ITU Centres of Excellence Network for Europe

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

Online Training Course on

CYBER INCIDENT RESPONSE

1 March – 31 December 2021

TRAINING COURSE OUTLINE

COURSE DESCRIPTION

Title	Cyber Incident Response
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.
Dates	1 March – 31 December 2021**
Duration	Flexible (About 4 weeks)
Registration deadline	There is no deadline for course registration. The course can be taken any time within indicated timeframe. An enrollment is happening continuously.
Training fees	USD 249
Course code	21OS26411EUR-E

DESCRIPTION OF THE TRAINING COURSE

The 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.

The course will be a self-studying course with an Q&A session (video conference) near the end of the course.
****While the course dates are open until December, participants are expected to finalize the course within 3 months counting as of March 1st. The following cohorts of students will start June 1st, September 1st and November 1st.**

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.

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.

ENTRY REQUIREMENTS

There are no specific requirements for this course; some knowledge of ICS basics would be an advantage tough.

TUTORS/INSTRUCTORS

NAME OF TUTOR(S)/INSTRUCTOR(S)	CONTACT DETAILS
Dmytro Cherkashyn	d.cherkashyn@uniss.org

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.

TRAINING COURSE SCHEDULE

Three weeks of self-studying the contents, after that, a live Q&A Session will help to clarify remaining questions. In the last week, the students will take the final exam.

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.
After completing the self-assessment, the students can discuss their remaining questions in an online live Q&A session (video conference) with their trainer before taking the final exam.

EVALUATION AND GRADING

Evaluation of participant success will happen through the series of multiple choice quizzes. Weights will be distributed as following next:

- 30% of the total grade will be the average grade for all interim quizzes;
- 70% of the total grade will be the final quiz grade.

TRAINING COURSE COORDINATION

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

REGISTRATION AND PAYMENT

ITU Academy portal account

Registration and payment should be made online at the ITU Academy portal.
To be able to register for the course you **MUST** first create an account in the ITU Academy portal at the following address: https://academy.itu.int/index.php/user/register

Training course registration

When you have an existing account or created a new account, you can register for the course online at the following link: https://academy.itu.int/training-courses/full-catalogue/cyber-incident-response-1

You can also register by finding your desired course in our training catalogue https://academy.itu.int/index.php/training-courses/full-catalogue

Payment

1. **On-line payment**

A training fee of USD 249 per participant is applied for this training. Payment should be made via the online system using the link mentioned above for training registration at https://academy.itu.int/training-courses/full-catalogue/cyber-incident-response-1 .

2. **Payment by bank transfer**

Where it is not possible to make payment via the online system, select the option for offline payment to generate an invoice using the same link as above. Download the invoice to make a bank transfer to the ITU bank account shown below. Then send the proof of payment/copy of bank transfer slip and the invoice copy to Hcbmail@itu.int and copy the course coordinator. **All bank transaction fees must be borne by the payer**.
Failure to submit the above documents may result in the applicant not being registered for the training.

3. **Group payment**

Should you wish to pay for more than one participant using bank transfer and need one invoice for all of them, create an account as **Institutional Contact. Institutional Contacts** are users that represent an organization. Any student can request to be an institutional contact or to belong to any existing organization.

To do this, head to your profile page by clicking on the **"My account"** button in the user menu. At the bottom of this page you should see two buttons:

a. If you want to **become an institutional contact**, click on the "**Apply to be an Institutional Contact"** button. This will redirect you to a small form that will ask for the organization name. After you fill the name of the organization you want to represent, click on **"continue"** and a request will be created. An ITU Academy manager will manually review this request and accept or deny it accordingly.

b. If you want to **belong to an existing organization**, click on the **"Request to belong to an Institutional Contact"** button. This will redirect you to a small form that will ask you to select the organization you want to join from an organization list. After you select the correct organization, click on **"continue"**, a request will then be created. The Institutional Contact that represents that organization will manually accept or deny your request to join the organization.

ITU BANK ACCOUNT DETAILS:	
Name and Address of Bank:	UBS Switzerland AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Beneficiary:	Union Internationale des Télécommunications
Account number:	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Amount:	USD 249
Payment Reference:	CoE-EUR 26411 - P.40595.1.07

4. Other method of payment

If due to national regulations, there are restrictions that do not allow for payment to be made using options 1 & 2 above, please contact the ITU coordinator for further assistance.