

SHOWCASE

A Proactive Approach to Generative AI for Cybersecurity

By Jon Oltsik, Distinguished Analyst and Fellow
Enterprise Strategy Group

January 2024

Abstract: Generative AI for cybersecurity is new, confusing, and somewhat scary for many infosec professionals. While this might be true, it also has great potential to help organizations improve threat detection and response, automate processes, augment staff, and mitigate risks. CISOs should remain open-minded, explore generative AI use cases, and select vendor partners with the right frameworks, large language models, coverage, and functionality.

Overview

Organizations face several simultaneous and difficult cybersecurity trends:

- **Increasing threats.** Enterprises face a rise in threat volume and sophistication—especially from nation-state and cybercriminal “apex attackers.”
- **Cyber workforce shortage.** According to [new research](#) from TechTarget’s Enterprise Strategy Group and ISSA International, 71% of organizations claimed they are affected by the cybersecurity skills shortage, leading to increasing workloads, open job requisitions, and employee burnout and attrition. Beyond staffing, many organizations lack advanced security skills in areas such as threat intelligence analysis, cloud security, and threat hunting—all increasingly necessary for risk mitigation and timely threat detection.
- **Hybrid IT support.** Threat detection and response capabilities over multi-cloud, distributed, and hybrid IT infrastructures require expertise, process automation, and orchestration across an army of associated security technologies. Many practitioners cite complexity as the No. 1 reason for job difficulty.

These trends only exacerbate other security operations challenges cited by Enterprise Strategy Group survey respondents (see Figure 1).¹ The following are the top three obstacles these organizations said they currently face:

- **Constant firefighting.** Security operations teams, often understaffed to begin with, are overwhelmed by critical alerts and high-priority remediation activities. As a result, the security operations center (SOC) team is continually stressed and never has time for process or strategic improvement, which can result in burnout. Increasing threats will add more fuel to the perpetual emergency mode fire.
- **Monitoring security across a growing attack surface.** Security teams are being asked to monitor security hygiene and respond to threats across environments made of remote user systems, cloud-native applications, SaaS providers, and third-party partners, resulting in a growing attack surface. Many enterprises regularly discover tens of thousands of vulnerabilities but struggle to triage and prioritize their highest risks. It is especially difficult for security teams to work with IT operations and software developers to prioritize and take the necessary remediation actions.
- **Operationalizing threat intelligence.** The task here is to transform raw information into blocking rules, threat hunts, and strategic decisions. Many organizations don’t have the right skills or processes to do this at scale. This is especially true given the increase in threat volume and sophistication combined with the impact of the skills shortage.

Clearly, security teams are getting buried by the volume and pace of modern cybersecurity requirements. The status quo won’t do, so CISOs must add scale, intelligence, and automation to their security programs as soon as possible.

¹Source: Enterprise Strategy Group Complete Survey Results, [SOC Modernization and the Role of XDR](#), September 2022.

Figure 1. Common Security Operations Challenges

Which of the following would you say are your organization’s current, primary security operations challenges? (Percent of respondents, N=376, three responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Generative AI to the Rescue?

To address the challenges described above, security technology vendors are introducing generative AI capabilities as part of security products and services, positioning them as assistants for improving security efficacy, operational efficiency, and staff productivity.

Some security professionals remain skeptical, citing potential issues with false positive results, data leakage, privacy, and hallucinations. Furthermore, AI systems used by organizations for other purposes are not foolproof. These can be manipulated by attackers through poisoning, creating new attack vectors that security tools might not detect.

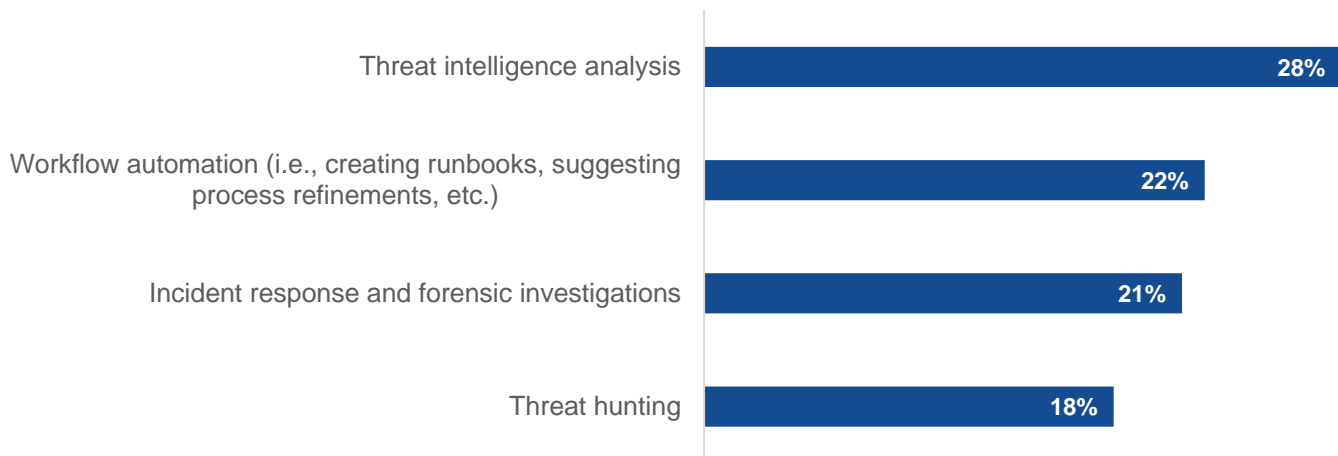
Security professionals should remain diligent and weigh generative AI risks, as these are legitimate concerns. Nevertheless, Enterprise Strategy Group encourages organizations to be open-minded about generative AI’s potential for cybersecurity, keeping mindful of risk while finding solid cybersecurity use cases. According to new research, many security professionals said they believe generative AI can help their organizations address their most difficult cybersecurity challenges. See Figure 2 for some of the top use cases cited for generative AI,² including the following:

²Source: Enterprise Strategy Group Complete Survey Results, [Beyond the GenAI Hype: Real-world Investments, Use Cases, and Concerns](#), August 2023.

- **Threat intelligence analysis.** Generative AI can be used to synthesize mountains of threat intelligence data into customized reports on threat actors, campaigns, and the tactics, techniques, and procedures used in targeted attacks on industries, regions, and their organization itself. This can help organizations operationalize threat intelligence toward mitigating cyber-risks and accelerating incident response. Threat intelligence analysis is a particularly resilient use, independent of common generative AI risks.
- **Workflow automation.** Upon a security alert, generative AI can piece together an entire kill chain, reference the Mitre ATT&CK framework, or suggest next steps. This can help organizations improve the productivity of understaffed security teams that might also lack some advanced skills. This is especially important to cope with the growing attack surface and align with DevOps continuous integration/continuous delivery automation processes.
- **Incident response and forensic investigations.** Generative AI can potentially help organizations accelerate the time from threat detection to response and recovery. How? By correlating events, reverse-engineering malware, piecing together an attack timeline, calculating the blast radius of attacks, and automating response actions (e.g., quarantining a system, blocking a network connection, etc.). These capabilities can help improve the accuracy and efficiency of security technologies and processes. There is also a desire for generative AI to assist with “natural language to query language” translation, as this can help SOC analysts conduct investigations and create new detection rules without the need for specialized knowledge of query language syntax. This, in turn, can enable new employees to ramp up and have impact more quickly.
- **Threat hunting.** Based on threat intelligence, generative AI can provide another low-risk use case by proactively looking for indicators of compromise or similar malicious behavior. Organizations employing threat hunters can accelerate their processes while those lacking this ability get generative AI assistance. Once again, this can help mitigate cyber-risks or minimize the impact of a cyber attack, adding to digital resilience with a low-risk/high-return use case.

Figure 2. Top Security Use Cases for Generative AI

For which of the following security use cases is your organization using or planning to use generative AI? (Percent of respondents, N=260, three responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Generative AI also can help organizations uncover new attack vectors that can be used to test the security of systems and networks, such as simulating attack paths to uncover vulnerabilities. This can help CISOs continuously assess and improve their cybersecurity programs.

CISOs and Security Practitioners Should Take a Proactive Approach to Generative AI

Enterprise Strategy Group believes generative AI has the potential to improve the efficacy and efficiency of security programs. Therefore, CISOs should do all they can to understand how generative AI works, determine its potential use cases, and investigate which vendors to choose as strategic partners. To maximize benefits while avoiding industry hype, CISOs should consider the following best practices:

- **Establish departmental guidelines.** Build a departmental governance model and train staff accordingly. This should include establishing policies, instituting controls for policy enforcement, and monitoring activities. A reference model—such as [Google's Secure AI Framework](#), a set of general guidelines for secure AI deployment—can help guide CISOs toward organizational best practices for safeguarding generative AI adoption and use.
- **Encourage experimentation and defined use cases.** While it's important to understand the limitations of generative AI, CISOs must start by emphasizing preliminary guardrails and training, and then push the cybersecurity team to play with available tools and models. As this transpires, security teams would benefit by promoting collaboration, communication, and feedback so the security team can educate themselves and learn what works in their environments. Beyond experimentation, it's worth choosing a few use cases, such as threat intelligence analysis or detection engineering, to test how generative AI can bolster efficiency, reduce complexity, and improve productivity in specific areas.
- **Schedule meetings with strategic partners.** Many security vendors have announced generative AI functionality, released products to market, or laid out future roadmaps. CISOs should take a hands-on approach by scheduling meetings with internal legal teams and external strategic partners. Security engineers and architects should participate in this process and report on their analysis. The goal here is to make sure that new generative AI offerings align with and support enterprise security programs and future plans, such as technology consolidation, SOC modernization, and zero-trust initiatives, among others.
- **Consider an AI red team.** Static risk assessments won't be adequate for generative AI. While this might be a very high bar, it can be worthwhile to establish continuous testing via a dedicated AI red team. This team should be composed of traditional ethical hackers with appropriate AI knowledge and skills. Organizations lacking the skills and staffing here should seek out managed services experts with AI proficiency. At the very least, AI red teaming should be part of initial generative AI use within cybersecurity and across the organization, involving others such as IT operations and software development.
- **Evaluate and choose vendors.** While it can be difficult to make choices, Enterprise Strategy Group recommends that CISOs select vendors based on their skills, track records, security-focused large language models, transparency, and support. Yes, it's always wise to do perform due diligence on vendors, but leading vendors will have checks and balances in place to safeguard generative AI while making it a compelling and value-added addition to existing security technologies.


©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com

 www.esg-global.com