COURSE TABLE OF CONTENTS

Cyber Range Environments

OEM: Koenig Original • Duration: 3 Days (24 hrs)

COURSE MODULES & TOPICS

Module 1: Cyber Range Fundamentals

- Types of ranges: training, exercise, testing, research
- Use cases: education, certification labs, team exercises
- Architectures: on-premises, cloud, hybrid
- Build or buy: platforms and trade-offs

Module 2: Scenario Design

- Defining learning objectives and difficulty levels
- Threat modelling and attack path design
- Mapping scenarios to MITRE ATT&CK
- Writing scenario storylines, briefs and walkthroughs

Module 3: Range Infrastructure

- Virtualization and containers for labs
- Network design and segmentation
- Orchestration and templating
- Infrastructure as code for repeatable deployments

Module 4: Building Target Environments

- Windows and Active Directory environments
- Linux and web application targets
- Introducing controlled vulnerabilities and misconfigurations
- Realistic user activity and noise generation

Module 5: Defensive Side of the Range

- Logging and telemetry collection
- SIEM and EDR integration
- Detection rules and alerting
- Blue team scenarios and incident response tasks

Module 6: Running Exercises

- Red, blue and purple team formats
- Exercise roles, rules of engagement and white cell
- Injects, timelines and facilitation
- Hands-on exercise run

Module 7: Scoring and Assessment

- Flags, objectives and scoring models
- Collecting metrics and evidence
- Feedback and after-action reviews

© Koenig Solutions

Module 8: Range Operations and Safety

- Deployment, resets and snapshots
- Scaling and cost control
- Isolation, containment and safe handling of malware
- Quality assurance and lab testing

Module 9: Capstone: Build a Lab

- Design and build a small lab end to end
- Peer review and instructor feedback