WHITE PAPER

Generative AI in Security Operations

Incorporating Artificial Intelligence into Security Tools and Workflows

Executive Summary

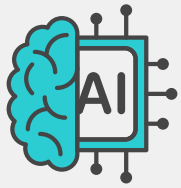
The cybersecurity landscape is rapidly evolving, characterized by increasingly sophisticated threats and a growing volume of attacks. Security operations (SecOps) teams face immense pressure to efficiently identify, investigate, and respond to these threats. Generative AI (GenAI) offers a transformative opportunity for SecOps teams to enhance decision-making, streamline operations, and improve the organization's overall security posture. By leveraging GenAI as a complementary tool within a cybersecurity platform, organizations can address key challenges such as alert fatigue, staffing shortages, and the need for rapid threat response.

Persistent Cybersecurity Challenges

Many cybersecurity challenges persist because organizations rely on outdated or poorly integrated tools and processes. Traditional security measures often can't adapt to the sophisticated tactics attackers use. The absence of a deeply integrated cybersecurity platform or security fabric creates gaps in coverage that attackers can exploit. By using advanced technologies like GenAI to enhance their capabilities, SecOps teams can take a more cohesive and adaptive approach to overcome these challenges.

The Role of GenAI in SecOps

Generative AI is revolutionizing many industries, including cybersecurity. In SecOps, even though tools like security information and event management (SIEM) systems handle collecting and analyzing vast amounts of data to identify patterns and anomalies, GenAI significantly enhances this process. GenAI can help analysts decipher complex data, provide best practices, and execute actions. GenAI facilitates a more intuitive and efficient workflow, enabling analysts to use natural language to interact with systems, quickly obtain relevant information, and receive guidance on the best course of action. Because artificial intelligence (AI) can prioritize alerts based on potential impact, it is crucial in environments overwhelmed by alert volumes. It can help with resource allocation and improve an organization's overall security posture.



By 2027, generative AI will contribute to a 30% reduction in false positive rates for application security testing and threat detection.[1]

The weaponization of AI is adding fuel to an already raging threat landscape. Ransomware activity was 13 times higher at the end of the first half of 2023 than at the start of the year, intensifying the need for advanced AI defenses.[2]

Implementing GenAI in SecOps

Integrating GenAI into SecOps involves embedding AI capabilities into security tools and workflows. This seamless integration can allow analysts to interact with the AI through their standard interfaces. The AI should support multiple sources, including central management and analytics tools, SIEM systems, threat intelligence platforms, and security orchestration automation and response (SOAR) solutions.

To maximize GenAI's benefits, organizations should train AI solutions with relevant data and continuously update it with new threat intelligence. This ongoing learning process ensures the AI tool can effectively identify and respond to emerging threats. It is crucial to establish clear protocols for how analysts should interact with the AI solution and ensure they understand its capabilities and limitations. Integrating GenAI into an existing security infrastructure allows for more cohesive and efficient operations. Because GenAI handles routine tasks and provides real-time assistance to analysts, it can improve SecOps efficiency in several ways.

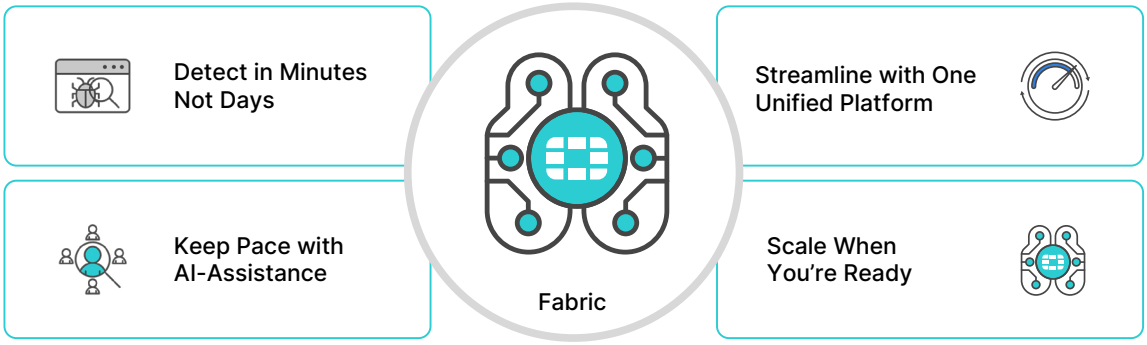


Figure 1: Unify threat response with help from AI.

Addressing staffing shortages and streamlining operations

Staffing shortages and burnout are significant challenges in the cybersecurity industry. With limited qualified professionals available and more work to go around than analysts, organizations often struggle to build and maintain effective SecOps teams. GenAI helps augment the capabilities of existing staff and reduces the dependency on highly specialized skills. GenAI enables security teams to operate more efficiently by automating routine tasks and providing actionable insights. Analysts can spend less time on manual data analysis and more on strategic decision-making and incident response.

Simplifying processes through GenAI also allows less experienced analysts to perform tasks that previously required senior-level expertise. This democratization of skills helps bridge the gap created by staffing shortages and ensures that the security team can maintain a high level of performance even with limited resources. GenAI alleviates the burden of high alert volumes and constant threat response pressures, reducing security analyst burnout.

By automating repetitive tasks and providing clear, actionable recommendations, GenAI allows analysts to focus on more engaging and rewarding aspects of their work, thereby improving job satisfaction and morale. The ease of interacting with GenAI using natural language reduces frustration and enhances productivity, enabling analysts to swiftly obtain necessary insights and guidance without navigating complex interfaces or extensive documentation.

Simplifying and accelerating complex threat investigations

GenAI plays a crucial role in simplifying and accelerating complex threat investigations. Traditional threat investigation processes can be time consuming and labor intensive. Often, analysts must manually investigate and correlate data from multiple sources and piece together the sequence of events. GenAI, with data management and analytics tools, automates much of this work by rapidly analyzing large datasets, identifying relevant patterns, and providing a coherent narrative of the incident. For example, GenAI can assist in generating reports on the top incidents over the last 30 days. This task would typically be resource intensive if performed manually, but this GenAI capability saves time and ensures analysts can quickly access critical information and focus on high-priority tasks. GenAI can help with these tasks:

- **Analyze alerts:** By examining alerts and logs, GenAI can generate detailed incident summaries, highlighting key aspects such as attack vectors, affected systems, and potential impact.
- **Correlate data:** GenAI can correlate information from various sources, including SIEM, threat intelligence, and endpoint data, to provide a comprehensive view of the incident.
- **Generate reports:** GenAI can generate reports, such as a summary of the top incidents in the last 30 days, which would otherwise be a manual process that drains resources.
- **Provide recommendations:** Based on the analysis, GenAI can suggest specific actions for containment, remediation, and further investigation, helping analysts make informed decisions quickly.

These capabilities speed up the investigation process, improve accuracy, and help reduce the potential for critical details to be overlooked.

Reducing mean time to detect and respond

One of the most critical metrics in SecOps is the time it takes to detect and respond to threats. Reducing mean time to detect (MTTD) and mean time to respond (MTTR) is essential for minimizing the impact of security incidents. GenAI helps reduce MTTD and MTTR by providing real-time analysis and recommendations that support the investigation process. With GenAI, alongside a security team's detection capabilities, analysts can quickly identify potential threats and understand their context without spending resources on false positive investigations. An AI solution can analyze historical data, identify patterns, and predict the potential impact of an incident. A proactive approach can result in faster detection and more informed decision-making during the response phase. By automating parts of the investigation and response processes, GenAI helps reduce the time required to remediate incidents and ultimately enhances an organization's resilience against cyberthreats.

Maximizing existing investments

Implementing GenAI in SecOps can also help organizations maximize their existing investments in security infrastructure. Organizations can enhance their capabilities by integrating GenAI with current tools and platforms without requiring extensive resources. GenAI can work with existing central and analytics management tools, SIEM systems, SOAR solutions, and threat intelligence platforms to provide deeper insights and more effective threat responses. Implementing GenAI can improve the return on investment for existing tools and help organizations leverage their security infrastructure's full potential. GenAI can help SecOps teams achieve better outcomes while controlling costs.

The Future of Security Operations

GenAI holds significant promise for transforming security operations. By enhancing decision-making, streamlining workflows, and improving productivity, GenAI addresses some of the most pressing challenges faced by SecOps teams today. As organizations continue to integrate AI into their security operations, they can expect to see improvements in their ability to detect, respond to, and mitigate threats, ultimately leading to a more secure and resilient cyber environment. The future of SecOps will undoubtedly be shaped by advancements in AI technology, driving more proactive and efficient security measures. By staying ahead of the curve and embracing GenAI, organizations can remain robust and agile in the face of evolving cyberthreats.

[1] Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook, Gartner Research, "4 Ways Generative AI Will Impact CISOs and Their Teams," ID G00793265, June 29, 2023.

[2] Fortinet, "Cyberthreat Predictions for 2024: An Annual Perspective from FortiGuard Labs," November 7, 2023.

July 16, 2024 10:25 AM / 2757450-0-0-EN