Training Course Outline

ITU and NRD Cyber Security

Title	CSIRT/SOC establishment and modernisation
Modality	Online instructor-led
Level	Intermediate
Dates	04/09/2023 – 06/09/2023
Duration	15 h
Language	English
Region	World or Multi-Regional
Registration type	Direct registration
Registration deadline	21/08/2023
Training fees	600 USD
Description	The CSIRT/SOC Establishment and Modernisation course is training program specifically designed to help organisations to establish an effective CSIRT/SOC team. The course provides a detailed guidance on the CSIRT/SOC team mandate and covers all the key elements required for its successful establishment. Our experienced instructors bring a wealth of knowledge and expertise to the course, drawing upon real-world cases to share the critical lessons learned. Through a combination of theory and practical exercises, participants will gain a clear and actionable understanding of how to build, modernize and manage a robust cybersecurity team. The course is comprehensive and methodical, covering all essential aspects of setting up a CSIRT/SOC team. Practical tips and tasks are provided to help participants plan their day-to-day activities, identify the services to provide to constituents, set KPIs, and choose the right tools to achieve their goals.

Training topics	*Cybersecurity*
Certification	*Certificate*
Code	*To be filled by ITU*

1. TARGET POPULATION

This training course is intended for non-technical professionals who are responsible for establishing, managing, modernising, and expanding cybersecurity teams (such as CSIRT/SOC/CIRT/CERT/PSIRT/ISAC) in both government and private sectors. These leaders must have a strong understanding of the unit's objectives, requirements, duties, and effective performance and be able to apply this knowledge in practice.

2. ENTRY REQUIREMENTS

No prerequisites required.

3. TRAINING OBJECTIVES

Upon completion of this course, 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
- Describe the technologies used by cybersecurity team
- Set up the requirements and timelines for cybersecurity team establishment

3. METHODOLOGY

This training course is designed to provide practical, real-world insights into cybersecurity team establishment and modernization. Participants will have the opportunity to learn from illustrative case studies and analysis, delivered through a range of teaching methods, including lectures, roundtable discussions, case studies, and group play activities.

All necessary course materials, including handouts (where applicable), slide sets, and additional resources, will be provided through the ITU Academy platform.

To ensure maximum engagement and retention, the 4MAT teaching methodology will be utilized in all sessions. This involves interactive discussions on a topic, practical exercises, discussions to identify learning points, and individual note-taking to reflect on relevant habits that can be changed moving forward. At the end of each day, individual notes will be reviewed to reinforce the key takeaways.

Finally, participants will be evaluated through a final test conducted on the ITU Academy platform at the end of the course. This approach ensures that participants leave the course with a comprehensive understanding of the material and are able to apply their newfound knowledge in practice.

4.ASSESSMENT 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%).

A total score higher than 70% is required to obtain the ITU certificate.

5. TRAINING DETAILS & INSTRUCTIONAL APPROACH

Day / Week / Module	Sessions/Topics covered	Key learning points (detail learning outcomes)	Training activities details
Module 1	**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.	An understanding on different types of cybersecurity teams	Lecturing, group work, discussions
Module 2	**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.	Set up the requirements and timelines for cybersecurity team establishment	Lecturing, group work, discussions
Module 3	**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.	Clearly define the position, role and responsibilities of cybersecurity team within an organisation or the state	Lecturing, group work, discussions
Module 4	**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.	Elaborate what services should be provided by CSIRT/SOC	Lecturing, group work, discussions
Module 5	**Incident Management** Incident management workflows and variations. CSIRTs alternatively use. Classification of incidents.	Ability to discuss Incident management workflow	Lecturing, group work, discussions
Module 6	**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.	An understanding of the technologies used by cybersecurity team and how it help in daily tasks	Lecturing, group work, discussions

Module 7	**Applied Threat Intelligence** Introduction to and discussion about Cyber Threat Intelligence.	What to expect from CTI and how it facilitates CSIRT operations	Lecturing, group work, discussions
Module 8	**Reporting** Simplified "6W" method: What (objectives and content), When (how often), how (attractiveness of report) ant to whom (the audience).	Experimenting with writing posts on the website and understanding how and how often to report	Lecturing, group work, discussions
Module 9	**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. Use cases: Adjusting own growth to a reference model; Diagnosis and planning for improvement; Certification.	Assessment of security services: how and when. Elaboration of KPIs, SLAs and related metrics.	Lecturing, group work, discussions
Module 10	**Upskilling of People and Partnering** 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. Guidance on partnerships. Best practices overview: service models and implementation guidelines.	Broader understanding of the team's need for competencies, preparation of training plan, and with whom and how it is necessary to cooperate	Lecturing, group work, discussions Final assessment

6. TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Title	Contact details
Dr. Vilius Benetis	Director of NRD Cyber Security CSIRT/SOC architect, cybersecurity incident handling expert, researcher practitioner, Director at NRD Cyber Security	vb@nrdcs.lt

7.TRAINING COURSE COORDINATION

Course coordinator	ITU coordinator
Title: Training Coordinator Name: Rūta Jašinskienė Email address: rj@nrdcs.lt	Title: Associate Capacity Development Officer Name: Célia Pellet Email address: hcbmail@itu.int