COURSE OVERVIEW IE0258
OT Cybersecurity

Course Title
OT Cybersecurity

Course Date/Venue
July 14-18, 2025/Glasshouse Meeting Room, Grand Millennium Al Wahda Hotel, Abu Dhabi, UAE

Course Reference
IE0258

Course Duration/Credits
Five Days/3.0 CEUs/30 PDHs

Course Description

This practical and highly-interactive course includes real-life case studies where participants will be engaged in a series of interactive small groups and class workshops.

This course is designed to provide participants with a detailed and up-to-date overview of OT Cybersecurity Setup. It covers the OT (operational technology) and its role in critical infrastructure; the fundamentals of OT systems; the threat landscape in OT environments and security assessment and risk management; the network segmentation, access control and security for industrial control systems (ICS); the incident response plan specific to OT systems and responding to cybersecurity incidents in OT environments; the physical security for OT systems, security monitoring and intrusion detection; and securing configurations and developing patch management strategies for OT systems.

During this interactive course, participants will learn the cybersecurity awareness and the human factor in OT cybersecurity; the role of encryption and cryptography in securing OT communications; the wireless communication technologies, securing wireless network configurations and addressing the unique challenges of wireless security in OT environments; the vendor and supply chain security, security testing and vulnerability management; the remote access for OT networks and security for cloud-based OT systems; the compliance and regulatory requirements; and the emerging trends, technologies in OT/cybersecurity, future challenges and considerations.

Course Objectives

Upon the successful completion of this course, each participant will be able to:-

- Apply and gain an in-depth knowledge on OT cybersecurity setup
- Discuss the OT (operational technology) and its role in critical infrastructure including the fundamentals of OT systems
- Identify threat landscape in OT environments and carryout security assessment and risk management
- Implement network segmentation, access control and security for industrial control systems (ICS)
- Develop an incident response plan specific to OT systems and identify and respond to cybersecurity incidents in OT environments
- Discuss physical security for OT systems and apply security monitoring and intrusion detection
- Implement secure configurations and develop patch management strategies for OT systems
- Promote cybersecurity awareness, design training programs and address the human factor in OT cybersecurity
- Recognize the role of encryption and cryptography in securing OT communications
- Secure wireless communication technologies, implement secure wireless network configurations and address the unique challenges of wireless security in OT environments
- Apply vendor and supply chain security, security testing and vulnerability management
- Secure remote access for OT networks and apply security for cloud-based OT systems
- Recognize the compliance and regulatory requirements including the emerging trends, technologies in OT/cybersecurity and future challenges and considerations

Exclusive Smart Training Kit - H-STK®

*Participants of this course will receive the exclusive "Haward Smart Training Kit" (**H-STK®**). The **H-STK®** consists of a comprehensive set of technical content which includes **electronic version** of the course materials conveniently saved in a **Tablet PC**.*

Who Should Attend

The course provides an overview of all significant aspects and considerations of OT cybersecurity setup for all industrial engineers, industrial control system (ICS) engineers, OT system operators, IT security professionals, executives and board members.

Course Fee

US$ 5,500 per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Certificate(s)

Internationally recognized certificates will be issued to all participants of the course who completed a minimum of 80% of the total tuition hours.

Certificate Accreditations

Haward's certificates are accredited by the following international accreditation organizations: -

- British Accreditation Council (BAC)

  Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. Haward's certificates are internationally recognized and accredited by the British Accreditation Council (BAC). BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.

- The International Accreditors for Continuing Education and Training (IACET - USA)

  Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

  Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units** (CEUs) in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

  Haward Technology Middle East will award **3.0 CEUs** (Continuing Education Units) or **30 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.

Accommodation

Accommodation is not included in the course fees. However, any accommodation required can be arranged at the time of booking.

Course Instructor(s)

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:

Dr. Peter Lalos, PhD, MSc, BSc, is a **Senior IT, Telecommunications, Control & Electronics Engineer** with over **20 years** of extensive experience in the areas of **IT Risk Management** Concepts, **IT Risk Management** Standard Approaches, I**T Risk Management** Planning, **IT Risk** Identification, **IT Risk Monitoring** & **Control**, **Information Technology** Architectures, **Application** Architecture, **Logical Applications**, **Interface**s & Services, Logical & Physical Components, **Portfolio** Management, **Application Security**, **Application Integration** Technologies & Strategies, **Solution Architecture** Patterns, **Web Applications** & Services, **Mobile** & **Cloud Applications**, **Blended Learning** Programs, **Web Programming**, **E-Commerce Strategies**, Advanced **Database Management** Systems, **Web Design**, **HCI**, 3D Animation, Multimedia Design, Gamification Techniques, Internal & External Auditing, **OS Architectures** and **Network Security**. Further, he is also well-versed in ACAD, ASP, PHP, JSP, MS Visual Studio, VB.NET, ASP.NET, Moodle administration, Design & Development, WAMP & LAMP, Oracle JDeveloper, Oracle 11g, PL/SQL, MS SQL Server, MySQL, MS Access, HTML5, CSS, XML, XSD/ XSL, JavaScript, Ajax, Angular, jQuery, Web Services Adobe Suite, MS Office 2013, IIS Servers, MS Exchange Server & Apache Tomcat, Open Source CMS Expert (Xaraya, Joomla, Mambo) & Module Development, Open Source E-commerce Expert (oscommerce, Joomla & Virtuemart) and Module Development. Currently, he is the **IT Instructor/Subject Matter Expert** and **Course Developer** of the **University of Liverpool**, **UK**, wherein he lectures various courses in **Information Systems Program** and develop courses in Information Technology project management and security risk management.

During his career life, Dr. Lalos has gained his practical and field experience through his various significant positions and dedication as the **IT Manager**, **Bid Manager** & **S/W Developer**, **Project Manager**, **E-Learning Software Manager**, **Scrum Master**, **IT Professor**, **IT Lecturer/Trainer**, **Telecommunications**, **Control** & **Electronics Lecturer**, **Physics Instructor**, **Scientific Advisor**, **E-Learning Specialist**, **Undergraduate** & **Postgraduate Thesis Supervisor**, **IT Contractor**, **Laboratory Administrator**, **Moodle Expert** & **Administrator** and **Telecommunications Engineer** for various companies and universities such as the University of Greenwich, Empire State College, Roehampton University, University of East London, Athens Technology Center, University of Athens, **ShellGas**, Advanced Services Group (ASG), Piraeus University, Chemmedia Hellas Ltd., Conceptum S.A, IEK and Frontistirio Apopsi.

Dr. Peter has a **PhD** in I**T**, **Telecommunications**, **Control** & **Electronics** from the **University of Athens**, a **Master's degree** in **Information Technology** with **Web Technology** from the **University** of **Paisley**, **UK** and a **Bachelor's degree** in **Physics** from the **Aristotelian University** of **Thessaloniki**, **Greece**. Further, he is a **Certified Instructor/Trainer**, a **Scrum Master**, a **Certified Administrator** and an **LMS Specialist**. He has further published several journals, participated as an author in various projects and conducted numerous trainings, courses, workshops, seminars and conferences internationally.

Training Methodology

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

30% Lectures
20% Practical Workshops & Work Presentations
30% Hands-on Practical Exercises & Case Studies
20% Simulators (Hardware & Software) & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

Course Program

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the course for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

Day 1: Monday, 14th of July 2025

0730 – 0800	*Registration & Coffee*
0800 – 0815	*Welcome & Introduction*
0815 – 0830	***PRE-TEST***
0830 – 1000	***Introduction to OT/Cybersecurity*** *Overview of OT (Operational Technology) & Its Role in Critical Infrastructure • Introduction to Cybersecurity in the Context of OT Systems • Understanding the Importance of Securing OT Systems & the Risks Involved*
1000 – 1015	*Break*
1015 – 1130	***Fundamentals of OT Systems*** *Exploring the Components of OT Systems (e.g., SCADA, PLCs, RTUS) • Understanding the Communication Protocols Used in OT Environments (e.g., Modbus, DNP3) • Identifying Vulnerabilities & Potential Attack Vectors in OT Systems*
1130 – 1230	***Threat Landscape in OT Environments*** *Examining Common Cybersecurity Threats Faced by OT Systems • Analyzing Real-World OT Security Incidents & their Impact • Discussing the Motivations Behind OT Attacks (e.g., Espionage, Sabotage)*
1230 – 1245	*Break*
1245 – 1420	***Security Assessment & Risk Management*** *Conducting Security Assessments in OT Environments • Identifying Vulnerabilities & Weaknesses in OT Systems • Understanding Risk Management Methodologies for OT Security*
1420 – 1430	***Recap***
1430	*Lunch & End of Day One*

Day 2: Tuesday, 15th of July 2025

0730 – 1000	***Network Segmentation & Access Control*** *Implementing Network Segmentation to Isolate Critical OT Assets • Configuring Firewalls & Access Control Lists (ACLs) for OT Networks • Discussing Best Practices for Secure Network Architecture in OT Environments*
1000 – 1015	*Break*
1015 – 1130	***Security for Industrial Control Systems (ICS)*** *Exploring Security Considerations for Industrial Control Systems • Discussing ICS Security Standards & Frameworks (e.g., NIST SP 800-82, IEC 62443) • Implementing Security Controls for ICS Devices & Networks*

1130 – 1230	***Incident Response in OT Environments*** *Developing an Incident Response Plan Specific to OT Systems • Identifying & Responding to Cybersecurity Incidents in OT Environments • Conducting Post-Incident Analysis & Lessons Learned*
1230 – 1245	*Break*
1245 – 1420	***Physical Security for OT Systems*** *Understanding The Importance of Physical Security in Protecting OT Assets • Implementing Physical Access Controls & Surveillance Measures • Discussing the Integration of Physical & Cybersecurity Measures*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Two*

Day 3: Wednesday, 16th of July 2025

0730 – 1000	***Security Monitoring & Intrusion Detection*** *Deploying Security Monitoring Tools for OT Environments (e.g., SIEM, 1DS/IPS) • Analyzing Network Traffic & Log Data to Detect & Respond to Intrusions • Configuring Security Event Correlation & Alerting Mechanisms*
1000 – 1015	*Break*
1015 – 1130	***Secure Configuration & Patch Management*** *Implementing Secure Configurations for OT Devices & Software • Developing Patch Management Strategies for OT Systems • Discussing Challenges & Best Practices for Maintaining Secure Configurations*
1130 – 1230	***Security Awareness & Training*** *Promoting Cybersecurity Awareness among OT System Operators & Employees • Designing Training Programs for OT Personnel on Security Best Practices • Addressing the Human Factor in OT Cybersecurity*
1230 – 1245	*Break*
1245 – 1420	***Encryption & Cryptography in OT Environments*** *Understanding the Role of Encryption & Cryptography in Securing OT Communications • Implementing Encryption Mechanisms for Data in Transit & at Rest • Evaluating Cryptographic Algorithms & Key Management Practices*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Three*

Day 4: Thursday, 17th of July 2025

0730 – 1000	***Security for Wireless OT Networks*** *Securing Wireless Communication Technologies used in OT Systems • Implementing Secure Wireless Network Configurations • Addressing the Unique Challenges of Wireless Security in OT Environments*
1000 – 1015	*Break*
1015 – 1130	***Vendor & Supply Chain Security*** *Assessing the Security Risks Associated with Third-Party Vendors & Suppliers • Implementing Vendor Risk Management Practices for OT Systems • Establishing Secure Supply Chain Processes for OT Infrastructure*
1130 – 1230	***Security Testing & Vulnerability Management*** *Performing Security Testing & Vulnerability Assessments for OT Systems • Conducting Penetration Testing & Vulnerability Scanning • Developing a Vulnerability Management Program for OT Environments*
1230 – 1245	*Break*

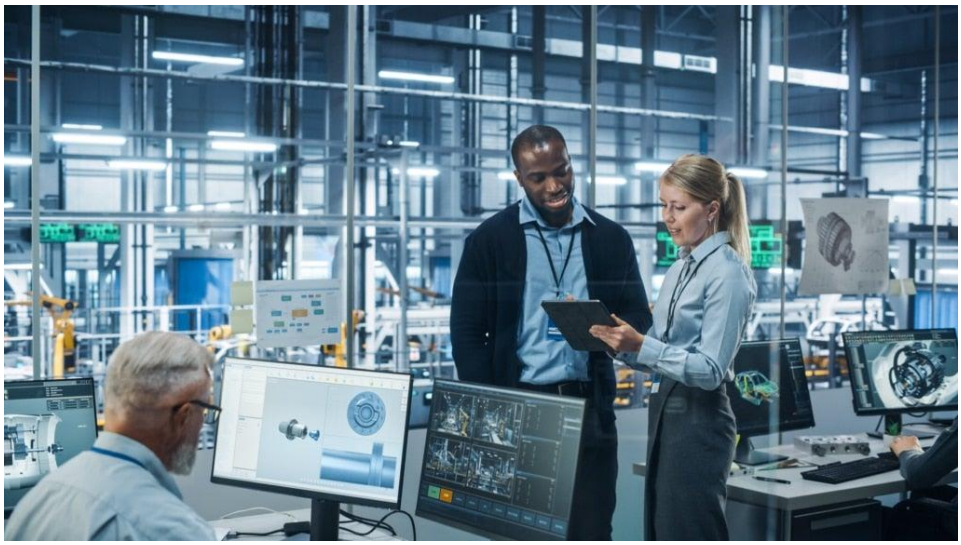
1245 – 1420	***Secure Remote Access for OT Systems*** *Implementing Secure Remote Access Solutions for OT Networks • Configuring VPNs & Two-Factor Authentication for Remote Access • Discussing Secure Remote Access Best Practices & Limitations*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Four*

Day 5: ***Friday, 18th of July 2025***

0730 – 1000	***Security for Cloud-Based OT Systems*** *Exploring Security Considerations for OT Systems Hosted in the Cloud • Understanding Cloud Security Controls & Shared Responsibility Models • Implementing Security Measures for Cloud-Based OT Deployments*
1000 – 1015	*Break*
1015 – 1130	***Incident Response Tabletop Exercise*** *Conducting a Simulated Incident Response Exercise for OT Systems • Testing the Effectiveness of Incident Response Plans & Procedures • Analyzing the Outcomes & Identifying Areas for Improvement*
1130 – 1230	***Compliance & Regulatory Requirements*** *Understanding Regulatory Frameworks & Compliance Requirements for OT Systems (e.g., NERC CIP, IEC 62443) • Aligning Security Practices with Industry-Specific Regulations • Conducting Audits & Assessments to Ensure Compliance*
1230 – 1245	*Break*
1245 – 1345	***Emerging Trends & Future Considerations*** *Exploring Emerging Trends & Technologies in OT/Cybersecurity • Discussing the Impact of Artificial Intelligence (Al) & Machine Learning (ML) in OT Security • Addressing Future Challenges & Considerations in OT Security*
1345 – 1400	***Course Conclusion***
1400 – 1415	***POST-TEST***
1415 – 1430	*Presentation of Course Certificates*
1430	*Lunch & End of Course*

Practical Sessions

This practical and highly-interactive course includes real-life case studies and exercises:-



Course Coordinator

Mari Nakintu, Tel: +971 2 30 91 714, Email: mari1@haward.org