CYBER MANAGEMENT ALLIANCE

Certified Training

in association with
National Cyber
Security Centre

NCSC-Certified Building & Optimising Incident Response Playbooks Course

Learning Objectives

Learn how to create and implement NIST-compliant Cyber Incident Response Playbooks

Learning objectives of the NCSC-Certified Training:

- Learn what it takes to create, review and optimise effective cyber incident response playbooks.
- Understand the significance of incident response playbooks in enhancing an organisation’s cyber resiliency.
- Gain knowledge of the technology that can underpin the creation, optimisation & automation of playbooks.
- Learn how to improve the organisation's speed of response to cyber-attacks through effective attack scenarios & supporting playbooks.

Through the 12 modules designed specifically for this training, course attendees will learn:

- The basic building blocks & key components of an effective playbook that meets NIST’s Incident Response Guidance.
- How to create basic to complex playbooks.
- Pitfalls to avoid when creating playbooks.
- How to use playbooks to meet compliance requirements like the GDPR and ISO 27001:2013’s Annex A.16.1 objectives.
- How to use playbooks to aid triage.
- A review of some common playbooks and how they help in incidents.
- How to create effective scenarios.
- The role of SOAR (Security Orchestration and Response) and the tools that you can use.
- How to assess, deploy & implement automation in incident response playbooks.

LEARNING OBJECTIVES

Learning Objectives Module 1: Case Study

- Deep dive into a case study that highlights the importance of incident response playbooks.

Learning Objectives Module 2: The Basics

- The core concept of playbooks.
- The different types of playbooks.
- The different purposes of playbooks.

Learning Objectives Module 3: Key Design Components

- Key attributes of a good incident analyst.
- How to use playbooks effectively by leveraging the link between them & analysts.

Learning Objectives Module 4: Designing Playbooks

- Building on the NIST Computer Security Incident Handling Guide, the four phases of creating playbooks.
- The relationship of the phases to each other.
- The relationship of the concept to creating effective playbooks.

Learning Objectives Module 5: Analyse for Context

- Importance of context & good analysis skills.
- What is context & how to use it in playbooks

Learning Objectives Module 6: Triggers

- The relevance of triggers in playbooks.

Learning Objectives Module 7: Participants & Stakeholders

- Understanding who can take which decisions in a crisis.

Learning Objectives Module 8: Automation

- Structured approach to automation before, during & after an attack.
- Why is implementation of automation essential to playbooks?
- How automation can lead to staff retention & motivation.

Learning Objectives Module 9: Creating scenarios

- How to plan and create cyber-attack scenarios.

Learning Objectives Module 10: Testing your playbooks

- The basics of testing playbooks for efficacy.
- Relevant use of cyber-attack scenarios for testing playbooks.

Learning Objectives Module 11: Technological Solutions

- The importance and role of technology in playbooks.
- Create effective IR checklists without specific technologies.

Learning Objectives Module 12: Creating Playbooks

- How to actually design and create playbooks?
- Using threat intel to create a playbook & examine its components.