Results-Focused Scenario-Based Organistaion-Specific

Interactive practical and immersive workshop

CYBER MANAGEMENT ALLIANCE

NCSC ASSURED TRAINING IN BUILDING AND OPTIMISING INCIDENT RESPONSE PLAYBOOKS

Operational Functional Incident Response Procedures for Your Business

"During cyber attacks organisations fail miserably due to lack of consistent, repeatable and auditable incident response playbooks"

Assured Service Provider

in association with National Cyber Security Centre

Training Course

Our primary objective in this workshop is to ensure that the attendees walk away with actionable steps, usable collateral and long-term learning through our deeply interactive and practical sessions.

LEARNING OBJECTIVES

- List the key benefits of playbooks and recognise their significance in enabling an organisation's cyber resiliency.
- Understand the basics of creating playbooks.
- Describe the key components required to create playbooks.
- Analyse and assess the scenario and select the appropriate playbook.
- Create organisation-specific scenarios.
- Construct simple and complex playbooks.

ACTIONABLE BENEFITS

- Actionable steps you can take immediately to ensure you have actionable playbooks.
- Useful templates and collateral you can use in your business.
- Applicable knowledge to create and use playbooks.
- Using SOAR and technologies to automate heavy lifting boring tasks.

"I gained a great deal from the day, particularly around the construction of bespoke playbooks."

Andrew Lock,
Information Security Consultant

"I would strongly recommend this training to anyone who is involved in Cyber `security or has control of infomation assets."

Kim Rose,
Information Governance Officer, Wye Valley NHS Trust

info@cm-alliance.com https://cm-alliance.com +44 203 189 1422 @cm_alliance

CYBER MANAGEMENT ALLIANCE

BUILDING AND OPTIMISING INCIDENT RESPONSE PLAYBOOKS

CYBER CRISIS INCIDENT PLANNING AND RESPONSE WORKSHOPS

WHAT YOU WILL LEARN

In this highly interactive workshop, you will learn:

- The basic building blocks of a good and effective playbook.
- Pitfalls to avoid when creating playbooks.
- Triage: what it is and it's role in incident management.
- How to use playbooks to aid triage.
- A review of some common playbooks and how they help in incidents.
- Definition of a breach – why you need this and how to roll this out in your organisation.
- Creating scenarios – deep dive into creating effective scenarios.
- Creating playbooks – starting from basic to complex playbooks (multiple interactive sessions).
- Management playbooks – how to build and engage management to use playbooks.
- Running internal workshops – how to ensure maximum participation and effective results.
- Understand the technology stack, the challenges and improvements you can make to improve your incident response.
- Understand the role of SOAR (Security Orchestration And Response) and the tools that you can use.
- Organisational capability and the role of playbooks in increasing staff skills and retention.

Topic	Details
The Foundations & Concepts	• Condensed version of the public training to ensure all core stakeholders are baselined and understand the key concepts
Threats, Threat Actors & Incidents	• Identify relevant threats and threat actors • Build and/or review the threat actor library • Review critical incidents/crisis related to IT and/or cyber • Review pen-test/security assessment reports
Critical Systems & Assets	• Review critical systems and applications, and review or build impact categories • Define a breach for each of the critical systems
Technology Stack	• Detailed review of an existing technology stack • Review of configurations and workflows • Review of control and control assessments (protective, detective and response) • Review of alerts
Scenario Definition & Planning	• Identify and build top attack scenarios – impact to critical assets and business objectives • Build high-level attack tree • Review existing use cases
Playbooks	• Review the scenarios and create/review specific response and recover procedures per scenario

info@cm-alliance.com https://cm-alliance.com +44 203 189 1422 @cm_alliance