Technische Hochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

Training course outline

ITU and
Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences

Title	Cyber Incident Response
Modality	Online self-paced
Dates	January 15 – December 31, 2022
Duration	Flexible
Registration deadline	There are no deadlines for course registration. The course could be taken any time within indicated timeframe. An enrollment is happening continuously.
Training fees	USD 249,00
Description	CIR course will provide students with all necessary knowledge of cyber incident response activities, what are main goals and challenges, and explaining main roles and responsibilities in such important process. They will get most up to date trends in this area with an emphasis on most important details of each cyber incident response stage. Upon the successful completion of this course, students will be able take a part in development and implementation of cyber incident plan.
Code	22OS28025EUR-E

1.LEARNING OBJECTIVES

Upon the successful completion of this course, students will be able to define and describe main steps taken in Cyber Incident Response, understand main roles and responsibilities in response process and how they could be implemented in organization’s Cyber Security Plan.

2. LEARNING OUTCOMES

As a result of the course, participants will know:
- why Cyber Incident Response is important;
- what could be consequences of poor handled Incidents;
- how to prepare Cyber Incident Response Plan;
- what are main phases of Incident Response Process.

As a result of the course, participants will understand:

- how are roles and responsibilities spreading in Cyber Incident Response Process;
- what are main techniques and best practices using during each of Cyber Incident Response phase.

3.TARGET POPULATION

The course will be necessary for all employees and managers within organization with any information security role to understand how Incident Response works and what should be their own responsibilities as well as how communicate with other parties of Incident Response process. Regulator and national authorities should also attend this course to be able react on Incidents, which are outside of licensee responsibilities, such as APT.

4.ENTRY REQUIREMENTS

Basic understanding of IT-Security concepts and methods are required.

5.TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Contact details
Dmytro Cherkashyn	d.cherkashyn@uniss.org

6.TRAINING COURSE CONTENTS

Main modules of this course will cover following topics:

1. Incident Response and Recovery Overview
— Computer event and incidents;
— Goals of Cyber Incident Response;
— Incident response procedures principles;
— Incident Management and Response Process.
2. Preparedness and prevention
— Organization of the security incident response capability;
— Type of incidents to consider during IR planning;
— Incident Handling Checklist;
— Incident response team and general responsibilities.
3. Detection
— Indicators of an incident;
— Intrusion Detection technologies overview;
— Comparison of detection methods;
— Detection phase: responsibilities and roles.
4. Analysis
— Goals of analysis;
— Incident analysis, documentation and prioritization;
— Analysis phase: responsibilities and roles.
5. Containment
— Containment activities and challenges;
— Containment strategies;
— Containment: responsibilities and roles.

6. Investigation
— Investigation goals;
— Digital forensics terms and principles;
— Typical forensic analysis process;
— Investigation: responsibilities and roles.
7. Eradication and recovery
— Eradication activities;
— Information and system recovery principles;
— Preventive and reactive measures to recover data;
8. Post-Incident Activity
— Evidence preservation;
— Using and storing collected incident data;
— Corrective and compensative actions.

7.TRAINING COURSE SCHEDULE

There is no fixed schedule.

8.METHODOLOGY (Didactic approach)

The course is self-paced online course with lecturing materials accompanied with different media. Each page of the course includes link to external sources of information, which could be used to get deeper knowledge of some particular topics.
Each course module has a self-assessment quiz.

9.EVALUATION AND GRADING

Evaluation of participant success will happen through the final test of multiple-choice quizzes. Only participants who have successfully completed final test with a pass mark of 80% shall be awarded the ITU Certificate.

10.TRAINING COURSE COORDINATION

Course coordinator: Name: Dmytro Cherkashyn Email address: d.cherkashyn@uniss.org	ITU coordinator: Name: Jaroslaw Ponder Email address: eurregion@itu.int