HOOYIA

E-HOOYIA

Defensive Security (Blue Team)

Presented by:
Hooyia

+237 691435485
+237 697907096

e-hooyia.com

Bafoussam, Cameroon

contact@e-hooyia.com

Module 2: Defensive Security (Blue Team)

Course Overview

This module serves as the essential counterpart to offensive security training, focusing on developing the skills required to protect, monitor, and react effectively to cyber-attacks. The curriculum centers on the operational side of cybersecurity, providing a deep dive into the technologies and processes used to maintain system integrity and ensure business continuity. This module prepares professionals to become the front line of defense, guarding against the very attack vectors studied in offensive security. When combined with the offensive mindset, this defensive training creates a well-rounded professional capable of bridging the gap between testing vulnerabilities and hardening systems, a comprehensive approach to security.

Targeted Audience

This module is tailored for individuals seeking careers in cybersecurity defense and operations. It is ideal for those who aim to become a Security Operations Center (SOC) Analyst, an Incident Responder, a Threat Hunter, a Forensic Analyst, or a Malware Reverse Engineer.[1]

Module Objectives

Upon successful completion of this module, participants will be able to:

- Understand the fundamental role and operations of a Security Operations Center (SOC).[1]
- Utilize real-time monitoring tools such as SIEM (Security Information and Event Management) and EDR (Endpoint Detection and Response) to manage logs and detect security events.[1]
- Apply the full incident management lifecycle, from detection and response to containment and eradication of threats.[1]
- Perform proactive threat hunting to search for undiscovered threats within an organization's network.[1]
- Conduct digital forensic analysis to collect digital evidence and perform post-mortem investigations of security incidents.[1]
- Reverse engineer malware to understand its logic and functionality, thereby developing more effective defensive countermeasures.[1]

Course Structure

The module is structured to build skills from foundational monitoring to advanced incident response.

- **Week 1: SOC Operations & Real-Time Monitoring**
  - Introduction to the Security Operations Center (SOC) and its operational framework.
  - Fundamentals of SIEM and EDR for network and endpoint surveillance.
  - Log management and analysis techniques for threat detection.
- **Week 2: Incident Response & Threat Hunting**
  - In-depth study of the incident management process, including detection, containment, and recovery phases.
  - Hands-on exercises simulating an incident response scenario.
  - Learning and applying threat hunting methodologies to proactively identify hidden threats.
- **Week 3: Digital Forensics & Malware Reverse Engineering**
  - Digital evidence collection and preservation techniques for forensic investigations.
  - Post-incident analysis and reporting.
  - Dissecting malware to understand its code and behavior for defensive purposes.