Enterprise Strategy Group | Getting to the bigger truth.™

TOWARD SECURITY OPERATIONS PROCESS AUTOMATION

Security operations can be complex, requiring highly skilled professionals and detailed processes. To overcome these issues, security teams tend to deploy an array of security analytics tools and technologies to collect, process, analyze, and act upon growing volumes of security telemetry. Despite this investment, however, many organizations continue to find it difficult to manage cyber-risk or detect and respond to cyber-incidents. To address these challenges, security operations teams are moving toward process automation and orchestration.

The security operations landscape continues to grow in complexity.

External adversary and internal IT changes have ramifications on security operations.

63%

of respondents said cybersecurity analytics/operations **is more difficult today than it was 2 years ago.**

MOST COMMON DRIVERS OF INCREASED CYBERSECURITY ANALYTICS AND OPERATIONS COMPLEXITY

- 41% — The threat landscape is evolving and changing rapidly
- 35% — We collect and process more security data today than we did two years ago
- 34% — The volume of security alerts has increased over the past 2 years
- 30% — The attack surface has grown over the past two years
- 29% — It is difficult to keep up with the operational needs

Top security operations challenges rooted in transitioning from reactive to proactive positions.

Keeping up with the expanding threat landscape and overwhelming alerts volume are the most common issues.

TOP SECURITY OPERATIONS CHALLENGES

- 27% — Monitoring security across a growing attack surface
- 23% — Keeping up with the volume of security alerts
- 22% — The cybersecurity team at my organization spends most of its time fire fighting
- 22% — Detecting/responding to security incidents
- 21% — Investigating security incidents

Security operations process automation is gaining momentum.

The emphasis on these efforts is bridging security and IT operations.

65%

of respondents **have already deployed technologies designed for security analytics and operations automation and orchestration.**

TOP USE CASES FOR SECURITY OPERATIONS AUTOMATION AND ORCHESTRATION

- 35% — Integrate security tools with IT operations systems
- [redacted] — Improving collaboration between security and IT operations staff
- 29% — Automate remediation tasks without involving IT operations
- 28% — Tracking the security event lifecycle from discovery through remediation
- 26% — Providing the capabilities for "hunting" activities

The Bigger Truth

Security operations requirements are diverse and rapidly changing. Organizations must keep up with dynamic cyber-threats across a growing attack surface, including public cloud infrastructure and new device types. Using disconnected point tools, manual processes, and a SOC team with limited personnel and skills is no longer sustainable. CISOs must address SOC deficiencies by assessing processes, identifying bottlenecks, and automating/orchestrating processes. By doing so, security operations teams can improve security efficacy, streamline security operations, and enhance staff productivity.

LEARN MORE

Source: ESG Research Report, *The Rise of Cloud-based Security Analytics and Operations Technologies*, December 2019.