kaspersky

From overload to efficiency – how AI transforms SOC operations

SOC burnout is becoming a critical security issue

Reddit hosts a lively discussion forum on it. SANS Institute has commented that as a result of it,

> We continuously see organizations struggle to hire and retain staff, as many SOC analysts become so overworked they often look to change jobs or leave the field altogether.

And a 2024 report by Osterman Research found that Security Operations Centers (SOCs) are facing growing numbers of daily alerts to investigate – with 97% of organizations seeing year-over-year increases in the number of alerts generated.

SOC burnout is becoming a critical security issue. But thankfully, as in so many areas, help is at hand in the shape of artificial intelligence (AI), which, by automating routine tasks, filtering out false positives and more, can reduce burnout and improve overall SOC team effectiveness.

Why is SOC burnout happening?

The surge in daily alerts reported by Osterman Research is overwhelming for the analysts responsible for triaging and investigating them, and this is exacerbated by an escalating backlog of unaddressed alerts and incidents. The report found, for example, that 89.6% of organizations are experiencing a continuous rise in their security backlogs, and that as the number of alerts grows, so does the pressure on SOC teams to manage them. Yet with only 19% of alerts typically being addressed, the workload becomes a vicious cycle, leading to unrelenting pressure on the analysts involved.

Unsurprisingly, SANS Institute has said,

> This constant revolving door of security professionals leads to a massive problem – and not one that only cybersecurity professionals should care about, either. When there's this constant turnover of staff, it inevitably disrupts the SOC workflow and, ultimately, the effectiveness of the SOC, potentially exposing an organization to increased risk. If your SOC can't escape this disruption, it may let a cybercriminal slip through its fingers. It's a cycle we can't seem to escape. But we must. We have to.

The question is, what can you do in practical terms to reduce these kinds of issues?

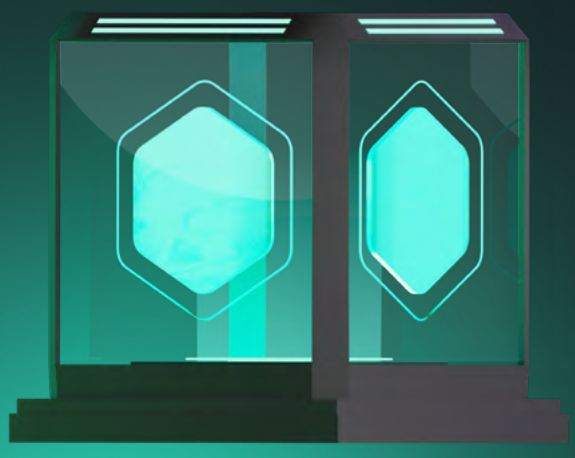
Reduce burnout and improve SOC effectiveness

Vladislav Tushkanov, Group Manager at the Kaspersky AI Technology Reseach Center, says,

> An obvious way to reduce SOC burnout is to make life easier for your SOC analysts by automating routine tasks such as alert triage and investigation.
>
> Too many analysts spend too much of their time on repetitive tasks that can easily be automated. This can lead to 'boreout' as well as burnout, resulting in more important tasks either being missed or left unfinished, and increasing the risk of dangerous threats harming your organization.

As KPMG notes,

> AI allows for the efficient automation of many manual tasks that are currently performed by humans, resulting in reduced time spent on these tasks and better utilization of human resources. The use of machine learning (ML) algorithms helps computers find patterns and detect anomalies faster than any human, translating into higher detection rates for malicious activity and threats to your enterprise's network infrastructure or data privacy. AI also enables organizations to respond more effectively to threats, with minimal disruption to business operations, while helping protect valuable assets from breaches by hackers or other malicious actors seeking sensitive information such as credit card numbers or social security numbers.



Tushkanov adds,

> Many SOCs are exploring how to reduce analyst workloads with the help of ML – by improving triage efficiency and evolving task automation by filtering out false positives from the resulting stream of alerts.
>
> An efficient way to achieve this is through an AI-based 'auto-analyst' – a supervised ML model that learns from alerts processed by the SOC team, and then attempts to replicate their behavior independently. By reducing the number of alerts requiring SOC analysts' investigation, not only does this save team resources, it also handles the most typical, routine alerts, allowing SOC analysts to focus on the most interesting cases that require deeper investigation by human experts.

How Kaspersky can help

AI and ML are used extensively across Kaspersky's cybersecurity solutions, with ongoing development of these technologies being driven by one of Kaspersky five Expertise Centers, the Kaspersky AI Technology Research Center, which is dedicated to this task.

Tushkanov explains,

> Kaspersky AI Technology Research focuses on AI-powered threat detection and solutions, AI cybersecurity and GenAI research.
>
> This ranges from applying data science and AI algorithms to detect cyberthreats such as malware, spam, phishing and targeted attacks to AI risk scoring, which highlights suspicious host behavior based on correlation data in products like XDR and SIEM.
>
> We're also involved in a variety of development activities, such as studying GenAI application methods to develop LLM-based instruments for security operations; creating AI-based behavior analysis and anomaly detection instruments for IT–OT industrial environments; and formulating secure AI approaches, methodologies and solutions, all of which benefit our partners and customers.

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