

ITU Regional Development Forum for Europe (RDF-EUR)

Information and Communication Technologies for attaining Sustainable Development Goals

organized by the International Telecommunication Union with the support of the National Authority for Management and Regulation in Communications (ANCOM) of Romania and cooperation with the European Conference of Postal and Telecommunication Administrations (CEPT)

22-23 May 2023
Timisoara, Romania

Remote participation at http://itu.int/go/RDF_EUR_23
(Meeting held back-to-back with Com-ITU of CEPT – 24-26 May 2023)

Please note that submitted information will be presented during the RDF-EUR P2C Roundtables and it will also be reflected on the pledging platform of the Partner 2 Connect Digital Coalition.

CONTRIBUTION FORM

ORGANIZATION: NRD Cyber Security, Lithuania

FOCAL POINT: Ruta Jasinskiene, Training coordinator, rj@nrdfs.lt, +37068632629

TITLE: ITU Academy Training Centre courses on cybersecurity

DESCRIPTION OF ACTION: [Provide a brief description up to 500 words]

NRD Cyber Security as one of the Academy Training Centers delivers high-quality ICT training and helps to build capacity for digital transformation across the globe. Our company aims to create a secure digital environment for countries, governments, businesses, and citizens. As part of our mission, we have developed two training courses that not only stand out for their relevance to today's challenges and the material they contain, based on the company's experience of projects around the world, but also because there are virtually no alternatives.

1. The National Cyber Crisis Management Course is the introductory two-day, scenario-based, purpose-built training designed to take participants to an intermediate level.

The course includes both theoretical and practical components covering a wide range of topics related to national cyber crisis management. Participants will explore the key concepts of cyber crisis management and understand the key roles and responsibilities of key stakeholders involved in national cyber security crisis management, including the role of CSIRTs.

In addition, the course will explain the importance of effective crisis communication. Finally, the course will include a scenario-based discussion where participants will be able to test the knowledge acquired during the training.

This training course is intended for national and sectorial CSIRTs, relevant national cyber crisis management authorities.

2. 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.

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.

COUNTRIES in FOCUS: [Name countries to be impacted by this action]

All countries are welcomed and could attend courses

YEARS of IMPLEMENTATION: [Tick the relevant boxes or delete the irrelevant items]

☒ 2023

RELEVANT ITU REGIONAL INITIATIVE: [Tick the relevant boxes or delete the irrelevant items]

☒ EUR4: Trust and confidence in the use of telecommunications/ICTs

RELATED ITU-D PRIORITIES AS DEFINED BY THE ITU WORLD TELECOMMUNICATION DEVELOPMENT CONFERENCE 2022

☒ Resource mobilization and international cooperation

☒ Inclusive and secure telecommunications/ICTs for sustainable development

RELATED ITU PRIORITIES AS DEFINED BY ITU PLENIPOTENTIARY CONFERENCE 2022

☒ Inclusive and secure telecommunication/ICT infrastructure and services

☒ Enabling environment

RELATED WSIS ACTION LINE: [Tick the relevant boxes or delete the irrelevant items]

☒ C4: Capacity building

☒ C5: Building confidence and security in the use of ICTs

☒ C6: Enabling environment

RELATED SDG: [Tick the relevant boxes or delete the irrelevant items]

☒ SDG 4: Quality Education

☒ SDG 16: Peace, Justice and Strong Institutions

☒ SDG 9: Industry, Innovation and Infrastructure

