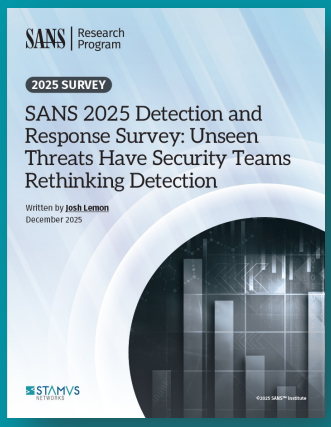
Solution Brief

STAMUS NETWORKS

# Ten Questions to Evaluate Your Detection & Response Strategy in 2026

The 2025 SANS Detection & Response Survey highlights widening visibility gaps and persistent challenges with false positives, cloud complexity, and analyst workload. The following questions can help you evaluate how closely your own detection strategy aligns with the trends identified in the report.

Use them as a quick internal review to understand where your current approach is strong and where the gaps SANS surfaced may also exist in your environment.




Insights from key trends identified in the 2025 SANS Detection & Response Survey

## SECTION 1: Visibility Coverage

The report shows that inconsistent visibility across hybrid and cloud environments remains one of the most common contributors to missed early indicators.

1

### Can we see activity across all major environments (on-prem, cloud, hybrid, remote)?

*Most teams cannot. SANS respondents cited hybrid and multi-cloud complexity as a major barrier to unified visibility.*

2

### Do we have visibility into East/West traffic and lateral movement?

*A common blind spot. The report highlights that early attacker movement often goes undetected when internal traffic isn't observable.*

3

Do we have a way to see unmanaged, unknown, or shadow assets?

*SANS findings reinforce that endpoints only cover what they're deployed on — leaving gaps where attackers can operate quietly.*

## SECTION 2: Alert Precision & Noise Reduction

The SANS survey results highlights alert noise as a persistent operational challenge, driving investigation delays, analyst fatigue, and missed signals.

4

Is our SOC able to reliably distinguish real threats from false positives?

*False positives remain the #1 operational burden, making signal quality a critical factor in effective detection.*

5

Do our alerts come with sufficient context to understand the details behind what actually happened?

*SANS respondents noted that low-context alerts significantly increase investigation time and cognitive load.*

6

Are analysts overwhelmed by alert volume or repetitive triage work?

*If yes, it's a sign your detection pipeline is producing noise instead of clarity — a problem echoed throughout the SANS data.*

## SECTION 3: Cloud & Distributed Environments

As cloud adoption increases, the SANS survey shows that many teams struggle to gain sufficient behavioral insight across dynamic, distributed environments.

7

Do we have behavioral visibility across cloud workloads and virtualized infrastructure?

*SANS findings suggest that cloud-native logging alone often lacks the behavioral depth needed to identify sophisticated or lateral activity.*

8

Are we confident we could detect lateral movement between cloud services or identities?

*The survey results highlight that cross-service and identity-driven movement is increasingly difficult to observe, even in mature environments.*

## SECTION 4: Response Effectiveness

Slowing response times in the SANS report indicate that many SOCs face challenges turning detection signals into timely action.

9

Do analysts have the evidence they need to quickly validate, escalate, or dismiss alerts?

*According to SANS findings, limited context and fragmented evidence contribute directly to longer investigation and response times.*

10

Do we have automated or semi-automated processes for enrichment, correlation, or containment?

*The survey shows growing adoption of automation and AI to reduce workload, while emphasizing that effectiveness depends on the quality and reliability of underlying signals.*

## How to Use This Checklist

**If you answered "yes" to most questions:** Your foundational detection strategy is solid. Your next step is optimization and strengthening areas of partial coverage.

**If you answered "no" to 3–5 questions:** You have meaningful detection gaps worth prioritizing, many of which align with the challenges highlighted in the SANS report.

**If you answered "no" to more than 5 questions:** You likely lack the behavioral visibility and coverage needed to detect modern attacker activity early — a pattern seen frequently in SANS survey responses.

These questions mirror many of the themes surfaced in the SANS findings, particularly around visibility gaps, signal quality, and operational capacity. If several of these areas remain uncertain or unresolved, your SOC is likely experiencing the same pressures raised in the report, making it a strong indicator that additional visibility, context, or refinement in detection strategy may be needed.

## Ready to Transform Your SOC?

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

Want to **close the visibility gaps** identified in the SANS report and effectively reduce alert noise?

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



STAMUS 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