IDC Analyst Brief, sponsored by SCC
March 2024

Integration of AI in Cybersecurity Operations: The Future-Ready MSSP

Romain Fouchereau
Research Manager
European Security, IDC Europe

Richard Thurston
Research Manager
European Security Services, IDC Europe

Joel Stradling
Research Director
European Security, IDC Europe

Integrating AI in Cybersecurity Operations: The Future-Ready MSSP

Introduction

The use of artificial intelligence (AI) is transforming cybersecurity, and U.K. organizations are increasingly leveraging its capabilities in security operations centers (SOCs). According to IDC's *European Security and Technology Survey, 2023*, 69% of organizations in the U.K. acknowledge the significant improvements AI brings to automating security operations, confirming growing interest in AI-driven solutions in the kingdom.

Selecting the right managed security service provider (MSSP) has thus become critical. Organizations must assess MSSPs' abilities and strategies regarding the use of AI technologies in their services.

AT A GLANCE

KEY TAKEAWAYS

- When selecting MSSPs, U.K. organizations should prioritize AI-enabled partners that offer advanced security capabilities, predictive analytics, and automated threat response mechanisms.
- Proactive AI integration not only enhances cybersecurity operations but also addresses skills shortages by augmenting existing SOC teams with AI tools and automation.
- Adopting AI-driven strategies and solutions is essential, as it enables organizations to effectively detect, respond to, and mitigate cybersecurity risks.

State of AI in SecOps

The current threat landscape is very dynamic and evolving fast, with cyberthreats continuing to increase in sophistication and frequency. Organizations are turning to AI to strengthen their security operations (SecOps) capabilities, enabling them to adapt and respond quickly.

The adoption of AI in SecOps is driven by the need for enhanced fast threat detection and response and by the growing complexity of cybersecurity. While AI presents opportunities for innovation and efficiency, it also brings challenges. AI poses both a threat, as a weapon to enhance or accelerate cyberattacks, and a promise, as a tool to augment and extend the capabilities and capacity of security teams. IDC's *EMEA Security Services Survey, 2023* revealed that 61% of U.K. organizations believe malicious actors using AI to build smarter cyberattacks pose a significant threat to their cyberdefenses, indicating a need for proactive measures to counter evolving threats.

Looking ahead, AI in SecOps holds much promise, particularly in areas such as predictive analytics, automation, and proactive threat mitigation. By leveraging AI, organizations can anticipate and respond to threats in real time, significantly improving their cybersecurity postures.

According to IDC survey data, the top 2 ways in which AI will improve the cybersecurity of the organization in the U.K. are:

- Faster detection and response to threats (44%)
- Transformation of the cybersecurity function (41%)

The adoption of AI in security information and event management (SIEM), security orchestration, automation, and response (SOAR), and SOC provides such benefits as improved threat detection accuracy, reduced response times, and greater operational efficiency.

The U.K. government has a supportive stance on AI innovation, which as significant implications for cybersecurity regulations. Given that policymakers encourage the development and adoption of AI, regulations will likely evolve to facilitate the responsible and ethical use of AI in cybersecurity.

AI in SOC Operations: Efficiency, Skills, and Trust

Integrating AI into SOC operations is transformative. AI technologies bring new benefits, including enhanced operational efficiency, skill augmentation, and digital trust in AI-powered actions.

Operational Benefits

The use of AI is transforming conventional threat detection and response approaches. With AI-powered algorithms, SOC teams can analyze large volumes of data in real time to find patterns and indications of malicious activity that might otherwise go unnoticed. These enhanced analytics capabilities enable organizations to identify and mitigate new threats proactively and enhance overall security posture. The automation of repetitive and menial tasks simplifies SOC operations, allowing analysts to focus their efforts on higher priority tasks that require human intervention. This accelerates incident resolution but also reduces the risk of alert fatigue, ensuring that critical threats are addressed promptly and efficiently.

AI integration enables security measures that are flexible and can adapt to changing threats. By learning from past incidents and adjusting to new attack methods, AI-powered SOCs can stay one step ahead of adversaries, keeping their organizations safe.

AI integration in SOCs enables organizations to achieve better outcomes faster. AI delivers advanced analytics, automation, and adaptive capabilities to SOC teams, enabling them to strengthen their defenses, mitigate risks faster, and protect critical assets more efficiently.

Addressing Skills Gaps

Demand for skilled security professionals continues to outpace supply, and AI technologies play a crucial role in addressing skills gaps within SOC teams by augmenting human capabilities with advanced analytics and automation. According to IDC survey data, only 11% of U.K. organizations have sufficient SOC analyst skills. AI tools enable SOC analysts to process security data more effectively, identify emerging threats proactively, and allocate resources strategically.

Working together, AI and human analysts strengthen SOC teams, making them better at reducing cyber-risks.

Trust in AI

Gaining trust in how AI algorithms work is central to achieving trust in AI-driven actions. Organizations should focus on being clear and honest about how AI makes decisions, keeping humans involved in key security tasks, and following ethical and regulatory rules. Such an approach will help to build confidence in AI actions, reducing worries about bias and privacy. Partnering with an MSSP can remove concerns, as organizations rely on the expertise of the MSSP to manage AI integration and operations, reducing the responsibility on internal resources and ensuring a simplified and more effective cybersecurity approach for deployment and integration.

IDC FutureScape: Worldwide Future of Trust 2024 Predictions — European Implications

According to research study *IDC FutureScape: Worldwide Future of Trust 2024 Predictions — European Implications* (IDC #EUR251753624), by the end of this year, 30% of large European companies will have deployed GenAI on first-party data in their SOCs. AI deployments in SOCs elevate analysts' capabilities and address concerns around hallucinations, bias, privacy, and reinforced learning.

The emergence of GenAI has accelerated the use of advanced AI technologies to enhance SOC capabilities and safeguard organizations against cyberthreats. By using GenAI's capabilities for threat detection, analysis, and response, U.K. organizations can strengthen their cybersecurity defenses and adapt more effectively. U.K. organizations must assess their readiness to adopt GenAI and capitalize on its potential to strengthen their cybersecurity postures.

Selecting a Forward-Thinking MSSP

When evaluating MSSPs, considering their approach to the adoption of AI technologies is important. An MSSP with a clear vision to integrate AI-driven solutions into its services will offer enhanced capabilities to address cybersecurity challenges. Such a vision should include the development of strategic road maps for AI implementation and investments in advanced threat detection capabilities, automated response capabilities, and predictive analytics tools.

The forward-thinking MSSP will engage with AI experts and collaborate with leading AI technology providers to be better positioned to leverage AI effectively in security operations. IDC's *Security Services Survey* findings reveal that 46% of U.K. organizations consider generative AI capability to be a very important or extremely important criterion when choosing a cybersecurity services provider, reflecting growing demand for advanced AI technologies in enhancing cybersecurity.

Organizations should also assess MSSPs based on their ability to customize AI-powered solutions to meet specific needs. MSSPs that offer flexible service options, scalable AI platforms, and personalized threat intelligence feeds tailored to the industry and specific business requirements of organizations will provide valuable support in enhancing cybersecurity posture.

MSSPs that offer AI-powered cybersecurity chatbots as part of their managed services will help organizations to access advanced threat intelligence and incident response capabilities without big internal teams. Chatbots that use GenAI and large language models can be tailored to meet clients' specific security needs and can provide real-time support to boost SOC efficiency.

By partnering with forward-thinking MSSPs that prioritize AI integration, organizations can benefit from advanced security capabilities and proactive threat detection, contributing to improved cybersecurity readiness and resilience to emerging threats.

Conclusion

IDC believes that proactive AI integration is crucial for improving cybersecurity operations. By leveraging AI technologies, organizations can stay ahead of emerging threats, detect anomalies in real time, and respond rapidly to security incidents. When seeking an MSSP, U.K. organizations should select a partner that can demonstrate a clear understanding of AI's role in cybersecurity. AI-enabled MSSPs offer advanced security capabilities, predictive analytics, and automated response mechanisms, contributing to more effective threat mitigation and incident management. To keep pace with evolving cyberthreats, organizations must adopt AI-driven strategies and solutions. Prioritizing proactive AI integration and strategic AI adoption in MSSP selection will result in an ability to effectively detect, respond to, and mitigate cybersecurity risks.

About the Analysts

Romain Fouchereau, Research Manager, European Security, IDC Europe

As research manager for IDC's European Security group, Romain Fouchereau has a specific focus on network security and security technologies linked to the extended enterprise, such as IoT, edge, and IT/OT convergence. Romain closely monitors the development, evolution, and market penetration of these technologies and the approaches vendors are taking to stimulate adoption, at both channel and end-user levels. Romain Fouchereau manages the IDC Security Appliance Tracker for Europe and co-leads the European Future of Operations practice.

Richard Thurston, Research Manager, European Security Services, IDC Europe

Richard Thurston leads IDC's European Security Services program. Richard has more than 20 years' experience in the technology sector, working as a journalist and an analyst (including in IDC's Infrastructure and Telecoms team), for U.K. regulator Ofcom, and in research, insight, and thought leadership roles for cybersecurity and communications service providers.

Joel Stradling, Research Director, European Security, IDC Europe

As research director for IDC's European Security practice, Joel Stradling leads the content and analyst team that tracks the European security segment. Joel's focus areas are zero trust network architecture, managed security services, and cyber risk and resilience. Joel has 22 years' experience as an analyst of cybersecurity, international managed enterprise networks, and IT services. Joel Stradling is a regular speaker at major industry conferences, covering such topics as security and privacy, digital trust, and managed security services in business-to-business enterprise services.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data, and marketing services company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.