



ITU Centres of Excellence Network for Europe

NRD Cyber Security

FACE-TO-FACE Training Course on

INCIDENT RESPONSE PRACTICE

Vilnius, Lithuania
8-11 November 2021



TRAINING COURSE OUTLINE (FACE-TO-FACE)

COURSE DESCRIPTION

| | |
|-----------------------|--|
| Title | Hands-on scenario-based training INCIDENT RESPONSE PRACTICE |
| Objectives | Deliver fundamental theoretical and practical skills to handle and respond to the computer security incidents using real life incident logs and investigation tools. |
| Dates | 8-11 November 2021 |
| Duration | 4 days |
| Registration deadline | 30 October 2021 (<i>if a visa is not requested</i>) |
| Training fees | USD 800 |
| Requirement | Participants are required to bring a laptop with them |
| Course code | 21WS26399EUR-E |

DESCRIPTION OF THE TRAINING COURSE

For the efforts towards strengthening cyber security to be successful, technical teams must be specifically trained on practicalities of incident response. The course is designed to empower incident handlers to be effective at their work.

The training course presents a comprehensive overview of cybersecurity teams' issues on a technical level, vulnerability handling, trend/technology watch, security tools, and also issues of artefact handling and forensics. The course is technical in nature, relying heavily on hands-on and practical experience. The most recent threats and vulnerabilities are treated.

The training is dedicated to measure the readiness of CSIRT to deal with the most often real-world cases of cyber hands-on scenario-based training security incidents. The course is composed of series of exercises by providing participants with questionnaires and practical assignments on specific types of cyber security incidents.

Participants will be provided a set of specific pre-defined real-life incident scenarios. Several different incident handling cases are simulated to students and focused on incident detection and description, information gathering, analysis tools and techniques and incident handling phases by using RTIR (or related) tool. Cyber threat hunting tips are also provided to deeper knowledge in incident handling.

LEARNING OUTCOMES

Upon completion of this training, participants will be able to:

- apply incident response general workflow principles;
- follow the incident response procedure by using RTIR tool;
- conduct basic analysis of email messages and retrieve actionable data from email headers;
- investigate incidents by executing the system event log analysis;
- carry on incident root cause analysis;
- perform basic network forensic analysis.

TARGET POPULATION

The course is designed for CIRT members and all incident handlers who wish to be effective at their work.

ENTRY REQUIREMENTS

Basic technical knowledge of incident handling.

TUTORS/INSTRUCTORS

| NAME OF TUTOR(S)/INSTRUCTOR(S) | CONTACT DETAILS |
|--------------------------------|-----------------|
| | |

| | |
|--|--|
| Marius URKIS NRD CIRT lead, cyber security incident handling and forensics expert | mu@nrdfs.lt |
| Rimtautas ČERNIAUSKAS Technical cyber security consultant and investigator | rc@nrdfs.lt |
| Lecturers have been working in numerous countries on strengthening national cybersecurity environments in Asia, Africa, Europe and South America. | |

TRAINING COURSE CONTENTS

Session 1 Introductions and expectations

- Global view on incident handling

Session 2 Incident management

- Incident management key components
- Different incident handling workflow (ENISA, NIST, SANS, etc) and current improvements. Processes, Procedures, Standard operating procedure
- Incident handling process step by step
- Incident categories, triage
- Hands-on exercise related to triage

Session 3 – 4 Ticketing system

- RTIR Introduction
- Incident triage: initial evaluation of the incident information, classification
- Demo- usage cases, dashboards, incident handling workflow.
- Hands-on exercise related to Incident report, Incident ticket, communication etc.

Session 5 - 6 Email incidents

- Overview of Incident types, related to email usage: Spam, Phishing, Malware delivery, Distortion emails etc.
- Email system architecture and SMTP relay
- Comparison of forgery prevention techniques
- Email investigation
- Hands-on exercises related to phishing and spam cases

Session 7 - 8 Malware delivery by e-mails

- Malware class incidents
- Cyber attack cycle
- Demo- weaponizing MS Office document
- Malware analysis tools
- Hands-on exercise related to detection and analysis of the malicious e-mails

Session 9 Overview of log analysis tools

- Actionable data provided by Logs.
- Log analysis in Linux
- SIEM solutions, some tools demo.

Session 10 -13 Website Vulnerabilities and Log Analysis

- Website vulnerabilities: CSS/XSS ; Code injections ; Remote File Injection; Cross site request forgery (XSRF).

- Attack methods and their reflections in the logs.
- Tools for vulnerabilities management.
- Hands-on exercises.

Session 13 Network traffic monitoring

- Network traffic data collection and logging (network capture, netflows)
- Overview of network traffic analysis tools
- Malicious activity patterns in network traffic and their detection;
- Hands-on exercise relevant to the day topic: collection of information, analysis, incident handling according to the procedures

TRAINING COURSE SCHEDULE / AGENDA

| Date | Time | Topics/Activities |
|------------------------------|---------------|--|
| Date for day 1 8/11/2021 | 9:00 – 10:30 | <u>Session 1</u> • Introductions and expectations • Global view on incident handling |
| | 10:30 – 11:00 | Coffee break |
| | 11:00 – 12:30 | <u>Session 2</u> • Incident management key components |
| | 12:30 – 14:00 | Lunch break |
| | 14:00 – 15:30 | <u>Session 3</u> • Ticketing system • Hands-on exercise relevant to session topic • Review of exercise results |
| | 15:30 – 16:00 | Coffee break |
| | 16:00 – 17:00 | <u>Session 4</u> • Hands-on exercise relevant to the topic of the day • Review of exercise results |
| | | Time |
| Date for day 2 09/11/2021 | 9:00 – 10:30 | <u>Session 5</u> • Email incidents |
| | 10:30 – 11:00 | Coffee break |
| | 11:00 – 12:30 | <u>Session 6</u> • Hands-on exercise related to phishing e-mails • Review of exercise results |
| | 12:30 – 14:00 | Lunch break |
| | 14:00 – 15:30 | <u>Session 7</u> • Malware delivery by e-mails: methods, detection and protection |
| | 15:30-16:00 | Coffee break |
| | 16:00 – 17:00 | <u>Session 8</u> • Hands-on exercise related to detection and analysis of the malicious e-mails • Review of exercise results |
| | | Time |
| Date for day 3 10/11/2021 | 9:00 – 10:30 | <u>Session 9</u> • Overview of log analysis tools |

| | | |
|-------------------------------|---------------|--|
| | 10:30 – 11:00 | Coffee break |
| | 11:00 – 12:30 | <u>Session 10</u> <ul style="list-style-type: none"> Website vulnerabilities, attack methods and their reflections in the logs |
| | 12:30 – 14:00 | Lunch break |
| | 14:00 – 15:30 | <u>Session 11</u> <ul style="list-style-type: none"> Hands-on exercise related to the topic of the day Review of Exercise results |
| | 15:30 – 16:00 | Coffee break |
| | 16:00 – 17:00 | <u>Session 12</u> <ul style="list-style-type: none"> Hands-on exercise to day topic Review of Exercise results |
| | Time | Topics/Activities |
| Date for day 4 11/11//2021 | 9:00 – 10:30 | <u>Session 13</u> <ul style="list-style-type: none"> Network traffic monitoring |
| | 10:30 – 11:00 | Coffee break |
| | 11:00 – 12:30 | <ul style="list-style-type: none"> Hands-on exercise relevant to the day topic Review of exercise results |
| | 12:30 – 14:00 | Lunch break |
| | 14:00 – 17:00 | <ul style="list-style-type: none"> Final Test Sum up of training course Q&A and feedback on training course |

METHODOLOGY (Didactic Approach)

The training course material is based on illustrative real-life cases and their analysis. The course will be delivered using lectures, case studies, roundtable and hands-on exercises.

Slide sets will be provided as well as access to online material will be granted where applicable.

EVALUATION AND GRADING

Besides the final test score (80% of total), the participants will be evaluated reflecting quantity of time spent on the training (20%).

TRAINING COURSE COORDINATION

| | |
|--|--|
| Course coordinator: Name: Ruta Jasinskiene Email address: ITUCoE@nrdfs.lt | ITU coordinator: Name: Jaroslaw Ponder Email address: Jaroslaw.ponder@itu.int |
|--|--|

COVID-19 MEASURES

The following basic general principles as well as the actual restrictions are implemented:

- Participant or/and staff who feels sick or have temperature not allowed to participate in the training (the measurement of temperature is mandatory on entry to the training room each day);
- Face mask wearing during the training is encouraged
- Distancing measures to reduce close contact among people during an event are followed;
- Soap and water or alcohol hand-sanitizers and tissues are easily accessible in all common areas;
- Information on hand hygiene and respiratory etiquette, including with visual/informational materials are provided;
- Other measures are introduced according relevant Lithuanian government, EU and WHO recommendations.

The most relevant information about Coronavirus (COVID-19) and restrictions in Lithuania: <https://koronastop.lrv.lt/en/>

Please consult the following official governmental website for the newest important information regarding the Coronavirus (COVID-19) necessary for traveling to Lithuania
<https://urm.lt/default/en/important-covid19>

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/incident-response-practice>

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 800 per participant is applied for this training. Payments should be made via the online system using the link mentioned above for training registration at <https://academy.itu.int/training-courses/full-catalogue/incident-response-practice> .

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 800 |
| Payment Reference: | CoE-EUR 26399 – P.40595.1.08 |

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.