Beyond Alert Fatigue

How AI Can Actually Reduce Cognitive Overload in Cybersecurity

by Dr. Dustin Sachs

The average SOC analyst makes more decisions in a single shift than most people do in a week, and the stakes are existential. Every blinking alert, every incomplete data trail, every ambiguous log entry demands judgment under pressure. And yet, the very tools meant to help, dashboards, threat feeds, SIEMs, often flood defenders with so much information that they become paralyzed, fatigued, or worse, desensitized. This is the real threat behind cognitive overload in cybersecurity. But what if AI didn't just accelerate detection, but actively reduced mental load? What if it could help us think better, not just faster? AI, when designed with behavioral insights in mind, can become not just an automation engine but a cognitive ally (Kim, Kim, & Lee, 2024).

Understanding Cognitive Overload in Cyber Contexts

Cognitive overload occurs when the volume and complexity of information exceeds a person's working memory capacity. In cybersecurity, this happens daily. Analysts must process thousands of alerts, each with its own potential consequence, often in noisy environments under time pressure. Drawing from Daniel Kahneman's System 1/System 2 thinking, most analysts oscillate between intuitive snap decisions and laborious, analytical reasoning. Under stress, they revert to mental shortcuts, increasing the risk of oversight (Kim & Kim, 2024).

A 2025 survey from Radiant Security found that 70% of SOC analysts suffer from burnout, and 65% are actively considering a job change. The primary driver is alert fatigue caused by the flood of false positives and manual triage demands. This constant barrage of low-value alerts overwhelms analysts' cognitive capacity, leading to mental exhaustion, slower response times, and decreased job satisfaction (Radiant Security, 2025). Additionally, cognitive overload contributes to higher error rates, inconsistent documentation, and a breakdown in team coordination (Cau & Spano, 2024).

A 2025 survey from Radiant Security found that 70% of SOC analysts suffer from burnout, and 65% are actively considering a job change. The primary driver is alert fatigue caused by the flood of false positives and manual triage demands.

When AI Makes It Worse

Despite the growing enthusiasm surrounding artificial intelligence in cybersecurity, the reality is more complex. Not all AI implementations are beneficial, some can actually exacerbate the very problems they were designed to solve. Poorly integrated AI systems often produce an overwhelming volume of false positives, bombarding analysts with alerts that require manual triage, draining their time and mental energy. These systems, rather than acting as force multipliers, become sources of frustration.

Another significant issue arises from the opacity of many AI models. Black-box algorithms that offer no insight into how or why a decision was made force users to make high-stakes decisions based on limited trust and understanding. This lack of explainability becomes a cognitive burden rather than a relief. Analysts are left to interpret raw algorithmic output without any contextual grounding, increasing the likelihood of misjudgments or unnecessary escalations.

Instead of cutting through the noise, such AI tools contribute to it. In many Security Operations Centers (SOCs), AI has become synonymous with "alert multiplicity," a flood of new signals with no clear sense of relevance or priority. These systems often trigger alerts for minor or benign anomalies, forcing analysts to waste time sifting through low-value notifications. Rather than providing clarity, AI often adds to the chaos, overwhelming analysts and leaving them with more questions than actionable insights (Camacho, 2024).

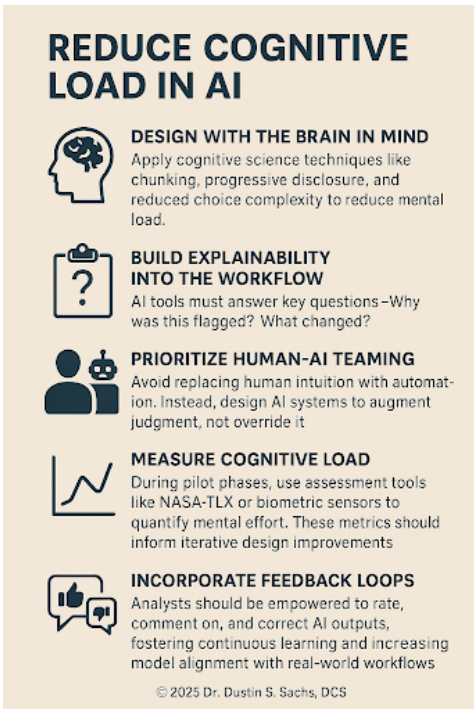
Reframing AI as a Cognitive Augmentation Tool

To realize AI's true potential, it must be reimagined not as an automated watchdog, but as a cognitive ally. The shift from detection engine to decision support system is not just semantic, it's strategic. AI must be designed to think with analysts, not for them. Intelligent prioritization is one such avenue. Instead of treating all anomalies equally, advanced systems can learn from historical triage behavior to rank alerts based on their likelihood of actionability. This helps analysts focus on meaningful threats rather than getting mired in low-priority noise (Romanous & Ginger, 2024).

Natural language summarization offers another path to cognitive relief. Rather than forcing analysts to parse dense logs or sift through raw data, AI-powered tools like Microsoft Security Copilot and IBM QRadar condense information into executive summaries. This allows rapid comprehension and speeds up decision-making (Akhtar & Rawol, 2024). Behavioral AI integration takes this even further by adapting to how individual analysts work. These systems learn usage patterns and present information in more digestible, chunked formats, minimizing unnecessary context-switching. Subtle nudges, such as highlighting inconsistencies or recommending secure defaults, can help ensure consistency under stress (Shamoo, 2024).

Strategic Recommendations for Implementation

To maximize impact, organizations should embed AI into their cybersecurity workflows using human-centered design principles.



Cybersecurity is ultimately a human endurance sport, demanding sustained attention, resilience under pressure, and rapid decision-making amid uncertainty. In this high-stakes landscape can become a trusted teammate rather than an overbearing taskmaster. By shifting the narrative from AI as an automation panacea to a strategic cognitive asset, security leaders empower their teams to make better, faster, and more informed decisions. This reframing fosters an environment where defenders not only keep pace with threats but develop the capacity to adapt, learn, and excel over time.

References

- Akhtar, Z. B., & Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. IT Journal Research and Development. https://doi.org/10.25299/itjrd.2024.16852
- Bernard, L., Raina, S., Taylor, B., & Kaza, S. (2021). Minimizing cognitive overload in cybersecurity learning materials: An experimental study using eye-tracking. Lecture Notes in Computer Science, 47–63. https://doi.org/10.1007/978-3-030-80865-5_4
- Camacho, N. G. (2024). The role of AI in cybersecurity: Addressing threats in the digital age. Journal of Artificial Intelligence General Science. https://doi.org/10.60087/jaigs.v3i1.75
- Cakır, A. M. (2024). AI driven cybersecurity. Human Computer Interaction. https://doi.org/10.62802/jg7gge06
- Cau, F. M., & Spano, L. D. (2024). Mitigating Human Errors and Cognitive Bias for Human-AI Synergy in Cybersecurity. In CEUR WORKSHOP PROCEEDINGS (Vol. 3713, pp. 1-8). CEUR-WS. https://iris.unica.it/retrieve/dd555388-5dd2-

4bb2-870d-92926d59be04

- Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., & Olawumi, T. N. (2024). Impact of AI on cybersecurity and security compliance. Global Journal of Engineering and Technology Advances, 21(1). https://doi.org/10.30574/gjeta.2024.21.1.0193

- Ilieva, R., & Stoilova, G. (2024). Challenges of AI-driven cybersecurity. 2024 XXXIII International Scientific Conference Electronics (ET). https://doi.org/10.1109/ET63133.2024.10721572

- Kim, B. J., Kim, M. J., & Lee, J. (2024). Examining the impact of work overload on cybersecurity behavior. Current Psychology. https://doi.org/10.1007/s12144-024-05692-4

- Kim, B. J., & Kim, M. J. (2024). The influence of work overload on cybersecurity behavior. Technology in Society. https://doi.org/10.1016/j.techsoc.2024.102543

- Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions. AI and Ethics, 1–28. https://doi.org/10.1007/s43681-024-00427-4

- Radiant Security. (2025). SOC analysts are burning out. Here's why—and what to do about it. Radiant Security. https://radiantsecurity.ai/learn/soc-analysts-challenges/

- Romanous, E., & Ginger, J. (2024). AI efficiency in cybersecurity: Estimating token consumption. 21st Annual International Conference on Privacy, Security and Trust (PST). https://doi.org/10.1109/PST62714.2024.10788078

- Shamoo, Y. (2024). Advances in cybersecurity and AI. World Journal of Advanced Research and Reviews. https://doi.org/10.30574/wjarr.2024.23.2.2603

- Siam, A. A., Alazab, M., Awajan, A., & Faruqui, N. (2025). A comprehensive review of AI's current impact and future prospects in cybersecurity. IEEE Access, 13, 14029–14050. https://doi.org/10.1109/ACCESS.2025.3528114