Training course outline

NRD Cyber Security
ITU Centres of Excellence Network for Europe

Title	CSIRT/SOC ESTABLISHMENT AND MODERNISATION
Modality	Online Instructor Led
Dates	14 – 17 March 2022
Duration	4 days
Registration deadline	13 March 2022
Training fees	800 USD
Description	The course dives deep into CSIRT/SOC establishment practice, where a combination of theory, unique experience with lessons learned, and hands-on practice give attendees a clear and actionable picture of how to build an effective cybersecurity team. Training delivers fundamental theoretical and practical guidance on CSIRT/SOC planning, involvement of relevant actors, defining CSIRT/SOC (including specific roles) duties and responsibilities, ensuring the governance of a team, and assessing the efficiency of services delivered.
Code	

1. LEARNING OBJECTIVES

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.

2. 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

3. 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.

4. ENTRY REQUIREMENTS

N/A

5. 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.	

6. 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.

7. TRAINING COURSE SCHEDULE

Week / Session/Day	Topic	Exercises and interactions
Date for day 1 14/03/2022	Session 1_Introductions and Expectations	
	Session 2_Cybersecurity Monitoring & Incident Response Teams	Group-work and discussion on cybersecurity responsibility handling
	Session 3_ Process of Building the CSIRT of SOC Team	Group-work and discussion on stakeholders & CSIRT establishers list elaboration
	Session 4_ CSIRT Mandate	Group work and discussion on CSIRT/SOC mandates Sum-up of the day
Date for day 2 15/03/2022	Session 5_ CSIRT Services	Group work and discussion on example of real CSIRT delivered services
	Session 6_Incident Management	Group work and discussion related to the topic
	Session 7_Automation of CSIRTs and SOCs	Group work and discussion on ticketing automation
Date for day 3 16/03/2022	Session 8_Applied Threat Intelligence	Group work and discussion on Threat Intelligence add value
	Session 9_Reporting	Group work and discussion on review of available CSIRTs' reports
	Session 10_ Maturity Models of CSIRTs	Use case_1_Adjusting own growth to a reference model Use case_2_ Diagnosis and planning for improvement Use case_3_ Certification
Date for day 4 17/03/2022	Session 11_ Upskilling of People	Group work and discussions on how develop skills profiles
	Session 12_Partnering	Group work and discussions on experiences working with LE on Cybercrime
	Session 13_Final exam	

8. 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.

9. 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 (20% of total), reflecting quantity of time spent on the training (10%).

10. TRAINING COURSE COORDINATION

Course coordinator: Name: Ruta Jašinskienė Email address: ITUCoE@nrdcs.lt	ITU coordinator: Name: Email address: