percent
- Disruption impact: 25 percent
- Attacker advantage: 20 percent
- Lean-team workload burden: 20 percent

Scores range from 0 to 5 per criterion, and ties are resolved using Verizon DBIR prevalence anchors referenced in the source-mapping approach.

Evidence standard

Issue profiles and rankings are grounded in the report's source-to-issue mapping approach, drawing on established research, standards validation, and vendor or incident-response telemetry sources used in the base material.



The 2026 Threat Reality for Lean Teams

Attackers continue to favor techniques that reduce friction and increase speed. Identity systems, email workflows, cloud control planes, and trusted third parties remain the highest-leverage paths because they blend into normal operations.

What changed for lean teams in practical terms

- **Ransomware timelines tightened.** The evidence set used here cites faster time-to-exfiltration, including meaningful exfiltration inside the first hour in ransomware scenarios.
- **Email compromise matured into repeatable fraud operations.** Phishing and BEC are ranked second, supported by evidence including 82.6 percent AI-enhanced phishing usage in the mapped research set.
- **Credential abuse hides in plain sight.** Identity-based compromise extends detection timelines and increases scoping work, with a cited 328-day detection time in certain credential scenarios (Improved to 292 days in 2024 and 246 days in 2025).
- **Third-party and cloud failures scale impact quickly.** Third-party involvement doubled to 30 percent of breaches, and cloud incidents are tied to weak credentials and misconfigurations in the supporting sources used for ranking.

Lean-team operational consequence

Every minute spent manually stitching alerts together becomes attacker dwell time. Lean programs need SIEM that reduces correlation labor and produces consistent actions from the same signals.

Industry Impact Lens

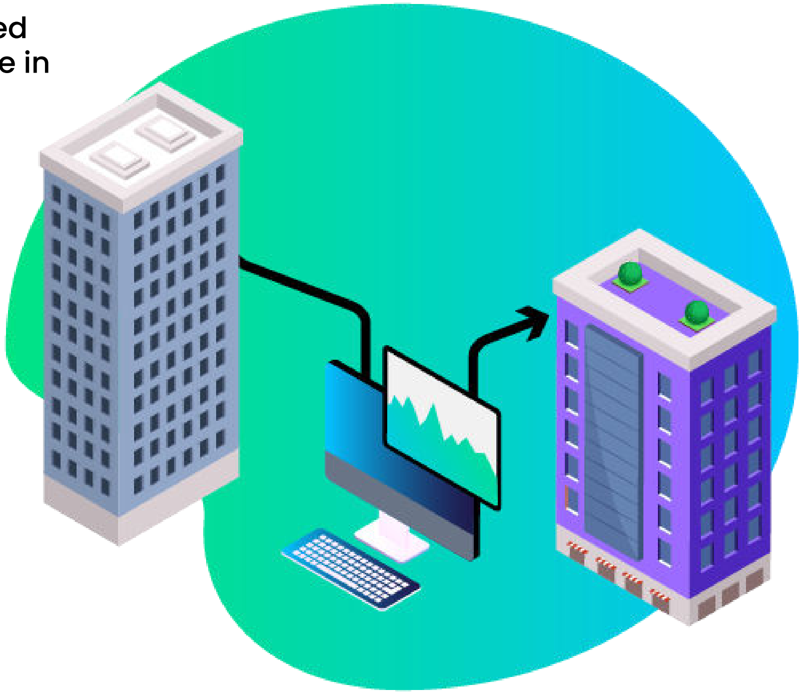
Threat priorities stay consistent, but impact varies by industry. The Enhanced Industry Impact Matrix classifies security issues by industry using factors like operational disruption, regulatory risk, and typical attacker targeting patterns.

Cross-industry patterns that affect SIEM requirements

- **Universal high-impact threats:** ransomware, credential abuse, and exploitation of legacy systems remain high-severity across most environments.
- **Third-party exposure is structural:** third-party breaches are cited as doubling to 30 percent of incidents in the cross-industry analysis inputs.
- **Nation-state pressure concentrates by sector:** the industry matrix notes a surge in Chinese APT operations of 150 percent in the referenced inputs, raising the premium on long retention and cross-domain correlation for targeted sectors.

Industry anchors for mid-market leaders

- **Healthcare:** cited with 444 incidents in 2024 and an average incident cost of $7.42 million in the industry matrix inputs, increasing pressure for audit-ready evidence and durable retention.
- **Manufacturing:** cited as the most attacked sector in 2024, with an 87 percent increase in ransomware attacks, with manufacturing accounting for 69 percent of these incidents, reinforcing the need for rapid containment workflows and segmented visibility.
- **Education:** cited at 3,574 cyber attacks per week per school, raising the value of fast triage and standardized playbooks in small teams.



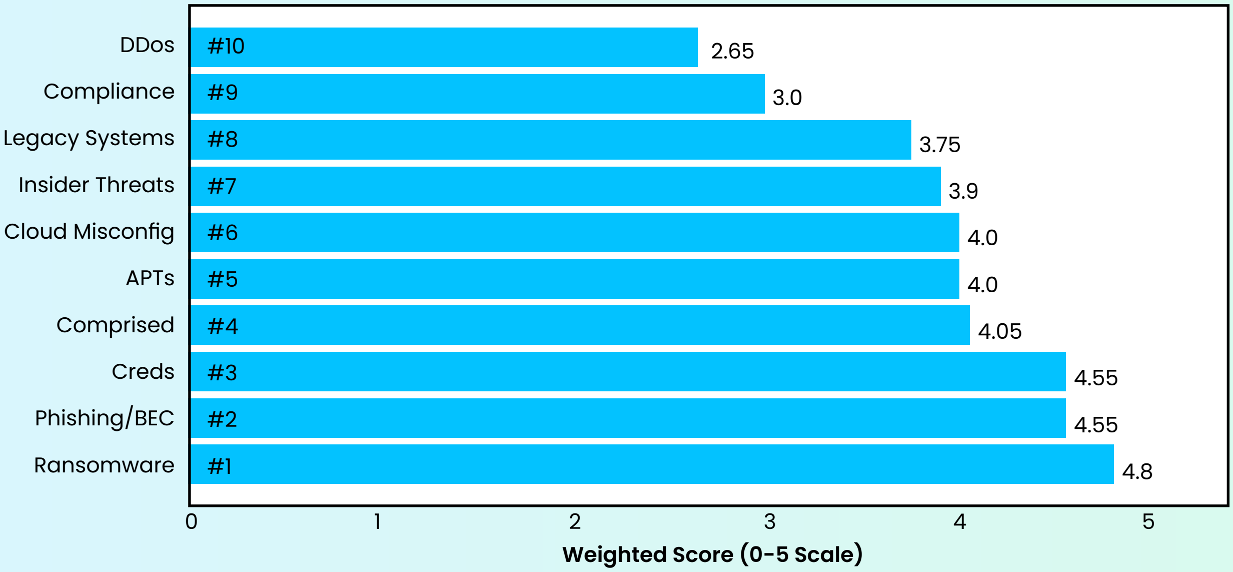
Ranked Threats Driving SIEM Requirements

Top 10 Security Issues for Lean Teams (2026)

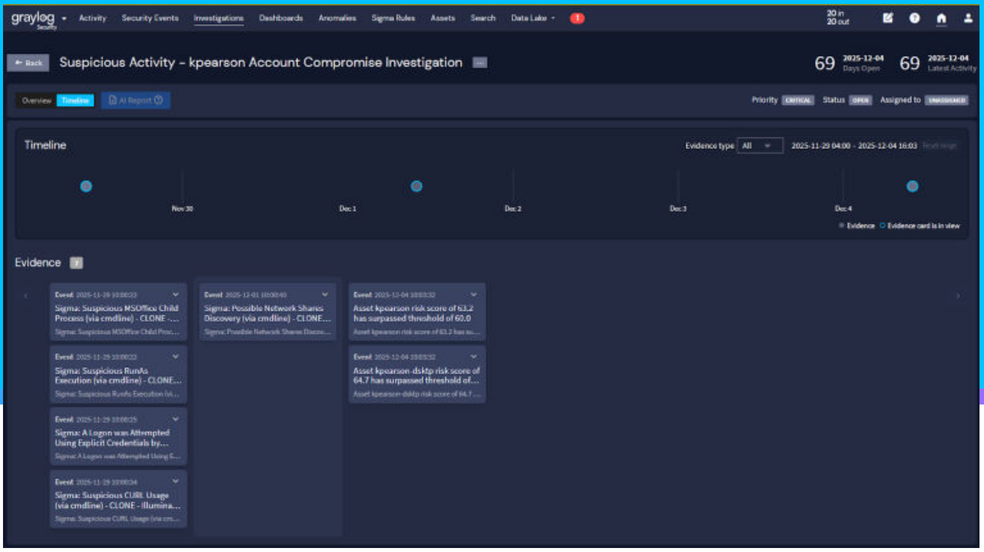
(Weighted scoring based on prevalence, disruption impact, attacker advantage, and lean-team workload burden.)

Rank	Issue	Weighted score	Primary drivers	Key anchor
1	Ransomware and file encryption attacks	4.80	Fast exfiltration, high disruption	44% global; 51% APAC; 20% exfiltration within first hour
2	Phishing and BEC	4.55	Fraud outcomes, identity pivot	82.6% AI-enhanced phishing
3	Compromised credentials and privilege misuse	4.55	Legitimate access abuse, long dwell	22% initial access; ~246 days mean time to identify and contain for stolen credentials
4	Advanced persistent threats	4.05	High attacker advantage, long hunts	75 zero-days exploited
5	Supply chain and third-party vulnerabilities	4.00	Trusted access, cascading impact	30% involvement; $4.91M average cost
6	Unmanaged cloud resources and misconfigurations	4.00	IAM drift, multi-cloud sprawl	47.1% weak creds; 29.4% misconfigs; $5.17M public cloud costs
7	Insider threats and accidental data exposure	3.90	High cost, complex investigations	$4.99M highest breach cost; 85-day detection time
8	Exploitation of unpatched or legacy systems	3.75	Exploitability and patch delay	34% increase in exploitation in cited set
9	Compliance violations and regulatory drift	3.00	Audit pressure and evidence gaps	Healthcare cited with 444 incidents
10	Denial of service attacks	2.65	Availability impact, coordination load	Resolution beyond one day

2026 Mid-Market Security Threat Rankings Weighted Scoring Model Results



Issue Profiles 1 to 3



Suspicious Activity - kpearson Account Compromise Investigation

69 2025-12-04 Days Open 69 2025-12-04 Latest Activity

Priority CRITICAL Status OPEN Assigned to UNASSIGNED

Timeline

Evidence type All 2025-11-29 04:00 - 2025-12-04 16:03

Evidence 7

Event 2025-11-29 10:00:23
Sigma: Suspicious MSOffice Child Process (via cmdline) - CLONE -...
Sigma: Suspicious MSOffice Child Proc...

Event 2025-11-29 10:00:22
Sigma: Suspicious RunAs Execution (via cmdline) - CLONE...
Sigma: Suspicious RunAs Execution (vi...

Event 2025-11-29 10:00:25
Sigma: A Logon was Attempted Using Explicit Credentials by...
Sigma: A Logon was Attempted Using E...

Event 2025-11-29 10:00:34
Sigma: Suspicious CURL Usage (via cmdline) - CLONE - Illumina...
Sigma: Suspicious CURL Usage (via cm...

Event 2025-12-01 10:00:40
Sigma: Possible Network Shares Discovery (via cmdline) - CLONE...
Sigma: Possible Network Shares Disco...

Event 2025-12-04 10:03:32
Asset kpearson risk score of 63.2 has surpassed threshold of 60.0
Asset kpearson risk score of 63.2 has su...

Event 2025-12-04 10:03:32
Asset kpearson-dsktp risk score of 64.7 has surpassed threshold of...
Asset kpearson-dsktp risk score of 64.7 ...

Issue 1: Ransomware and file encryption attacks

Why it ranks first

Ransomware combines high prevalence with fast time-to-impact, including cited data showing ransomware presence in 44 percent of breaches globally and 20 percent of exfiltration occurring within the first hour in the referenced set.

High-signal detection priorities

- Mass file modification and extension changes across multiple directories
- Backup access anomalies and deletion attempts
- Lateral movement bursts paired with privilege escalation
- Data staging and high-volume outbound transfer patterns

SIEM requirements for lean teams

- Telemetry: identity, endpoint, file system access, backup logs, DNS, network flow
- Correlation: authentication patterns plus file anomalies plus backup targeting
- Response actions: endpoint isolation, credential revocation, backup protection triggers

KPIs

- Mean Time to Containment targeting sub-hour response
- Recovery Time Objective for critical systems
- Prevention effectiveness rate before encryption spreads

Issue 2: Phishing and Business Email Compromise

Why it ranks second

Phishing and BEC tie directly to fraud outcomes and fast identity takeover. The evidence set used here cites 82.6 percent AI-enhanced phishing usage, increasing campaign throughput and realism.

High-signal detection priorities

- New inbox rules that forward externally or suppress finance workflows
- OAuth consent grants to unusual apps with high privileges
- Risky sign-ins correlated with email link clicks and session creation
- Payment instruction changes correlated to account takeover indicators

SIEM requirements for lean teams

- Telemetry: email gateway, Microsoft 365 or Google Workspace audit logs, OAuth grants, sign-in logs
- Correlation: email events to identity sessions, MFA anomalies, risky OAuth grants
- Response actions: token revocation, session reset, mailbox rule rollback, quarantine workflow

Issue 3: Compromised credentials and privilege misuse

Why it ranks top three

Credential abuse is cited as 22 percent of initial access vectors, with 327-day detection time reported for stolen credentials in the referenced set, creating long investigations that drain small teams.

High-signal detection priorities

- Privileged group membership changes followed by admin actions
- Session token reuse from unusual ASN or device fingerprint
- Service account key creation followed by sensitive access
- Lateral movement across multiple systems in short windows

SIEM requirements for lean teams

- Telemetry: AD or Entra ID, SSO, VPN, PAM, cloud identity logs
- Correlation: identity behavior plus privilege changes plus workload access
- Response actions: revoke sessions, step-up authentication, rollback privileged roles

Issue Profiles 4 to 6

Issue 4: Advanced persistent threats

Why it ranks high

Advanced threats drive long hunts and timeline reconstruction. The referenced set cites **75 zero-day vulnerabilities exploited in 2024** and long dwell time ranges in the supporting research list.

SIEM requirements

- Long retention across endpoint, identity, cloud audit, DNS, and proxy logs
- Low-frequency correlation across weeks, not hours
- Hunt workflows with templates and evidence packaging

Issue 5: Supply chain and third-party vulnerabilities

Why it ranks high

Supply chain involvement is cited as **30 percent** of breaches, with average cost cited at **$4.91 million** in the mapped evidence set.

SIEM requirements

- Vendor identity tagging and monitoring tiers
- Integration coverage for third-party apps, API gateways, vendor VPN and SSO
- Response actions that suspend vendor sessions and rotate keys fast

Issue 6: Unmanaged cloud resources and misconfigurations

Why it ranks high

Cloud compromise frequently blends weak credentials and misconfiguration drift. The ranked evidence set includes **47.1 percent** tied to weak credentials and **29.4 percent** tied to misconfigurations, plus public cloud breach costs cited at **$5.17 million** in the mapped sources.

SIEM requirements

- CloudTrail, Azure Activity Logs, GCP Audit Logs normalized into a common investigation view
- IAM change correlation to data access and network exposure changes
- Cost-aware retention tiers for high-volume cloud telemetry

Issue Profiles 7 to 10

Issue 7: Insider threats and accidental exposure

Why it ranks high

The mapped evidence set cites insider-related incidents as the highest cost category at **$4.99 million**, with an **85-day** detection timeline noted in the referenced inputs.

Lean-team SIEM requirement

File access visibility, SaaS sharing logs, identity context, and evidence bundles built for audit review

Issue 8: Exploitation of unpatched or legacy systems

Why it ranks high

The ranked evidence table cites a **34 percent** increase in exploitation in the referenced set, penalizing slow patch cycles and unmanaged legacy assets.

Lean-team SIEM requirement

Vulnerability and patch telemetry linked directly to exploitation signals and isolation actions

Issue 9: Compliance violations and regulatory drift

Why it ranks high

Healthcare is cited with **444 incidents**, reinforcing audit readiness as an operational requirement, not an annual project.

Lean-team SIEM requirement

Automated evidence collection, retention controls, and reporting templates

Issue 10: Denial of service attacks

Why it ranks high

Availability attacks create response coordination burden. The ranked evidence set notes resolution time beyond one day in the referenced reporting set.

Lean-team SIEM requirement

CDN, WAF, load balancer, and network telemetry unified with incident communications templates

Why SIEM Programs Stall Lean Teams

Many SIEM programs still assume dedicated content engineering and large tuning cycles. Lean teams face a different operating model, where every hour spent tuning detections reduces time available for containment.

Where programs stall first

- Alert overload without entity context
- Slow onboarding of new telemetry sources
- Separate tools for SIEM, SOAR, email, and endpoint that fragment investigations
- Retention decisions driven by cost spikes instead of investigative need

Selection priorities that change outcomes

- Automation that removes manual correlation and produces response actions
- Entity-centric investigations that organize by user, endpoint, and workload
- Retention economics that stay predictable across data growth
- Analyst workflow design that reduces clicks and context switching

Buying Criteria Checklist and 12-Month Implementation Plan

Mid-market SIEM buying criteria checklist

This checklist maps to the ranked threats and lean-team constraints in the base material:

- □ **1. Automation and response orchestration**
- □ **2. Identity-centric detection and behavioral analytics**
- □ **3. Cloud-ready architecture with multi-platform support**
- □ **4. Rapid deployment with minimal tuning**
- □ **5. Transparent pricing with predictable scaling costs**
- □ **6. Threat intelligence enrichment workflows**
- □ **7. Email security correlation and forensics**
- □ **8. Endpoint and network correlation for ransomware defense**
- □ **9. Vulnerability and patch correlation**
- □ **10. Compliance automation and audit trail management**
- □ **11. Third-party access monitoring**
- □ **12. Scalable log management with advanced analytics**

12-month implementation priority framework

A phased rollout aligns early work to the highest-impact threats and typical lean-team capacity.

Phase 1 (Months 1-3): Core capability

- Stand up identity, endpoint, email, and core network telemetry
- Deploy correlation and response automation for ransomware, phishing, and credential abuse

Phase 2 (Months 4-6): Expand coverage

- Add cloud audit logs and workload telemetry
- Implement threat intelligence enrichment
- Formalize BEC playbooks with token revocation and mailbox rollback actions

Phase 3 (Months 7-12): Sustain and scale

- Integrate vulnerability and patch telemetry
- Add compliance reporting and evidence workflows
- Expand vendor access baselines and third-party monitoring

Why Graylog Fits Lean Security Teams

Lean teams need full visibility, fast response, and budget stability. Graylog is built to support that operating model through a consistent experience across deployment types and a data architecture that supports long retention without cost surprises.

What to validate in a Graylog SIEM evaluation

- **Entity-centric detection** that prioritizes risk by user, endpoint, and workload
- **Automated investigations and response workflows** that reduce manual correlation
- **Tiered retention strategies** that support long history planning
- **Consistent workflows across cloud and self-managed deployments**

Proof points to run during a hands-on trial

- Time to onboard your top five telemetry sources
- Time from first detection to containment action using a playbook
- Cost model clarity for 12 months of ingest and 12 to 24 months of retention

Voice of the Customer

Lean teams judge SIEM by time compression and cost stability. These customer results show what Graylog looks like in production when speed, clarity, and scale matter.

Kaizen Gaming (Online Gaming and Sports Betting)

"It was very cost-efficient to switch. Even with the same resources, the new setup operates ten times faster thanks to the guidance from the Graylog team." *- Marinos Giamouridis, Site Reliability Team Lead*

- Processing latency dropped to **2 to 3 seconds** from **20 to 30 seconds**.
- Message-handling time moved from **30 seconds** to **fewer than 3 seconds.**
- Sustained **99.95% availability** during global traffic peaks while supporting **600+ microservices.**

Circles Asia Pte Ltd. (Telecommunications)

"Before Graylog, security operations at Circles were almost non-existent. Today, Graylog is the centerpiece of our SOC maturity. It gives us visibility across cloud, on-prem, and partner workloads, strengthens our defense against threats, helps us meet compliance demands, and builds confidence with both stakeholders and customers." *- Somanath Varanasi, Manager II: SOC, Cyber Defence and DFIR*

- Threat detection coverage for newly onboarded resources improved from **weeks to hours.**
- SOAR workflows triggered through Graylog webhooks reduced **IOC isolation and containment to minutes.**

NetAssist Sdn Bhd (Managed Security Services Provider)

"Detection speed is non-negotiable for our customers. With Graylog, we can search across massive datasets instantly without restricting logging due to cost." *- Hon Fun Ping, Managing Director*

- Mean Time to Detect improved by **40%**, dropping from **about 4 hours** to **under 45 minutes.**
- Absorbed a **300% increase in log volume** without expanding SOC staffing levels.
- Achieved a **50% reduction in SIEM licensing costs** and **30% savings in hardware and cloud compute resources.**

Kennedy Krieger Institute (Healthcare)

"After evaluating multiple competitors, including Splunk, Sentinel, QRadar, CrowdStrike SIEM, and Devo, the Institute selected Graylog Cloud for its predictable cost model, faster onboarding, analyst-friendly workflows, and ability to support a stronger security posture without extra headcount." *- Director of IT Support*

- Deployed Graylog Cloud on AWS at **200GB/day** with **Security Cloud Onboarding Services**, eliminating SIEM infrastructure overhead.

- Improved long-term log retention for audit and compliance needs **without escalating storage costs**, staying within strict purchasing constraints.

- Enabled **faster, more confident investigations** with fused alerts, contextual views, and guided response steps, reducing manual triage effort for a lean SOC team.

- Simplified onboarding of new cloud and network log sources so teams can add critical data **without time-consuming mini-projects**.

Australian Media Company (Telecommunications)

"Graylog's real-time analytics completely changed how we operate. The support team has been outstanding." *- IT Support Specialist*

- Delivered real-time dashboards that **speed up issue identification and incident response** across a hybrid deployment model.

U.S. Education IT Provider (Education and IT Services)

"Graylog empowers our team to work smarter. Developers can access logs without touching the servers." *- Director, IT Services*

- Enabled secure, role-based log access through web dashboards and supported rapid rollout.

Request a Graylog SIEM demo

to see faster detection, clearer investigations, and predictable retention costs.

See demo now >>

ABOUT GRAYLOG

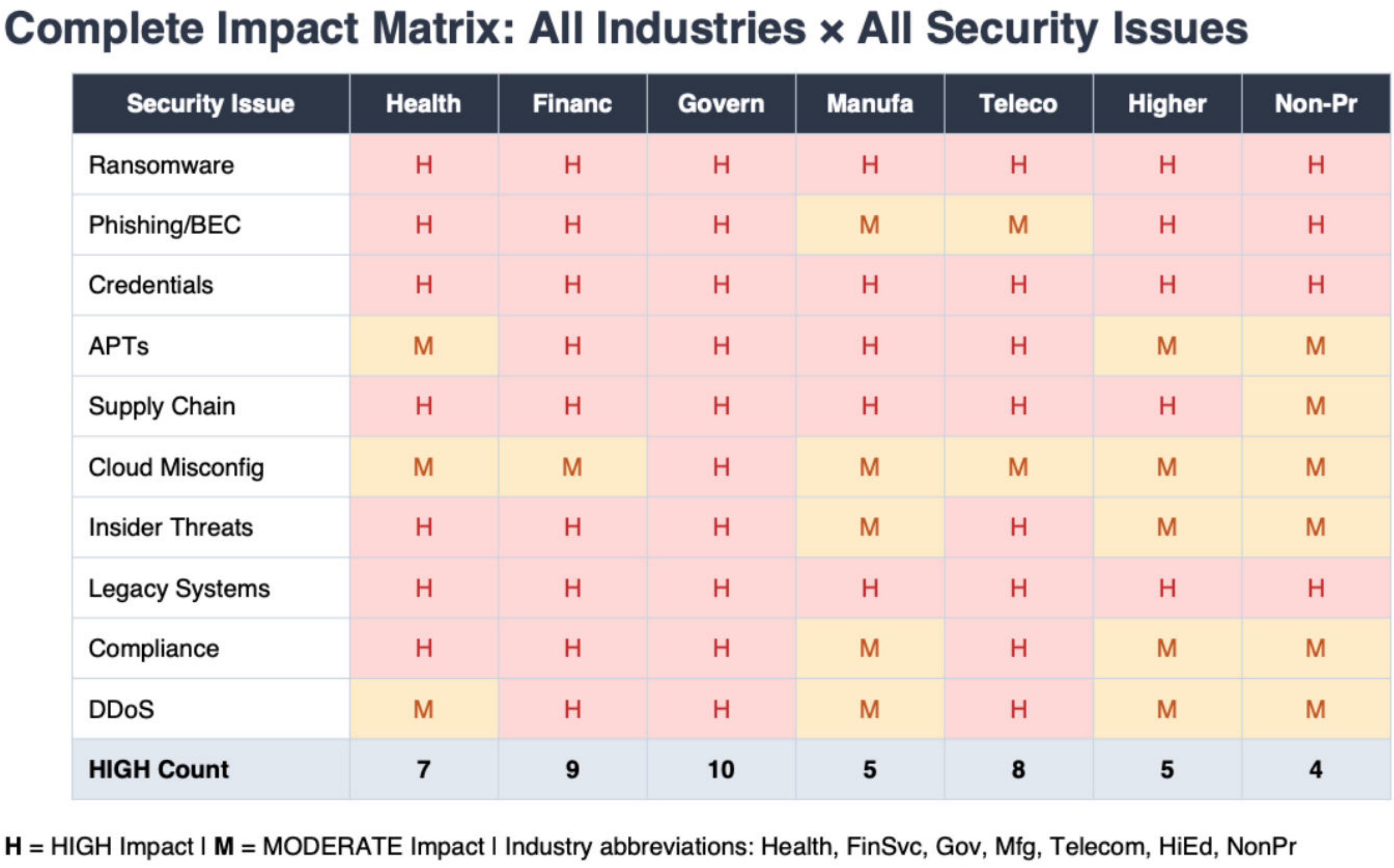
Graylog is the no-nonsense SIEM that cuts through noise and complexity. It delivers what security teams need most: full visibility, faster investigations, and smarter detection—without trade-offs or surprise costs. From automated workflows to correlation and anomaly detection, Graylog helps analysts move faster and stay focused. With a product suite spanning Graylog Enterprise, Security, API Security, and Open, we support everyone from large enterprises to lean teams. Trusted by over 60,000 organizations around the world. Learn more at graylog.com or connect with us on Bluesky and LinkedIn.

graylog

Appendix A: Industry impact matrix

References

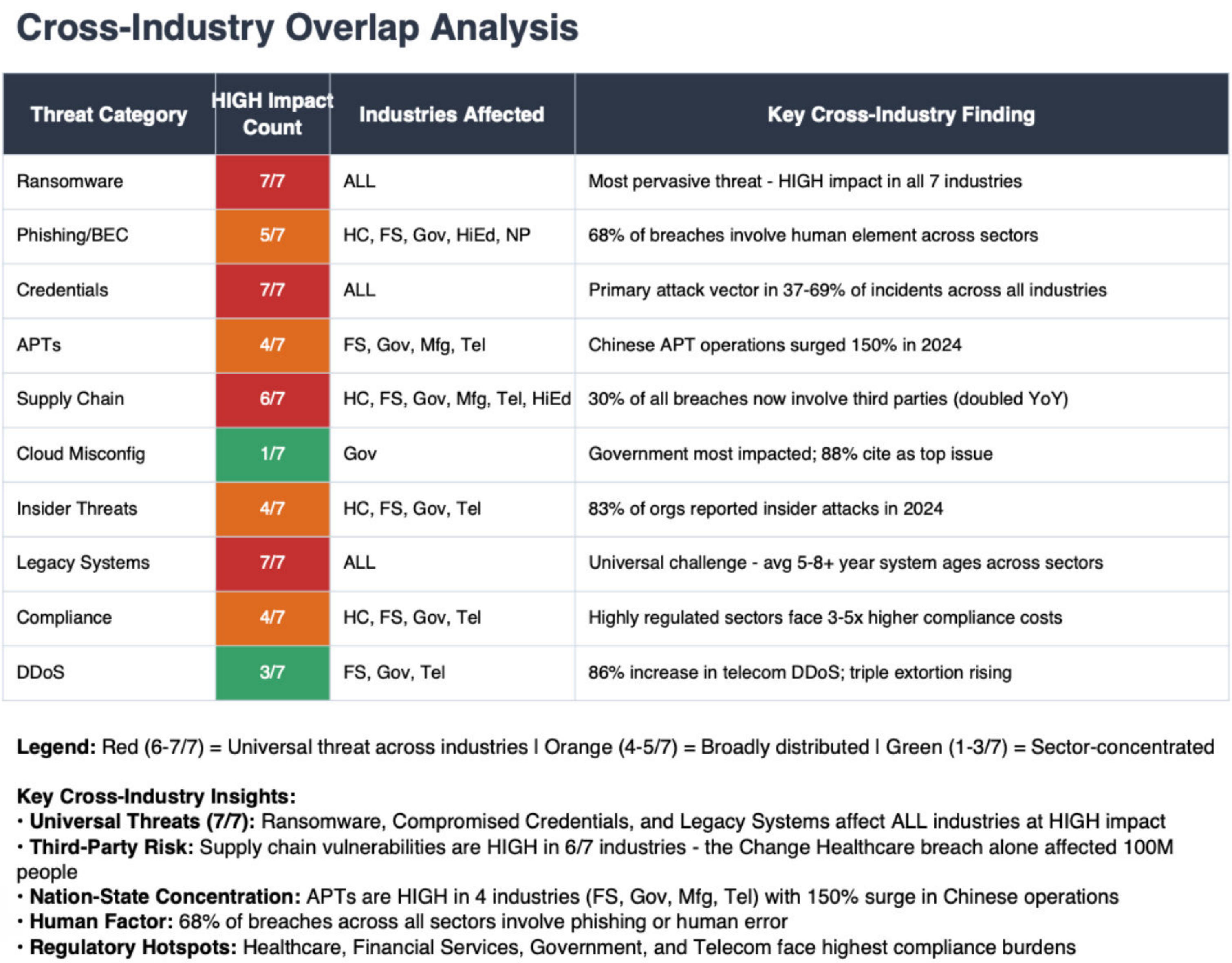
- Verizon DBIR 2025
- knowbe4 2025 Phishing by Industry Benchmarking Report
- IBM Cost of a Data Breach 2024 to 2025
- WEF Global Cybersecurity Outlook 2026
- NCSC Annual Review 2025
- CISA Known Exploited Vulnerabilities catalog
- NIST Cybersecurity Framework 2.0
- Elastic Global Threat Report 2025
- Palo Alto Unit 42 Global Incident Response Report 2025
- Google Mandiant M-Trends 2025
- Google Cloud Threat Horizons H2 2025
- Cisco Talos Year in Review 2024
- Cloudflare DDoS Threat Report Q3 2025
- OWASP Top 10 2025



Complete Impact Matrix: All Industries × All Security Issues

Security Issue	Health	Financ	Govern	Manufa	Teleco	Higher	Non-Pr
Ransomware	H	H	H	H	H	H	H
Phishing/BEC	H	H	H	M	M	H	H
Credentials	H	H	H	H	H	H	H
APTs	M	H	H	H	H	M	M
Supply Chain	H	H	H	H	H	H	M
Cloud Misconfig	M	M	H	M	M	M	M
Insider Threats	H	H	H	M	H	M	M
Legacy Systems	H	H	H	H	H	H	H
Compliance	H	H	H	M	H	M	M
DDoS	M	H	H	M	H	M	M
HIGH Count	**7**	**9**	**10**	**5**	**8**	**5**	**4**

H = HIGH Impact | **M** = MODERATE Impact | Industry abbreviations: Health, FinSvc, Gov, Mfg, Telecom, HiEd, NonPr



Cross-Industry Overlap Analysis

Threat Category	HIGH Impact Count	Industries Affected	Key Cross-Industry Finding
Ransomware	7/7	ALL	Most pervasive threat - HIGH impact in all 7 industries
Phishing/BEC	5/7	HC, FS, Gov, HiEd, NP	68% of breaches involve human element across sectors
Credentials	7/7	ALL	Primary attack vector in 37-69% of incidents across all industries
APTs	4/7	FS, Gov, Mfg, Tel	Chinese APT operations surged 150% in 2024
Supply Chain	6/7	HC, FS, Gov, Mfg, Tel, HiEd	30% of all breaches now involve third parties (doubled YoY)
Cloud Misconfig	1/7	Gov	Government most impacted; 88% cite as top issue
Insider Threats	4/7	HC, FS, Gov, Tel	83% of orgs reported insider attacks in 2024
Legacy Systems	7/7	ALL	Universal challenge - avg 5-8+ year system ages across sectors
Compliance	4/7	HC, FS, Gov, Tel	Highly regulated sectors face 3-5x higher compliance costs
DDoS	3/7	FS, Gov, Tel	86% increase in telecom DDoS; triple extortion rising

Legend: Red (6-7/7) = Universal threat across industries | Orange (4-5/7) = Broadly distributed | Green (1-3/7) = Sector-concentrated

Key Cross-Industry Insights:

- **Universal Threats (7/7):** Ransomware, Compromised Credentials, and Legacy Systems affect ALL industries at HIGH impact
- **Third-Party Risk:** Supply chain vulnerabilities are HIGH in 6/7 industries - the Change Healthcare breach alone affected 100M people
- **Nation-State Concentration:** APTs are HIGH in 4 industries (FS, Gov, Mfg, Tel) with 150% surge in Chinese operations
- **Human Factor:** 68% of breaches across all sectors involve phishing or human error
- **Regulatory Hotspots:** Healthcare, Financial Services, Government, and Telecom face highest compliance burdens