ITU Centres of Excellence Network for Europe

NRD Cyber Security

Online Instructor Led Training Course on

BUILDING AN EFFECTIVE CYBERSECURITY TEAM

Vilnius, Lithuania
19-22 April 2021

TRAINING COURSE OUTLINE

COURSE DESCRIPTION

Title	**Building an effective cybersecurity team**
Objectives	Deliver fundamental theoretical and practical guidance on building an effective cybersecurity team and knowledge necessary to plan it, involve relevant actors, define duties and responsibilities, ensure the governance of a team, and assess the efficiency of services delivered.
Dates	19-22 April 2021
Duration	4 days, 32 academical hours (CPE available)
Registration deadline	Registration should be submitted by 10 April 2021
Training fees	800 USD, paid to ITU
Course code	21OI26398EUR-E

DESCRIPTION OF THE TRAINING COURSE

The training will be run online only.

The course dives deep into CSIRT/SOC establishment practice, where combination of theory, unique experience with lessons learned, and hands-on practice give attendees a clear and actionable picture on how to build an effective cybersecurity team.

This training helps to successively prepare for cybersecurity team establishment and answers the main questions raised before starting:

1. How to build an effective cybersecurity team? Overview, discussion, and practice about a mandate, governance, team and its structure, timeline, lessons learned from similar establishments, financial planning.
2. What services in addition to incident management to introduce and how? Applied mandatory and complimentary services, best international practice for services models, incident management, incident management workflows and variations.
3. What technology is behind it? Scrutiny of principal architecture for CSIRT stack, integrations and managerial (not technical) look into technologies, automation vs manual, and technology trends.
4. How to mature security services and when? Elaboration of KPIs, SLAs and related metrics, security briefings, weekly/monthly/quarterly/yearly reports, analysis of examples and exercises on how to plan improvements for security services provided.
5. What is the baseline for it? Presentation of best international models measuring the maturity of cybersecurity team and its various components, advice on how to use them and how they help in operational environment.

LEARNING OUTCOMES

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

1. Lead security team establishment activities
2. Clearly define the position, role and responsibilities of cybersecurity team within an organisation or the state
3. Elaborate and measure the services provided by cybersecurity team
4. Understand the technologies used by cybersecurity team
5. Set up the requirements and timelines for cybersecurity team establishment

TARGET POPULATION

The training is designed for non-technical professionals who are (or will be) responsible for cybersecurity teams/CSIRT/CERT/SOC establishment, management and growth in governmental and private sectors. Such leader must possess strong understanding about the

purposes, requirements, duties and effective performance of the unit and be able to implement it in practice.

ENTRY REQUIREMENTS

No prerequisites required.

TUTORS/INSTRUCTORS

NAME OF TUTOR(S)/INSTRUCTOR(S)	CONTACT DETAILS
Dr. Vilius Benetis CSIRT/SOC architect, cybersecurity incident handling expert, researcher practitioner, Director at NRD Cyber Security	vb@nrdcs.lt
Trainer has been working in numerous countries on strengthening national cybersecurity environments in Asia, Africa, Europe, South America.	

TRAINING COURSE CONTENTS

Session 1. Introductions and Expectations

Session 2. Cybersecurity Monitoring & Incident Response Teams
An overview of the different types of cybersecurity teams: similarities and differences. Essential elements for national incident handling capabilities. Use cases for centralized and decentralized models. Different CSIRT/SOC stacks**.**

Session 3. Process of Building the CSIRT or SOC Team
Detailed explanation what stages elements are mandatory and what must be done during these stages. Typical implementation roadmap drawing. Initial idea and purpose.

Session 4. CSIRT Mandate
What it is and what content: Authority given to a CSIRT to serve and act in their constituency. Responsibility for what a CSIRT will be accounted for. Requirements, Objectives, and Tasks.

Session 5. CSIRT Services
Best international practice for cybersecurity team services models. Services typical sets. What services in addition to incident management to introduce and how? Free or charged services.

Session 6. Incident Management
Incident management workflows and variations. CSIRTs alternatively use. Classification of incidents.

Session 7. Automation of CSIRTs and SOCs
Scrutiny of principal architecture for CSIRT stack, integrations and managerial (not technical) look into technologies, automation vs manual, and technology trends. RTIR, MISP etc.

Session 8. Applied Threat Intelligence
Introduction to and discussion about Cyber Threat Intelligence.

Session 9. Reporting
Simplified "6W" method: What (objectives and content), When (how often), how (attractiveness of report) ant to whom (the audience).

Session 10. Maturity Models of CSIRTs
Presentation of the best international models measuring the maturity of cybersecurity team: SIM3 model, SOC-CMM model. Various components of cybersecurity team maturity assessment, advice on how to use them and how they help in operational environment.
Assessment of security services: how and when.
Elaboration of KPIs, SLAs and related metrics.
Use cases: Adjusting own growth to a reference model; Diagnosis and planning for improvement; Certification.

Session 11. Upskilling of People
What skills are needed. How decrease the gaps between your team current competence level and desired level. Training plan. Overview of actual possible on the market training courses.

Session 12. Partnering
Guidance on partnerships. Best practices overview: service models and implementation guidelines.

TRAINING COURSE SCHEDULE / AGENDA

Date	Time	Topics/Activities
day 1 **19/04/2021**	9:00 – 10:30	**Session 1** • Introductions and Expectations **Session 2** • Cybersecurity Monitoring & Incident Response Teams
	10:30 – 11:00	Coffee break
	11:00 – 12:30	**Continuation of Session 2** • Cybersecurity Monitoring & Incident Response Teams • Group-work and discussion
	12:30 – 14:00	Lunch break
	14:00 – 15:30	**Session 3** • Process of Building the CSIRT or SOC Team • Examples and lessons learned from similar establishments • Group-work and discussion
	15:30 – 16:00	Coffee break

Date	Time	Topics/Activities
	16:00 – 17:00	**Session 4** • CSIRT Mandate • Group work and discussion • Sum-up of the day
day 2 **20/04/2021**	9:00 – 10:30	**Session 5** • CSIRT Services • Group work and discussion
	10:30 – 11:00	Coffee break
	11:00 – 12:30	**Session 6** • Incident Management • Group work and discussion
	12:30 – 14:00	Lunch break
	14:00 – 15:30	**Session 7** • Automation of CSIRTs and SOCs • Round table on “what can be automated”
	15:30 – 16:00	Coffee break
	16:00 – 17:00	**Continuation of Session 7** • Automation of CSIRTs and SOCs • Group work and discussion • Sum-up of the day
day 3 **21/04/2021**	9:00 – 10:30	**Session 8** • Applied Threat Intelligence • Group work and discussions
	10:30 – 11:00	Coffee break
	11:00 – 12:30	**Session 9** • Reporting • Group work and discussions
	12:30 – 14:00	Lunch break
	14:00 – 15:30	**Session 10** • Maturity models of CSIRTs
	15:30 – 16:00	Coffee break
	16:00 – 17:00	**Continuation of Session 10** • Maturity models of CSIRTs • Group work and discussions • Sum up of the day
day 4 **22/04/2021**	9:00 – 10:30	**Session 11** • Upskilling of People • Group work and discussions
	10:30 – 11:00	Coffee break
	11:00 – 12:30	**Session 12** Partnering • Group work and discussions • Sum-up of training course
	12:30 – 14:00	Lunch break
	14:00 – 17:00	• Final Test (approx. 2-3 hours) • Evaluation Form (approx. 10 min)

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 discussions, and group play methods.

Hand-outs (where applicable), slide sets and additional material will be provided on ITU Academy platform.

4MAT is to be used in following application for all sessions: interactive discussion on a topic, practicing the topic, interactive discussion identifying if/what learning points were achieved, noting down individually what habits are relevant to change from now. Individual notes to be reviewed at the end of the day.

At the end of the course the final test will be conducted on the ITU Academy platform.

EVALUATION AND GRADING

Besides the final test score (70% of total), participants will be evaluated according to their active participation in roundtables, exercises sessions and other course activities (30% of total).

TRAINING COURSE COORDINATION

Course coordinator:	**ITU coordinator:**
Name: Ruta Jašinskienė	Name: Ana Maria Meshkurti
Email address: ITUCoE@nrdcs.lt	Email address: ana.maria.meshkurti@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/building-effective-cybersecurity-team-0

You can also register by finding your desired course in our training catalogue https://academy.itu.int/index.php/training-courses/full-catalogue and in search field entering "Building an effective cybersecurity team".

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/building-effective-cybersecurity-team-0

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 26398 – 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.