DIGI SAMURAI

Get the flavour of CYBER SECURITY From Experts

Cyber Security Awareness

The Future – Cyber Security

Empowering Security in Every Click – Cyber Awareness Starts Here!!!

Why Cyber Security?

Protecting sensitive data is no longer an option but a necessity in today's interconnected dynamic world, where the cyber threats are pervasive & constantly evolving.

A career in cybersecurity offers numerous advantages, including high demand, the opportunity to address the skills gap, diverse roles, challenging work, the ability to mitigate the cyber threats, attractive compensation, and the ability to contribute toward a safer digital world. Choosing a cybersecurity career can provide both professional satisfaction and the opportunity to make a positive impact in today's increasingly digital and interconnected society.

Prepare yourself with critical knowledge to safeguard personal information securely and traverse the digital world safely

Understand the Future of Security

COURSE OVERVIEW

1. Introduction to Cyber Security

1. Program Overview
2. Introduction to Cyber Security
3. What is Cyber Security?
4. Why do we need Cyber Security?
5. Scope and opportunities of Cyber Security in Future
6. How is it different from Information Security?
7. Cyber Security Foundation – CIA Triad vs DAD Triad
8. Understanding Key Concepts – Asset, Vulnerability, Threat & Risk
9. Types of Cyber Security – Offensive, Defensive & Compliance (Proactive & Reactive)
   - 9.1. Offensive – VAPT, Red Team, Secure Config Review, etc.
   - 9.2. Defensive – IAM, SOC, ACL, Secure Architecture, Zero Trust, etc.
   - 9.3. Compliance – Standards and Benchmarks (ISO, NIST, CIS, etc.)
10. Organisational Aspect of Cyber Security – People, Process & Technology
11. Discussion – Few recent major cyber attacks
12. Understanding – Common Cyber Threats
13. Discussing – Key Challenges of Cyber Security

2. Exploring the Power of Information Gathering (OSINT)

1. What is OSINT?
2. Importance of OSINT
3. Different OSINT Methodologies
   - 3.1. Footprinting through Search Engines
   - 3.2. Footprinting using Advanced Google Hacking Techniques
   - 3.3. Website Footprinting
   - 3.4. Email Footprinting
   - 3.5. Competitive Intelligence
   - 3.6. WHOIS Footprinting
   - 3.7. DNS Footprinting
   - 3.8. Network Footprinting
   - 3.9. Footprinting through Social Engineering
4. Understanding the requirement – What to search for?

3. Learn Application Security from Experts

1. What is web application?
2. Web Application Architecture – Front End & Back End
3. Types of Web Pages – Static vs Dynamic

4. Understanding HTTP Headers
5. Unauthenticated and Authenticated Web Application Security Testing
6. OWASP Top 10 Web Application Security Vulnerabilities
7. Hacking Websites with SQLi, XSS, etc.
8. Understanding the risk of mobile
9. Understanding the spyware
10. Impact of mobile malware and payloads
11. Mobile Security Best Practices

4. Network & Infrastructure VAPT

1. What is Network Security?
2. Discovering the asset and their service
3. How to exploit Windows & Linux Systems
4. Do's & Don'ts for system configurations

5. Firewall & Defensive Security

1. How organization ensure Cyber Defence?
2. Realizing the importance of Threat Intelligence
3. Viewing Real-time Threats
4. Understanding the firewall
5. Playing with firewall rules and creating access control

6. Trending Cyber Threats

1. Understanding Top 5 Cyber Risks
    - 1.1. Social Engineering
    - 1.2. Ransomware
    - 1.3. Spyware
    - 1.4. Misconfiguration
2. Way Forward for Industry Opportunities

Course Pre-requisite

Basic working knowledge of Internet

Course Duration

30 Hours to be Aware of the Cyber Security