CYBER SECURITY FUNDAMENTALS COURSE

MODULE DESCRIPTION

INTRODUCTION TO CYBER SECURITY

- This Module introduces students/participants to Cyber Security. It explores different concepts needed for most parts of the course and also used in the Cyber Security Industry. At the end of the module, participants will be able to identify different Cyber Threats and also learn some attack terminologies.

UNDERSTANDING COMPUTER NETWORK

- This Module is the basis for participants with little or no knowledge about the computer system. It is also a foundational skill required to explore major hacking techniques. It generally explores the computer network system and how it operates with the very key concept of Information System Assets. This module builds the foundational skills to pursue a Network Administration/Analyst career.

IDENTITY THEFT, INTERNET/COMPUTER FRAUD & ABUSE

- This module reveals crime as it relates to Cyber Security. It induces an understanding of Cyber Fraud and Identity Theft. The abnormal use of an information system will also be explored in this module. At the end, some very key measures to prevent falling victim of Cyber Crime will be revealed.
- **Note:** Contains some Hands-on Training

MALWARE

- This Module is dedicated to making participants have a broader understanding of Computer Malware, how they are created and operate in a Computer System and with some preventive measures. It impacts the knowledge and skills required to build a career as a Malware Analyst.

HACKING METHODOLOGY

- This Module explores the techniques used by Attackers to attack an Information System. Participants will be exposed to the tools used for each technique. A major Hands-on training will be the reconnaissance phase of an attack using Google Docking/Hack. This module builds your skills to become a Penetration Tester/Ethical Hacker.

ESPIONAGE IN THE CYBER WORLD

- This module brings understanding to Computer data and how it should be protected. It also reveals techniques used for Cyber Espionage both in the corporate world and government. This module befits a professional Information System Analyst or Risk Manager.

TECHNOLOGIES FOR CYBER SECURITY

- This module reveals different important and necessary technologies used in the protection of Information System Assets. It also explains a detective and preventive approach to Security Technology. Anyone interested in becoming a Cyber Defender must have the skills revealed in this Module.

CORPORATE SECURITY POLICIES

- This module introduces policies needed in the corporate world to protect Information System Assets and limit the risk of impact in the case of an attack. It also reveals some international standards and regulation bodies. It concludes with a plan needed in the case of a cyber attack.

VULNERABILITIES

- This module introduces how the computer systems are exposed to Cyber Attacks. It reveals areas of concern and tools required for Vulnerability Assessment. It is the right skill to develop your profession as a Vulnerability Assessor.
- Note: May contain some Hands-on Training

CYBER TERRORISM & WARFARE

- This module reveals terrorism in the cyber world. It broadens understanding on Cyber warfare with different case studies. It also reveals what is called the dark-web and technologies used to become almost invisible while connected to the internet.
- **Note:** It may contain some Hands-on training