COURSE TABLE OF CONTENTS

Cyber Kill Chain

OEM: Koenig Original • Duration: 2 Days (16 hrs)

COURSE MODULES & TOPICS

Module 1: Introduction to the Cyber Kill Chain
- Concept and purpose of the Cyber Kill Chain
- Overview of attack stages in cybersecurity

Module 2: Reconnaissance Phase
- Techniques for gathering information about targets
- Identifying reconnaissance activities

Module 3: Weaponisation Phase
- Creation of tools to exploit vulnerabilities
- Understanding weaponisation methods

Module 4: Delivery Phase
- Methods of delivering malicious payloads
- Recognising delivery techniques

Module 5: Exploitation Phase
- Exploiting vulnerabilities to gain access
- Mitigating exploitation risks

Module 6: Installation Phase
- Installing malware to maintain access
- Persistence techniques used by attackers

Module 7: Command and Control Phase
- Establishing communication with compromised systems
- Detecting command and control activities

Module 8: Actions on Objectives Phase
- Final steps to achieve attacker goals
- Understanding attacker objectives

Module 9: Detection and Mitigation Techniques
- Strategies to detect attacks at each stage
- Mitigation methods for each kill chain phase

Module 10: Case Studies and Real-World Applications
- Analysing real-world attack scenarios
- Applying Cyber Kill Chain knowledge in practice

© Koenig Solutions