kaspersky

The human–AI partnership in cyberdefense: empowering analysts for better outcomes

The future of defense is hybrid, humans and AI working together

Everyone has seen the movies where man takes on machine in a dystopian future and will recognize this as fiction. But with the emergence of generative AI and increasingly capable bots, there is a real-world battle brewing in the job market. People are increasingly worried that their roles could be usurped by technology, and their fears aren't unwarranted. Goldman Sachs has predicted that up to 300 million jobs could be lost to automation.[1]

In the cybersecurity industry, some are espousing AI's ability to counter cyberattacks as the answer to the skills shortage. More than 40% of IT security pros say their organization's security teams are understaffed,[2] and they need all the help they can get – human or otherwise.

But while AI can indeed help specialists to triage and respond to alerts, it is not a panacea. And it won't be replacing human analysts any time soon. Automating a security operations center (SOC) fully would require machines to take abstract concepts across different situations and reframe them. This level of creativity and critical thought still belongs to people, even if machine learning (ML) algorithms can do much of the heavy lifting.

1. Goldman Sachs. Generative AI Could Raise Global GDP by 7%. (Goldman Sachs, 2023).
2. Kaspersky. The Portrait of Modern Information Security Professional. (Kaspersky Daily, 2024).

Head of Unified Platform at Kaspersky Ilya Markelov says,

> In large enterprises, full automation isn't possible because of the huge, ever-changing infrastructures. A dedicated team is still required to monitor rules that can become obsolete overnight.

The reality is that a combination of people and AI works best. The latter should augment human expertise – not eliminate it – to ease security teams' workloads and allow them to focus on critical tasks.

Security analysts are stretched thin and burning out

SOCs are being plagued by burnout as they fight increasingly complex and frequent attacks. The skills shortage is compounding this at a time when attack surfaces are growing rapidly, with businesses diving ever deeper into their digital transformation.

Major contributors to staff burnout include alert fatigue (many of which may be false alarms), repetitive work and sleep disruption, with employees often working irregular shifts.

High volumes of alerts are particularly problematic because they limit deep analysis, which is crucial for security teams to understand how threats work. Stress too increases risk, as it makes it likelier that an analyst will miss an incoming threat. This was evidenced in a recent report, wherein 83% of IT security pros admitted they (or someone in their department) had made burnout-related errors that led to a security breach.[3]

Business leaders are therefore throwing more and more money at relieving the knock-on effects of burnout in the SOC. But in a red-hot job market where security pros can name their price, increased hiring isn't necessarily the answer – and retaining talent can be just as hard as finding it. A quarter of IT security staff, in fact, feel they must leave their business in order to escape burnout.[3] And why shouldn't a stressed-out analyst jump ship – especially if it's for greater reward?

Kaspersky AI does the legwork so humans can focus on business-critical tasks

Skills shortages and overwhelming workloads are leading to staff burnout and churn in security teams. These teams need help, which is where Kaspersky and its AI-driven solutions come in. The company's solutions are designed to alleviate pressure on security teams by managing time-intensive tasks, such as automating triage and initial response steps. They also enable lesser-skilled staff to assume more complex tasks.

Markelov says,

> Kaspersky AI helps to reduce burnout by minimizing routine work, with the system offering actions the user can simply accept or reject. Automation also saves resources. For example, playbooks (fully automated chains of action) can be triggered to deal with threats automatically.

One good example is the AI Analyst in Kaspersky Managed Detection and Response, which helps to reduce the workload of SOC teams by automatically filtering out false positives, allowing experts to respond to threats faster and avoid burnout. Elsewhere, Kaspersky Machine Learning for Anomaly Detection (MLAD), a predictive analytics software solution, is helping industrial enterprises to avoid downtime, as it picks up early signs of impending equipment failure, process disruption, human error or cyberattack in telemetry signals. The result is faster detection-to-decision workflows.

3. Devo. 83% of IT Security Professionals Say Burnout Causes Data Breaches. (Devo, 2023).

Augmentation, not just automation: AI and humans in tandem

While Kaspersky's AI can achieve lots alone, it can enable security teams to achieve even more, such as shutting down complex, targeted attacks. Human-involved AI means that while AI can operate semi-freely and make suggestions, it is still directed by an expert who will always have the final say. And there are many reasons this is important. Firstly, AI may flag legitimate behavior as suspicious, which could result in a wrongful action. Humans, however, can verify or dismiss alerts with the context that AI lacks (e.g., business operations, one-off tasks), reducing unnecessary disruptions and freeing up time to handle real threats. Humans and AI working in harmony means analysts can focus exclusively on the alerts AI is unsure about.

Decision-making is generally an area where humans excel. AI is great at pattern recognition but often lacks business context or situational awareness. Human analysts understand organizational norms, regulatory requirements and exceptions, enabling them to make more nuanced decisions – especially in complex scenarios. And because cybersecurity decisions can have legal and ethical implications, keeping people in control reduces the likelihood of policy violations or criminality.

Smarter decisions, faster response, stronger defense – but still "human AI"

Kaspersky's key belief is that its AI should make cybersecurity more human – not less. It is an empowering tool designed for usability, with visual dashboards, explainable decisions and automated detection and response. It is a means to an end, not an end unto itself.

At its best, AI doesn't replace analysts; it amplifies their insight, filters out noise and helps them focus on what matters most. The result is security teams that aren't just faster but also smarter, more proactive and more resilient. And by keeping humans in control, decisions are grounded in business context, ethical responsibility and strategic judgment.

Kaspersky's AI-driven solutions can also be a big cost saver because they reduce hiring needs.

Markelov explains,

> The number of threats, attacks and unique malware samples increases every year. Beyond this, infrastructure complexity is also increasing as organizations adopt new systems and open new offices. To address this growing complexity, our solutions implement AI and automation, eliminating the need for organizations to grow security teams proportionately.

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.

Conclusion

Cybersecurity isn't a case of AI versus humans but rather humans plus AI. Kaspersky's goal is not to replace analysts but to empower them, giving them the tools to respond faster, act more precisely and stay ahead of evolving threats.

Kaspersky builds AI solutions to augment human defenders, enabling them to stay focused, fresh and prepared, even in the face of overwhelming alert volumes and sophisticated attacks.

www.kaspersky.com