CERT–MU

Training course outline

ITU and National Computer Board / Computer Emergency Response Team of Mauritius

Title	**Building an effective Cyber Incident Response Team**
Modality	Online
Dates	16 – 18 November 2022
Duration	3 days
Registration deadline	11 November 2022
Training fees	Free
Description	The frequency and complexity of today's cyber-attacks makes incident response a critical function for organizations. The management of an incident response team is a very often-neglected topic. Incident response is the last line of defense against cyber-attacks for many organisations or even countries. Detecting and efficiently responding to incidents requires strong management processes and driving an incident response team requires special skills and knowledge. A background in information security management or security engineering is not sufficient for managing incidents. On the other hand, incident responders with strong technical skills do not necessarily become effective incident response managers.
Code	22OI28040AFR-E

1.LEARNING OBJECTIVES

The main objective of this training course is to allow participants to acquire sufficient knowledge on how to empower an incident response team for effective incident resolution and mitigate the impact of security threats within their organizations. Other objectives include:

- Learning the fundamentals of incident response, different incident response approaches from established international frameworks, the need for setting up a dedicated team and types of incident response teams

- Learning the basic requirements of an incident response team and assessing the team's effectiveness
- Learning about different strategies that can be employed to enhance an existing incident response team's functions

2. LEARNING OUTCOMES

This 3-day training course examines the key elements required to develop and improve the effectiveness of an incident response team. By the end of the course, participants will be able to understand the functions of an incident response team, how to assess their maturity and how to improve on existing capabilities.

3.TARGET POPULATION

The target audience for this course is as follows:

- Current and future CSIRT/CIRT/CERT managers and team members
- C-level managers such as CIOs, CSOs, CROs, CISOs
- Project leaders interested in establishing or starting a CSIRT/CIRT/CERT
- Cybersecurity professionals such as information security analysts, security engineers, incident handlers, network security administrators, malware analysts, IT professionals from ISPs, RENs, IXPs, SOCs, NOCs, TLDs, amongst others
- Other staff who work closely with CSIRTs/CIRTs/CERTs and would like to gain a deeper understanding of how these teams operate, e.g. CSIRT/CIRT/CERT constituents, higher-level management, media relations, human resources, audit or risk management professionals.

4.ENTRY REQUIREMENTS

Knowledge in cybersecurity and incident response

5.TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Contact details
Kaleem Usmani	kusmani@cert.ncb.mu
Sachindra Reechaye	sreechaye@cert.ncb.mu
Selvana Naiken Gopalla	sgopalla@cert.ncb.mu

6.TRAINING COURSE CONTENTS

Topics to be covered in this course are as follows:

- Introduction to incident response and management
  - What is incident response?
  - Types of incidents

  - Existing incident response frameworks
  - Incident response from a CERT's perspective
  - The rational behind setting up an incident response team
  - Types of incident response teams

- Design, establishment and assessment of incident response teams
  - Requirements for the setup of an incident response team
  - Operationalisation of the team
  - Assessment of the team

- Incident response teams' improvement strategies
  - Enhancement strategies

7.TRAINING COURSE SCHEDULE

Week / Session	Topic	Exercises and interactions
Day 1 **16 Nov 2022** **10am – 1pm** **(Geneva Time)**	Introduction to incident response and management	Presentations Discussion Group work Case studies
Day 2 **17 Nov 2022** **10am – 1pm** **(Geneva Time)**	Design, establishment and assessment of incident response teams	Presentations Discussion Group work Case studies
Day 3 **18 Nov 2022** **10am – 1pm** **(Geneva Time)**	Incident response teams' improvement strategies	Presentations Discussion Group work Case studies

8.METHODOLOGY (Didactic approach)

The training will be carried out online through the ITU Academy Platform. It will include presentations, discussion, group work, case studies and an exam.

9.EVALUATION AND GRADING

An exam will be conducted at the end of the course. Participants are required to get 60% of the marks in order to pass the exam. It is also to be noted that Presentations, Discussions, Group works, and Case studies will not be graded.

10.TRAINING COURSE COORDINATION

Course coordinator: Name: Manish Lobin Email address: mlobin@cert.ncb.mu	ITU coordinator: Name: Mr. Emmanuel NIYIKORA Programme Officer, ITU Area Office for West Africa, DAKAR Tel : +250 788312939 Email address: emmanuel.niyikora@itu.int