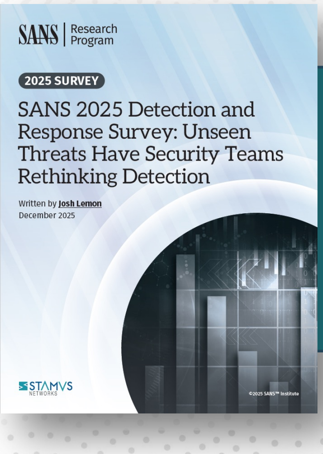
White Paper

Closing Detection Gaps: A Practical Playbook for SOC Teams

This playbook, based on the *2025 SANS Detection & Response Survey*, serves as a strategic guide for SOC teams to address the widening disconnect between evolving threats and current detection capabilities.

Key findings reveal persistent challenges, including high alert noise and false positives, limited cloud and hybrid visibility, undetected lateral movement, and mounting analyst workload -- all of which stem from fragmented, tool-centric security approaches.

The guide provides a five-step framework to assess coverage, identify blind spots, evaluate fidelity, measure analyst load, and prioritize remediation, emphasizing that a resilient strategy requires layered visibility, unified context, and complementary network-centric detection to help teams see more, understand more, and respond faster.



SANS | Research Program

2025 SURVEY

SANS 2025 Detection and Response Survey: Unseen Threats Have Security Teams Rethinking Detection

Written by Josh Lemon
December 2025

STAMVS NETWORKS

©2025 SANS™ Institute

This Strategic Guide is Based on Findings from the 2025 SANS Detection & Response Survey

The Growing Gap Between Threats and Detection Capabilities

The findings from the 2025 SANS Detection & Response Survey highlight a widening disconnect between the threats organizations face and the visibility their security teams actually have. Despite continual investment in security tools, SOCs continue to struggle with:

- Expanding attack surfaces
- Alert fatigue
- Limited cloud visibility
- Lateral movement that evades traditional controls
- Slowing response times
- Staffing and expertise shortages

These challenges aren't new, but they're intensifying. More importantly, they're converging.

Attackers now routinely exploit blind spots between systems, clouds, endpoints, and signals. Meanwhile, SOC teams are overwhelmed by noise from low value alerts while still missing the deeper behavioral patterns that matter most.

This playbook was designed to help practitioners close the widening gap between what is happening inside their environment and what their tools can actually detect.

It builds on SANS research, real-world SOC observations, and modern detection practices, providing a practical look at how to develop more precision, context, and confidence in your threat detection and response program.

Understanding the 2025 Detection Gap Landscape - What the SANS Survey Reveals

The SANS survey surfaced several central challenges that define today's detection landscape:

- 73% struggle with false positives
- 58% lack cloud security expertise
- More than half face multi-cloud complexity
- Response times are slowing
- Teams feel increasingly under-resourced
- Visibility gaps are now the top barrier to effective detection

These issues aren't happening in isolation, they're interrelated.

More tools → more alerts → more noise → more fatigue → slower responses → bigger gaps.
More cloud → more fragmentation → more blind spots → harder correlation → higher risk.

Why Gaps Are Expanding

According to the SANS 2025 Detection & Response Survey, visibility gaps continue to widen as organizations expand into hybrid and multi-cloud environments. These findings suggest that many traditional detection approaches still rely on assumptions built for earlier network models, such as centralized infrastructure, consistent traffic patterns, and long-lived assets.

Today's environments change far more rapidly, with workloads shifting locations, identities spanning platforms, and telemetry arriving in inconsistent or incomplete forms. As teams adopt new services faster than monitoring strategies evolve, SANS respondents report growing pockets of limited visibility that accumulate into meaningful detection gaps.

The survey results also point to another challenge: detection tools often operate independently, each offering only a partial view. Without sufficient context across these sources, analysts struggle to form a cohesive picture of activity, increasing the risk that early indicators will be overlooked.

The Limits of Tool-Centric Security

The SANS report shows that most SOCs rely heavily on EDR, SIEM, IDS/IPS, cloud-native monitoring, and log pipelines, each of which provides valuable but incomplete visibility. Respondents noted that while these tools are essential, no single category captures enough context to explain what is happening across modern hybrid environments.

SANS findings reinforce that when detection relies too heavily on one perspective — whether endpoint, log, or cloud-native telemetry — gaps emerge in the areas those tools were not designed to observe. This fragmentation makes it harder for analysts to piece together activity and increases the likelihood that subtle behaviors will go undetected.

The Four Most Common Detection Gaps

1

Alert Noise & False Positives

High alert volumes overwhelm analysts and obscure genuine threats. False positives drain time and attention, forcing SOC teams to sift through large amounts of low-value data before finding what truly matters. As the SANS survey reinforces, this remains the most persistent and disruptive operational challenge for security teams today.

Why it matters: A SOC focused on filtering noise is a SOC that cannot execute timely, accurate detection and response. When teams are buried in alerts, subtle but meaningful behaviors are the first to slip through the cracks.

2

Cloud & Hybrid Visibility Blind Spots

Cloud workloads change rapidly, scale automatically, and often communicate in ways that traditional monitoring cannot easily track. Multi-cloud adoption introduces different telemetry formats, inconsistent data depth, and fragmented visibility. Cloud-native logs provide useful information but often lack the behavioral context needed to identify stealthy or low-and-slow activity.

Why it matters: Attackers purposely take advantage of the areas where organizations struggle to maintain consistent visibility. Cloud environments, especially when distributed across multiple platforms, create natural blind spots that can mask attacker movement.

3

Lateral Movement & "Invisible" Behaviors

Sophisticated adversaries rarely limit their operations to a single compromised asset. Once inside, they pivot between systems, identities, and services, often using legitimate pathways rather than overt malicious techniques. Many endpoint- or log-centric tools only detect activity at the asset level, not the pathways between assets, leaving lateral movement largely unobserved.

Why it matters: If detection only occurs after an attacker has successfully moved within the environment, the breach is already well underway. Early-stage behaviors are the most important—and the easiest to miss without broad, independent visibility.

4

Analyst Workload & Skill Shortages

Even experienced SOC teams face growing demands for triage, correlation, and deeper investigation. As environments expand and toolsets become more complex, analysts are expected to interpret more signals with less time, contributing to burnout and slowing response. Many organizations rely heavily on on-the-job training to keep up with new threats and platforms, which creates variability in detection quality.

Why it matters: Detection is ultimately constrained by human capacity. When analysts are overloaded or forced to navigate scattered, low-context data sources, detection gaps expand regardless of the technology in place.

Why Detection Gaps Persist (Even in Well-Resourced SOCs)

The SANS survey highlights that even well-resourced SOCs face persistent detection gaps, often due to how environments and data sources are structured. Respondents reported difficulty correlating signals across legacy systems, cloud platforms, and container workloads, each producing telemetry with different formats and levels of detail.

These findings reflect a broader operational reality: investigations frequently require pivoting between multiple consoles, reconciling conflicting data, or compensating for missing context. According to SANS, this contributes directly to slower response times and increased analyst workload.

A Framework for Closing Your Detection Gaps

The SANS findings highlight several recurring challenges that contribute to missed signals and slower response. Building on these themes, the following framework helps teams identify where their own gaps originate and prioritize improvements.

Assess Your Current Coverage - Start by mapping all existing detection sources across endpoints, networks, cloud platforms, identities, and logs. This exercise reveals what each tool actually observes versus what you expect it to observe. Many organizations discover that strong coverage in one area masks sparse or inconsistent telemetry elsewhere.

Once the map is complete, identify systems, workloads, or communication paths where no telemetry is collected at all. These are your coverage gaps: places where activity may be *occurring without any corresponding visibility. Understanding these blind zones is essential before evaluating detection quality.*

Identify Visibility Blind Spots - After mapping coverage, focus on the specific areas where visibility tends to break down. East-West traffic inside the environment, container networking, unmanaged or unknown assets, cloud workloads, and SaaS application activity are common blind spots that appear across industries. These gaps rarely exist because of misconfiguration; they occur because many tools were not designed to observe these domains comprehensively.

Recognizing blind spots early helps teams determine whether gaps stem from tooling limitations, architectural constraints, or inconsistent telemetry. This clarity is crucial for prioritizing what to address first.

Evaluate Detection Fidelity - Coverage alone does not guarantee effective detection. The next step is to examine how clear, actionable, and trustworthy your existing detections are. Evaluate false positive volume, alert clarity, evidence depth, escalation criteria, and the availability of contextual data. Even with broad visibility, low-fidelity alerts slow investigations and allow important behaviors to blend into background noise.

This assessment highlights where improvements in correlation, normalization, or data enrichment may be needed before introducing additional detection sources.

Measure Analyst Load - Detection quality is closely tied to analyst capacity. Measure how long it takes analysts to triage alerts, correlate data, and complete investigations. Assess how much of the process is automated versus manual, and identify areas where tooling complexity increases cognitive load.

High analyst burden is often a sign that detection is fragmented or lacks sufficient context. Understanding these operational pressures helps ensure that remediation efforts support both technology and the people who rely on it.

Prioritize Remediation - With coverage, blind spots, fidelity, and analyst capacity understood, teams can prioritize meaningful improvements. Remediation may include consolidating overlapping tools, improving correlation workflows, expanding visibility into underserved areas, optimizing alert quality, or introducing deeper behavioral detection.→ higher risk.

This is often the point where organizations begin evaluating network-based detection technologies, which provide independent visibility across environments and help validate or enhance existing detection sources. By anchoring remediation efforts in a structured framework, SOC teams can strengthen detection maturity in a deliberate and measurable way.

The Role of Network-Centric Detection in Modern SecOps

The SANS survey makes clear that many of today's visibility and detection challenges come from relying on isolated or incomplete telemetry sources. Respondents cited difficulty correlating data across tools, understanding behaviors that occur between systems, and maintaining visibility as infrastructure becomes more distributed.

These themes underscore why network-centric detection has become an essential complementary layer in modern SecOps. While the SANS report is technology-neutral, its findings align with the strengths that network-based visibility provides:

- Independent coverage across cloud and on-prem environments
- Behavioral insight where endpoint or log data may be limited
- Context for lateral movement and cross-system activity
- Stronger signal quality for meaningful alerts
- Gap coverage in areas without existing instrumentation

Network-centric detection does not replace other tools. Instead it strengthens them by adding perspective where traditional telemetry sources struggle.

Building a More Resilient Detection Strategy

The SANS findings show that organizations are facing challenges simultaneously across visibility, signal quality, cloud complexity, and analyst workload. A resilient detection strategy must address these pressures holistically.

A modern strategy requires more than adding new tools or expanding data collection. It demands an approach that can adapt to shifting infrastructure, emerging attacker techniques, and the operational realities faced by SOC teams. The most effective programs combine multiple forms of visibility with the context and efficiency needed to separate meaningful activity from background noise.

Layered visibility ensures that no single blind spot becomes an entry point for attackers. Behavioral detection adds depth by identifying actions and patterns that fall outside normal operations, even when they appear benign in logs or endpoint activity. Cloud-aware monitoring acknowledges that today's workloads behave differently than traditional systems, requiring visibility that follows applications and identities wherever they run. Unified context brings signals together into a coherent view so analysts spend less time correlating data and more time understanding what it means.

Automation plays an important role by reducing the manual effort associated with repetitive tasks such as triage, enrichment, and escalation. When routine steps occur automatically, analysts can focus their attention on investigation, validation, and response. Finally, a resilient strategy centers on workflows that match how analysts actually work, giving them clear evidence, fewer distractions, and the ability to act quickly when high-risk activity emerges.

The goal is simple:

- See more.
- Understand more.
- Respond faster.

A detection program built around these principles is better equipped to handle the scale, complexity, and speed of modern environments, no matter how they evolve.

Detection Gap Checklist: A 10-Point Review for Your SOC

This checklist gives you a quick way to spot potential detection gaps in your environment. It highlights the areas where visibility, context, or analyst capacity may be weaker than expected.

The goal is not to generate a score but to highlight areas where visibility, context, or operational efficiency may be weaker than expected. If you find yourself answering “no” or “not consistently” to several items, it’s a strong signal that your current detection stack may be missing important pieces of the picture.

- ✓ We have visibility across endpoints, network traffic, and cloud workloads.
- ✓ Lateral movement paths are monitored and understood.
- ✓ Cloud-native telemetry is enriched with behavioral context.
- ✓ False positive rates are manageable and decreasing.
- ✓ Alerts include enough evidence for analysts to act without pivoting tools.
- ✓ Unmanaged or unknown assets are discovered automatically.
- ✓ Analyst triage and investigation times are improving, not increasing.
- ✓ Automation supports repetitive tasks rather than overwhelming workflows.
- ✓ Our detection sources complement each other rather than duplicate effort.
- ✓ We can identify early-stage attack activity - not just confirm incidents after escalation.

This checklist gives you a quick way to spot potential detection gaps in your environment. It highlights the areas where visibility, context, or analyst capacity may be weaker than expected.

The goal is not to generate a score but to highlight areas where visibility, context, or operational efficiency may be weaker than expected. If you find yourself answering “no” or “not consistently” to several items, it’s a strong signal that your current detection stack may be missing important pieces of the picture.

If several of these questions reveal uncertainty or inconsistent coverage, your SOC may be experiencing the same pressures documented in the SANS survey, particularly around visibility gaps, alert volume, and operational workload. Many organizations address these gaps by adding complementary detection layers that provide network-based, behavioral, and precise visibility to help analysts operate with greater confidence.

The Future of Detection: Clarity, Context, and Confidence

The SANS findings make one thing clear: detection challenges are growing, not shrinking.

Attackers are adapting faster than detection programs evolve, and distributed infrastructures create gaps where early signals are easily missed. In this environment, visibility and context determine whether teams detect subtle indicators or end up responding only after an incident escalates.

Closing detection gaps is no longer optional, it is foundational to modern security operations.

A complete, resilient detection strategy delivers clarity instead of noise, context instead of guesswork, and precision instead of uncertainty. It brings together multiple perspectives across the environment and gives analysts the evidence they need to make confident decisions without being overwhelmed.

This playbook outlines a practical framework for strengthening your detection strategy, helping SOC teams operate with greater clarity, confidence, and control. For organizations looking to strengthen their coverage with network-based visibility and precise, behavior-aware detections, Clear NDR provides the kind of insight that supports this approach and helps close many of the gaps highlighted throughout this guide.

As detection continues to evolve, solutions that deliver clarity, context, and precision will define the future of effective SecOps — and Clear NDR is built to support teams on that path.

Ready to Transform Your SOC?

Ready to see how Clear NDR can **transform your SOC operations**?

Want to **close the detection gaps** identified in the SANS report and effectively bring clarity, context, and confidence to your security operations?

Request a **personalized demonstration today** to see Clear NDR's precision detection and complete evidence in action, or dive in immediately with a **30-day no-obligation evaluation** to experience the clarity your security team has been missing.

Contact Stamus Networks for a consultation and live demonstration to determine if Clear NDR is a good fit for your organization: contact@stamus-networks.com

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR® – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

STAMVS® NETWORKS

229 rue Saint-Honoré
75001 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

✉ contact@stamus-networks.com

🌐 www.stamus-networks.com