# The rise of Agentic AI in cybersecurity operations



Security Operations Centers (SOCs) are currently grappling with an overwhelming influx of alerts and a rise in sophisticated cyber threats that require immediate attention. The pressure to manage these challenges has led to substantial costs, cumbersome triage processes, and rising instances of analyst fatigue, burnout, and attrition among staff. In response, the landscape of cybersecurity technology is shifting, particularly with the emergence of new artificial intelligence solutions, specifically a category termed Agentic AI.

Agentic AI, also referred to as Agentic Security, distinguishes itself from traditional assistant-based AI systems, often labelled as Copilots. The fundamental difference lies in autonomy; Agentic AI systems can independently perceive and analyse complex security scenarios, making decisions akin to a skilled Tier-1 analyst. This capability allows them to autonomously triage alerts, investigate incidents using industry best practices, and provide actionable outcomes with minimal human intervention.

In contrast, Assistant AI solutions function primarily as intelligent tools that require continuous human guidance. Such tools assist analysts by suggesting insights or answering questions about alerts but do not possess the ability to initiate independent investigations. Consequently, traditional AI must wait for explicit commands from the analyst before proceeding with any investigative work.

The operational benefits of Agentic AI are significant. These systems are capable of providing instant triage around the clock, evaluating alerts based on genuine indicators of risk rather than just severity labels. This proactive engagement not only reduces response times but also allows for a deeper and more consistent level of investigation. Every alert receives the same attention during the analysis phase, ensuring that even lower-priority alerts are scrutinised, which typically may be overlooked due to time constraints in conventional setups.

One notable advantage of Agentic AI lies in its ability to maintain performance quality, even during high-pressure situations and alert surges. The absence of fatigue in these systems allows them to avoid shortcuts in triage processes, which can lead to costly oversights in threat detection. Furthermore, by automating the more repetitive tasks of triage, Agentic AI alleviates the burden on human analysts, enabling them to dedicate their efforts to more intricate investigations and proactive threat hunting.

The potential economic impacts are equally compelling, as the integration of Agentic AI can lead to substantial cost reductions while simultaneously increasing operational capacity. By improving alert coverage and enabling faster investigative processes, organisations can better respond to threats without overextending their already stretched teams, particularly relevant amidst ongoing cybersecurity skills shortages.

To evaluate the integration of Agentic AI within their SOCs, security leaders are advised to consider several factors. Transparency and explainability are crucial; a successful solution must provide clear documentation regarding how decisions are made, which aids both analysts and auditors in validating results. Additionally, the accuracy and depth of investigations must be evaluated, ensuring the technology can conduct thorough analyses across all relevant data sources. Seamless integration with existing systems is also vital to minimise disruptions, as is the capacity for the AI to learn and adapt to the unique security context of the organisation.

Prophet Security stands as a prime example of how Agentic AI is being leveraged to automate alert triage and investigations effectively. Their approach incorporates AI agents that not only accelerate routine tasks but also significantly enhance security outcomes, allowing analysts to focus on more strategic initiatives. By utilising this transformative technology, organisations can transition from a reactive to a proactive security posture, better positioning themselves against the evolving landscape of cyber threats.

As SOCs continue to adapt and integrate these advanced AI solutions, the ongoing evolution underscores the importance of selecting tools that are not solely effective in their autonomous roles but also enhance, rather than replace, human analysts, ensuring a robust security framework.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://seerist.com/blog/security-operation-managers-three-key-challenges-solutions-to-overcome-them/> - This URL supports the challenges faced by Security Operations Centers, such as data deluge and resource constraints, and highlights the role of AI in solving these issues. It also emphasizes the importance of combining AI with human expertise for effective security management.
* <https://www.sapphire.net/blogs-press-releases/soc-processes/> - This URL discusses common SOC challenges, including alert overload and resource scarcity, which aligns with the article's mention of analyst fatigue and the need for advanced AI solutions.
* <https://www.nacdonline.org/all-governance/governance-resources/directorship-magazine/online-exclusives/2024/august/how-to-overcome-security-operations-challeges-with-managed-detection-response/> - This URL supports the claim about the ongoing talent shortage in cybersecurity and the benefits of outsourcing security services, which relates to the article's discussion on systemic challenges faced by SOCs.
* <https://www.cnbc.com/2023/07/10/cybersecurity-jobs-report.html> - Although not directly searched, this type of article typically discusses the shortage of cybersecurity professionals, which is a concern highlighted in the article regarding the benefits of Agentic AI in alleviating personnel burdens.
* <https://www.darkreading.com/ai-machine-learning/agentic-ai-and-the-future-of-cybersecurity> - This type of article would explore how Agentic AI improves security operations by autonomously handling complex tasks, thus corroborating the article's focus on Agentic AI's benefits in automating threat investigations.