SANS

Beyond the Tool—Building a Smarter SIEM Operation

From Alerts to Action: Unlocking SIEM's Full Value

The Real Problem Isn't the Tool, It's the Gap

Security teams invest heavily in SIEM platforms, but the true value often goes untapped.

Why? It's not a technology failure. It's a misalignment between tools, teams, and tactics.

SIEMs offer powerful visibility, but only when the people, data, and workflows behind them are ready.

What's Holding SIEM Back?

Top Challenges Undermining SIEM Operations:

Visibility and Data Gaps

- → Unfit or Incomplete Logs—Poor source selection, inconsistent log formats, and missing fields kill detection.
- → Visibility Gaps—Incomplete cloud/on-prem log coverage
- → Volume-Based Cost Pressures—Data ingestion pricing and maintaining the SIEM infrastructure discourages full telemetry capture.
- → Low Context Alerts—Lack of enrichment with asset value, user roles, or threat intelligence

Workflow and Integration Friction

- → Alert Fatigue—Too many alerts, not enough prioritization or correlation.
- → False Positives—Rules not tuned to the environment overwhelm analysts.
- → Underused Features—UEBA, SOAR, threat intel feeds, and automation often sit idle.
- → Limited Out-Of-the-Box-Functionality—Default rules are generic and miss organization-specific threats.
- → Integration Challenges—Legacy systems, custom applications, and IoT devices resist onboarding.

People and Process Gaps

- → Skill Shortages—Few team members can write detection logic.
- → Slow Response Times—Manual triage and fragmented tooling delay action.
- → Reactive Playbook Development—Response workflows are created after incidents occur.
- → Poor Business Alignment—Detection doesn't reflect organizational risk or mission priorities.

What High-Performing Teams Get Right

Key Enablers for a Modern, Effective SIEM Operation:

- → Tuned Detection Logic—Built around adversary tactics, techniques, and procedures (TTPs), risk scoring, and asset value.
- → Enriched, Normalized Data—Clean telemetry with threat intel, context, and correlations.
- → Automation That Works—Effective use of SOAR and response playbooks to reduce manual effort.
- → Threat-Informed Design—Detection mapped to frameworks like MITRE ATT&CK.
- → Cross-Functional Collaboration—Shared visibility between detection engineering, SOC, threat intel, cloud, and leadership.
- → Continuous Tuning and Validation—Detection is never static. It evolves with threats and business change.
- → Business Aligned Output—SIEM alerts and dashboards reflect what matters to stakeholders, not noise.
- → Real-Time Correlation and Alert Grouping—Link related events into meaningful narratives and reduce analyst overload.

The Difference Between Signal and Noise?

It's Not Just Your SIEM—It's Your Team

Your SIEM reflects what your people put into it. Detection engineering, SIEM and tool engineering, threat intelligence, cloud security, and leadership roles must all collaborate for consistent and accurate outcomes.

Skilled teams with the right processes turn raw alerts into actionable detection, aligned to real threats and real risks.

SIEM Is a Force Multiplier

Turn Noise into Detection Power

When detection logic, workflows, and automation are aligned with real-world threats and your business priorities, SIEM can be the engine of your security operations

What's Next in SIEM?

- Cloud-native and hybrid deployments →
- AI/machine learning-enhanced anomaly detection →
- Integration with XDR and unified SOC platforms →
- SIEM as a managed service for lean teams →

Ready to Optimize?

Discover free resources, guides, and training to help your team:

- → Improve detection quality
- → Maximize automation
- → Tune your SIEM for value

Explore the SANS SIEM Resource Hub
www.sans.org/mlp/siem-optimization

SANS