Stockholm, Sweden
October 4, 2023

Enea Report Reveals Majority of Cybersecurity Professionals Believe Offensive AI Will Outpace Defensive AI

Seventy-six percent (76%) of cybersecurity professionals believe the world is very close to encountering malicious artificial intelligence (AI) that can bypass most known cybersecurity measures. More than a quarter (26%) see this happening within the next year, and 50% in the next 5 years. Phishing, social engineering tactics, and malware attacks are those most likely to become more dangerous with the use of AI.

These are some of the sobering findings from a new global study of IT and cybersecurity professionals conducted by research firm Cybersecurity Insiders, and detailed in the report “Artificial Intelligence in Cybersecurity”. The report will be published on October 5th and the results of the survey will be discussed by AI specialists from Enea, Arista Networks, and Zscaler in a webinar presentation on the same day.

The report provides an in-depth, holistic view of how cybersecurity professionals see AI and its impact on the industry, including their anticipations, apprehensions, and various strategies for integrating AI into their network defenses. The results are complemented by insights and recommendations, established through collaboration with Enea analysts, on how to build the capabilities, confidence, and resilience required to counter the emerging use of AI to execute cyberattacks.

The report breaks down key survey findings into fears, hopes, and plans around AI/ML in cybersecurity:

- **Fears:** In addition to the concern about offensive AI outpacing defensive AI, a significant 77% of professionals express serious worries about rogue AI, where AI behavior veers away from its intended purpose or objectives and becomes unpredictable and dangerous. Phishing, social engineering and malware attacks are seen as the top threats that will be strengthened by AI, but identity fraud, data privacy breaches, and distributed denial-of-service (DDoS) attacks were also cited as likely to become more effective.

- **Hopes:** Respondents are nonetheless optimistic about AI's positive impact on cybersecurity. AI is anticipated to bolster threat detection and vulnerability assessments, with intrusion detection and prevention identified as the domain most likely to benefit from AI. Deep learning for detecting malware in encrypted traffic holds the most promise, with 48% of cybersecurity professionals anticipating a positive impact from AI. Cost savings emerged as the top KPI for measuring the success of AI-enhanced defenses, while 72% of respondents believe AI automation will play a key role in alleviating cybersecurity talent shortages.

- **Plans**: While a majority (61%) of organizations are yet to deploy AI in any meaningful way as part of their cybersecurity strategy, 41% consider AI as a high or top priority for their organization. And a hopeful 68% of respondents expect a budget increase for AI initiatives over the next two years.

Workforce impact and training needs

Half (50%) of cybersecurity leaders report that their organization has "extensive knowledge" regarding AI /ML in cybersecurity, and another 19% report “moderate knowledge," with the remaining roughly one-third reporting no-to-minimal knowledge. When asked what steps organizations should take to prepare for sophisticated or overwhelming AI attacks, 68% cited increased cybersecurity training and awareness for employees.

Developing AI-specific incident response plans followed close behind (65%), and 61% said regular security assessments and audits. Over half of all respondents said that strengthening traditional security controls such as zero-trust protocols, multi-factor authentication, next-gen firewalls, and threat intelligence were key to preparing for sophisticated AI attacks.

Moving from understanding to action

"Understanding the profound impact of AI on cybersecurity is crucial for navigating the evolving threat landscape,” said Laura Wilber, Sr. Industry Analyst at Enea. “That begins by listening closely to the concerns and hopes of cybersecurity leaders and their teams on the front lines.”

“This report confirms growing concerns around the malicious use of AI, but it also highlights some remarkable innovations in the use of AI to streamline and automate defenses. Significant gains have already been made, such as a reduction in the average time it takes to detect and contain threats. However, AI is not a one-size-fits-all solution – it’s essential that businesses take a clear and methodical approach to implementing AI strategies in order to achieve maximum readiness and resilience. As we say at Enea – don’t be surprised, be ready.”

To learn more, we invite you to attend the webinar "Get Ready for the AI Revolution – Fears, Hopes, and Plans for AI in Cybersecurity: Surprising Results from New Survey," which will be hosted by Cybersecurity Insiders, and features a panel of AI specialists from Enea, Arista Networks and Zscaler. The webinar will take place on Thursday, October 5.

To attend the webinar and receive a full copy of the AI report, register here.

Contact
Stephanie Huf, Chief Marketing Officer
E-mail: stephanie.huf@enea.com

Notes to Editors

Survey methodology

The Artificial Intelligence in Cybersecurity Report is based on the results of a comprehensive worldwide online

survey of 457 cybersecurity professionals, conducted in September 2023 by Cybersecurity Insiders, sponsored by Enea, Arista Networks and Zscaler. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

Enea’s cybersecurity offering includes the following:

- Signaling, messaging and voice protection trusted by the world’s largest Mobile Network Operators and CPaaS providers to secure communications infrastructure and services. The portfolio includes firewalls for mobile network signaling, voice and messaging security, A2P (application to person) message protection, as well as global signaling intelligence, and threat intelligence services.
- Enea’s embedded traffic intelligence products classify traffic in real-time and provide granular information about network activities. The portfolio includes the Enea Qosmos ixEngine, the Enea Qosmos Probe and the Enea Qosmos Threat Detection SDK. The products support a wide range of protocols and are delivered as software development kits or standalone network sensors to network equipment manufacturers, telecom suppliers, and vendors of cybersecurity software.

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for fixed and mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day.

Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security.

Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

For more information: www.enea.com