Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for Security
and Safety

ISS Training Plan

Guido Gluschke – February 8, 2019

Courses

ISS‘ Priority Area:

- Cybersecurity

ISS would like to provide two online courses in this area:

- Cybersecurity Techniques, starting in April
- Cyber Incident Response, starting in June

Module Description: Cybersecurity Techniques

A. Course title

Cybersecurity Techniques

B. Course objectives

Upon the successful completion of this course, students will be able to explain and give examples of IT and cyber security and use computer and communication security measures. They will be able to apply different intrusion detection methods and establish network management practice.

C. Short description

The course will provide theoretical and practical knowledge of IT and cyber security and security methods for computer, network and electronic communication.

Module Description: Cybersecurity Techniques

D. Main modules

1. Computer security and access control

— Prevention;

— Physical security;

— Computer operating systems;

— Access control principles;

— Remote maintenance.

2. Authentication and cryptography

— Authentication methods;

— Practical application.

Module Description: Cybersecurity Techniques

3. Computer security architecture

— Threats and vulnerabilities to computing infrastructure;

— Consequence analysis;

— Security levels, multilevel security;

— Security zones

4. Network security

— Network devices and services;

— Expected threats;

— Firewalls;

— VPNs;

— Secure LAN;

— E-mail communication.

Module Description: Cybersecurity Techniques

5. Intrusion detection and information recovery

— Common intrusion methods;

— Network attacks;

— Intrusion detection;

— Responses to intrusion;

— Computer forensics;

— Recovery plan.

6. Network management practice

— Automated vulnerability detection;

— Scanning techniques and approaches;

— Countermeasures against network threats.

Module Description: Cyber Incident Response

A. Course title

Cyber Incident Response

B. Course objectives

Upon the successful completion of this course, students will be able to define and describe main steps taken in Cyber Incident Response, understand main roles and responsibilities in response process and how they are implemented in organization's Cyber Security Plan.

C. Short description

The course will provide theoretical and practical knowledge of Cyber Incident Response activities, define their main goals and challenges, showing dominating roles in this process with responsibilities explained and make an emphasis on most important details of each Cyber Incident Response stage.

Module Description: Cyber Incident Response

D. Main modules

1. Incident Response and Recovery Overview

— Computer event and incidents;

— Goals of Cyber Incident Response;

— Incident response procedures principles;

— Incident Management and Response Process.

2. Preparedness and prevention

— Organization of the security incident response capability;

— Type of incidents to consider during IR planning;

— Incident Handling Checklist;

— Incident response team and general responsibilities.

Module Description: Cyber Incident Response

3. Detection

— Indicators of an incident;

— Intrusion Detection technologies overview;

— Comparison of detection methods;

— Detection phase: responsibilities and roles.

4. Analysis

— Goals of analysis;

— Incident analysis, documentation and prioritization;

— Analysis phase: responsibilities and roles.

5. Containment

— Containment activities and challenges;

— Containment strategies;

— Containment: responsibilities and roles.

Module Description: Cyber Incident Response

6. Investigation

— Investigation goals;

— Digital forensics terms and principles;

— Typical forensic analysis process;

— Investigation: responsibilities and roles.

7. Eradication and recovery

— Eradication activities;

— Information and system recovery principles;

— Preventive and reactive measures to recover data;

8. Post-Incident Activity

— Evidence preservation;

— Using and storing collected incident data;

— Corrective and compensative actions.

Module Overview

CYBERSECURITY

CYBERSECURITY TECHNIQUES [April]

ORGANISED BY

Technische Hochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

LANGUAGE
ENGLISH

FEES
250 USD

MODE
ONLINE

This online course will provide theoretical and practical knowledge of IT and cyber security and security methods for computer, network and electronic communication. The course consists of various chapters and will cover fundamentals, such as IT verses ICS, Threats and their Sources, Authentication, Computer Access Control, Cryptography, Network Security, Network Firewall Concepts, Intrusion Detection. The student will get a comprehensive view on security in the cyber space.

CYBERSECURITY

CYBER INCIDENT RESPONSE [June]

ORGANISED BY

Technische Hochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

LANGUAGE
ENGLISH

FEES
250 USD

MODE
ONLINE

The CIR course will provide students with all necessary knowledge of Cyber Incident Response activities, what are main goals and challenges, and explaining main roles and responsibilities in such important process.
They will get most up to date trends in this area with an emphasis on most important details of each Cyber Incident Response stage. Upon the successful completion of this course, students will be able take a part in development and implementation of Cyber Incident Plan.

Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for Security
and Safety

Thank you for your attention!

g.gluschke@uniss.org
www.uniss.org