



**Telecommunication
Development Bureau (BDT)**

Ref.: BDT/EUR/DM/107

Geneva, 24 June 2019

Administrations of ITU Member States,
Regulators, ITU-D Sector Members and
Academia Members in Europe

Subject: ITU Centres of Excellence face-to-face hands-on training course on Incident response practice, Vilnius, Lithuania, 17-20 September 2019

Dear Sir/Madam,

I am pleased to invite your organization to participate in the face-to-face, hands-on scenario-based, training course **“Incident response practice and training”**, which will be held in **Vilnius, Lithuania, from 17 to 20 September 2019**. This training is organized jointly by the International Telecommunication Union and NRD Cyber Security as part of the cybersecurity programme under the auspices of the ITU Centres of Excellence for Europe. The training will be delivered in English.

This training course aims to deliver fundamental theoretical and practical skills to handle and respond to the computer security incidents. The course addresses underlying principles and techniques for detecting and responding to current and emerging computer security threats. Several different incident handling cases will be simulated to students with a focus on: incident detection and description; information gathering; analysis tools and techniques; incident handling phases by using RTIR (or related) tool. Additionally, cyber threat hunting tips will be provided to broaden knowledge in incident handling.

All teaching material is based on illustrative real-life cases and their analysis that will be delivered by two prominent experts who will use lectures, case studies, roundtable and group play methods to make the course interactive.

After the course participants are expected to be able to:

- apply incident response general workflow principles;
- follow the incident response procedure by using RTIR tool;
- conduct basic analysis of email messages and retrieve actionable data from email headers;
- investigate incidents by executing the system event log analysis;
- carry on incident root cause analysis;
- perform basic network forensic analysis.

Detailed information on this training course is described in the course outline which can be downloaded from the ITU Academy Portal at the following link: <https://academy.itu.int/>. Please be informed that participants are required to bring a laptop with them.

The course is designed for CIRT, SOC members, all incident handlers, IT professionals and anyone who is interested in incident handling and response. Participants from all global regions are welcomed.

Registration should be made online at the aforementioned link no later than **30 August 2019**. Payment details are specified in the course outline.

Mr. Jaroslaw Ponder, Head of the ITU Office for Europe (euregion@itu.int), is at your full disposal should you require any information.

Additional information on this training course, such as an information note for participants, including a list of recommended hotels, is available at the ITU Academy portal at <http://academy.itu.int/>.

We look forward to your active participation in this training course.

Yours faithfully,

[Original signed]

Doreen Bogdan-Martin
Director