Pafos Chamber of Commerce & Industry
Εμπορικό & Βιομηχανικό Επιμελητήριο Πάφου

Security by Design: Navigating Cyber Challenges with IoT and Blockchain

Day 1: Understanding the Landscape			
9:00	–	10:45	**Session 1 (1h & 45 mins): Introduction to Emerging Technologies** ● Overview of IoT, and Blockchain ● Applications and implications in various industries ● Understanding the security challenges emergent tech introduce
10:45	–	11:00	Break (15 mins)
11:00	–	12:45	**Session 2 (1h & 45 mins): Threat Landscape Analysis** ● Identifying common cybersecurity threats associated with IoT, and Blockchain ● Targets of cyberattacks and vulnerabilities ● Assessing the impact of security breaches ● Risk assessment methodologies ● Group work/practical example on risk assessment
12:45	–	13:30	Lunch Break (45 mins)
13:30	–	15:15	**Session 3 (1h & 45 mins): Security Principles and Frameworks** Introduction to IoT security by design principles ● End-to-End Encryption ● Authentication and Authorization ● Secure Communication Protocols ● Resilience and Redundancy ● Monitoring and Logging ● Device Identity and Lifecycle Management
15:15	–	15:30	Break (15 mins)
15:30	–	17:15	**Session 4 (1h & 45 mins): Risk Management in IoT Technologies** ● OWASP IoT Top 10 Identifying and prioritizing security risks ○ ISO/IEC 27001 STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) ○ FAIR (Factor Analysis of Information Risk) ○ Privacy Impact Assessment (PIA) ● Developing risk mitigation strategies ○ Threat Intelligence Analysis ○ Penetration testing ● *Evaluation (**Διαμορφωτική**): online assessment*

Day 2: Implementing Security Strategies			
9:00	–	10:45	**Session 5 (1h & 45 mins) – Secure Development Lifecycle** ● Understanding the secure development lifecycle (SDLC) ○ Implement Principle of Least Privilege ● Integrating security into the development process ○ Use Secure Authentication Mechanisms ○ Secure Communication Protocols ● Best practices for secure coding ○ Secure Firmware and Software Update ○ Secure Coding Standards and Guidelines ○ Secure Configuration Management, Secure Data Storage and Encryption ○ Regular Security Testing and Code Reviews ○ Security Awareness Training ● Case Study
10:45	–	11:00	Break (15 mins)
11:00	–	12:45	**Session 6 (1h & 45 mins) Secure Deployment and Configuration** ● Securing IoT and Blockchain deployments ○ Device Authentication and Authorization ○ Secure Provisioning and Onboarding ○ Vendor and Supply Chain Security ● Configuration management best practices ○ Update and Patch Management ○ Incident Response and Contingency Planning ● Network Segmentation and Isolation Implementing access controls and encryption techniques ● Monitoring and Logging ● Physical Security Measures ● Role-Based Access Control (RBAC) ● Case Studies ○ Mirai - Designed to hijack Internet of Things (IoT) devices and turn them into remotely controlled “bots” capable of launching denial of service (DDoS) attacks on websites, networks and other digital infrastructure. ○ Stuxnet - Highly advanced computer worm Stuxnet that was designed to only affect specific Siemens SCADA (Supervisory Control and Data Acquisition) systems.
12:45	–	13:30	Lunch Break (45 mins)
13:30	–	15:15	**Session 7 (1h & 45 mins) Monitoring and Incident Response** ● Implementing continuous monitoring for IoT and Blockchain systems ○ Real Time Monitoring ○ Anomaly Detection and Threat Intelligence ● Developing incident response plans

			○ Reporting and Escalation ○ Post incident analysis and Improvement ○ Compliance Reporting and Auditing ● Case studies and exercises on incident handling ● Case Study: Doncaster: Managing a cyber attack ○ Malware – in this case a piece of ransomware called TeslaCrypt managed to get onto the council's network.
15:15	–	15:30	Break (15 mins)
15:30	–	17:15	**Session 8 (1h & 45 mins) – Future Trends and Conclusion** ● Exploring upcoming trends in cybersecurity and emerging technologies ● Review of key takeaways and best practices ● Q&A and discussion on implementation challenges and solutions ● *Final Evaluation (***Απολογιστική***)*

Day 3: Consulting Sessions

Electi Consulting's team will circulate a questionnaire to the companies ahead of time in order to assess the security levels and tech maturity of the company (e.g., existence of data and their quality, information systems used, security protocols in place, culture etc.), the challenges faced and future goals.
The team will then arrange a meeting and will visit the physical premises of interested companies to:

- Share the material prepared on how to address cybersecurity challenges specifically to the industry the company operates in
- Discuss use cases relevant to the business
- Recommend pilot projects the company can start on involving IoT and Blockchain to navigate cyber challenges