RESILIENCE IN FOCUS FOR CISO

Round Table Report

CYBER.
LONDON

CloudSEK

Cyber Security Round Table Breakfast

Date: January 22, 2025

Venue: Room C103, Tait Building, City St. George’s University of London

Organized by: CloudSEK and Cyber London

Topic: Resilience in Focus for CISOs

Introduction and Welcome

The "Cyber Security Round Table Breakfast" brought together cyber security professionals, consultants, industry experts and postgraduate students to discuss resilience strategies for Chief Information Security Officers (CISOs). Hosted at City St. George’s University of London, the event was organized by CloudSEK and Cyber London and chaired by Mark Child, Co-founder of Cyber London.

Mark Child, alongside Izak Oosthuizen (Co-founder of Cyber London) emphasized the importance of collaboration between academia, industry and SMEs in combating emerging cyber threats. The session was characterized by dynamic discussions, thought-provoking presentation and practical takeaways for attendees.

Keynote Presentation: Emerging Cyber Threats by Bofin Babu

Bofin Babu, Co-founder of CloudSEK delivered a keynote presentation focusing on:

- **Cyber Threat Landscape:** Highlighting the growing sophistication of cyberattacks, particularly in the software supply chain and phishing schemes targeting enterprise vulnerabilities.

- **Agenda:** The presentation agenda included discussions on:
    - Software Supply Chain Attacks
    - AI-Enhanced Cyber Attacks and Scams

- **Software Supply Chain Complexity:** Bofin illustrated the complexity of managing software supply chain risks. Using examples such as vulnerabilities in plugins (e.g., ScriptRunner, BigPicture) and dependencies (e.g., TensorFlow, Numpy), he highlighted challenges organisations face in securing their digital assets. The presentation featured real-world incidents like PyPI repository hijacks, which exposed API keys and sensitive data.

- **Postman Workspace Data Leaks:** A case study revealed how over 30,000 leaked workspaces exposed API keys, business data, and customer PII (Personal Identifiable Information). These risks were attributed to improper access controls and accidental sharing, emphasizing the need for secure development practices and external secrets management.

- **Deepfake Threats:** Through case studies of scams involving Elon Musk and Brad Pitt, Bofin demonstrated the misuse of AI-generated deepfake technology to exploit trust and deceive victims. For example:
    - An Elon Musk deepfake promoted fraudulent cryptocurrency schemes.
    - A Brad Pitt deepfake scammed a French woman out of €830K by creating fake hospital scenarios.

- **CloudSEK's Tools:** Bofin introduced CloudSEK's Deepfake Analyzer, which detects AI-generated content with high accuracy, and the BeVigil app for assessing mobile app security. These tools were presented as vital solutions for staying ahead of emerging threats.

Round Table Discussions and Key Insights

The interactive discussions expanded on Bofin’s presentation and covered critical cyber security topics:

1. **Supply Chain Security:** Participants explored challenges in monitoring third-party vendors and ensuring compliance with regulations like DORA (Digital Operational Resilience Act) and CMMC (Cyber Security Maturity Model Certification). The importance of continuous monitoring and collaboration between SMEs and larger enterprises was emphasized. CloudSEK’s DORA compliance solutions, including predictive threat detection and real-time insights, were highlighted as examples of proactive risk management.
2. **AI and Deepfake Threats:** Deepfakes were identified as a growing concern in spreading misinformation and influencing public opinion. Attendees debated the ethical implications of AI and stressed the importance of educating the public and cyber security professionals about detecting and mitigating such threats.
3. **Human Factor in cyber security:** The consensus was that humans remain the weakest link in cyber security. Educating end-users and professionals to recognize phishing attempts, manage passwords, and implement basic security measures was viewed as essential. It was noted that 93% of breaches could be avoided through fundamental precautions.
4. **Support for SMEs:** SMEs face significant financial and technical challenges in adopting robust cyber security frameworks. Suggestions included fostering collaborations where larger corporations provide guidance and support to smaller vendors.
5. **Education and Awareness:** Several participants highlighted the need for integrating cyber security education at all levels, from school curricula to professional development programs, to build a resilient workforce and reduce susceptibility to social engineering and AI-based scams.

Key Takeaways

1. **Collaboration:** A unified approach involving private companies, government bodies, and academia is essential for tackling cyber security challenges.
2. **Adoption of Best Practices:** SMEs must implement basic cyber security measures like regular updates, strong passwords, and compliance with industry standards.
3. **Leveraging Technology:** Tools like CloudSEK's Deepfake Analyzer and BeVigil app were recognized as critical assets for identifying risks and bolstering security.
4. **Regulatory Compliance:** Compliance with frameworks like DORA and CMMC was identified as a strategic priority for mitigating risks, particularly in supply chain management.

Closing Remarks

Mark Child and Izak Oosthuizen concluded the event by emphasizing the necessity of collaboration and knowledge sharing to tackle cyber security challenges effectively. Mark Child's observation that "cybercrime employs more people globally than many major industries" underscored the scale of the challenge and the need for continuous innovation and education.

Special thanks were extended to Bofin Babu for his insightful presentation and CloudSEK for sponsoring the event. Attendees were encouraged to leverage collective expertise and continue collaborating to secure the digital landscape.

Conclusion

The "cyber security Round Table Breakfast" served as a valuable platform for exchanging ideas and strategies among stakeholders in the cyber security domain. By addressing pressing issues like deepfake threats, supply chain security, and SME challenges, the event paved the way for future collaborations and actionable insights. With shared commitment and innovation, the cyber security community can collectively build a safer digital world.

By integrating case studies, real-world examples, and collaborative discussions, the event not only highlighted existing challenges but also inspired actionable solutions to drive progress in the field of cyber security.