




E-HOOYIA

Cyber-intelligence and
Awareness

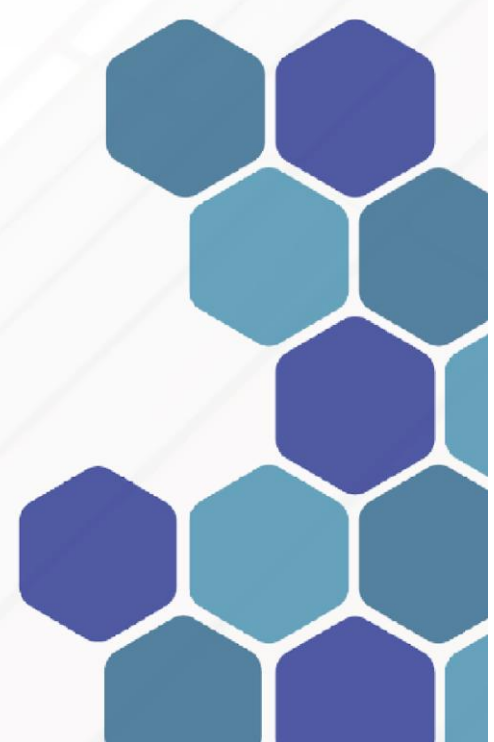
Presented by:
Hooyia

 +237 691435485
+237 697907096

 e-hooyia.com

 Bafoussam, Cameroon

contact@e-hooyia.com



Module 5: Cyber-intelligence and Awareness	2
Course Overview	2
Targeted Audience.....	2
Module Objectives	3
Course Structure	3

Module 5: Cyber-intelligence and Awareness

Course Overview

This module provides a critical perspective on cybersecurity that extends beyond technological defenses. It focuses on the proactive gathering of intelligence to anticipate threats and the crucial role of human education in mitigating risk. By understanding how to leverage open-source information and conduct digital investigations, professionals can move from a reactive stance to a predictive one. The curriculum's explicit focus on the "human factor" demonstrates a comprehensive understanding of the cybersecurity landscape, acknowledging that technology alone is insufficient to protect an organization. This module recognizes that a significant number of security incidents are the result of human error, and by training professionals in awareness and education, the program provides a truly holistic security solution.

Targeted Audience

This module is designed for individuals who possess a blend of analytical, technical, and communication skills. It is an ideal fit for those seeking roles as a Threat Intelligence Analyst, Cybercrime Investigator, OSINT Specialist, Cybersecurity Trainer, or an Awareness Specialist.¹

Module Objectives

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

- Collect and analyze threat intelligence to understand the motivations, capabilities, and tactics of cyber threat actors.¹
- Utilize Open-Source Intelligence (OSINT) techniques to conduct digital investigations and track cybercriminals.¹
- Develop an understanding of the human factor in security and how to manage and mitigate associated risks.¹
- Create and deliver effective training and awareness programs using a range of pedagogical techniques.¹
- Provide strategic security consulting to advise on best practices and human-centric security strategies.¹

Course Structure

The module is structured to first cover intelligence-gathering techniques and then move to the application of that intelligence for human-centric defense.

- **Week 1: Threat Intelligence & OSINT**
 - Introduction to the threat intelligence cycle.
 - Fundamentals of OSINT and its use in digital investigation.
 - Using specialized search engines and social media for information gathering.
- **Week 2: Cyber-Investigations & The Human Factor**
 - Practical application of OSINT in a simulated cyber-investigation scenario.
 - Analyzing the psychology of social engineering attacks.
 - Understanding how to build security awareness and manage human risk.¹
- **Week 3: Security Training & Strategic Consulting**
 - Techniques for designing engaging and effective security awareness programs.
 - Developing a strategic approach to security consulting for organizations.
 - Final project: Designing a multi-faceted security awareness campaign.