# Cybersecurity executives and analysts divided on AI’s impact, new report finds



New research conducted by Exabeam reveals significant discrepancies between cybersecurity executives and frontline analysts regarding the real-world impact of artificial intelligence (AI) on cybersecurity operations. The findings emerge from a global survey of 1,000 cybersecurity professionals commissioned by Exabeam and carried out by Sapio Research. The resulting report, titled "From Hype to Help: How AI Is (Really) Transforming Cybersecurity in 2025," highlights both the widespread adoption of AI technologies and the differing perceptions of their effectiveness within security teams.

A central theme of the report is the pronounced divide between executives and analysts on AI’s contributions to productivity. While 71% of executives believe AI has significantly boosted productivity across security teams, only 22% of analysts—who use AI tools daily—agree with this view. Analysts reported that rather than reducing their manual workloads, AI often changes the nature of their duties. They frequently contend with challenges such as false positives and alert fatigue, which necessitate ongoing human oversight.

The report explains, "This perception gap reveals more than a difference in opinion; it underscores a deeper issue with operational effectiveness and trust. Executives often focus on AI's potential to reduce costs, streamline operations, and enhance strategy. But analysts on the front lines report a very different experience — one shaped by false positives, increased alert fatigue, and the ongoing need for human oversight."

Steve Wilson, Chief AI and Product Officer at Exabeam, commented on these findings, saying: "There's no shortage of AI hype in cybersecurity — but ask the people actually using the tools, and the story falls apart. Analysts are stuck managing tools that promise autonomy but constantly need tuning and supervision. Agentic AI flips that script — it doesn't wait for instructions, it takes action, cuts through the noise, and moves investigations forward without dragging teams down."

Despite these challenges, the report identifies areas where AI is delivering clear benefits. Over half of security teams (56%) report improvements in threat detection, investigation, and response (TDIR) productivity attributed to AI. In particular, AI helps alleviate repetitive analytical tasks, reduces alert fatigue, and accelerates time to insight. Enhanced anomaly detection, quicker mean time to detect (MTTD), and improved user behaviour analytics are also linked to AI deployment.

Nevertheless, trust in AI operating autonomously remains low. Only 29% of all cybersecurity respondents express confidence in AI’s independent functioning, with trust dwindling to just 10% among analysts. According to the report, "The industry is aligned on one thing: performance precedes trust. In security operations, organisations aren't looking to hand over the reins — they're counting on AI to exceed the limits of the human mind at scale. By consistently delivering accurate outcomes and automating tedious workflows, AI can become a force multiplier for analysts, enabling faster, smarter threat detection and response."

The introduction of AI is also reshaping cybersecurity team structures. More than half of organisations surveyed have restructured their teams following AI adoption. While 37% reported workforce reductions linked to automation, 18% indicated increases in hiring focused on AI governance, automation oversight, and data protection. This points to a developing operational model where agentic AI supports faster decisions and more complex investigations, while human analysts handle sophisticated tasks.

Regional variations in AI adoption and perceived productivity gains were evident. The highest improvements were reported in India, the Middle East, Turkey, and Africa, with 81% of organisations noting significant productivity increases. The UK, Ireland, and Europe followed at 60%, Asia Pacific and Japan at 46%, and North America reported the lowest gains at 44%.

The report concludes that successful integration of AI in cybersecurity depends on bridging the gap between leadership expectations and frontline realities. It stresses the importance of involving analysts in AI deployment decisions and aligning AI capabilities with operational needs, focusing on measurable rather than promotional outcomes.

The survey involved cybersecurity professionals from a variety of roles, industries, and organisation sizes. The broad definition of AI used in the survey encompassed technologies such as machine learning, generative AI, and agentic AI systems currently in use within the cybersecurity landscape.

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

## Bibliography

1. <https://www.exabeam.com/hubs/how-ai-is-transforming-cybersecurity-in-2025/> - This URL provides information on the Exabeam report highlighting the disconnect between executives and analysts regarding AI's impact on cybersecurity productivity. It also discusses areas where AI delivers value, such as threat detection and investigation.
2. <https://www.exabeam.com/resources/reports/how-ai-is-transforming-cybersecurity-in-2025/> - This URL offers access to the Exabeam report, which details observations from a global survey of cybersecurity professionals, focusing on AI's actual transformation in security operations and perceived benefits versus challenges.
3. <https://cybertechnologyinsights.com/technology/exabeam-research-reveals-ai-disconnect-between-security-leaders-and-practitioners/> - This article corroborates the concept of a disconnect between security leaders and frontline analysts in their views on AI's effectiveness in cybersecurity, as revealed by Exabeam's research.
4. <https://www.exabeam.com/blog/security-operations-center/theres-hope-beyond-the-hype-why-agentic-ai-is-the-future-of-cybersecurity/> - This blog post discusses the potential of agentic AI in addressing challenges such as false positives and alert fatigue by taking proactive measures, aligning with the themes of operational effectiveness and trust in AI.
5. <https://www.exabeam.com/blog/infosec-trends/beyond-the-hype-seven-ai-trends-every-security-pro-needs-to-know-for-2025/> - This article highlights seven AI trends in cybersecurity for 2025, including AI-powered attack sophistication and defensive enhancements, which complements the report's focus on AI's role in threat detection and response.
6. <https://www.noahwire.com> - This source provides a summary of the Exabeam report findings, though it does not offer additional details beyond what is already covered by the other URLs. It encapsulates the report's core themes, such as the AI perception gap and restructuring of cybersecurity teams.
7. <https://news.google.com/rss/articles/CBMingFBVV95cUxNRU1wUlJBdHhLZHpBQ3pJLTdBT21mUGNrM3dxTWc0OXJkdG5IUnU2UFJYdjlmMHdjTHE2YUlCQ0ZhYjdKbTlpWXNPRktHS1dIbFlnbDI2OUUyV2JCbExvWmc5Zy1xVVZxT0hXMWhCM3NCbHloRVdzMzBQOFZqWmVMbDhCU3cwbE5teEgzSnVTaFl1cUM3dXR5Tl81M181dw?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data