IDC

ANALYST BRIEF

Sponsored by: Lumu

Security is not enough. As companies expand their digital footprint, the adversary has more opportunities to cause disruption. Continuous monitoring and operational context provide optimal protection.

Unified SecOps: A Resilience Model for an Evolving Era of Compromise

February 2026

Written by: Chris Kissel, Vice President, IDC Security & Trust

Introduction

Tool proliferation, alert fatigue, and workforce constraints are straining and fragmenting security operations (SecOps). At the same time, attackers are leveraging AI and exploiting gaps across siloed controls, raising operational complexity and risk. In response, organizations are shifting toward unified SecOps models that consolidate detection, response, intelligence, workflow, and automation into integrated operations and operating practices.

IDC research indicates that unification improves detection fidelity, speeds response through automation, and enhances resilience by reducing operational friction and enabling continuous visibility across hybrid environments. So it is no surprise that unified SecOps is becoming the next operating model — one that is driven by AI era realities, regulatory expectations for continuous monitoring, boards' demand for simplification and outcomes, and consolidation toward platforms that unify telemetry, policy, and automation.

AT A GLANCE

KEY STAT

According to IDC's March 2025 *Exposure Management Survey,* security silos and integration across different systems are the biggest challenges in developing a vulnerability prioritization and management strategy.

WHAT'S IMPORTANT

A SecOps approach requires subtle transitions. SecOps teams should move from tools to outcomes, away from silos into integrated operations, and from reactive approaches to continuous compromise assessment.

Understanding the problem

The term *SecOps* comes from two disciplines: "security" and "operations." While these concepts seem inextricably tied, in reality, they are often treated as two silos. Operations is somewhat self-explanatory, as it refers to the protocols and maintenance required to keep a network functioning. Security starts with prevention, goes through detection and response, and then ends with mitigation. If security is lagging, the results can range from adversarial theft to breaches and exposures or shuttering operations. In terms of the physical network, while security and operations are in the same boat, they do not perform the same function.

However, if there was ever a case for better together, unified SecOps it is. Unified SecOps is an operating model that converges detection, response, threat intelligence, workflow, and automation across domains (e.g., endpoint, identity, application, cloud, network) to deliver continuous, real-time visibility of compromise and orchestrated outcomes. Unified SecOps is not a product category or vendor platform, but an implementation-agnostic operating model that can be adopted on top of existing security tools. It emphasizes unified telemetry, AI-assisted analytics, automated playbooks, and closed-loop feedback between runtime and development processes.

In the next section, we will describe where security tools fall short and the role of AI for both defenders and attackers. The most important concept to understand at the moment is that to maximize security outcomes, it is necessary to maintain continuous monitoring, and this is the essence of operations.

Fragmented security operations

A general maxim is that for each digital opportunity, a new digital exposure is possible. Businesses create and deploy applications to enhance customer experience and improve employee productivity. The data and these applications may come from SaaS applications, on-premises databases, public or private cloud instances, or from IoT and OT devices. To protect each surface, there must be policies for access, data handling procedures, performance, and security monitoring. The age of AI and large language models (LLMs) will truncate the time required to search for meaningful content and synthesize data to create new correlations of data. Unfortunately, AI also gives the adversary the same machine-speed capabilities.

While there is an ongoing battle that pits lightning-fast adversarial tactics against equally quick adaptable defenses that match pace in real time, there are legacy security concerns that need to be addressed:

- **Too many tools, not enough integration:** Enterprises are limited by hybrid security architectures with too little integration; platform intention is driven by unified telemetry, but it is difficult to normalize logs and to refine meaningful alerts from multiple security appliances, applications, and surfaces.
- **High operational overhead:** Fragmented telemetry and manual triage strain security operations centers (SOCs); automation quality and real-time prioritization are now table stakes for coping with alert volumes.

Even though it is called security, security alone doesn't cut it.

- **Attacker sophistication outpacing tool-centric SOCs:** Breakout is the time that it takes for an adversary to breach a network initially and then exfiltrate data. Breakout times were once measured in weeks and now can occur in a matter of hours.
- **Talent shortages and unsustainable workloads:** Culturally, the SOC itself must change. The act of triage, in which staff perform an investigation of why an alert occurs and its severity, is still too much of a manual process (although this is improving in software). Scaling SecOps requires automation and AI-assisted workflows to reduce manual work and accelerate triage and response. The days of manual IT tickets prompting actions should be sunset.

The case for unified SecOps now

Several dynamics are in play when considering a unified SecOps approach. Perhaps the most relevant point is that AI shifts the balance of power between attackers and defenders. The attacker can generate volumes of malware through agentic AI and also create highly individualized/personalized attacks. The attacker only has to be right once; the defender has to be right every time. Regulatory pressures encourage continuous monitoring. Different jurisdictions require disclosure of breaches anywhere from three to seven days. One factor that determines a company's liability for damages is whether the company can prove it uses continuous monitoring. Last, SecOps encourages unified telemetry, correlation, and automation to reduce operational complexity and improve outcomes, especially across multicloud and hybrid estates.

Unified SecOps requires a transition from technology-centric security programs to an operations-centric security model. Table 1 describes the drivers for unified SecOps and the actions that a SecOps team can initiate.

TABLE 1: ***Drivers and action for unified SecOps***

Driver	What it means	Near-term action
AI-driven risk expansion	New attack surfaces, agentic workflows, and dynamic logic	Pilot AI-assisted correlation and investigations under governance
Regulatory pressure and compliance priority	Continuous monitoring, reporting, and board visibility	Automate compliance evidence collection and audit reporting
Platform convergence of SOAR, XDR, and CNAPP	Integrated detection/response and cloud posture	Integrate SOAR playbooks with XDR/CNAPP for unified actions
Hybrid architectures with limited integration	Telemetry fragmentation and process friction	Normalize data across domains; centralize case management
Network/infrastructure criticality	Connectivity impacting SecOps efficacy	Include network observability signals in SecOps correlation

Source: IDC, 2026

There are foundational approaches that can lead to the best SecOps outcomes. These approaches focus on operational alignment rather than tool consolidation. These are:

- **Continuous compromise visibility:** Unified, normalized telemetry and correlation deliver end-to-end visibility across hybrid cloud/multicloud, aligning SecOps to detect exposure and indicators of compromise in real time.
- **AI-assisted detection and response:** GenAI/AI enhances alert correlation, playbook generation, investigations, and response recommendations to reduce noise and accelerate actions.
- **Automation at the center:** Automated triage, prioritization, and response actions reduce mean time to detect/prioritize/respond and alleviate workforce constraints.
- **Integrated feedback loops:** Runtime signals inform earlier testing and policy, creating closed-loop security from code to cloud to operations.

Benefits

Perhaps the best way to demonstrate the advantages of unified SecOps is to match them with the desired outcomes within an SOC.

The first thing an SOC does is work through a set of alerts. Alerts are problematic because many are benign and the result of an ephemeral condition, such as a power surge or a misconfiguration. However, other alerts indicate a very serious vulnerability or an active breach. Detection and response tools are designed to help provide the necessary visibility and prioritization of alerts. But if the SOC adds operational concerns, it can improve the alert's fidelity. Along the same lines, if an SOC can establish unified telemetry ingestion and normalization across endpoint, identity, application, cloud, and the network, it can pinpoint the problem. Finally, AI-enhanced correlation and automated playbooks elevate prioritization and accelerate remediation.

Unified SecOps enhances resilience. Stronger resilience, especially versus EDR evasion, creates a closed-loop and runtime-informed detection, reducing gaps from single-control evasion; unified visibility hardens against multivector threats. An important part of resilience is the ability to build toward continuous assessment. SecOps incorporates runtime signals and compliance automation for persistent risk and posture management.

The reality is that traditional SOCs are task oriented, and many of these tasks are manual. Automation and AI reduce repetitive tasks, enabling analysts to focus on high-value investigations. Consolidated telemetry and workflow automation help cut manual triage and integration overhead.

Considerations

While there is a better approach to SecOps, there are also potential roadblocks along the way:

- **Normalization of data and processes:** Security point products often use different application programming languages (APL). In security, connectors or SDKs often exist to help with normalization. Still, latencies or missed communications can occur even in the most cohesive environments.
- **Lack of in-house talent to help facilitate unified SecOps:** Every now and then, custom code may be required, someone must develop automations or filters, and other policy hierarchies need to be created. While unified SecOps may be desired, the reality is that hidden costs such as professional services may occur.
- **Technical debt and cultural adaptability:** Any new tooling requires that people spend time on training. While many security processes are manual and often tedious, they are nonetheless repeatable and accountable. To move from security to SecOps, there will need to be a learning curve.

Conclusion

Unified SecOps is emerging as the dominant operational model. Early adopters will gain efficiency, resilience, and clarity while aligning the executive board's focus on business outcomes with regulatory realities and AI era risks. Unlike detection-centric or platform-driven approaches, unified SecOps focuses on how security teams operate, not on replacing existing security technologies. The future SOC is defined by simplicity, visibility, and automation, with unified

telemetry, AI-assisted analytics, and closed-loop feedback delivering continuous compromise assessment and orchestrated outcomes across hybrid environments.

About the analyst

Chris Kissel, *Vice President, IDC Security & Trust*

As the global lead analyst in the cloud-native XDR and security AI analytics domain, Mr. Kissel covers several domains, including threat intelligence, NDR, XDR, security automation/SOAR, and security agentic AI use cases. In addition to technologies, his studies also include adjacent considerations such as SOC management, compliance, and the regulations that affect product development.

MESSAGE FROM THE SPONSOR

Lumu helps organizations optimize security operations by enabling a unified approach to detecting and responding to confirmed compromise in an evolving threat environment. Its compromise-driven assessment and response model provides unified visibility across network, endpoint, identity, cloud, and email activity to confirm real incidents and reduce uncertainty during investigations. By integrating with existing security and IT tools, Lumu supports faster threat validation, automated response workflows, and evidence-based decision making across distributed environments. Organizations use Lumu to improve operational efficiency, reduce time to containment, and increase confidence in their security execution across the enterprise.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com