Cyber Security and Operational Technologie (OT)

Maritemex
Holistic Cyber Security Resilience

1. COURSE

This seminar is dedicated to:

- An understanding of OT network components and functionality (PLCs, SCADA, switches,
- LAN, DSL, MODBUS etc)
- Drivers for Security – 'without security we can't be safe' – component of 61511. A
- component part of functional safety is 62443, NISD, Cyber Assessment Framework and
- OFGEM's guidance notes
- Myths in OT
- Social Engineering
- Supply Chain Security
- What is malware? How it works, and some examples of relevant malware
- What are threat actors, what ones do we need to worry about and how do they work?
- Physical access, how could someone compromise a remote site?
- Insider threats, local privilege escalation.
- Cyber Risk Identification & Management
- Kill Chain
- Mitre ATT&CK
- How to defend against compromise – Break the Chain

2. COURSE CONTENT

The integration of operational technology (OT) and information technology (IT) has a significant impact on industrial cybersecurity. Specifically, industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems that have historically been air gapped are now being connected to IT systems — and therefore to the internet.

As the air gap is removed, these systems are exposed to an increasingly advanced threat landscape and are targets for hackers involved in terrorism, cyber warfare, and espionage. This course will ensure that candidates understand the implications of OT security and give practical solutions to progressing and securing a business's Cyber Security footprint.

4. COURSE FORMAT

Learners will engage in an interactive workshop which will allow them to develop theoretical knowledge and apply it to their own situations. Delivery will be through a blended approach that will allow learners to fully engage in the session and gain practical examples of how to turn theory into practice.

5. DETAILED COURSE PROGRAM (unrolled training sequences)

Delivery will progress the theoretical and knowledge base of the required modules for the formal qualification. Sessions will be spread across the five days and progress at the pace of the learners using detailed activities that both develop practical application and real life implementation of the learning.

5. COURSE PREPARATION

This is a specialist course that is specific to anyone who requires to develop skills in OT as a means of supporting Cyber Security resilience across the business.

6. COURCE EVALUATION

Participant engagement and contribution is essential in this course. It is expected that all learners fully interact with the learning and the group activities.

7. BIOGRAPHY

All course tutors will have the following professional credentials.

- UK National Cyber Security Centre Certified Trainers
- Higher level professional and teaching qualifications, gained over a career in Cyber Security practice.
- Contribution to the profession, giving back to the community at large, through voluntary engagement and seats on esteemed industry panels, working groups and special interest groups.
- Wide experience of professional roles in Cyber Security, leading to national and in many cases international reputations in domain.

- A complete and extended understanding of Cyber Security, Information Governance across a number of sectors
- A wide-ranging understanding of Finance and Procurement in relation to Cyber Security related practices

Our experienced, expert and engaging NCSC and Executive Trainer pool includes the following profiles:

NCSC Certified and Executive Trainer: Experienced strategy adviser and solution implementer, with international leadership experience in both government and commercial organisations. Over 22 years' experience in the fields of Cyber Security, Information Assurance and Information and Communications Technology after a background in Computer Science and Computing Information Systems. A Visiting Teacher of Cyber Security at the Oxford Martin School of Oxford University. Leads on audits and compliance-related activities with a focus on Critical National Infrastructure, including Central Government and Law Enforcement.

NCSC Certified Executive Trainer: Extensive financial services sector, developing Cyber Security and Information Assurance strategies, delivering Board briefings, leading audits and training and mentoring Senior Executives. Clients include G7 banks, central banks, retail banks and private equity firms. A thought leader in the area of Cyber Security and Information Assurance, speaking at conferences with articles regularly published. A visiting Professor at Oxford University.

NCSC Certified and Executive Trainer: Extensive experience includes mentoring Senior Executives in both the private and public sector. An established and highly effective leader with operational and commercial experience spanning private and defence sectors in the UK, Europe and the Middle East. Led Cyber Health Checks and Audits for multi-national clients, identifying key Cyber risks and threats and advising on improving Cyber resilience.

NCSC Certified and Executive Trainer: Expertise and experience in delivering training and workshops to Board and senior audiences across government and the commercial sector. Background includes geopolitical risk and global threats, information risk and security, as well as risk mitigation, crisis management and prevention. Fostered networks for sharing best practice with Cyber Security organisations in the US, the EU and across the Commonwealth and was a member of the Cyber Assessment Advisory Panel at the UK National Cyber Security Centre (NCSC).

NCSC Certified and Executive Trainer: coaches and trains leadership on Cyber and Risk across sectors and in the Critical National Infrastructure. Brings significant operational and field experience to his practitioner and academic work and specialises in the human dimension of cyber security. Previously, he was Chief Executive of a UK national body and author of a number

of Cyber Security books sold internationally.

NCSC Certified and Executive Trainer: Experience of wide ranging oganisational support. Advises on information governance policy development and Cyber Security leadership and strategy. Background in education, academia and the not-for-profit sector has seen him advise government on national skills strategies and develop skills programmes in Cyber Security across the UK. Vice Chairman of the Information Assurance and Advisory Council. Working with national and regional bodies, and private sector parties, he focuses on developing regional cyber resilience strategy. Recipient of a National Cyber Security Award for his work with young people and cyber security.