Fundamentals of Cybersecurity - Syllabus

SECTION 1: THE CYBERSECURITY WORLD AND CRIME

The learner will begin by gaining an understanding of the need for cybersecurity in every organization, the fundamental procedures that must be followed by cybersecurity professionals, the most prevalent security threats, and how they are carried out and affect various industries, including energy, health care, and finance.

Topics Covered:

- The need for cybersecurity
- Ensuring cybersecurity
- Valuable data types and personal information
- Security threats: DoS/DDoS, brute force, MITM, social engineering, phishing, and spear phishing
- Malware types: ransomware, trojan, virus, worm, adware
- Malware analysis approaches - static and dynamic analysis
- The impact of cyberthreats on healthcare, energy, and finance industries

SECTION 2: ATTACKERS AND APTS

The learner will gain understanding about the hacking aspect of cyber by studying the various kinds of attackers, their motivations, and how they launch and distribute their objectives. The learner will gain insight into advanced persistent threats and the most well-known groups over the past few years. The learner will understand the cyber kill chain and all the processes that attackers follow, from initiating an attack to achieving their goals.

Topics Covered:

- Attacker types: Cyber terrorists, industrial spies, insiders, hacktivists, cybercriminals
- Advanced persistent threats: APT goals, stages, the famous groups, case studies, and warning signs.
- The cyber kill chain stages
- Types of hackers
- Stages of ethical hacking

SECTION 3: MITIGATING THE RISK AND TAKING CONTROL

The learner will delve into the significance of ethical hacking and discover how employee education, such as enforcing password policies, can prevent cyberattacks. The learner will then explore the risk management processes, the most well-known policies, procedures, standards, and guidelines, including PCI, PHI, and PII, as well as practice managing a risk process.

Topics Covered:

- Exploits, vulnerabilities, zero-day attack, payload, and RAT.
- Enforcement of strong passwords
- Risk management processes
- CIA triad
- PII, PCI, PHI
- Practicing risk management