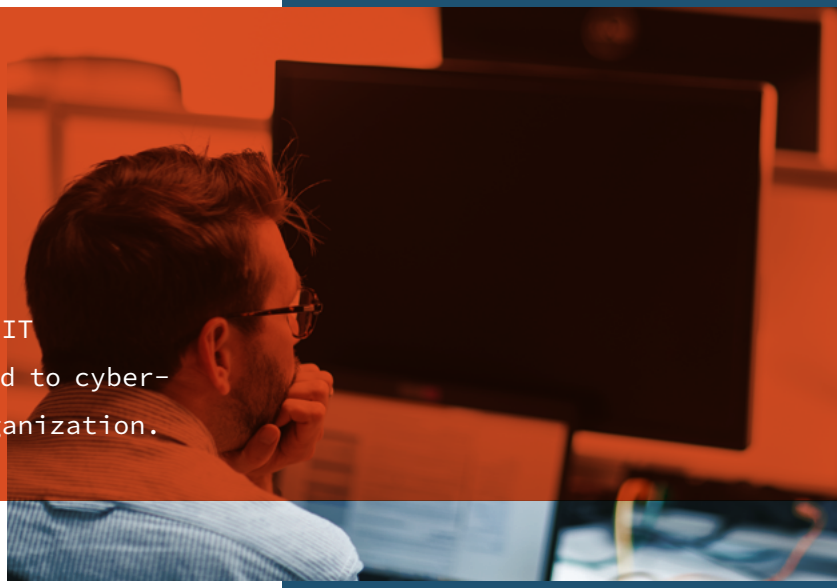
MWR

Training
Proactive First Response

A two day course designed to familiarize IT professionals with the knowledge to respond to cyber-security incidents that threaten your organization.



The role of an on-site first responder is critical to the success of any Incident Response investigation.

This course trains your staff to quickly contain an incident and to make appropriate decisions based on the potential severity of the impact to your business. Proficient application of the principles taught in this training significantly reduces the risk associated to a compromise and increases the success of later investigative activity.

Who should attend?

The training is aimed at IT staff who are on the frontlines defending their systems and responding to attacks.

First responder training does not require any prior knowledge of digital forensics or cyber-security techniques but does require a user-level proficiency with the basics of UNIX/Windows systems and network fundamentals.

Course highlights

- You will gain an in-depth understanding of the Incident Response process and the lifespan of an incident.
- You will learn to make critical decisions that will affect the business continuity of your network estate.
- You will learn the technical skills required to support the incident investigation (disk and memory acquisition, network capture and triaging).
- You will understand the process and importance of evidence tracking and handling throughout an incident.

Benefits to your organizations

- Ensure you are prepared to respond effectively to incidents threatening your organization, reducing response times and increasing the ability of your business to survive an attack.
- Maximize the value of an investigation – having first responders who can perform the acquisition tasks allows experienced investigators to conduct analysis and investigate much sooner.
- Reduce the impact of an attack – time is of the essence when there is an active threat actor in your network estate, your first responders can greatly reduce the time during which hostiles remain in control and ensure optimum containment and remediation.

Why Choose this course?

This course is delivered by experienced incident responders, who help clients manage and contain incidents on a daily basis.

We focus on teaching the core principles that can be applied and adapted to respond successfully to any incident.

This is practical, hands-on training. We've developed labs to show students the key techniques and tools that are needed to acquire and triage data in the first steps of the incident handling process.

Topics / Syllabus

Introduction to Key Principles

_Digital Forensics/Incident Response Differences

_Actors, Motivations and Methods

_Threat Intelligence
Practical: Threat Intelligence Sources and Their Relevance

Incident Response

_Preparation

_Detection & Analysis

_Containment, Eradication & Recovery

_Post-Incident Activity

Policies and Procedures

_Procedures & Forms

_Evidence Handling

_Chain of Custody
Practical: Seize that machine

Data Acquisition

_Memory
Practical: Windows/Linux Memory Collection Techniques

_Disk
Practical : Windows/Linux Disk Acquisition Techniques

_Network Traffic and Log Acquisition
Practical: Network and Log Data Collection

Analysis & Triaging

_Memory
Practical: Linux/Windows Key Memory Artefacts

_Network Traffic
Practical: Searching for the Needle

_Disk
Practical: Linux/Windows Key Disk Artefacts

For more information,
call +44 (0)1256 300 920
or go to our web page
mwr.to/training

MWR