Edge Service Awareness - With CISO

Quick recap

The meeting focused on cybersecurity and digital accessibility challenges, particularly how advanced AI language models have complicated phishing detection and His university under consideration's efforts to address digital accessibility compliance through organized documentation and vendor evaluations. CISO shared his experience managing cybersecurity at His university under consideration, including procurement processes, cloud infrastructure management, and the operation of a remote cybersecurity team using hybrid work models. The discussion concluded with an exploration of AI's dual role in cybersecurity, examining both its potential benefits in vulnerability detection and mapping policy documents while acknowledging challenges around AI-generated false positives, trust and safety measures, and the need for proper governance.

Summary

AI and Cybersecurity Challenges

CISO discussed the evolving role of AI in cybersecurity, noting that advanced language models have made it more challenging to detect phishing attempts. He highlighted His university under consideration's focus on digital accessibility, where his team curated and organized documentation across functional units to address digital accessibility compliance. CISO explained that his team used a SharePoint site to collect and organize accessibility data from various stakeholders, leveraging their expertise in data management and audits to support the initiative.

IT Vendor Accessibility and Security

CISO explained the process of evaluating IT services and platforms for digital accessibility and cybersecurity. He described the use of VPAT (accessibility statement) and HECVAT (cybersecurity posture) documents as key indicators for vendor evaluation. CISO noted that while these assessments are conducted during initial vendor selection, ongoing annual reviews are not typically performed due to resource constraints in higher education procurement management.

Cybersecurity Procurement Challenges at Stockton

CISO discussed the challenges of procurement in cybersecurity and accessibility, highlighting the lack of subject matter experts and the need to balance affordability with necessary investments. He shared his experience as a working manager, emphasizing the value of

firsthand experience in managing cybersecurity at His university under consideration. Despite limited funding, CISO and his team strive to maximize the impact of their cybersecurity efforts, given Stockton's revenue size.

Cloud Security and Ransomware Recovery

CISO discussed his experience with cloud infrastructure at His university under consideration, where he was responsible for procurement through a purchasing cooperative to comply with state regulations. He explained how they use AWS and conduct security scans similar to on-premises infrastructure using tools like Nessus and PowerShell scripts. Anushka shared her experience with a similar approach at a previous company to recover from a ransomware attack. CISO also described his role as a virtual Chief Information Security Officer, which involved managing a fully remote team for cybersecurity, similar to his experience at Stockton.

Hybrid Cybersecurity Team Management

CISO shared his experience managing a remote cybersecurity team at His university under consideration, where his unit operates a hybrid model with 2 days in the office and 3 days remote. He explained how they maintain productivity through daily JIRA tickets for task management and a mandatory Zoom virtual office environment where employees are expected to be present during working hours, similar to an in-person office setting. Anushka expressed interest in this approach, noting that her own experience with remote work had mixed results, with some employees preferring remote work while others advocating for in-person attendance.

Career Transitions in Cybersecurity

CISO and Anushka discussed their career paths, which both began in audio-visual technology before transitioning into network administration and cybersecurity. CISO shared how he leveraged his background in AV to advance into systems administration and later pursued a master's in computational science. Anushka described her experience managing AV systems across multiple locations before moving into network segmentation and cybersecurity, particularly focusing on cloud migration during a cyber-attack at her previous employer. They concluded by discussing AI use cases in cybersecurity detection, though this part of the conversation was not captured in the transcript.

AI Challenges in Cybersecurity

CISO discussed the dual nature of AI in cybersecurity, highlighting both its potential to discover vulnerabilities and the challenges it presents, such as AI-generated false positives that burden developers. He mentioned ongoing issues with AI hallucinations in vulnerability discovery, using Google and FFmpeg as examples, and noted that AI is increasingly being used in steganography, creating new challenges. Anushka acknowledged the efficiency of AI

in steganography and raised questions about handling compliance, data ethics, and governance in AI projects, to which CISO did not provide a direct answer.

AI Adoption and Safety Concerns

CISO discussed his personal approach to AI in documentation and code generation, emphasizing the importance of testing, particularly for edge cases. He expressed concerns about the adoption of AI in engineering roles, highlighting a lack of understanding and proper guardrails among decision-makers. CISO also criticized the trust and safety measures in AI development, citing examples of companies dismantling such teams.

AI in Risk Management Frameworks

CISO discussed how AI could be valuable in mapping existing policy documents into risk management frameworks like NIST 800-171 for higher education institutions and 800-53 for federal institutions. He shared an example from his experience overseeing a team that developed an 800-171 risk management framework for the university, which could now be completed more efficiently with AI in a shorter timeframe. Anushka acknowledged this and asked about AI's potential in cybersecurity fields like red teaming, blue teaming, GRC, and forensics, to which CISO suggested that while AI can significantly speed up processes, the quality of results might not be as deep as manual analysis, but could be improved with regression testing and human oversight.

AI Trust and Safety Challenges

CISO and Anushka discussed the trust and safety challenges of AI algorithms, including autonomous actions and potential vulnerabilities. They explored the current cybersecurity framework at His university under consideration, highlighting the use of in-house staff, temporaries, and student workers, as well as a 24/7 managed service provider for continuous monitoring. CISO shared his vision for AI's influence on cybersecurity over the next 3-5 years, emphasizing the importance of AI governance and the need to educate users about AI risks. They also briefly touched on Stockton's recent contract with Edge for digital accessibility consulting.