SANS | Research Program

2025 SURVEY

SANS SOC Survey 2025

Written by **Christopher Crowley**

July 2025

Dropzone AI

elastic

FORTINET

Google

infoblox.

prophet

SWIMLANE

ThreatConnect.

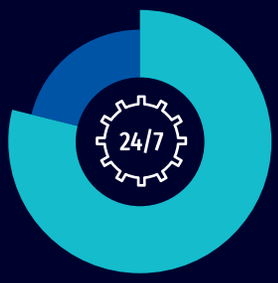
tines

WIZ

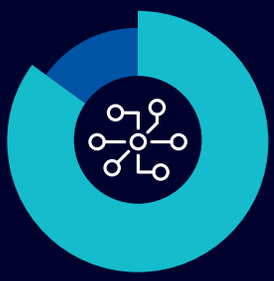
SANS 2025 SOC SURVEY

Key Findings

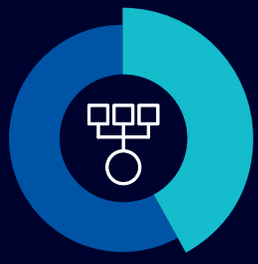
Operations and Technology Use



79% of SOCs are operational **24/7**.

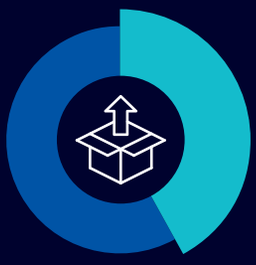


85% of respondents say **endpoint security alerts** are their **primary trigger for response**.



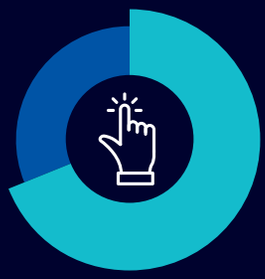
42% of SOCs **dump all incoming data into a SIEM**, often without a retrieval or management plan.

43% of respondents say **SIEM** is the **top tech skill** they seek when hiring—**more than double** the next highest response.



42% of SOCs use **AI/ML tools "out of the box"** with **no customization**.

69% of SOCs use **cyber threat intelligence (CTI)** data primarily for **incident response**.



69% of SOCs still rely on **manual or mostly manual processes** to report metrics.

Staffing and Workforce Dynamics

2–10 people is the most common size for a fully staffed SOC.

3–5 years is the most common tenure for SOC staff.

73% of organizations allow remote work for SOC team members at least some of the time.

62% of SOC professionals say their organization isn't doing enough to retain top talent.

42% of SOC staff don't know the SOC's budget, indicating a disconnect between technical and business teams.

Survey Author

VIEW PROFILE

Christopher Crowley
SANS Senior Instructor

CURRENTLY TEACHING

SEC595: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™

SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring™

SEC504: Hacker Tools, Techniques, and Incident Handling

FORMERLY TAUGHT

FOR585, SEC401, SEC503, SEC560, SEC575, SEC580 MGT535, MGT517

Christopher Crowley has 25 years of industry experience managing and securing networks. He has authored numerous courses and is considered a leading expert in building an effective SOC. He currently works as an independent consultant in the Washington, DC, area focusing on effective computer network defense. His work experience includes penetration testing, security operations, incident response, and forensic analysis. Chris holds several industry certifications including the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GPYC, GMOB, GMLE, GASF, GREM, GXPN, and CISSP.

Chris was awarded the SANS 2009 Local Mentor of the Year Award. The Mentor of the Year Award is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. He is also a faculty member of the SANS Technology Institute and the NSA Center of Academic Excellence in Cyber Defense as well as a multi-time winner of the National Cyber League Competition. Chris spends his spare time mountain biking, rock climbing, and savoring epicurean treats.

Executive Summary

Over the past nine years, the SANS Institute has conducted an annual industry survey to better understand how security operations centers (SOCs) are built, staffed, and run, and to learn more about SOC analysts' biggest challenges and potential industry improvements. This year's goal was to provide insights into SOC performance against peers, prioritize improvements for the coming year, and gain insight into valued and less-effective technologies across the industry.

This year's report outlines data and insights behind SOC structure comparisons, outsourcing trends, technology considerations, areas for improvement, and ways in which various technologies are being implemented.

Although AI is the latest technological trend, it's notable that over the nine years of conducting this survey, capabilities, staffing levels, outsourced services, and challenges in security operations have remained largely consistent.

Security operations is a long-term, gradually maturing effort that demands both patience and persistence.

Demographics

Most respondents were based in the United States, with participants from 57 different countries. The top industries represented were the usual mix of respondents from banking/finance (16%), cybersecurity (14%), technology (14%), and government (14%) and there was a diverse representation of organization size. Figure 1 shows the survey demographics in detail.

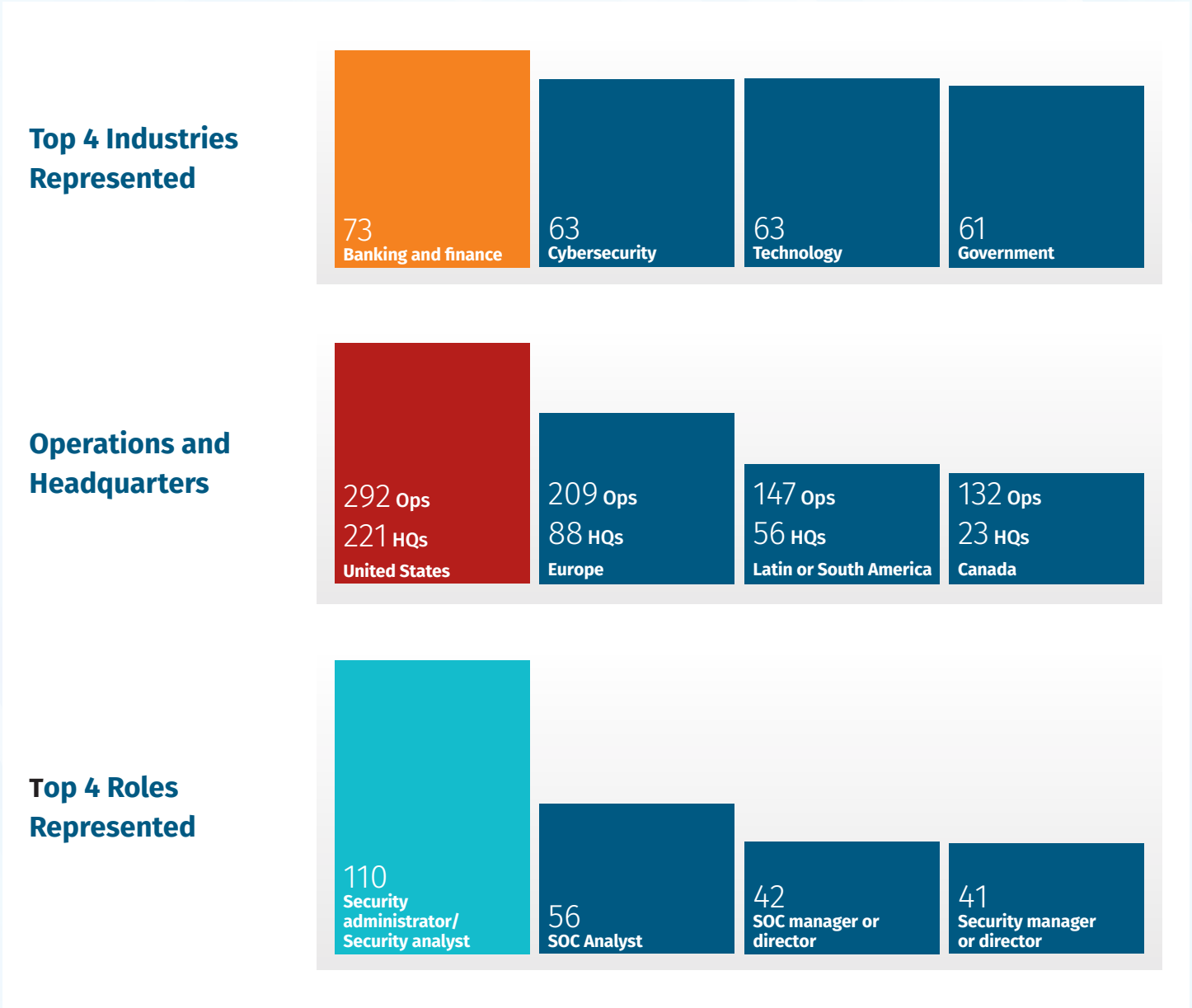


Figure 1. Demographics of Survey Respondents

Security Operations Center (SOC) Defined

The modern SOC in 2025 is built around a few foundational elements that define how it functions, where its strengths lie, and how it adapts to evolving threats. These include its core capabilities, operational model (in-house vs. outsourced), data architecture, and staffing strategy. Based on current survey data, a typical operational SOC reflects the following four characteristics:

- **Capabilities—**The core functions of a SOC and the tasks it handles on a routine basis
- **In-house vs. outsourced functions—**The tasks that are handled internally vs. by third parties
- **Architecture—**The structure for how and where data is collected, stored, and accessed
- **Staffing and hours of operation—**Details on team size, roles, expected skill set, and whether the SOC operates around the clock or during limited hours

In addition, according to the data, a baseline SOC can be defined as:

- **Prioritizes alert triage, threat detection, and incident response as core functions** with threat intelligence, vulnerability management, and hunting as supporting functions.
- **Employs 10 full-time team members** (or full-time equivalent) with the average length of employee tenure of three to five years.
- **Handles most monitoring, detection, and incident response in-house,** while outsourcing pen-testing, digital forensics, some threat intel, and other functions requiring higher levels of expertise or specialization.
- **Operates a centralized architecture,** with cloud adoption growing but still lagging behind the cloud adoption volume of IT.
- **Maintains 24/7 operational coverage in most cases,** with some still relying on rotating coverage or “as-needed” escalation.
- **Reports metrics manually,** even though nearly half say it’s too time-consuming. Automation remains limited.
- **Relies heavily on EDR** as the most trusted and mature tool in use. AI/ML is at the bottom of the satisfaction list.
- **Stores more data than ever before,** often dumping everything into SIEM or syslog without a clear plan in place to manage or analyze it, creating visibility issues.

Capabilities and Outsourcing

The expectations of SOC functions are robust and comprehensive. Survey responses make it clear: Failing to cover core responsibilities, whether in-house or outsourced, results in a SOC that is ineffective at detecting and responding to threats.

Although there is variety in the activities split between internal teams and external vendors, such as MSSPs, the core expectations for what a SOC must be able to do remain largely consistent year-over-year with the top three activities reported as security roadmap and planning (80%), security administration (80%), and security architecture and engineering (78%) (see Figure 2).

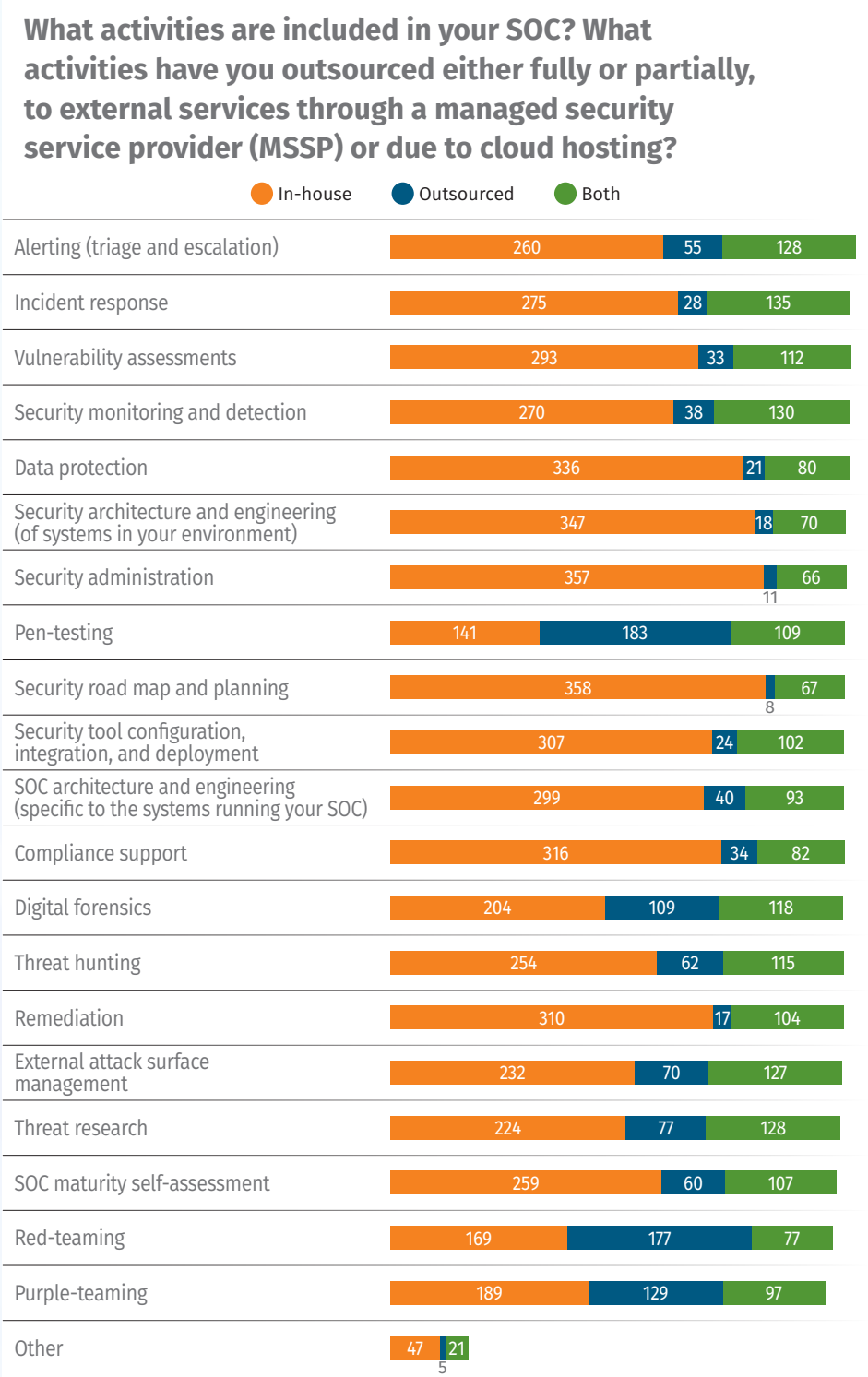


Figure 2. Response Count on SOC Operations Activities Related to Outsourcing

In-House vs. Outsourcing SOC Capabilities

Core SOC functions like architecture, monitoring, and compliance are typically kept in-house. This is likely because these areas demand a deep understanding of internal systems, business priorities, and organizational context. They also involve close coordination with legal and executive stakeholders, making them more effective when owned internally (see Figure 3).

On the other hand, outsourcing makes strategic sense for tasks that are highly specialized, repeatable, and resource intensive. Services like penetration testing and red teaming often fall into this category. These are typically project-based efforts where third-party firms can provide targeted expertise and scalability more efficiently than internal teams.

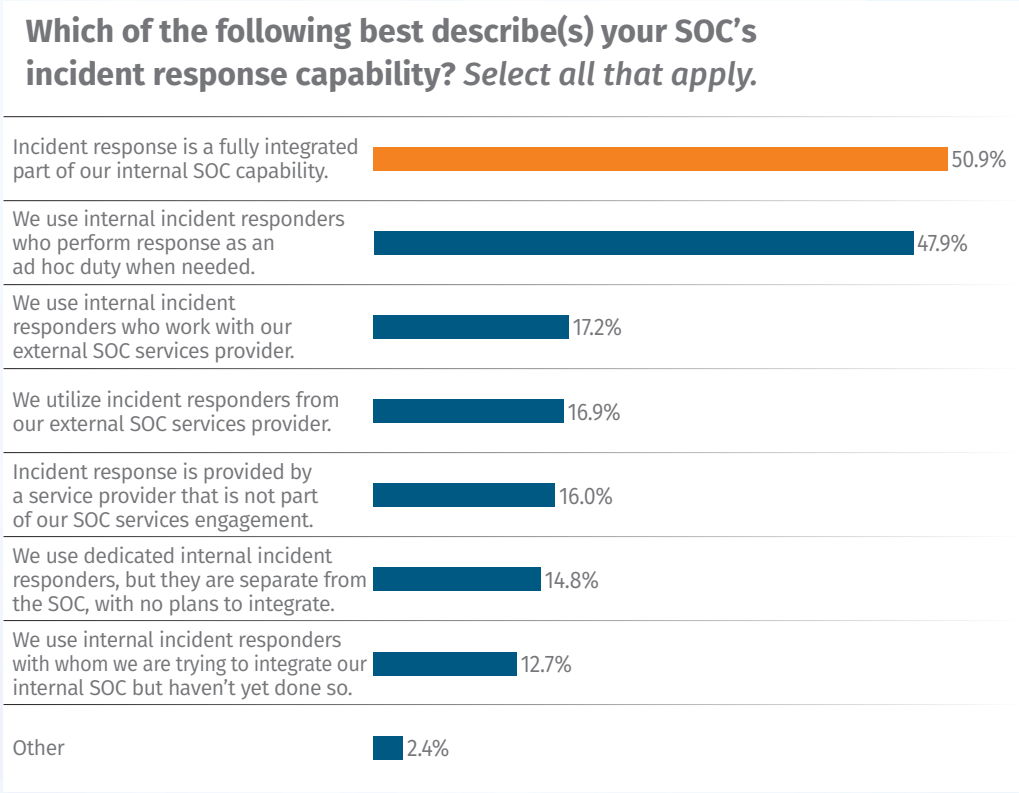


Figure 3. Incident Response Capabilities

Security monitoring and incident response are often hybrid models—partially staffed in-house, with external providers filling in for overflow or specialized coverage. This blended approach allows for flexibility while maintaining core control.

Interestingly, 55% of respondents say SOC use is mandatory across their organizations, and another 30% say there's latitude to use external providers. That indicates SOCs are still viewed as foundational—but organizations are open to flexible deployment models depending on institutional requirements and resources. Incident response remains the most internally managed function. Given its role in real-time crisis management, it makes sense that most organizations keep this capability under their control.

Architecture

Most respondents (38%) report operating a single, centralized SOC, making it the most common architecture today. Cloud-based SOC deployments follow at 24%, but respondent's indicate planned changes will increase that number to 29% over the next 12 months indicating growing interest in cloud-native security operations.

Despite the hype around cloud-based SOCs, centralized, on-prem architectures remain the prevailing model. The gap between stated cloud ambitions and current deployments highlights the reality: Cloud migration, particularly for security operations, is still in transition.

Although single, centralized SOCs continue to lead, year-over-year data doesn't yet point to a decisive architectural shift to the cloud (see Figure 4).

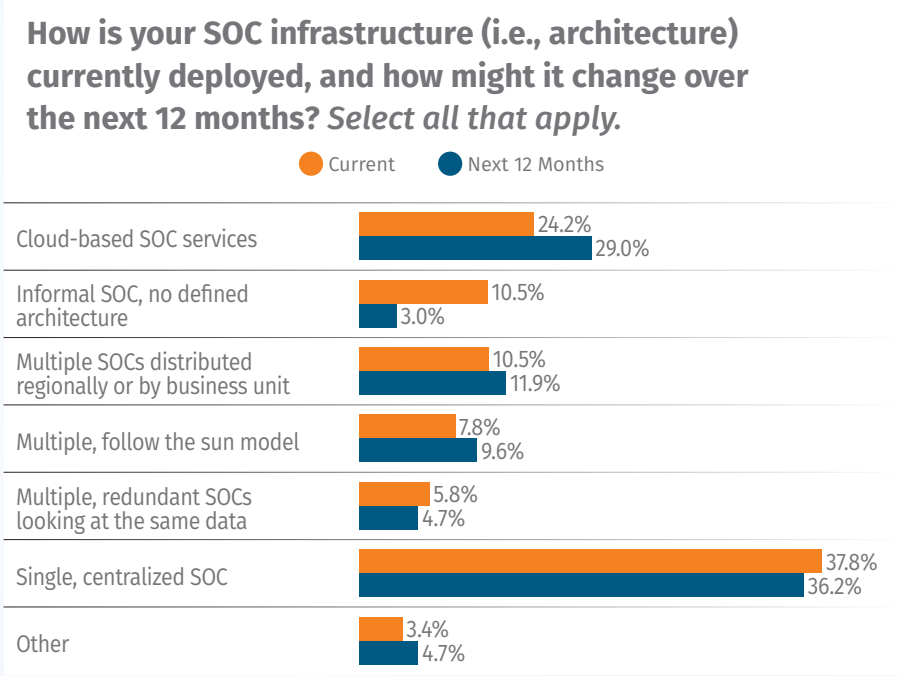


Figure 4. SOC Architecture, Current and Planned

As global political uncertainty intensifies through 2025 and into 2026, SOCs can expect increased scrutiny around international data flows. Geopolitical conflict is driving greater regulatory and organizational focus on how and where data is stored, who can access it, and which entities are monitoring it.

SOCs should be prepared to respond to tough questions around cross-border visibility, third-party monitoring, and data residency. These aren't just technical issues—they're legal and strategic concerns. Security leaders should anticipate deeper engagement from legal, compliance, and business stakeholders as these topics rise on the agenda.

Modern SOC Challenges

Today's SOCs are under pressure to deliver faster, smarter, and more proactive security outcomes—but several critical gaps are holding them back. AI/ML tools are being adopted rapidly, yet without intentional integration and oversight, they often waste budget, increase risk, and fail to provide meaningful support. At the same time, threat intelligence—while abundant—is frequently underutilized due to inconsistent application and a lack of objective analysis, keeping teams stuck in reactive mode. And although not a direct source of intel, TLS interception has emerged as a flashpoint in the visibility debate, raising concerns about privacy, performance, and trust. These issues collectively reflect a deeper need for strategic alignment and smarter operational practices across the SOC.

SOC employees are making abundant use of AI/ML tools without intentional integration and oversight. AI/ML tools provide value, but potentially waste budget, add risk, and fail to deliver meaningful support to SOC operations—technology satisfaction is low, but reported use is nonetheless high.

Artificial Intelligence (AI) and Machine Learning (ML)

With the substantial influence of AI and ML tools on the SOC in recent years, learning more about the influence of both will continue to be important. **Interestingly, data shows that the majority (40%) use the tools, but they are not part of the defined operations** (see Figure 5).

A SOC likely has two internal tasks to address:

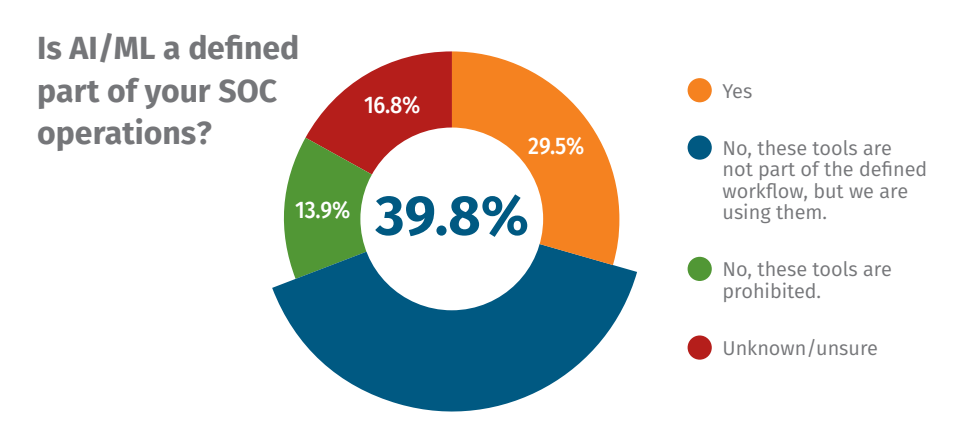


Figure 5. AI/ML Within SOC Operations

1. **Internal SOC priority—**Shift from uncoordinated, individual use of AI/ML tools to a team-approved, standardized implementation—one that maximizes their strengths while minimizing risk.
2. **External SOC priority—**Maintain oversight of data flowing from the organization to AI/ML platforms and unsanctioned shadow IT deployments. Although much of this data may seem low-risk, it's essential to have host-based data loss prevention (DLP) tools in place as part of your standard deployment to ensure visibility and control.

Expert Corner

The 2025 SOC Survey highlights a worrisome juxtaposition; SOCs struggle to hire and retain skilled analysts, while AI/ML and automation are the most commonly planned expansions, despite ranking lowest in value delivered. AI should augment analysts, not replace them. My concern is that leadership may see AI as a shortcut to fill staffing gaps, instead of investing in the talent and thoughtful integration of AI needed for substantive SOC improvement.

VIEW PROFILE

Seth Misner
SANS Faculty Fellow and author of two SANS courses: **LDR414: SANS Training Program for CISSP® Certification, SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring,** and **SEC411: AI Security Principles and Practices: GenAI and LLM Defense**.

Cybersecurity teams may not own the risk of AI hallucinations or inaccurate outputs, but the SOC can play a key role in mitigating their business impact. Governance, risk, and compliance (GRC) teams need technical support to monitor how AI tools are used and what systems or data they interact with.

Threat Intelligence

Threat intelligence activities are a significant part of SOC operations (73%) with the primary usage as incident response (69%). Figure 6 outlines the various ways in which CTI data and information are being used. CTI information is typically disseminated through email or documents (56%) and/or reports (55%).

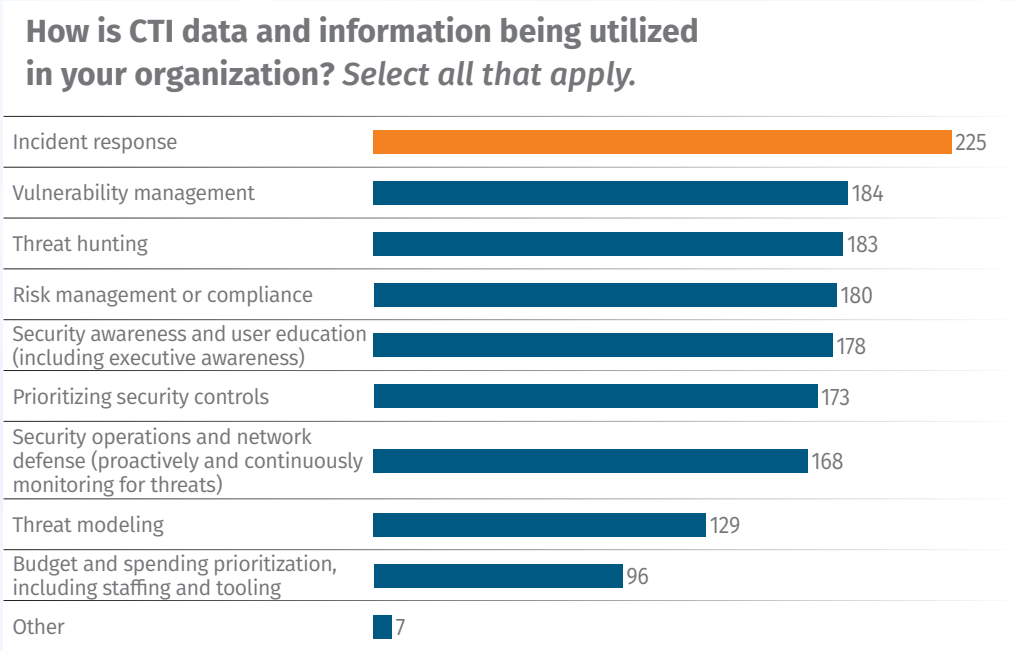


Figure 6. Count of Responses on CTI Data usage Within the Organization

Because threat intelligence is largely analysis-driven, respondents were asked about the analysis methods they most use. The most common answer (72%) was that analysts use their experience and intuition. Although expertise is essential, there's a strong case for incorporating more structured analytical approaches, such as conceptual or inductive methods, to improve consistency and reduce bias.

Additionally, most information comes from external sources, indicating there's a growing need to generate threat intelligence from internal data sources and not just rely on external feeds. Leveraging internal data can enhance risk assessment, threat hunting, and response capabilities. The most effective way to build internal threat intelligence is through collaboration and information sharing. However, SOC-based threat intelligence teams may lack organizational support for this. In such cases, informal peer collaboration can serve as a practical and acceptable alternative.

Incident Response Is Reactive, Not Proactive

The SOC's incident response capability is primarily described as either fully integrated as part of the internal SOC (51%) or provided through internal incident responders who perform ad hoc as needed (48%). The data also showed that incident response starts are primarily triggered by internal security alerts (85%). When asked about satisfaction levels for incident response capabilities, respondents are most satisfied with EDR and adversary containment and are least satisfied with deception technologies, a consistent trend since 2022. Only AI/ML tools have ranked worse in recent years.

When asked about threat hunting, the picture was similar. Most teams described partially automated hunting using vendor-provided tools (48%). Although technically a form of hunting, this often amounts to retroactive analysis rather than true, technique-driven hunts. The distinction matters because effective hunting requires skilled analysts, who remain in short supply. A lack of skilled staff remains the top-cited barrier for why teams aren't taking the time to do more sophisticated hunting (16%). More details on this in the next section.

Running Windows Defender with updated signatures and scanning the file system is not threat hunting. It's basic detection. Although historical search capabilities are improving due to advancements in vendor tools, SOCs need to stop calling this "hunting." There's still real value in doing it the hard way. True threat hunting relies on proven methodologies, hypothesis-driven analysis, and deep familiarity with attacker behavior. Alerts are designed to catch known threats, but sophisticated adversaries don't always trigger them. They operate quietly, below the detection threshold—and if you're not actively hunting, you're not going to find them.

Running Windows Defender scans isn't threat hunting, it's basic detection. True threat hunting involves hypothesis-driven analysis and deep knowledge of attacker behavior to uncover stealthy threats that evade alerts.

SOC Staff and Retention

Despite a growing "return to office" (RTO) trend in the United States, 73% of respondents indicated that SOC staff *can* work from home. However, responses show that if they are permitted, it depends on the specific role and skill set. In short, although most SOCs support remote work in principle, not every team member is granted that flexibility—even when the necessary technology is in place.

SOC teams are perennially short on highly skilled staff. It's a continuous struggle, and SOC leaders say their organizations aren't doing enough to keep the best people they have. Retention isn't just an HR issue. It's a signal of leadership's priorities. And it's hard to keep a SOC operating at its highest efficiency and effectiveness if the turnover rate is too high. If you want your team to stay, show them you're serious about understanding the factors that lead to job satisfaction.

One of the most common questions SOC leaders face is: *How many people does it take to run a SOC?* The most common answer is 10 (expressed as fulltime equivalents) and it's a good place to start your planning. This allows for adequate coverage across key functions like monitoring, incident response, threat intelligence, and engineering. Of course, in large, multinational enterprises, SOC teams can easily scale into the hundreds. But for most organizations aiming to maintain a solid internal capability, 10 is the number to plan around.

While the lack of skilled staff continues to be cited as the top challenge facing SOCs, 62% of respondents express a clear lack of confidence in their organization's ability or willingness to address it through meaningful retention efforts (see Figure 7). This disconnect highlights a deeper issue: Retention strategies may exist, but they aren't visible or credible to the people they're meant to support. Improving transparency around retention programs and demonstrating real follow-through—not just marketing platitudes—can go a long way toward rebuilding trust and keeping talent in place. Interestingly, even with this lack of confidence, respondents tend to stay employed three to five years in a SOC environment (31%) with very few staying 10-plus years (4%).

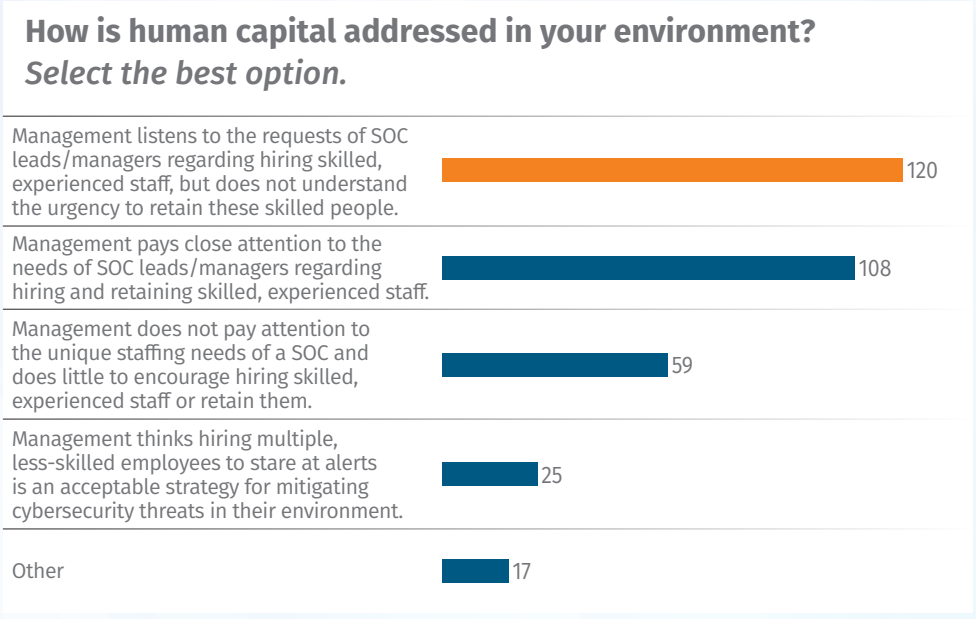


Figure 7. Count of Responses on Retention Efforts

Year-over-year comparisons show that compensation and engaging work are increasingly seen as effective retention strategies. Although career progression opportunities dipped in importance in 2024, they appear to be making a strong comeback in 2025 (see Figure 8).

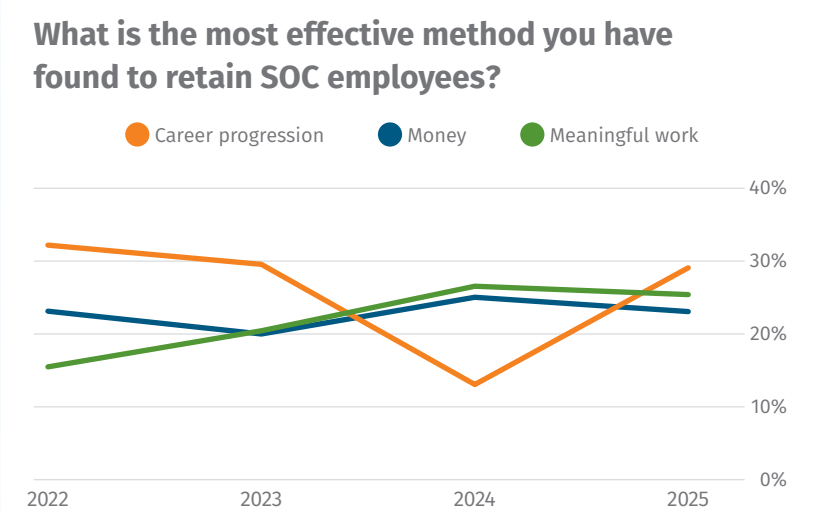


Figure 8. Effective Methods for Employee Retention

What SOC Leaders Want in an Employee

When asked about the most important technical skill deficit when hiring staff for technical roles (i.e., which skill is most lacking), respondents identified information systems and network security (14%) and digital forensics (12%) as the highest, followed by a broad range of other competencies outlined in Figure 9. For nontechnical skills, risk management topped the list at 14%.

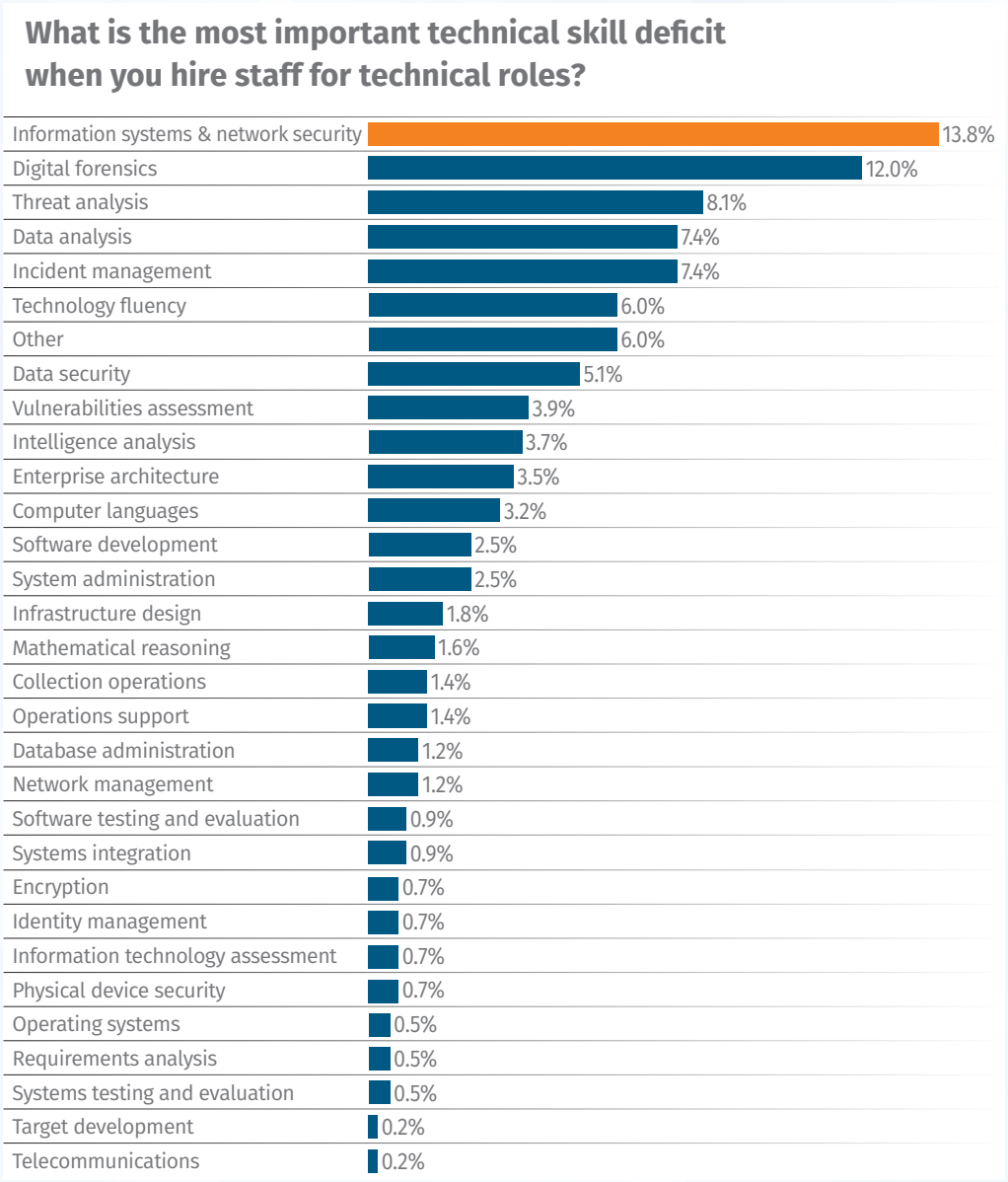


Figure 9. Skill Deficits

Expert Corner

Survey indicates that 62% of SOC professionals say their organization isn't doing enough to retain top staff. A great SOC isn't created by tooling, it's created with culture that recognizes and rewards the analysts who do amazing work. When analysts feel connected to the company mission and understand their contributions are an important part of that mission, they bring the energy, resourcefulness, and creativity needed to be successful. Managers need to recognize the talented analysts who set the model for success at all levels of technical ability and empower them to be leaders for others to follow.

Joshua Wright
SANS Faculty Fellow and Author of **SEC504: Hacker Tools, Techniques, and Incident Handling**.

VIEW PROFILE

What's Hot, What's Not in SOC Technology

If company leadership isn't prepared to fully commit the resources to make a tool effective, it would be better not to deploy it at all. A shiny new technology that seems like a great solution requires budget, training, time, and integration into workflow.

Endpoint or extended detection and response (EDR/XDR) once again tops the list for satisfaction, and it's the only technology this year to earn a score above a 3 out of 4 (when comparing technologies used and level of satisfaction). It's the most fully deployed, most trusted tool in the stack. EDR/XDR earns high satisfaction ratings because it's fully deployed, effective for initiating incident response workflows, and backed by proper training and support.

AI/ML tools continue to underperform. Of the three AI/ML technologies measured, two ranked at the very bottom, including generative language tools, which scored just a 2 out of 4. AI/ML tools underperform because they're new, often introduced without clear ownership or authorization, adequate deployment budget, or plans for integration into day-to-day operations.

Overall, established tools continue to earn the highest marks. EDR remains the top-rated technology, because it's trusted for its reliability and maturity. These are the workhorses of the SOC: well understood, widely deployed, and proven over time.

In contrast, newer technologies like AI/ML and deception are still struggling to meet expectations. Satisfaction remains low, suggesting that although interest is high, real-world performance and integration haven't caught up yet. This is very likely to change over time, and vendors of AI/ML technology shouldn't despair. Back in 2017, "asset discovery and inventory" held the bottom spot and now it's solidly mid-pack. Progress for AI is likely.

Conclusion: Encouraging Trends, but There's Still Work to Do

The 2025 SOC Survey confirms that the SOC is continuing to evolve encouragingly in the direction of established trends, but very slowly in some areas. Core capabilities are strong, but the balance still tilts toward reactive work. AI/ML remains underwhelming. Threat hunting is limited by staffing. And tool satisfaction, as always, depends on full deployment and thoughtful integration.

The 2025 SOC Survey paints a familiar picture: solid capability, some hopeful trends, but limited forward motion and ongoing staff dissatisfaction.

What's clear is that progress takes intention—in hiring, training, architecture, and tool use. Collecting data is easy. Using it wisely is the hard part.

SOC teams know what they need—tools that work, staff who stay, and time to do more than respond to alerts. But budget, turnover, and shifting priorities continue to get in the way. Metrics are tracked, but still manually. Cloud adoption ebbs and flows. AI/ML tools remain overhyped and under-delivering.

Meanwhile, a growing number of organizations are defaulting to "just store everything in the SIEM," a trend that's easy to justify today and hard to pay for tomorrow. It's a visibility strategy that risks collapsing under its own weight.

Tools don't solve these problems on their own. People do. And while progress is happening, it's uneven and often held back by the same structural issues year after year. The bottom line is that SOCs aren't stuck—but they're not moving fast either. Real gains will come from clarity, coordination, and the decision to stop calling retroactive workflows "hunting."

Five Reasons to Be Optimistic About the Future of the SOC

Widespread 24/7 coverage
79% of SOCs now operate around the clock, signaling SOC maturity and commitment to continuous monitoring and support from business stakeholders who recognize the seriousness of global cyber threats.

Increased cloud use
Although centralized SOCs are the most common architecture, migration to cloud resources is reportedly planned for the SOC systems.

Growing reporting of proactive detection
Even if it's still a minority, more teams report using SIEM searches and threat hunting, not just alerts.

More clarity on AI/ML use
Organizations are very slowly starting to intentionally integrate AI/ML tools into workflows, which proves it can be done when there's a plan.

Career progression tops retention factors
People want to stay where they are, but only if they see a future. That's a call to action for leadership.

Sponsors

SANS would like to thank this survey's sponsors:

SANS | Research Program

About the SANS Research Program

The SANS Research Program is a key initiative by the SANS Institute and a premier global provider of cybersecurity research and information. SANS Research Program is designed to provide cybersecurity practitioners and leaders with data-driven insights, thought leadership and solutions that help them better understand and respond to evolving security challenges. All content is authored by SANS instructor experts from around the world who apply their years of experience from hands-on practitioner work in the field, advisory roles and the classroom to provide education, guidance, and actionable insights that help make the cyber world a safer place.

To learn about Sponsorship opportunities for research and content, in-person, or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.

SANS | Research Program

Product Briefings for SOC

The 2025 SOC Survey represents the latest edition of SANS Institute's poll of security professionals. The sponsors of this year's survey all offer advanced capabilities that we believe will be of interest to SANS' clients, and, for this reason, we're presenting the following product briefings on a relevant offering.

Dropzone AI

SANS | Research Program

PRODUCT BRIEFING

Eliminating Alert Fatigue and Empowering Security Teams with Dropzone AI

Insights from the 2025 SANS Institute SOC Survey

July 2025

Organizations face critical gaps that keep their security operations centers (SOCs) reactive and under immense pressure: alert overload and fatigue, staffing and retention crisis, reactive posture and limited threat hunting, and unperforming AI tools. To secure the organization and outperform attackers, organizations need sophisticated and automated guidance and support.

Dropzone AI: Your Autonomous AI SOC Analyst

Dropzone AI's AI SOC Analyst is purpose-built to autonomously investigate security alerts, addressing these pain points and transforming security operations for enterprises and managed security service providers (MSSPs).

Dropzone AI offers a pretrained, autonomous AI SOC analyst that replicates the investigative techniques of elite analysts and autonomously investigates every alert. Designed to seamlessly integrate into existing security stacks, Dropzone AI eliminates the need for playbooks, code, or prompts, delivering fast time-to-value.

Dropzone AI's process for alert investigation mimics human analysts through three core stages (see Figure 1):

- **Collect—**Dropzone AI connects and retrieves relevant data from your fragmented security tools and data stack, including email server logs, SIEM, EDR, IAM, IDP, IDS, FW, and SaaS applications. It leverages over 60 integrations with platforms like Microsoft Defender, CrowdStrike, Splunk, Google Workspace, Okta, and Palo Alto Networks.

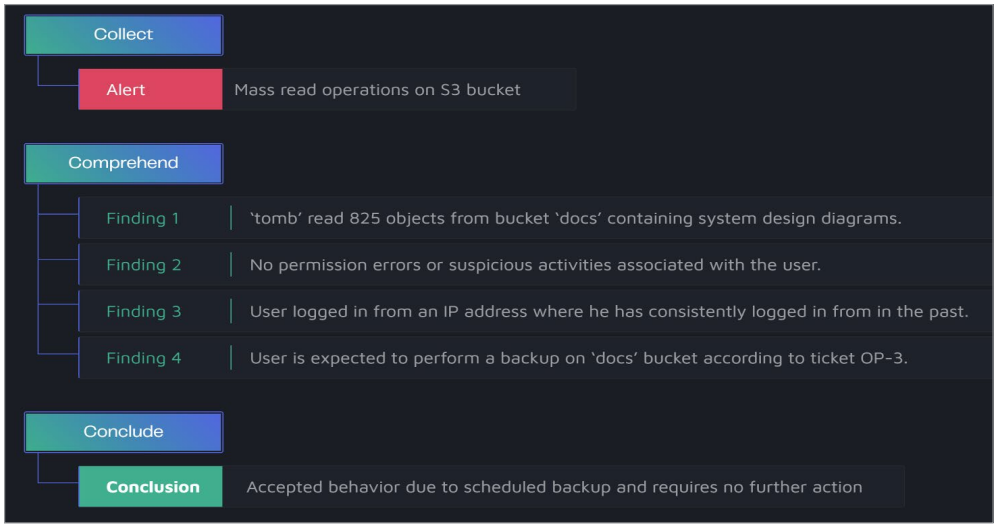


Figure 1. Dropzone AI's Three Core Stages of Alert Investigation

Key Findings

Alert Overload and Fatigue

85% of SOC analysts say endpoint security alerts are the primary trigger for response.

42% of SOCs dump all incoming data into a SIEM, often without a retrieval or management plan.

Staffing and Retention Crisis

62% of SOC professionals feel their organization isn't doing enough to retain top talent.

82% of SOCs are operational 24/7, yet staffing for this continuous coverage is a major challenge. The most common SOC size is 2–10 people.

Reactive Posture and Limited Threat Hunting

48% of teams use partially automated threat hunting.

Underperforming AI/ML Tools

30% formally use AI/ML tools in the SOC.

42% of SOCs using AI/ML tools don't tune or customize the tools.

- **Comprehend—**Leveraging large language models (LLMs), security pretraining, and your organization's unique context, Dropzone AI runs a full end-to-end investigation. It reasons through investigative threads, from URL and attachment analysis to previous organizational communications. This includes organizational context memory, which learns company-specific details like owned IP ranges, allowed VPN services, and critical servers, to ensure tailored and accurate analysis.
- **Conclude—**Dropzone AI generates detailed, decision-ready reports with a severity conclusion, executive summaries, and key evidence, providing full insights in plain English. Human analysts can quickly validate the AI's logical reasoning based on a complete report of crucial factors and a chain of raw evidence to support its conclusion.

In addition, the Dropzone AI system can be configured to take automatic containment actions, such as blocking IPs or disabling users. The system learns from user feedback and previous investigations.

Addressing SOC Challenges Head-On

Dropzone AI directly tackles the most pressing challenges identified in the 2025 SANS SOC Survey, delivering concrete benefits to security teams:

- **Eliminating alert overload and reducing mean time to resolution (MTTR)—**Dropzone AI reduces manual alert analysis time by 95%. By automating Tier 1 alert triage, it dramatically shortens MTTR by up to 90%, from hours to minutes. This allows SOCs to achieve 100% alert coverage, ensuring no alerts, even low-severity ones, go uninvestigated.
- **Empowering analysts and boosting retention—**Dropzone AI acts as a "Tier 1 SOC analyst always in the zone," handling the repetitive, time-consuming investigations. This frees up human analysts for higher-value work, such as threat hunting, policy updates, incident response planning, and strategic projects. By reducing burnout and increasing job satisfaction, Dropzone AI can help organizations retain top talent and make the SOC analyst job more enjoyable. Furthermore, it speeds up the onboarding of junior analysts, allowing them to learn from Dropzone AI's investigations and quickly understand the environment and available data sources.
- **Achieving proactive security—**By automating triage and investigations, Dropzone AI generates significant time savings that SOCs can then reinvest into proactive security activities like true threat hunting. Dropzone AI enables SOCs to quickly identify important alerts that are worth escalating, further reducing risk.
- **Delivering on the promise of AI—**Unlike many AI tools that underperform due to poor integration, Dropzone AI is designed for seamless, no-code integration with existing security tools via APIs. It includes guardrails to protect against hallucinations and prioritizes explainability and data lineage, ensuring humans can easily verify decisions and the evidence on which they are based. This intentional integration ensures Dropzone AI provides meaningful support and helps organizations finally realize the potential of AI in their security operations (see Figure 2).

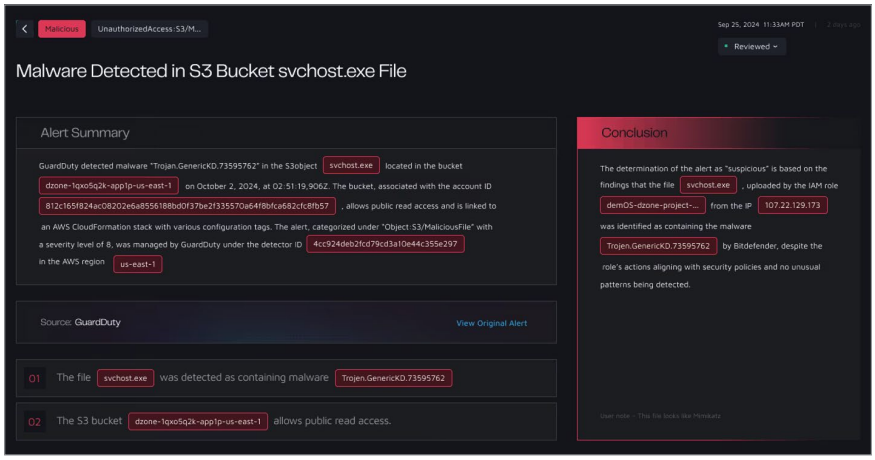


Figure 2. Dropzone AI's AI-Driven Alert Investigation with Detailed Reports and Evidence

- **Comprehensive coverage and seamless integration—**Dropzone AI supports a wide range of alert types, including phishing, endpoint, network, cloud, identity, and insider threat.
- **Built for trust and security—**Dropzone AI is SOC 2 Type 2 certified and employs a single-tenant architecture with no data comingling. Critically, Dropzone AI does not use any customer data to train its AI models or its sub-processors' models and contractually prohibits its LLM providers from storing or retaining customer data beyond immediate query processing. Dropzone AI encrypts data at rest and in transit and undergoes annual third-party penetration tests.

Dropzone AI is a trusted teammate that adapts to your environment, works 24/7, and always shows its work, bringing unlimited intelligence to your analysts for fast, detailed, and accurate investigations.

Empower your SOC. Transform your security operations.

To experience Dropzone AI autonomously investigating security alerts, try the self-guided demo at **www.dropzone.ai/self-guided-demo** or forward a suspicious email to **scan@try-dropzone.ai** for a tailored analysis report in minutes.

elastic

SANS | Research Program

PRODUCT BRIEFING

Elevate Your SOC with Elastic Security's AI-Driven Capabilities

Insights from the 2025 SANS Institute SOC Survey

July 2025

Security operations centers (SOCs) are contending with a multitude of significant challenges—from the sheer volume of incoming data to staffing woes and the practical integration of advanced technologies—that hinder their effectiveness and put organizations at heightened risk. Key challenges facing modern SOCs include overwhelming alert fatigue and low signal-to-noise ratio, persistent cyber skills shortages and staffing deficiencies, challenges with data onboarding and legacy SIEM lock-in, underperformance and underutilization of AI tools, reactive incident response, and limited proactive threat hunting.

Addressing Core SOC Challenges with AI-Driven Solutions

Elastic specifically designed its AI and automation features to tackle these real-world problems head-on.

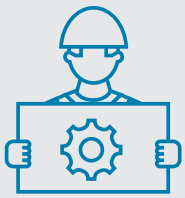
- Attack Discovery is an innovative feature that holistically assesses incoming alerts to reveal advancing attacks, guiding analysts to stop them. Instead of individual one-off events, Attack Discovery processes alerts as a cohesive narrative, enabling analysts to prioritize actual attacks, not just isolated alerts. It automates the time-consuming task of alert triage and suggests the next steps for investigators. Using LLMs, Attack Discovery surfaces, labels, and maps to MITRE ATT&CK™ the most significant attacks. This provides a simple, quick summary of the attack chain and details the chronological order of events, vastly accelerating the investigation process. Attack Discovery reduces the triage time for hundreds of alerts from hours to minutes or seconds.
- Elastic designed the AI Assistant for Security to make every user a power user, elevating every practitioner regardless of their experience level. It guides analysts through triage, investigation, and response, and assists administrators with routine tasks. The AI Assistant provides a natural language interface for query generation. This provides actionable guidance, tailored to the organization-specific knowledge through retrieval augmented generation (RAG), and much more (see Figure 1 on the next page).

Key Findings

Overwhelming Alert Noise

85% of SOC analysts say endpoint security alerts are the primary trigger for response.

42% of SOCs dump all incoming data into a SIEM, often without a retrieval or management plan.



Persistent Cyber Skills Shortage

62% of SOC professionals feel their organization isn't doing enough to retain top talent.

16% say a lack of skilled staff is the top barrier to threat-hunting.

Slow Data Onboarding and Legacy SIEM Migration

Organizations often struggle to quickly integrate custom data sources and migrate existing detection rules from legacy SIEMs.

- Elastic's Automatic Import enables rapid onboarding of custom data sources in minutes, not days. This feature uses AI to develop, test, and tweak new integration packages until they pass validation, expanding visibility and powering detection rules with minimal manual effort. Elastic ships with over 400 prebuilt data integrations, but for unique custom logs, Automatic Import provides a seamless capability that reduces the time to collect and normalize a new data source from one to four days to just 10 minutes.

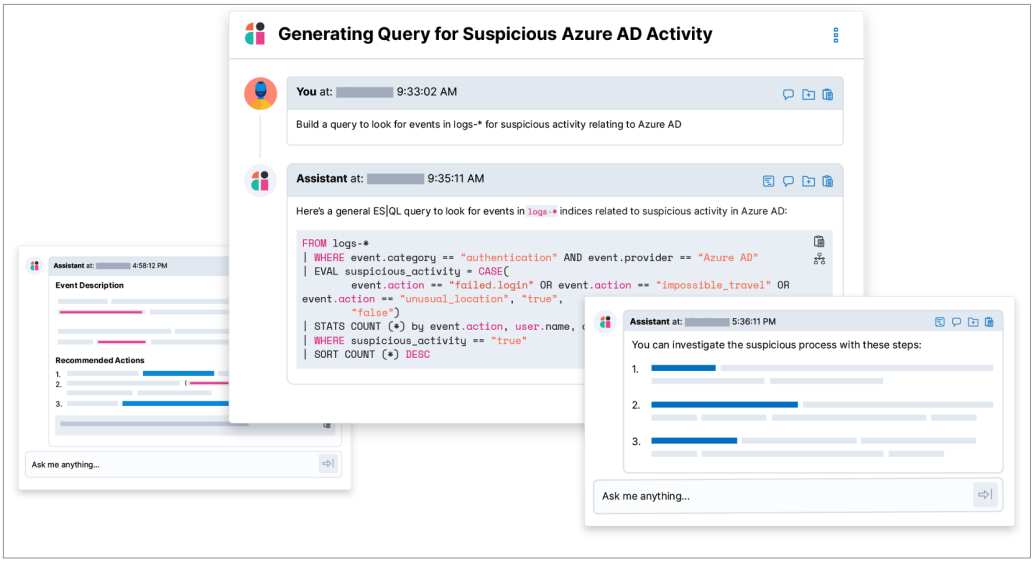


Figure 1. Automatic Query Generation

- Automatic Migration minimizes the time and expertise needed to move legacy detection rules to Elastic Security, streamlining SIEM adoption and reducing risk. It expedites the translation of complex rules, including lookups and macros, and ensures detection continuity by minimizing translation errors. It also helps streamline rule upkeep by mapping legacy SIEM detections to Elastic Security Labs' prebuilt rules. This feature can create or convert a detection rule in 15 minutes, down from one to three hours. Automatic troubleshooting leverages LLMs to detect conflicting EDR and AV software running on a host with Elastic Defend and suggests processes to be trusted to resolve the conflict.

Powered by the Elastic Search AI Platform

Elastic's AI capabilities are built upon the robust Elastic Search AI Platform, which acts as a powerful vector database. This platform safely surfaces hyper-relevant knowledge, enabling public LLMs to perform as if custom-trained for private use cases.

- **RAG—**A core component, RAG grounds responses in proprietary data by enriching user prompts with real-time organizational context. This approach provides meaningful results without the need to build and retrain bespoke LLMs on constantly changing internal data. Elastic uses its search capabilities to retrieve and surface uniquely relevant data to the LLM, ensuring accurate and helpful answers.
- **Flexible LLM connectors and ecosystem—**Elastic understands that the state of generative AI is rapidly evolving. It provides flexibility through a growing set of integrated models and services, including Google Vertex AI, OpenAI, Amazon Bedrock, and Azure OpenAI Service and also offers a managed LLM out of the box. The multitude of choices ensures users can control cost, speed, accuracy, and privacy, now and in the future.
- **Security and privacy—**Elastic prioritizes data safety, making it easy for organizations to anonymize or redact confidential data by default and as needed, with document-level control. This prevents accidental relaying of sensitive internal data by analysts.

The Tangible Impact of Elastic AI in the SOC

Elastic's AI capabilities ensure SOC teams can focus on finding and stopping threats, rather than being bogged down by data wrangling or schema modification. AI acts as an acceleration of the team, not a replacement for analysts.

Real-world results demonstrate the power of Elastic's AI:

- Sitecore has automated 96% of its security workflows with Elastic.[1]
- Proficio has seen a 34% improvement in alert triage time.[2]
- The Texas A&M University System saves over 100 analyst hours per month by automating documentation and other security processes with Elastic Security.[3]
- Studies indicate that Elastic's security solutions have:
  - Reduced false-positive security alerts by 75%
  - Reclaimed 74% of full-time security employee hours with AI
  - Reduced security incidents by 90%
  - Reduced annual risk exposure by 36%

Elastic is uniquely positioned to help SOC teams harness generative AI by providing LLMs access to an unrivaled corpus of information, retrieving uniquely relevant data, and dramatically reducing the cost and complexity of data collection, storage, and analysis.

Elastic Security's AI capabilities empower SOC teams to gain an unfair advantage, accelerating onboarding, triaging alerts down to critical attacks in seconds, and boosting productivity by augmenting analyst and admin expertise with generative AI. This is the future of SIEM, delivered today.

---

[1] "Sitecore wins new business, reduces costs, and accelerates security operations with Elastic," www.elastic.co/customers/sitecore-security
[2] "Proficio protects global customers with advanced cyber threat detection and response tools from Elastic Security," www.elastic.co/customers/proficio
[2] "The Texas A&M University System protects students, emergency responders, and leading research institutions with Elastic Security," www.elastic.co/customers/tamus

FORTINET

SANS | Research Program

PRODUCT BRIEFING

Fortinet SecOps Platform: Unified AI-Driven Security for Modern Threat Landscapes

Insights from the 2025 SANS Institute SOC Survey

July 2025

Modern security operations centers (SOCs) face formidable hurdles in defending against an increasingly sophisticated and pervasive threat landscape. Attack campaigns are continuously evolving in their tactics and procedures, making detection more difficult. The expansion of digital presence, including remote work environments, connected IoT/OT devices, and cloud applications, significantly broadens the attack surface. This growing complexity leads to an overwhelming volume of security products, information, and alerts, making it challenging for security teams to identify genuine threats amidst the noise. Furthermore, a persistent industry-wide shortage of cybersecurity expertise frequently results in overburdened security teams, hindering their ability to effectively manage and respond to these complex threats.

The Fortinet Security Operations (SecOps) Platform

Fortinet designed its Security Operations (SecOps) Platform to provide comprehensive, AI-driven security for organizations at any stage of their security journey. It seamlessly integrates behavior-based sensors to detect and disrupt threat actors across the entire attack surface and along the cyber kill chain. Backed by FortiOS, Fortinet's operating system, the platform delivers centralized investigation and remediation SecOps teams can orchestrate, automate, and augment to reduce cyber risk, cost, and operational effort.

This platform offers a broad range of sensors that use AI and other advanced analytics to continuously assess activity across devices, users, files, networks, email, applications, clouds, logs, and even the dark web, helping to identify signs of cyber threats. This approach fundamentally shifts the security operations paradigm from merely "detect and respond" to "detect and disrupt," followed by "investigate and respond," resulting in faster containment and more time for thorough investigation and comprehensive remediation. The platform unifies and automates threat response using AI-driven analytics, threat intelligence, and generative AI (GenAI) assistance (see Figure 1).

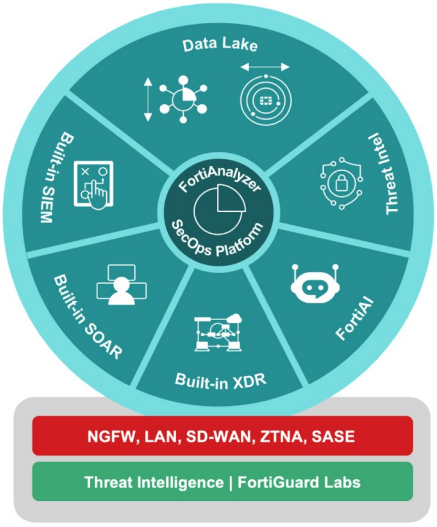


Figure 1. Fortinet SecOps Platform

Key Findings

Alert Overload and Fatigue

85% of SOC analysts say endpoint security alerts are the primary trigger for response.

Staffing and Retention Crisis

62% of SOC professionals feel their organization isn't doing enough to retain top talent.

Suboptimal Integration and Underperformance of AI/ML Tools in SOC Operations

42% of SOCs using AI/ML tools don't tune or customize the tools.

40% of SOCs report using AI/ML tools, but they are not part of the defined workflow.

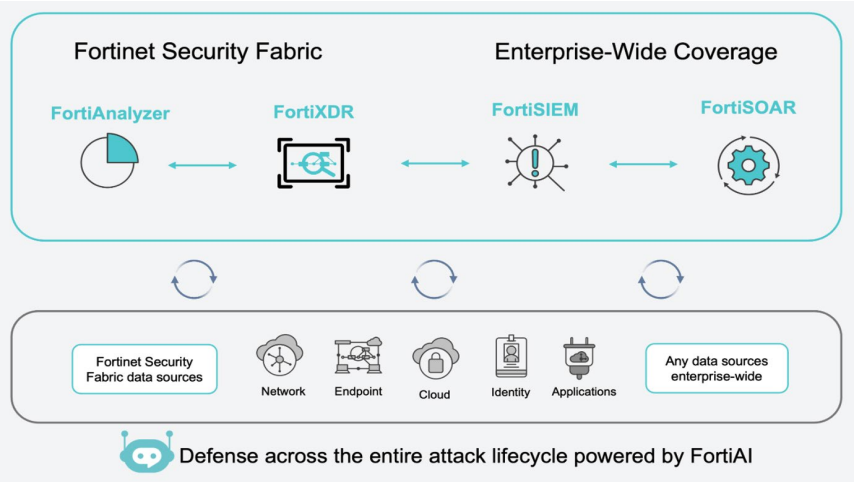


Figure 2. Fortinet SOC Automation

The platform's proactive exposure assessment, comprehensive threat intelligence, and AI-powered analysis include:

- **AI-driven security and automation** reduces cyber risk by speeding detection and containment, as well as investigation and remediation. The FortiAI GenAI assistant is built into analyst workflows to inform and expedite incident management and threat hunting. This includes capabilities like automated alert triage, adaptive threat hunting, root-cause tracing, and auto configuration.
- **Complete digital asset visibility** with automated asset discovery and monitoring offers real-time insights into networks, cloud environments, and web applications. Advanced analytics and risk scoring help prioritize vulnerabilities and strategically allocate resources.
- **Comprehensive threat intelligence** from FortiGuard Labs, an elite research team with over 15 years of AI experience, provides proactive risk mitigation and ensures security teams stay ahead of potential attackers.
- **Rapid incident response** aims to significantly reduce detection and response times. With correlated alerts, reduced attack surface, and improved overall visibility, the Fortinet SecOps Platform can achieve an average time to detect and contain threat actors of one hour and an average time to investigate and remediate incidents of 11 minutes.
- **Consolidated platform and seamless integration** with Fortinet's broad range of security products provides a single vendor look to security operations. Fortinet Security Fabric enables deeper visibility, offers a wider range of actions, and supports 500-plus connectors for multivendor security infrastructure.

Fortinet SecOps Platform: Directly Tackling the SOC's Pressing Challenges

Fortinet SecOps Platform directly addresses the most pressing challenges identified in the 2025 SANS SOC Survey, delivering concrete benefits to security teams (see Figure 2):

- Fortinet's platform uses AI-powered detection to improve accuracy and reduce false positives. FortiAI-Assist is designed to prioritize notifications, suppress duplicate alerts, and only flag high-confidence threats, directly combating alert fatigue.
- Fortinet designed its SecOps solutions for rapid detection, investigation, and response. Timely protection and proactive defense are a result of AI-powered security and GenAI assistance built into analyst workflows, which expedites incident management and threat hunting.
- Fortinet's SecOps Platform provides broad sensors to avoid blind spots. It offers continuous threat exposure management and complete digital asset visibility through automated discovery and monitoring.
- Fortinet's automation and augmentation speeds response and eases the burden on in-house security teams. FortiAI-Assist boosts analyst effectiveness by providing instant answers and detailed guidance as well as automating tasks like alert triage, configuration, and policy creation, enabling security teams to be more efficient and consistent.
- Fortinet's SecOps Platform supports adaptive threat hunting by scanning logs, network traffic, and user behavior for threats without constant human input. Solutions like FortiDeceptor offer deception-based breach protection for early detection and isolation of sophisticated attacks, while FortiNDR identifies incidents in progress based on anomalous network activity.

The Fortinet SecOps Platform is a flexible, integrated solution that unifies and optimizes threat response using GenAI and AI-driven analytics, threat intelligence, and automation. FortiAI-Assist, Fortinet's GenAI offering, is embedded throughout the Fortinet Security Fabric, combining intelligent analytics and automation to accelerate detection, reduce overhead, and improve operational efficiency at AI speed.

Customers choose Fortinet for its comprehensive security solutions, which have proven to deliver significant operational efficiencies and improved risk management. Case studies illustrate how Fortinet solutions help organizations cut outages, identify network weaknesses, streamline network management, and drastically reduce suspicious emails.

infoblox

SANS | Research Program

PRODUCT BRIEFING

Infoblox Threat Defense: Preemptively Blocking Threats and Unifying Security Operations

Insights from the 2025 SANS Institute SOC Survey

July 2025

Organizations are drowning in security alerts despite massive investments in cybersecurity tools. Security operations center (SOC) teams battle overwhelming alert fatigue as multiple systems flood security information and event management (SIEM) platforms with duplicates and false positives, driving up costs while ransomware and breaches persist. Meanwhile, fragmented security across hybrid and multicloud environments leaves blind spots at critical egress points. Without clear attribution linking malicious activity to specific users and devices, incident response crawls to a halt just when speed matters most.

Infoblox Threat Defense: The Foundational Protective DNS Solution

Infoblox Threat Defense directly addresses these pervasive challenges by leveraging the critical role of DNS as the first point of detection for cyberattacks. By blocking attacks early, Infoblox Threat Defense reduces the volume of malicious traffic reaching downstream security tools and the number of alerts they generate.

The core strength of Infoblox Threat Defense lies in its predictive DNS threat intelligence and advanced algorithmic protections, enabling it to detect threats before other tools and that other tools often miss. This preemptive approach transforms security effectiveness by putting DNS at the center of protecting all infrastructure, from cloud to core.

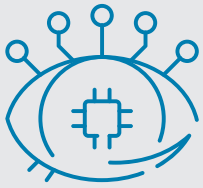
Key Capabilities and Preemptive Power

- **Preemptive and predictive protection,** which enables detection and disruption of cybercrime often before attacks are even launched. Infoblox can block 82% of threats before the first DNS query. Furthermore, Infoblox identifies high-risk or suspicious domains an average of more than two months before the rest of the industry confirms them as malicious, while maintaining an ultra-low false-positive rate of 0.0002% out of more than 20 million indicators.
- **Comprehensive DNS monitoring** with full DNS behavior monitoring to meticulously track all DNS record types for malicious activity
- **Lookalike domain detection and mitigation** to proactively identify and mitigate lookalike/doppelganger domains, which are frequently used in phishing and other advanced targeted attacks to deceive users and compromise brands
- **Zero-day DNS protection** that identifies new or emerging domains that could pose a threat to an organization, offering protection against previously unknown threats

Key Findings

Alert Overload and Fatigue

42% of SOCs dump all incoming data into a SIEM, often without a solid plan for retrieval or management.



Fragmented Security and Lack of Unified Visibility

85% of SOC analysts say endpoint security alerts are their primary trigger for response.

Slow and Inefficient Incident Response

69% of SOCs still rely on manual or mostly manual processes to report metrics.

- **Behavior-based DNS tunneling detection,** which often is used for data exfiltration/infiltration and command and control (C2) communications
- **Proactive suspicious/high-risk domain protection** that identifies and preemptively blocks suspicious domains that are likely to be used in future malicious campaigns
- **Proactive threat distribution systems (TDS) detection and disruption,** which is used to identify threat actor TDS infrastructure to counter threat actors rotating across numerous domains to evade detection
- **Simplified and intuitive UI** that lets security teams understand what's happening within their environment and suggest ways to decrease security risks
- **"Protection Before Impact" monitor** that enables CISOs and security teams to confidently report to the board with clear, quantifiable metrics on threats neutralized before impact

Automating Asset discovery, Context and Enhancing SOC Efficiency

Infoblox Threat Defense enhances SOC efficiency through intelligent automation and AI-driven analytics. With automatic asset context enrichment, correlating network context without the need for clients or sink holing, it provides direct attribution to impacted users, devices and cloud workloads that is crucial for accelerating investigations.

Infoblox applies AI-driven analytics to correlate DNS threat and asset data. It distills tens of thousands of alerts into a handful of actionable SOC insights, alleviating the need for manual processes to report metrics and analyze incoming data. By automating correlation and triage, Infoblox drastically reduces the amount of data sent to SIEM systems and the time required for remediation (see Figure 1).

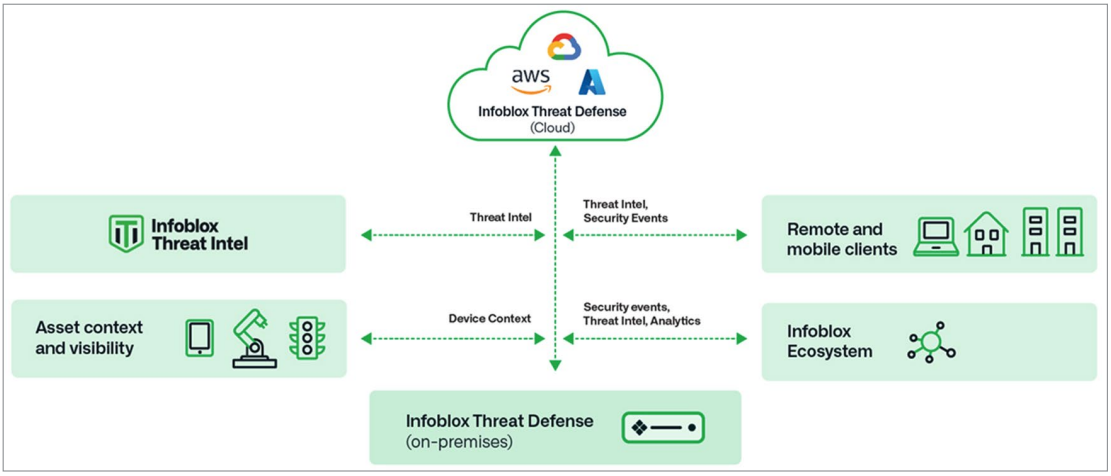


Figure 1. Integrating Infoblox Threat Defense into the Environment

Tangible Benefits and Accelerated ROI

Infoblox Threat Defense transforms security operations (SecOps) and provides a strong return on investment:

- **Substantial manpower and cost savings—**By blocking threats much earlier and reducing alert volume, Infoblox Threat Defense saves SOC analysts an average of 500 hours per month. In fact, customers have reported as much as a 50% reduction of alerts on next-generation firewalls (NGFW) and endpoint detection and response (EDR) tools alone. The reduction in alerts and increase in productivity drives both employee cost savings—as much as $400,000 per year—and a concomitant reduction in data sent to SIEMs, which further reduces costs.
- **Enhanced security ecosystem integrations—**Infoblox Threat Defense maximizes existing security investments by seamlessly integrating with various tools across the security stack, including SIEM; security orchestration, automation, and response (SOAR); vulnerability management (VM); threat intelligence platforms (TIP); network access control (NAC); NGFW; IT service management (ITSM); and IT operations management (ITOM). This breaks down silos, enhances threat detection, automates workflows, and improves response capabilities across hybrid, multicloud, and on-premises environments, addressing the pervasive challenge of fragmented security.
- **Improved threat intelligence utilization—**The SANS SOC survey highlights that 69% of SOCs primarily use cyber threat intelligence (CTI) data for incident response. Infoblox provides highly accurate, predictive DNS-based threat intelligence, filling potential gaps in an organization's CTI and significantly enhancing incident response capabilities.

Infoblox Threat Defense, whether deployed on premises, in the cloud, or in a hybrid model, offers foundational security for protection anywhere, enabling organizations to take a more proactive stance against evolving cyber threats.

To learn more about how Infoblox Threat Defense can strengthen your cybersecurity posture and uplift SecOps efficiency, talk to an expert or enroll in a security workshop today.

prophet

SANS | Research Program

PRODUCT BRIEFING

Prophet Security: The AI Force Multiplier That Accelerates Security Operations

Insights from the 2025 SANS Institute SOC Survey

July 2025

Security operations centers (SOCs) are frequently overwhelmed by an unmanageable influx of security alerts, leading to a state of alert fatigue that hinders their ability to effectively triage and investigate every potential threat. This often necessitates extensive manual effort to piece together fragmented data from disparate systems, consuming valuable analyst time on repetitive tasks rather than proactive defense. The resulting alert fatigue contributes to a backlog of alerts, increasing the risk of critical incidents being missed. Furthermore, existing automation and orchestration tools often prove complex to implement and difficult to maintain, plus they lack the adaptability required to keep pace with evolving attacker techniques.

The Prophet AI SOC Platform: A Smarter, Scalable SOC Powered by Agentic AI

Prophet Security designed its AI SOC platform to revolutionize how SOCs function, transforming manual, resource-intensive processes into streamlined, AI-powered workflows that empower analysts and enhance an organization's security posture (see Figure 1).

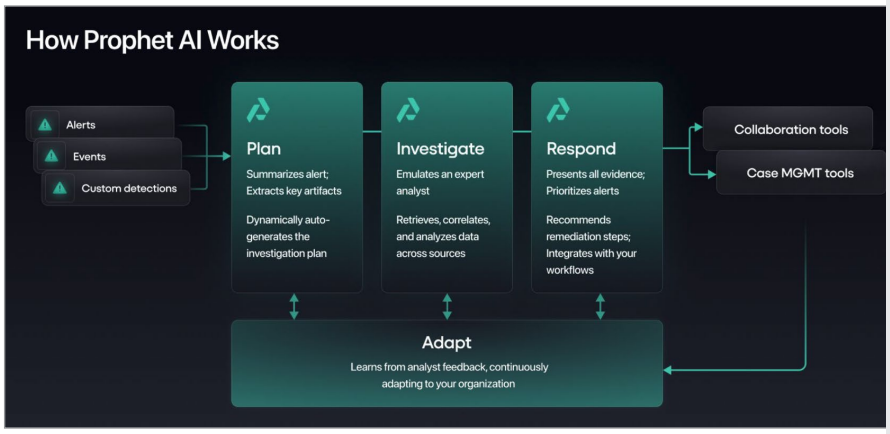


Figure 1. Prophet AI SOC Platform

Key Findings

30% of SOCs
identify lack of skilled staff or high staffing requirements as their biggest challenge

69% of SOCs
continue to depend on manual or largely manual processes for reporting metrics.

18% of SOCs
call out a silo mentality between incident response and operations, lack of context, or too many alerts as their biggest challenge

13% of SOCs
cite a lack of adequate orchestration and automation as their biggest challenge

Prophet AI's workflow is structured around five key stages:

- **Plan:** Prophet AI immediately deduplicates and summarizes incoming alerts, extracts key artifacts, classifies them, and dynamically constructs an investigation plan. This plan outlines the critical questions an expert analyst would typically ask to determine if an alert is a true or false positive.
- **Investigate:** Emulating an expert analyst, Prophet AI executes the investigation plan by autonomously retrieving, correlating, and analyzing relevant information. It gathers context from diverse sources, including SIEMs, security data lakes, security tools, and object storage, to arrive at its conclusions. Furthermore, its "Dig Deeper" capabilities allow analysts to ask additional questions about a single investigation or across multiple investigations, or to create custom investigations using existing playbooks. Prophet AI Threat Hunter works with your team to perform the collection, processing, and lead generation of hypothesis-driven threat hunting activities across your environment.
- **Respond:** After completing an investigation, Prophet AI assigns a severity level based on its findings, prioritizing critical alerts for immediate attention. It provides concrete, one-click remediation steps to accelerate response. Prophet AI integrates seamlessly with existing collaboration and case management tools to ensure rapid adoption and minimal disruption to current workflows.
- **Adapt:** Prophet AI continuously learns and adapts to the environment by ingesting organizational context from analyst feedback, ensuring the system refines its accuracy and effectiveness over time.
- **Report:** The platform provides a real-time view of critical SOC metrics, such as alert dwell time, and Mean Time to Investigate (MTTI) and Mean Time to Respond (MTTR). Additionally, Prophet Security's Detection Advisor identifies the noisiest alerts and detection gaps, providing insights to detection engineering teams for alert tuning and optimization.

Accelerating Security Operations by Addressing Key Challenges

Extend the Impact of Your Existing Team

The 2025 SANS SOC Survey underscored a persistent talent gap in security operations. Teams are either understaffed or stretched thin. Prophet AI SOC Platform addresses this head on by offering an expert-level AI SOC Analyst capable of autonomously triaging and investigating every alert. By eliminating manual, repetitive effort, the platform allows existing teams to scale their capacity and focus on the most impactful tasks.

Move Beyond Playbooks to True Investigative Automation

Automation in many SOCs is either too rigid or too shallow to handle complex, dynamic investigations. The Prophet AI SOC Platform goes beyond traditional playbooks or prompt-based AI chatbots by using agentic AI to conduct end-to-end investigations in under three minutes, compared to a 30-minute industry average. This drastically reduces dwell time and MTTR.

Reduce Noise, Add Context, Connect the Dots

The Prophet AI SOC Platform cuts through the noise by prioritizing the alerts that matter most and surfacing them with full context. Its AI SOC Analyst rapidly analyzes telemetry, correlates signals across tools, and presents clear investigative findings for human review.

See how the Prophet AI SOC Platform can help your team investigate faster, reduce noise, and focus on what really matters. Request a demo to experience agentic AI built for security operations.

SWIMLANE

SANS | Research Program

PRODUCT BRIEFING

Streamlining Security Operations with Swimlane Turbine

Insights from the 2025 SANS Institute SOC Survey

July 2025

Security operations centers (SOCs) face a perfect storm of challenges just when organizations need them most: talent hemorrhaging, data chaos, and operational blindness.

Top SOC analysts leave faster than they can be replaced, taking critical expertise with them. Meanwhile, poorly managed security information and event management (SIEM) systems inundate teams with false positives, making it nearly impossible to spot real threats. Manual reporting processes leave leadership blind to operational health, creating a vicious cycle of overwhelmed teams and persistent staffing shortages, all while cyber threats become increasingly sophisticated.

Swimlane Turbine: The AI Automation Platform for Every Security Function

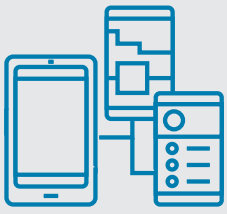
Swimlane Turbine, an AI hyperautomation platform for every security function, provides powerful AI-driven solutions to address these critical gaps, enabling SOCs to operate with unprecedented efficiency, scale, and effectiveness. Swimlane provides a robust set of capabilities, through the Turbine platform, that streamline and enhance security operations across the board:

- Hero AI is a collection of agentic and generative AI capabilities in Turbine, built on the private Swimlane LLM. Hero is contextually aware and trustworthy. Its AI functions can act as an AI assistant for any role, with capabilities including summarizing cases, recommending actions based on case data and Knowledge Base (KB) articles, and generating executive summaries and after-action reports—all while ensuring that sensitive customer data is not sent to third parties or used to train the model (see Figure 1 on the next page).

Key Findings

62% of SOC professionals believe their organization isn't doing enough to retain top staff.

42% of SOCs dump all incoming data into a SIEM system, often without a solid plan for retrieval or management.



85% of SOC analysts state that alerts from endpoint security tools are their primary trigger for response.

69% of SOCs still rely on manual or mostly manual processes to report their metrics.

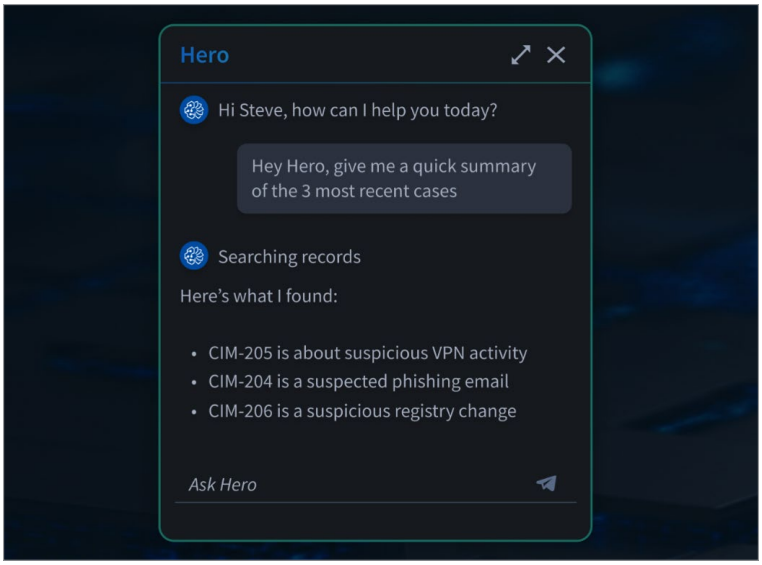


Figure 1. Swimlane Hero Chat Interface

- Swimlane Turbine Canvas is the platform's low-code playbook-building studio. It allows users to build playbooks three times faster using modular and reusable components. To further accelerate automation building, users can download and edit more than 2,500 prebuilt playbooks in the Swimlane Marketplace. Using conditional logic, Swimlane Turbine can trigger playbooks based on a variety of events and offers no-code capabilities such as data transformation, conditional logic, parallel execution, schema inference, and more. It also allows for custom HTTP actions, enabling integration with any API. Robust debugging and testing functionalities are integral to the playbook-building experience.
- Swimlane Turbine offers robust and customizable AI-driven case and incident management, serving as a single system of record for the SOC and streamlining incident response from escalation to resolution. The case management application enables analysts to focus on the most relevant data points while maintaining access to raw payload data. The system integrates human intelligence by referencing KB and supports the correlation of alerts using fuzzy hashing to link similar incidents.
- The platform allows for the enrichment and normalization of indicators of compromise (IoCs) from any source. Swimlane Turbine integrates with third-party threat intelligence platforms (TIPs) to enhance the effectiveness of existing feeds. It maintains a reciprocal reference between IoCs and cases, enabling SOCs to see trends and commonalities for improved threat hunting.
- Swimlane Turbine is built for speed and scalability, enabling it to execute 25 million daily actions for a single customer. With a multi-tenant architecture, enterprises and managed security service providers (MSSPs) can maintain strict data isolation and privacy for each customer or business function.

Swimlane Solves the SOC's Critical Challenges

Swimlane addresses the pain points that surfaced in the 2025 SANS SOC Survey with targeted solutions that deliver measurable results for security teams. Turbine picks up precisely where the SIEM leaves off, utilizing AI automation to handle the "last mile" of alert triage and incident response for signals originating from the SIEM or endpoint security controls, thereby reducing dwell time and accelerating response. The Swimlane SOC Automation Solution significantly reduces alert volume, achieving a 95% reduction in SIEM, EDR, and XDR alerts.

Acting as a comprehensive system of record for the SOC, Swimlane Turbine provides highly composable and self-documenting dashboards that offer real-time visibility to SOC leaders, analysts, vulnerability management teams, compliance teams, and beyond. Swimlane provides an environment-agnostic tool that can integrate with all other sources to pull in data, ensuring that teams don't have to navigate disparate tools to collect metrics. Swimlane provides visibility into both SOC KPIs, the actions taken, and the decisions made during incident response.

The Swimlane Turbine platform promises a 240% return on investment (ROI) in the first year with fast and seamless implementation, professionally implemented by Swimlane in two to four weeks. Additionally, customers can expect a 20% increase in efficiency when using Hero AI. Leading cybersecurity professionals have endorsed Swimlane, with feedback highlighting its ability to provide a robust look into the environment, enhance analyst efficiency, unify diverse customer environments, and serve as the powerhouse of the SOC.

By taking mundane, tedious, and dreaded work off analysts' plates, Swimlane Turbine enables analysts to focus on strategic tasks that foster career growth. This makes AI automation a powerful enabler for career development and retaining top talent. AI can empower a junior analyst to operate at a level far beyond their years, accelerating their professional development. Furthermore, when turnover inevitably occurs, AI automation can pick up the slack. Swimlane customers have reported that with Turbine, they can operate at the capacity of 20-plus additional SOC analysts compared to their previous SOAR/SIEM bundled platforms.

By addressing critical challenges in staff retention, alert management, and operational visibility, Swimlane Turbine empowers SOCs to move beyond reactive operations, enabling them to achieve true hyperautomation and deliver faster, smarter, and more proactive security outcomes.

ThreatConnect.

SANS | Research Program

PRODUCT BRIEFING

Empowering Threat and Risk-Informed Cyber Defense with ThreatConnect

Insights from the 2025 SANS Institute SOC Survey

July 2025

Security operations centers (SOCs) are constantly under pressure, grappling with a multitude of challenges that hinder their ability to effectively detect, prioritize, and respond to threats. SOC analysts are often overwhelmed by the sheer volume of alerts and disparate data sources, struggling to identify what is truly relevant amidst the noise. All too frequently, they miss critical threats and waste valuable time on false positives. Furthermore, security leaders persistently find it difficult to demonstrate the tangible value of cybersecurity investments to leadership in business terms, making it challenging to secure necessary resources and combat the high rates of staff burnout and turnover that plague the industry.

ThreatConnect's Integrated Approach: The Intel Hub

ThreatConnect offers a comprehensive approach to cyber defense, integrating threat intelligence, risk quantification, and security operations to build cyber resilience and enhance security effectiveness, efficiency, and collaboration. ThreatConnect designed the Intel Hub to address these critical challenges by combining three core products: Threat Intelligence Operations (TI Ops), Risk Quantifier (RQ), and Polarity, bringing together threat intelligence, cyber risk management, and security operations teams to foster effective, efficient, and collaborative cyber defense, powered by AI.

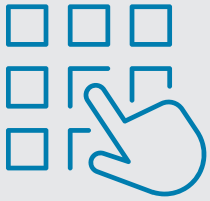
- TI Ops moves beyond traditional threat intelligence platforms (TIPs) by operationalizing all intelligence for faster, more precise detection and response. It aggregates, normalizes, and enriches intelligence from over 300 open, commercial, and internal sources using AI, making the intelligence actionable and ready for querying. TI Ops helps create a unified threat library, provides AI-powered analytics, automates analyst work with playbooks, and enables visualization of threat actor behaviors. With built-in reporting for effective dissemination of intelligence, TI Ops also enables CTI teams to manage threat intelligence and inform security operations and leadership. Thanks to its innovative Intelligence Requirements feature, it's the only solution that streamlines the entire threat intelligence life cycle end to end (see Figure 1 on the next page).

Key Findings

62% of SOC professionals say their organization isn't doing enough to retain staff.

Lack of skilled staff continues to be cited as the top challenge facing SOCs.

69% of SOCs use cyber threat intelligence (CTI) data primarily for incident response.



69% of SOCs still rely on manual or mostly manual processes to report metrics.

- RQ quantifies cyber risk in financial terms, enabling organizations to make better decisions, prioritize vulnerabilities and actions, and communicate effectively with leadership. RQ analyzes real-world risk, loss, and attack data and uses AI to automate cyber risk analysis and provide defensible financial impact insights. This ensures that security leaders can prioritize risk remediation for maximum impact, communicate ROI of cybersecurity investments in business terms, and understand material risk.

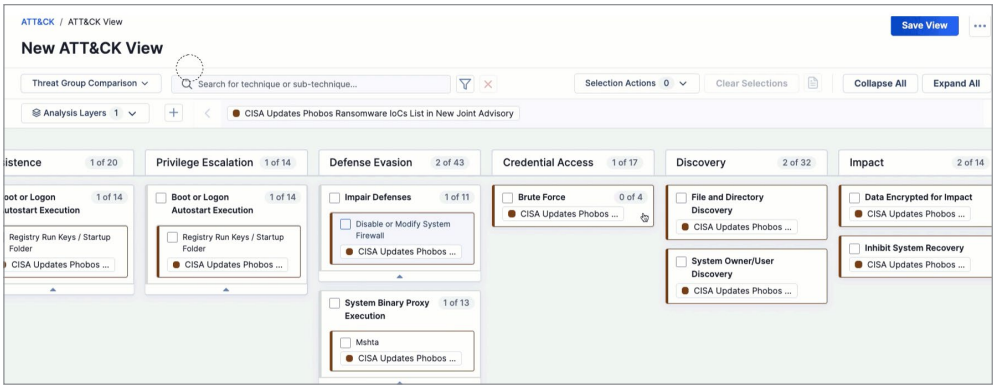


Figure 1. ThreatConnect TI Ops

- Polarity is an investigative assistant that unifies threat intelligence, context, and knowledge at the point of analysis and decision-making. It acts as a federated search, correlation, and analysis tool that scans what analysts are looking at across any application, including images or videos, using OCR to extract text and instantly search hundreds of data sources. This streamlines investigations by providing a consolidated summary view, eliminating the need to learn complex query languages, and reducing context switching and cognitive overhead for analysts (see Figure 2).

Solving Key Pain Points with ThreatConnect

ThreatConnect directly addresses the critical findings identified in the SANS SOC Survey, focusing on improving the effectiveness and retention of security teams.

The SANS survey highlights that AI/ML tools often underperform due to lack of clear ownership and poor integration into daily operations. ThreatConnect's philosophy is that AI is a tool, not an end, and they apply AI only where it can securely, safely, and effectively solve known customer problems:

- ThreatConnect uses AI to correlate and enrich data across sources, uncover meaningful relationships, and classify unstructured intelligence into consistent, structured data. This helps map intelligence to specific industries or attack techniques, making it easier for analysts to find relevant information without sifting through massive volumes of data.
- Polarity uses AI to accelerate analyst workflows by delivering quick, plain-English summaries of intelligence reports and tailoring insights for different stakeholders. Unlike traditional approaches that require direct integrations with each system, Polarity overlays any tool on the analyst's desktop, scanning what's on the screen and correlating it across dozens of intelligence sources and internal tools. This dramatically reduces cognitive load, accelerates understanding, and empowers rapid, informed decision-making right at the point of analysis.

The survey reveals a significant concern about staff retention and burnout in SOCs. ThreatConnect tackles this by focusing on capacity management, automating mundane tasks, reducing cognitive load, and empowering SOC teams to prove their value to the business in the following ways:

- ThreatConnect's highly scalable playbook automation runs in the background, handling repetitive tasks like enriching indicators or performing first-pass triage. This frees analysts to focus on more complex, fulfilling, and meaningful work, which directly contributes to job satisfaction and retention.

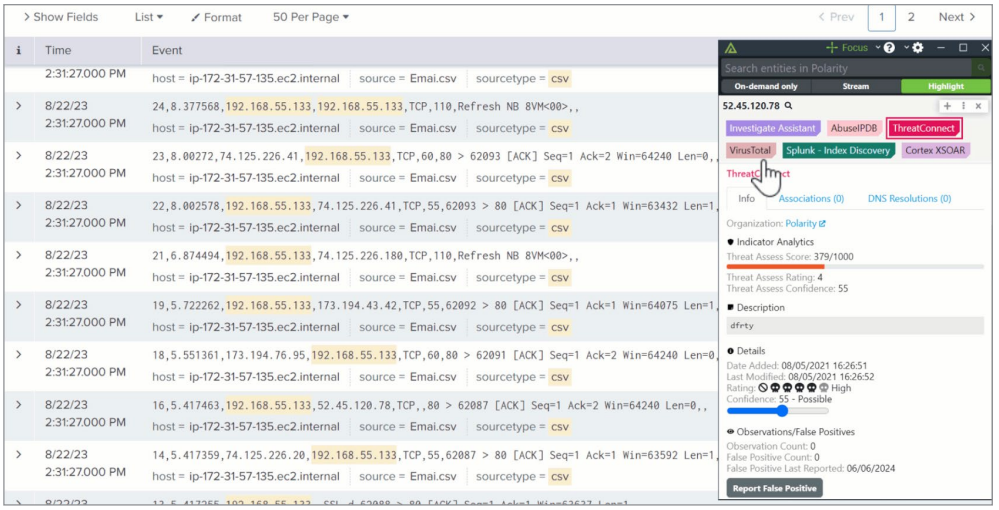


Figure 2. ThreatConnect Polarity

- Polarity directly contributes to reducing analyst burnout by minimizing context switching. Instead of navigating between multiple tools and windows, Polarity provides a single window for federated search across all data and intelligence sources, streamlining investigations and providing instant context. This drastically cuts down time on tasks and enables faster decision-making.
- ThreatConnect enables SOC teams to prove their value to the business by translating cyber risks into financial terms using Risk Quantifier. By aligning security activities and resources with business priorities, the platform helps security teams focus on threats that pose the greatest financial impact. This allows SOC teams to show tangible ROI for their efforts, which can lead to increased budget, more competitive salaries, and greater investment in the team, all contributing to better retention.

By providing relevant, high-fidelity intelligence, automating routine tasks, and enabling security teams to communicate their impact in business terms, ThreatConnect empowers defenders to proactively address threats, optimize resources, and foster a more engaged and effective workforce.