Prophet Security Research: One-Third of Security Alerts Go Uninvestigated as AI Adoption Grows

New research reveals 96% of organizations are using or evaluating AI for the SOC as AI-driven threats and analyst shortages accelerate.

LAS VEGAS AND PALO ALTO, CA, UNITED STATES, August 4, 2026 /EINPresswire.com/ -- Black Hat 2026 USA— Security operations centers are facing mounting pressure from growing alert volumes, increasingly sophisticated AI-powered attacks, and persistent staffing constraints. According to Prophet Security's Second Annual State of AI in Security Operations Report, organizations are responding by rapidly adopting artificial intelligence to automate investigations, improve response times, and give analysts more time for proactive security work.

> The organizations seeing the greatest success are using AI to investigate every alert, reduce response times, and free experienced defenders to focus on higher-value work like threat hunting."
>
> *Kamal Shah, co-founder and CEO of Prophet Security*

The independent research, conducted by ViB among 250 IT and cybersecurity professionals, illustrates a fundamental shift in how security operations centers (SOCs) are evolving. AI is no longer viewed as an emerging capability; it is becoming foundational to modern security operations as defenders race to keep pace with adversaries increasingly using AI themselves.

"Security operations has reached an inflection point," said Kamal Shah, co-founder and CEO of Prophet Security. "The challenge isn't simply that organizations want to use AI, it's that traditional security operations can no longer keep pace with today's alert volumes or AI-powered attackers. The organizations seeing the greatest success aren't replacing analysts with AI. They're using AI to investigate every alert, reduce response times, and free experienced defenders to focus on higher-value work like threat

hunting, detection engineering, and incident response."

Prophet Security's Agentic AI SOC Platform autonomously investigates alerts, accelerates incident response, performs continuous threat hunting, and optimizes detections across the full security operations lifecycle.

Security teams are overwhelmed by alert volume

The research paints a picture of security teams struggling to keep pace with today's threat landscape.

Nearly three-quarters (74%) of organizations receive more than 50 security alerts every day, while more than one-quarter receive over 500 daily alerts. The average security investigation takes approximately 75 minutes, and organizations report leaving an average of 28% of alerts uninvestigated because they lack the time or resources to review them all.

Perhaps most concerning, 60% of respondents said an alert that was never investigated later became a material security incident, exposing customer data, disrupting operations, or creating measurable business risk.

Additionally, 40% reported that their organizations have disabled—or considered disabling—detection rules because they lacked the resources to investigate the alerts they generated.

AI has become an operational necessity, not an experiment

Organizations are increasingly turning to AI to close the widening gap between growing security workloads and limited analyst capacity.

The study found that:
- 40% already use AI as part of their day-to-day SOC workflows.
- 56% are actively evaluating or piloting AI-powered SOC solutions.
- Just 4% have no plans to adopt AI.

Among organizations already using AI in security operations:
- 72% reduced alert investigation time by at least 25%.
- 18% reduced investigation time by more than 50%.
- The most common measures of success include faster mean time to respond (MTTR), improved around-the-clock coverage, fewer false positives requiring analyst review, and faster investigations overall.

Attackers are operationalizing AI as quickly as defenders

The report also finds that security teams are increasingly confronting AI-powered attacks.

More than half (56%) of respondents reported seeing an increase in AI-driven attacks during the past year, rising to 63% among financial services organizations and 58% within healthcare. The most frequently observed attack involved phishing and social engineering campaigns showing clear signs of large language model-generated content, followed by deepfake-enabled fraud and increasingly sophisticated credential attacks.

AI is reshaping analyst roles, not replacing them

Despite ongoing discussion around AI replacing cybersecurity professionals, respondents overwhelmingly expect AI to augment rather than eliminate security teams.

Fifty-seven percent expect AI to significantly reshape SOC responsibilities without reducing headcount over the next two years, while another 9% anticipate security teams will grow. Instead of replacing analysts, organizations expect AI to absorb repetitive investigation work so analysts can focus on incident response, proactive threat hunting, adversary simulation, and detection engineering.

The report reinforces that strategy. Organizations conducting proactive threat hunting weekly or continuously uncovered malicious activity their existing detection tools missed nearly half the time, demonstrating how AI-generated efficiency can translate directly into stronger security outcomes.

Organizations are becoming more selective about how they deploy AI

While adoption continues to accelerate, organizations are becoming increasingly disciplined in evaluating AI platforms.

Data privacy (44%) and AI transparency (41%) emerged as the two most significant barriers to broader AI adoption, highlighting growing demand for explainable AI systems, transparent decision-making, and deployment models that protect customer data. The research also found that nearly half of organizations attempting to build their own AI-powered SOC capabilities ultimately abandoned those efforts or replaced them with commercial platforms, underscoring the operational complexity of maintaining production-grade AI for security operations.

Access the Research
The complete 2026 State of AI in Security Operations report is available now.

About Prophet Security

Prophet Security's mission is to be a force multiplier for security teams by delivering a comprehensive Agentic AI SOC Platform that automates the manual processes across security

operations - from alert triage, investigation and incident response to threat hunting, and detection engineering. Prophet AI reduces mean time to investigate, mean time to respond, and delivers a 10x increase in team productivity.The platform reduces risk by finding and closing the gaps in your detection coverage that let attackers operate undetected. Prophet Security's investors include Accel, Bain Capital Ventures, Amex Ventures and Citi Ventures. Learn more at https://www.prophetsecurity.ai.

Kari Ritacco
RedIron PR
+1 703-928-9996
email us here
Visit us on social media:
LinkedIn
X
