NEWS RELEASE

Global State of Security Report Reveals Critical Need for Connected Security Operations

2025-05-20

- ***Security remains a key focus as organizations cautiously approach AI, with only 11% fully trusting it for mission-critical tasks***
- ***Nearly half (46%) spend more time maintaining tools than defending the organization***
- ***78% say sharing data with observability teams resolves incidents faster***

SAN FRANCISCO, May 20, 2025 /PRNewswire/ -- Splunk, the cybersecurity and observability leader, today released its "State of Security 2025" global research report, highlighting the mounting challenges faced by Security Operations Centers (SOCs). The report uncovers the pain points that mire down organizations and open their doors to threats **–** 46% of respondents said they spend more time maintaining tools than defending the organization, while only 11% trust AI completely for mission-critical tasks. Furthermore, 66% experienced a data breach in the past year, making it the most common security incident.

With new threats such as AI-powered attacks, organizations must be fully prepared and confident in protecting themselves and their customers. The common thread in addressing these concerns is to build a unified SOC that combines human expertise with AI advancements.

"Organizations are increasingly leaning on AI for threat hunting and detection, and other mission-critical tasks, but we don't see AI taking complete oversight of the SOC – for good reason," says Michael Fanning, CISO at Splunk. "Human oversight remains central to effective cybersecurity, and AI is used to enhance human capabilities to help where it truly matters: defending the organization."

"As cyber threats grow in volume and sophistication, security teams are under constant pressure," said Nate Lesser, CISO at Children's National Hospital. "According to Splunk's State of Security report, the industry is struggling with escalating workloads, alert fatigue, and a shortage of skilled talent. Integrating AI and automation helps us address these risks and empowers our teams with smarter tools to ensure our organization remains resilient."

Security teams plagued by technological inefficiencies while external threats increase
When SOC workflows aren't operating at their peak, it creates major barriers to effective threat detection and response. The report highlights areas of inefficiencies that create risk for organizations:

- 59% say tool maintenance is the main source of inefficiency
- 78% say their security tools are dispersed and disconnected
- 69% say disconnected and dispersed tools creates moderate to significant challenges

Tool maintenance, data silos, and alert fatigue bog down SOC teams. These day-to-day burdens drain valuable time and impact an analyst's ability to respond quickly and decisively. The report revealed:

- 57% report losing valuable investigation time to data management gaps
- 59% have too many alerts
- 55% have to address too many false positives

SOC analysts are overworked and understaffed
Beyond operational hurdles, the report sheds light on the immense pressure for SOC analysts. High stress levels, chronic understaffing, and burnout are taking a toll and put talent retention and long-term team stability at risk. Findings show that:

- 52% say their team is overworked
- 52% say stress on the job has prompted them to think about leaving cybersecurity altogether
- 43% face unrealistic expectations by leadership

GenAI in the SOC is paying long-term dividends for organizations
Organizations see how AI can alleviate operational and staff shortage problems, as 59% have moderately or significantly boosted their efficiency with AI. Over half (56%) have prioritized the application of AI to security workflows this year, while 1 in 3 (33%) plan to fill skills gaps with AI and automation.

Compared to publicly available tools, 63% agree that domain-specific AI significantly or extremely enhances security operations. However, AI is not running solo as organizations keep humans in the loop to deliver trustworthy AI outcomes. The top three tasks that GenAI is helping across SOCs included:

- Threat intelligence analysis (33%)
- Querying security data (31%)
- Writing/editing security policies (29%)

A unified approach accelerates operations
Minimizing tool maintenance is just the starting point for the benefits of a unified security platform. Adopting a unified approach for threat detection and response leads to tighter collaboration, bringing more context and speed to investigations. Sharing information across security and observability isn't fully embraced yet, but those who have made the leap report noteworthy advantages. Specifically, 78% of respondents cited faster incident detection, and 66% noted quicker remediation as moderate to transformative benefits.

To learn more and see the full findings, download the 2025 State of Security Report here.

Methodology
In collaboration with Oxford Economics, researchers surveyed 2,058 security leaders (including directors of security, vice presidents of cybersecurity, directors of security operations, and security analysts) October 2024 through December 2024. Respondents were in Australia, France, Germany,

India, Japan, New Zealand, Singapore, United Kingdom and United States. They also represented 16 industries: Business services, construction and engineering, consumer packaged goods, education, financial services, government (federal/national, state, and local), healthcare, life sciences, manufacturing, technology, media, oil/gas, retail/wholesale, telecom, transportation/logistics, and utilities.

About Splunk LLC
Splunk, a Cisco company, helps build a safer and more resilient digital world. Organizations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions, and accelerate digital transformation.

View original content to download multimedia:https://www.prnewswire.com/news-releases/global-state-of-security-report-reveals-critical-need-for-connected-security-operations-302460307.html

SOURCE Cisco Systems, Inc.