MODULE **DESCRIPTOR**

MODULE TITLE	CYBER INCIDENT HANDLING		
MODULE CODE	CO4833 (L7)	**CREDIT VALUE**	20 UK CREDITS / 10 ECTS
SCHOOL	SCHOOL OF SCIENCES		

MODULE **AIMS**

The aims of this module are to:

•Provide an in-depth understanding of theoretical and practical aspects for incident handling.
•Introduce incident handling standards and best practices that students will most likely encounter as a security professional.
•Increase knowledge for collecting, handling and analysing evidence of incidents.
•Gain experience in using tools and techniques for incident analysis.

MODULE **CONTENT**

Introduction to Incident Handling

- Definition, goals and importance of incident handling
- Overview and main characteristics of Computer Emergency Response Teams
- Overview of the incident handling process, identification of incident response tasks, tools, classification
- Real-world incidents

Industry Standards and Best Practices, e.g.

- ISO/IEC 27035-1:2016 - Principles of incident management
- ISO/IEC 27035-2:2016 - Guidelines to plan and prepare for incident response
- NIST 800-61r2 - Computer Security Incident Handling Guide
- ENISA guides

Incident Detection and Characterization

- Incident scope, investigation setup, collection of initial facts, maintenance and prioritization
- Definition and usage of indicators
- Threat feeds
- Honeypots

Data Collection, Tools, Analysis and Reporting

- Define the analysis methodology and tools
- Network monitoring and evidence
- Malware analysis
- Visualization
- Remediation process
-

Legal framework and issues around incident handling

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:

1. Evaluate and compare theoretical and practical aspects of incident handling
2. Plan and design an incident investigation in accordance with standards and legal issues
3. Critically discuss and evaluate evidence of incidents
4. Identify and assess tools and techniques for incident handling

TEACHING METHODS

The theoretical material will be delivered during the lectures. The students are expected to actively participate and prepare for workshops, assessment briefs and other matters relating to the acquisition and evaluation of evidence. During the workshops, students will be introduced to incident response tools, processes and techniques. Furthermore, students will participate in hands-on labs for supporting incident response actions. Synchronous (i.e. in class) and/or asynchronous (i.e. blogs) discussions will take place to further discuss the students' practical findings. As a result of the discussions, additional directed reading may be required. There will be occasions when speakers from leading security organisations will be invited to share their industry experiences with the students.

Distance Learning

The module tutor will deliver the theoretical material through live online lectures in Adobe Connect. During the live lectures the participating students will have the opportunity to engage in discussions, present their views and ask questions. The lecture sessions will be recorded and made available to the students through Blackboard. Students who cannot participate in the live lectures will have the opportunity to answer and reflect on guided questions in the subsequent live lectures or participate asynchronously on discussion boards. Where appropriate, students will also be provided with relevant further reading, Web links and resources for independent study. Speakers from leading security organizations will be invited, where possible, to deliver live invited talks and enhance the students' experience.

. Virtual laboratories will be utilized to give the opportunity to students to apply their practical skills. Students will be provided with access to virtual laboratories through which they will be able to complete the practical components of the module. The students will obtain the practical worksheets from Blackboard and they are expected to follow the instructions included in the practical worksheets to complete the lab work. If students have difficulties with a particular exercise, they are expected to contact the module tutor or post a question on the discussion forum, where the module tutor and their peers can provide feedback. Different means of communication will be utilized by the tutor to offer support to the students based on the reported issue, i.e. email, Skype, MS Teams, virtual laboratories, etc.

Through the virtual laboratories, the students are expected to apply their theoretical knowledge to solve security problems in a professional and legal way. Feedback to the students will be provided asynchronously through Blackboard. If the need arises, the module tutor will schedule live sessions to provide further feedback to the students.

ASSESSMENT METHODS

This module is assessed through a report and an examination.