# Cybersecurity strategies must evolve with AI-driven threats



The cybersecurity landscape is rapidly transforming due to the proliferation of artificial intelligence (AI), as highlighted by various executives at OPSWAT. As organisations grapple with this evolving threat vector, the need for advanced protective measures and strategies becomes increasingly imperative.

Matt Wiseman, Director of Product Marketing at OPSWAT, articulated the threats posed by AI, noting that its rapid expansion has enabled less sophisticated attackers to elevate the quality of their cyber-attacks significantly. This change includes enhanced grammar and design in phishing emails and improved social engineering tactics. Wiseman highlighted that organisations often lag in adopting protective AI tools, necessitating a reassessment of their cybersecurity frameworks. He emphasised the importance of revisiting foundational security measures, particularly within Operational Technology (OT) environments, to safeguard critical assets and maintain visibility and operational integrity despite the threats.

He outlined that by implementing proper segmentation and developing secure conduits, organisations can enhance their overall security without compromising the connectedness necessary for operational efficiency. He advocated for utilising data-diodes for safe, one-way data transfers, thus retaining access to critical operational data while safeguarding against external threats.

Adding to the discourse, Pedram Amini, Chief Scientist at OPSWAT, addressed the growing sophistication of cyber threats and the potential for AI misuse. He indicated that as machine learning (ML) becomes more accessible, organisations should prepare for an uptick in the volume and believability of ML-assisted scams. Amini cautioned that this evolution could lead to increased attacks on personal devices, urging organisations to prioritise targeted training and innovative detection methods to counter social engineering tactics enhanced by AI.

Irfan Shakeel, Vice President of Training and Certification Services, underscored the importance of cyber hygiene and organisational accountability. During a recent panel discussion at GITEX Global, Shakeel noted that many successful cyberattacks exploit fundamental vulnerabilities such as unpatched software. He stressed the need for businesses to integrate basic cybersecurity hygiene with advanced threat detection systems, highlighting the critical role of human factors in security breaches. Despite substantial investment in training, individuals frequently fall victim to cyber scams, which necessitates a focus on dynamic, tailored continuous training to keep pace with evolving threats.

In the context of the Industrial Control Systems (ICS) and OT environments, Erik Knapp, CTO, addressed challenges stemming from increased cloud adoption. He advocated for robust network security controls, particularly perimeter security, to safeguard devices interacting with cloud services. Knapp suggested that safe, one-way data transfers should be channelled through data diodes, while secure pathways should be established for remote access to OT systems. He expressed optimism about observing increased adoption of layered security measures to manage cloud connections effectively by the year 2025.

Itay Glick, Vice President of Products at OPSWAT, observed a heightened emphasis on data privacy and compliance, particularly in light of regulations like GDPR and CCPA. He cited a significant enforcement case where Ireland's Data Protection Commission fined Meta €1.2 billion for non-compliance, underscoring the financial ramifications organisations may face for breaches of data protection laws. Glick also reflected on the rising incidence of ransomware attacks, particularly in critical infrastructure sectors. He cited an April 2023 incident involving the ALPHV group’s attack on NCR, which disrupted crucial payment systems, underscoring the necessity for advanced detection and incident response capabilities.

Glick indicated a noteworthy trend in which many organisations are transitioning from cloud services to on-premises solutions, seeking to enhance data control and mitigate cloud-related vulnerabilities. This shift has gained traction following high-profile breaches such as the MOVEit cyberattacks in 2023, which exposed weaknesses in cloud infrastructure. By opting for on-premises systems, organisations aim to strengthen their security posture and better align with compliance requirements while reducing dependency on third-party providers.

As businesses continue to navigate the complexities of cybersecurity augmented by AI, the imperative to adopt comprehensive and adaptive strategies is clear, with a focus on addressing both technological and human factors in order to mitigate emerging threats effectively.

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

## References

* <https://www.opswat.com/blog/looking-ahead-5-cybersecurity-threats-to-consider-in-2024> - Corroborates the rise of AI and Machine Learning in cyberattacks, and the need for advanced protective measures against evolving threats.
* <https://www.opswat.com/blog/national-coding-week-2023-5-ways-ai-is-shaping-cybersecurity-development> - Supports the impact of AI on cybersecurity, including advanced threat detection, predictive analysis, and automated incident response.
* <https://www.opswat.com/blog/national-coding-week-2023-5-ways-ai-is-shaping-cybersecurity-development> - Highlights the use of AI by threat actors and the importance of AI in critical infrastructure protection.
* <https://www.opswat.com/solutions/threat-intelligence> - Details the importance of threat intelligence and how AI-driven solutions can detect and respond to evolving threats.
* <https://www.opswat.com/solutions/threat-analysis> - Explains the role of AI in detecting unknown threats, identifying TTPs and IOCs, and streamlining threat analysis.
* <https://www.opswat.com/blog/artificial-intelligence-next-ot-cybersecurity-influencer> - Discusses the impact of AI on OT cybersecurity, including the collaboration between human operators and AI systems.
* <https://www.opswat.com/blog/looking-ahead-5-cybersecurity-threats-to-consider-in-2024> - Addresses the targeting of critical infrastructure and the importance of robust security measures, including data diodes for safe data transfers.
* <https://www.opswat.com/solutions/threat-analysis> - Supports the need for robust network security controls, particularly perimeter security, to safeguard devices interacting with cloud services.
* <https://www.opswat.com/blog/national-coding-week-2023-5-ways-ai-is-shaping-cybersecurity-development> - Highlights the importance of human factors in security breaches and the need for continuous, tailored training to counter social engineering tactics enhanced by AI.
* <https://www.opswat.com/solutions/threat-intelligence> - Emphasizes the financial ramifications of data protection law breaches and the rising incidence of ransomware attacks, particularly in critical infrastructure sectors.
* <https://www.opswat.com/blog/artificial-intelligence-next-ot-cybersecurity-influencer> - Discusses the trend of organisations transitioning from cloud services to on-premises solutions to enhance data control and mitigate cloud-related vulnerabilities.
* <https://news.google.com/rss/articles/CBMiigFBVV95cUxNbEE2WGFUcEdsUkI0VjlaWUJhSVZSSmVjd0tDVWItQi1YYno5bVZOSVdDeUtOQ3hucklvWWl6RHFLcU1TOVRWNTNkeHBpQkRicnktNnZLS2tvSjVaMkc0WFQyMW0ybGFuUi1CTjU5b3hjd2hBd19xTVdtTTNrZ09nblJTMjFzNVNBdXc?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data