ITU Centres of Excellence Network for Europe

NRD Cyber Security

FACE-TO-FACE Training Course on

BUILDING AN EFFECTIVE CYBERSECURITY TEAM

Vilnius, Lithuania
4-7 May 2020

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	4 - 7 May 2020
Duration	4 days
Registration deadline	24 April 2020 (*if a visa is not requested)*
Training fees	USD 800

Course code	20WS24820EUR-E

LEARNING OUTCOMES

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

- Lead security team establishment activities
- Clearly define the position, role and responsibilities of cybersecurity team within an organisation or the state
- Elaborate and measure the services provided by cybersecurity team
- Understand the technologies used by cybersecurity team
- 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.

TUTORS/INSTRUCTORS

NAME OF TUTOR(S)/INSTRUCTOR(S)	CONTACT DETAILS
Dr. Vilius BENETIS CSIRT/SOC architect, cybersecurity incident handling expert, researcher practitioner, CEO of NRD Cyber Security	vb@nrd.no
Sigitas ROKAS Corporate Governance of Information Security Expert and the manager for CSIRT/SOC establishment projects	sr@nrdcs.lt
Trainers have been working in numerous countries on strengthening national cybersecurity environments in Asia, Africa, Europe, South America	

EVALUATION

Besides the final test score (60% of total), participants will be evaluated according to their active participation in roundtables, exercises sessions and other course activities (30% of total), reflecting quantity of time spent on the training (10%).

TRAINING SCHEDULE AND CONTENTS / AGENDA

Agenda

Date	Time	Activity
1st day		
04/05/2020 Monday	9:00 – 10:30	Session 1 • Introductions and expectations

		• An overview of the different types of cybersecurity teams: similarities and differences
	10:30 – 11:00	Coffee break
	11:00 – 12:30	Session 2 • Round table and practice about cybersecurity team mandate, governance, timeline, financial planning.
	12:30 – 13:30	Lunch break
	13:30 – 15:00	Session 3 • Discussion and practice about cybersecurity team size and structure. • Examples and lessons learned from similar establishments.
	15:00 – 15:30	Coffee break
	15:30 – 17:00	Session 4 • Overview on mandatory services of cybersecurity team. • Discussion • Sum-up of the day
2nd day		
05/05/2020 Tuesday	9:00 – 10:30	Session 5 • What services in addition to incident management to introduce and how? • Best international practice for cybersecurity team services models. • Roundtable discussion.
	10:30 – 11:00	Coffee break
	11:00 – 12:30	Session 6 • Incident management, incident management workflows and variations.
	12:30 – 13:30	Lunch break
	13:30 – 15:00	Session 7 • Scrutiny of principal architecture for CSIRT stack, integrations and managerial (not technical) look into technologies, automation vs manual, and technology trends.
	15:00 – 15:30	Coffee break
	15:30 – 17:00	Session 8 • Assessment of security services: how and when. • Elaboration of KPIs, SLAs and related metrics • Exercises • Sum-up of the day
3rd day		
06/05/2020	9:00 – 10:30	Session 9

Wednesday		• Security briefings, weekly/monthly/quarterly/yearly reports, analysis of examples and exercises on how to plan improvements for security services provided
	10:30 – 11:00	Coffee break
	11:00 – 12:30	Session 10 • Presentation of the best international models measuring the maturity of cybersecurity team
	12:30 – 13:30	Lunch break
	13:30 – 15:00	Session 11 • Various components of cybersecurity team maturity assessment, advice on how to use them and how they help in operational environment. • Practical exercise.
	15:00 – 15:30	Coffee break
	15:30 – 17:00	Session 12 • Final Test • Sum up of training course • Q&A and feedback on training course
4th day	Time	Topics/Activities
07/05/2020 Thursday	10:00 – 15:00	Session 13 Site visit • CSIRT/SOC technologies on the spot. Attendees will be led through service desks / incident tracking systems, vulnerabilities assessment and penetration testing tools, stack for cyber threat intelligence

METHODOLOGY

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 group play methods. In addition, the participants will benefit from SOC site visit.

Hand-outs and slide sets will be provided as well as access to online material will be granted where applicable.

COURSE COORDINATION

Course coordinator:	**ITU coordinator:**
Name: Ruta Jasinskiene Email address: ITUCoE@nrdcs.lt	Name: Mrs Rosheen Awotar-Mauree Email address: Rosheen.awator@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/user/register

Training 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

You can also register by finding your desired course in our training catalogue https://academy.itu.int/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/building-effective-cybersecurity-team

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:	20WS24820EUR-E - WBS: 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.