DIGI SAMURAI

Post Graduation Certificate in Information Security

ENTER THE WORLD OF INFORMATION SECURITY

Learn Information Security

We don't teach only cyber security here. Learn the broader spectrum of enterprise level security!

1. *Learn from Leading Industry Experts about Information Security*

2. *Get Assured Paid Internship and Job Opportunities*

Grooming Sessions for Interview Appearance

Life-time Access to Study Materials & Many More

15 Months Course with Live Project Exposure

Choosing a career in information security holds significant importance for several reasons:

- Increasing Demand
- Addressing the Skills Gap
- Variety of Roles and Specializations
- Challenging and Dynamic Work
- Mitigating Cyber Threats
- Salary and Career Advancement
- Contribution to a Safer Digital World

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 cyber threats, attractive compensation, and the ability to contribute to 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.

COURSE OVERVIEW

Module 1: Building Block

1. Understand Networking – See how system communicates
2. Learn Linux – The Hacker's Way
3. Bash & Power Shell Script – Feel the power of scripting
4. Learn how Active Directory (AD) works
5. Know different types of Servers & Databases
6. Python – Grasp as a Hacker
7. Cryptography – The secret way of communication
8. Introduction to the World of Information Security
9. The Pillar of Information Security – CIA Triad
10. Redefining DAD – Disclosure, Alteration & Destruction
11. Understanding People, Process & Technology (PPT) Concept
12. Understanding Information Security Core Terminologies

Module 2: Network Security & Secure Architecture

1. Understanding different Network Security Device (FW, IPS/IDS, WAF, DAM, LB, CAS, etc.)
2. Learning different aspect of Network Security (Proactive & Reactive Security)
3. Enterprise Network – Making a Network Fault Tolerant
4. Learn to Design a Secure Network
5. Assess and Review Network Architecture

Module 3: Red Teaming

1. Network Penetration Testing
2. System/Host Penetration Testing
3. Active Directory (AD) Penetration Testing
4. Wireless Penetration Testing
5. Web Application Penetration Testing
6. API Penetration Testing
7. Mobile Application Penetration Testing (Android & iOS)
8. Secure Configuration Review of Network Devices

Module 4: Blue Teaming

1. Learning SoC Lifecycle and it's Components
2. Understanding Security & Monitoring Devices – SIEM, SOAR, DLP, XDR, etc.
3. Phishing Mail Analysis
4. Network Traffic/PCAP Analysis
5. Registry, Process & Log Analysis (Windows & Linux)
6. SIEM Implementation & Fine-tuning
7. Threat Intelligence & Threat Hunting (TI/TH)
8. Incident Handling & Incident Response (IR/IH)
9. Digital Forensic
10. Ransomware Management

Module 5: Vulnerability Management

1. Vulnerability Management Lifecycle
2. Requirements of Vulnerability Management
3. Challenges of Vulnerability Management
4. Vulnerability Management – Detection Cycle, Reporting Cycle, Remediation Cycle
5. Defining a Vulnerability Analysis & Resolution Strategy
6. Develop a Plan for Vulnerability Management
7. Implement the Vulnerability Analysis & Resolution Capability
8. Assess and Improve the Capability

Module 6: Information Security Compliance

1. Learning Auditor's Behavior – ISO 19011
2. ISMS Implementation & Auditing In-depth – ISO 27001:2022 & ISO 27002:2022
3. Risk Management – ISO 31000, ISO 27005, NIST Risk Management Framework, CRISC
4. BCMS Auditing – ISO 22301, ISO 22313
5. Privacy – GDPR, ISO 27701, Digital Personal Data Protection Bill
6. Payment Security – PCI DSS & PA DSS
7. IT General Controls (ITGC)
8. Introduction to COBIT 5 Framework

Module 7: Trending Technologies

1. IoT Security
2. Cloud Security
3. DevOps & DevSecOps
4. Understanding Artificial Intelligence for Cyber Security
5. Releasing Blockchain Impact on Cyber Security

Course Pre-requisite

Basic working knowledge of Computer, Internet & Network

Course Duration

15 Monthsrs to Master Information Security from ZERO to HERO

OTHER COURSES OFFERED

Foundation Courses

- Networking for Hackers
- Linux for Hackers
- Python for Hackers
- Java Script for Hackers
- Cryptography for Hackers

Offensive Security Courses

- Ethical Hacking
- OSINT
- Network Penetration Testing & Config Review
- Web Application penetration Testing & GIGW
- Mobile Application Penetration Testing
- API Penetration Testing
- IoT Penetration Testing
- Wireless Penetration Testing
- Cloud Security Testing
- Vulnerability Management

Defensive Security Courses

- Security Operation Centre (SOC)
- IAM & System Admin
- Threat Intelligence & Threat Hunting
- Cyber Crime & Digital Forensic

Compliance Courses

- ISO 27001 (ISMS)
- ISO 27701 (PIMS)
- ISO 22301 (BCMS)
- ISO 31000 (RMS)
- ISO 9001 (QMS)
- ISO 20000
- ITGC
- PCI DSS & PCI DA
- WFH Assessment

CONTACT US

www.digisamurai.co.in

+91 8910632224

+91 7595887833