CYBER DEFENCE TACTICS & TECHNIQUES

focal point

Cyber Defence Exercises as a Service

http://www.focalpoint-sprl.be

Course Description

1st Day: Interactive Training

- A highly interactive Course, where we will demonstrate attack and defensive scenarios of sophisticated attacks that most organisations face.
- Suggested responses & advice on how to evaluate strategies, tools, procedures and how to effectively collaborate with other team members.

KNOWLEDGE SHARING

Interactive way of learning

TARGET AUDIENCE

Ethical hackers, penetration testers, IT security professionals.

DURATION

2 days (9:00am – 5:00pm)

Course Description

2nd Day: Hands-On Training

- During the "hands-on" training, we will provide live & technical demonstrations of Cyber Attacks on a virtual infrastructure (Cyber Range).
- Participants will be trained on how to recognize the cyber attack and develop cyber situational awareness.

CYBER RANGE

Dedicated cyber range with a virtual infrastructure.

TARGET AUDIENCE

Ethical hackers, penetration testers, IT security professionals.

HANDS ON

Hands-on required for each exercise. Laptop is required.

Course Description

Organisation's Cyber Security Preparation

Most organisations do not exercise their defences, so they are uncertain about their capabilities and unprepared for identifying and responding to cyber-attacks.

In this Course we will answer the questions, and provide an overview on how your organisation can be benefit through training, testing, good practice and Cyber Defence Exercises.

Key questions

- Have you ever experienced a Cyber-related incident?
- Are your Security / Incident Response Teams ready to detect / respond to APT attack?
- Are your security monitoring and incident response processes good enough?
- Are your security solutions adequate to detect intrusions?
- Have you prepared your ''playbook'' in advance, before the Cyber incident?
- Are there any blind spots you've missed?

Course Description

After completing the Course, you will be able to:

- Evaluate strategies, tools and procedures
- Apply System Administration and prevention of attack
- Monitoring of networks, detecting and responding to attacks
- Handling cyber incidents
- Create a playbook for incident response
- Identify blind spots in your current processes

http://www.focalpoint-sprl.be