Accelerate threat detection and response services with generative AI

Reduce noise, increase accuracy and respond faster to threats in your security operations center

Security operations centers (SOCs) face a daunting challenge in identifying and manually investigating threats. With the rapid increase in cyberattacks and limited resources to counter them, analysts struggle with the sheer volume of alerts, often resulting in false positives, delayed response times and compromised incident response. This approach can lead to burnout, decreased accuracy and increased risk of missing critical threats.

IBM Security Services offers cybersecurity assistant capabilities that are designed to offer better intelligence on operational questions and augment SOC analyst research. When an analyst asks a question, the generative AI (gen AI) engine automatically triggers relevant actions to provide more context to potential threats. It also explains complex security events and commands. The analyst then validates suggestions and recommends remediation. With this automation, clients receive a more unified experience, reduce noise, increase efficiency and empower analysts to focus on high-priority tasks.

IBM Threat Detection and Response services can auto-disposition or remediate up to 85% of alerts for clients, and the new gen AI capabilities empower analysts to investigate the remaining 15% of alerts even faster.[1]

The threat investigation capability cross-correlates historical alerts and insights across security information and event management (SIEM) networks, endpoint detection and response (EDR), vulnerabilities and other telemetry data.

This capabilities provide automatic, AI-driven actions based on patterns of the attackers' activity to reduce their dwell time. By automating routine tasks and augmenting analyst capabilities, you can reduce the investigation time, enabling an accurate threat response for clients.

IBM Security Services can help reduce investigation time by providing intelligence on operational questions, automating tasks, explaining complex security events and enabling faster threat investigations. How can your organization benefit from faster threat response?

→ Request a complimentary threat management workshop
→ Learn more about IBM Threat Detection and Response Services

1. Based on IBM's experience. Individual results may vary.