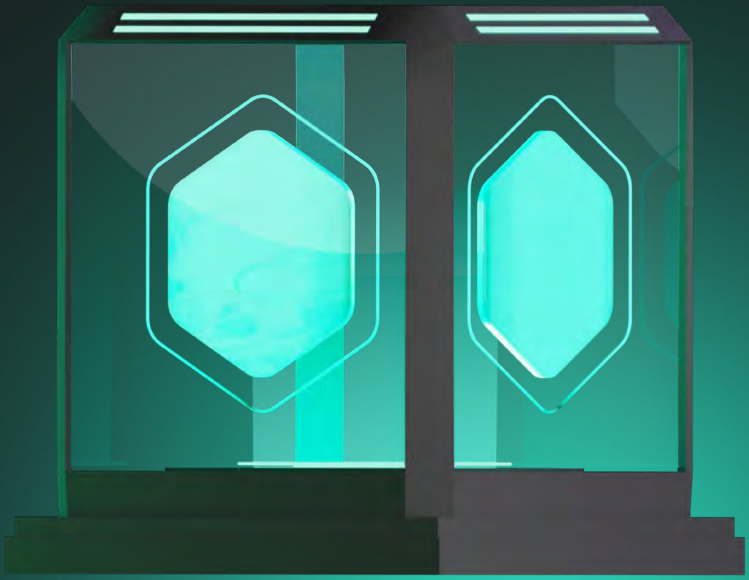
kaspersky

Overcoming SOC challenges with AI



Overcoming SOC challenges with AI

AI has become an indisputable force multiplier. A single developer can orchestrate a swarm of AI coding agents working on multiple tasks, while marketing professionals can work on strategy as they wait for Deep Research tasks to finish to provide necessary background. Cybercriminals, however, have also taken note, and the number of cyberattacks is rising. Low-level criminals are launching attacks that were previously far above their capability, while APT-level groups are automating entire parts of their workflows.

For enterprises, this means that the cybersecurity workforce should harness the power of AI too. Luckily, this doesn’t mean that they should rush to hire data scientists, who can be as hard to come by as security operations center (SOC) analysts, if not harder. On the contrary, it means that cybersecurity vendors – if they want to stay competitive – must integrate AI technologies, from tried-and-true machine learning algorithms to cutting-edge generative AI (GenAI) tools.

Cutting through noise

The first challenge that AI solutions can help with is the overwhelming amount of noise facing modern SOCs. Large modern infrastructures used by real people generate lots of potential alerts that eat away analysts' precious time, leading to burnout and increasing the risk of a genuine threat slipping through.

One example is someone logging in to a corporate PC from an unusual place: is this a hacker who has usurped an admin account or just a sales manager checking something on a business trip? In a moderately big company, it is impossible to manually verify them all. This is where AI comes to the rescue. Special algorithms, such as those used in Kaspersky MDR and being introduced to Kaspersky SIEM and XDR, will help to find those cases where the pattern is broken and that require immediate attention.

Another example is threat intelligence (TI). An analyst working with TI might need to sift through a dozen sources in different languages to understand whether a particular indicator of compromise (IoC) – say, a suspicious web address – presents a threat to the company. By integrating GenAI solutions such as Kaspersky Threat Intelligence Portal, an analyst can understand this data as actionable information; for example, what cybercriminal gang is associated with an IoC and what industries are being targeted. This expedites the decision-making process greatly.

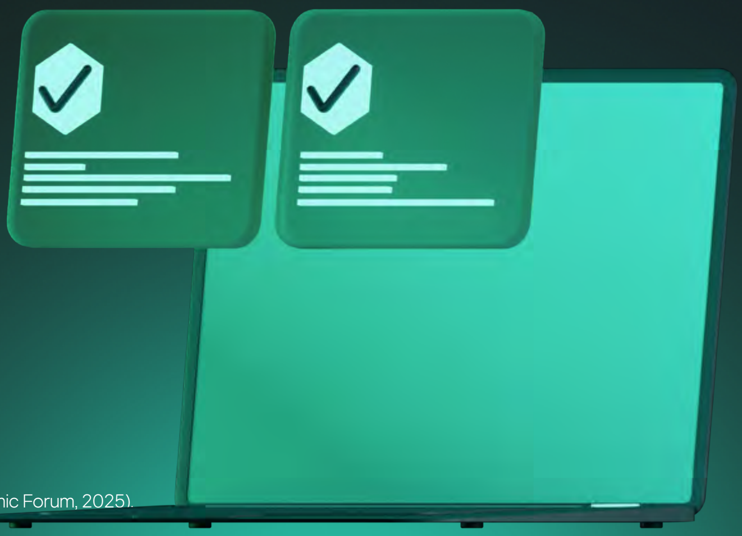
Such tools – for example, AI-assisted alert scoring and prioritization in Kaspersky SIEM and XDR – do not aim to replace the analyst. Rather, the idea is to augment the analyst by letting them focus on important things instead of wading through the sea of noise.

Closing the talent gap

According to the World Economic Forum, 67% of organizations report a moderate-to-critical skills gap in cybersecurity[1]. Due to an acute talent shortage and high burnout rates, the SOC analyst workforce is dominated by junior specialists.

One way to help enterprises is to advise their analysts on handling unknown threats – educating them along the way. This is where GenAI assistants, such as Kaspersky Investigation and Response Assistant (KIRA), come in handy. Using the huge amount of knowledge acquired by large language models during training, these assistants are able to provide critical insights into security events during analysis, facilitating decision-making.

For example, KIRA can analyze complicated PowerShell commands (a common way to execute commands used by administrators and attackers alike), explaining them element by element and assessing the level of threat these commands pose. Not only does it help junior analysts but also serves as a second opinion for more senior staff. Of course, GenAI assistants can solve many other tasks – from summarizing incidents into actionable reports to assessing security risks of Docker images – and the range of applications continues to expand.



[1] World Economic Forum, Global Cybersecurity Outlook, (World Economic Forum, 2025).

Power of integration

AI is known for being hungry for data, which is why data-driven companies are usually also AI leaders. Global coverage and developed data culture translate into insights that are becoming new technologies. For example, thanks to Kaspersky Security Network, or KSN, Kaspersky is uniquely positioned to study the behavior of software in the wild around the globe, which translates into unique capabilities, such as the DLL Hijacking Detection technology in Kaspersky MDR, SIEM and XDR. This AI component enables the products to detect DLL hijacking, a popular technique (especially in targeted attacks) that bad actors use to embed malicious code in trusted software. This attack is notoriously hard to detect, but with AI, SOC analysts can gain unprecedented visibility into anomalous behavior of software, giving them the power to stop the attack as it happens.

There is no single solution, AI or not, that can solve all the cybersecurity problems and satisfy all the cybersecurity needs of a modern business. However, methodical integration of increasingly advanced technologies into SOC workflows can make quantitative benefits – such as lower mean time to respond – become qualitative, resulting into a more secure infrastructure. And with AI, this qualitative shift may be closer than we think.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. With over a billion devices protected to date from emerging cyberthreats and targeted attacks, Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection, specialized security products and services, as well as Cyber Immune solutions to fight sophisticated and evolving digital threats. We help over 200,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

www.kaspersky.com