Why Analytics is the Key to Increasing Your Cybersecurity Resilience

With increased IT complexity, new hybrid work models, the urgent need for modernization and evolving security threats, government agencies face unprecedented cybersecurity challenges.

Agencies have employed a range of security approaches to protect their data and systems but increasing their analytics capabilities may be one of the most effective ways they can safeguard their critical infrastructure. In this Q&A, Lee Imrey, cybersecurity advisor at Splunk, a leading Data-to-Everything™ Platform that enables IT, Security & DevOps teams, shares how an analytics-driven security operations center (SOC) can help governments achieve cyber resilience.

What are the most pressing security threats today for government agencies?
Government agencies manage a growing number of critical applications in an increasingly complex environment. They face significant risks from targeted phishing attacks and ransomware, along with increasingly stringent demands from their constituents to lower costs and effectively protect their data.

What capabilities do agencies need to combat these threats, and what barriers currently prevent them from strengthening their security posture?
Agencies face a range of challenges, including the need to support both legacy and newer technologies, competing with the private sector for experienced cybersecurity professionals, and a limited appetite for proactive investments in cybersecurity.

To confront these challenges, agencies need qualified staff, proactive processes and scalable tools to manage the risks associated with their business functions. These tools should incorporate modern cybersecurity and risk-management theory, current threat intelligence and automation to enable timely response to detected threats. Employing an analytics-driven SOC can also help them strengthen their security posture.

What is an analytics-driven SOC and how does it differ from a traditional security operations center?
Traditional SOCs use a Security Incident Event Management (SIEM) solution to gather voluminous quantities of security information, apply fixed rules to flag suspicious behavior and offer standard responses to different types of attacks. An analytics-driven SOC combines the rules-based approach of a traditional SOC with the investigation-friendly approach of a purpose-built data platform. It encompasses five core capabilities: advanced analytics, threat intelligence, automation, the ability to proactively hunt and investigate, and the adoption of an adaptive security architecture.

With an analytics-driven SOC, analysts can apply advanced analytics and machine learning (ML) to different datasets, enhance the data with applicable threat intelligence and quickly pivot to explore areas of interest.

Why is an adaptive security architecture like Splunk so critical in today’s threat environment?
An adaptive security architecture enables SOC teams to correlate security-relevant data at scale, apply advanced analytics, and interact with third-party products and services to improve detection and automate remediation. This lets the analyst detect and respond to security issues more effectively, and even predict and prevent certain types of attacks and downtime.

If you were to give agencies a roadmap for how to build cyber resilience, where would you tell them to start?
Engage organizational leaders in discussions and tabletop exercises focusing on how to deliver critical services in the absence of IT systems or network connectivity, so your organization is better prepared during times of crisis. You also have to focus on your agency’s core requirements and build capabilities to resume or replace services that rely on systems that are vulnerable to cyberattacks. By being proactive and implementing a holistic security strategy, agencies can increase their cyber resilience.