Certification in Cyber Security (C-CS)

3 Months | Extensive Learning | Live Projects & Case Studies | E-labs & Simulators

"**As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture**." — Britney Hommertzheim, Director, Information Security, AMC Theatres, at SecureWorld Kansas City

CAREER OPPRTUNITIES IN CYBER SECURITY

- Chief Information Security Officer
- Forensic Computer Analyst
- Information Security Analyst
- Penetration Tester
- Security Architect
- IT Security Engineer
- Security Systems Administrator
- IT Security Consultant

UNIQUE PROGRAMME FEATURES

- The platform supports project based learning
- The platform offers e-Labs with which the student/candidate can practice the basics of technology
- Industry mentors who can guide the students and candidates through individual sessions
- Live interactions with Machine Learning experts and Corporate leaders
- e-learning activities with Case studies, Live-projects, and Assignments

PROGRAMME TAKEAWAY

- End-to-End Security Management
- Risk Assessment
- Software Application Security
- Database Security
- Cryptography Algorithms and Protocols
- Malware
- Network Threats and Defenses
- Web Security
- Mobile Security
- Legal and Ethical Issues and Privacy

WHAT WILL YOU LEARN

Course Topics

Modules	Objectives
Module 1—Security Basics	Cyber Security Fundamentals – What Is Cyber Security? – Why Cyber Security? – Objectives of Cyber Security – CIA Triad – Confidentiality Breach – Example – Integrity Breach – Example – Availability Breach – Example Challenges of Cyber Security Cyber Security Terminology – Security Terminology Holistic View – Various Threat Sources – Threat Consequence of Attacks – Threats and Assets Vulnerabilities and Attacks – Vulnerabilities and Attacks – An Example Case Study What Needs to be Done to Address Cyber Security? – Lines of Defense – Basic Design Principles of Secure Systems – Security Mechanism Standards – Security Requirements
Module 2—Software and Application Security Using Micro Focus Fortify	An introduction to Software and Application Security – Software Security Vulnerabilities – Programming Input vulnerabilities Buffer Overflow and its Exploitation – Buffer Overflow – Overview – Buffer Overflow – Basics – Buffer Overflow – An Example – Buffer Overflow Code Cases – Explained – Buffer Overflow Exploitation Defenses against Buffer Overflow – Source Code Review using the Micro Focus Fortify Software Tool
Module 3—Database Security	Database Security – What Is a Database System – Databases – What They Hold – Database System – Access – DBMS – An Example Need for Database Security Relational Databases – Elements of RDBMS Structured Query Languages Database Attacks – SQL Injection – SQL Injection Avenues – SQL Injection Types Defense against SQL Injections – SQi Countermeasure

WHAT WILL YOU LEARN

Modules	Objectives
Module 4—Malware Threats	Malware Threats – What Is Malware? – Types of Malware – Trap Doors – Logic Bombs – Trojan Horses – Viruses – Viruses Phases – Types of Viruses – Worms Malware Prevention and Detection Approaches Modern Malware – Botnets – Botnets: Attacks and Frauds Advanced Persistent Threat (APT) – APT – Steps – APT – Examples Malware Analysis – Static Analysis – Dynamic Analysis
Module 5—Firewall	Firewalls How Deep Is Our Defense? Firewall – An Introduction Firewall – Access Policy Firewall – Constraints Types of Firewalls – Firewall – Methods of Filtering – Packet Filtering Firewall – Packet Filtering – Advantages – Packet Filtering – Drawbacks – Packet Filtering – Countermeasures – Session Filtering Firewall Other Types of Firewalls – Bastion Hosts – Host-based Firewalls Firewall Deployments – Internal Firewall Deployment – Distributed Firewall Deployment Environment
Module 6—Intrusion Detection System	How Deep Is Our Defense? Intrusion – Introduction – Intrusion Detection System – Characteristics – Intrusion – Examples – Intrusion Detection System – IDS – IDS with Other Strategies – Patterns and Methodology of an Intruder – Elements of Intrusion Detection – Components of IDS

WHAT WILL YOU LEARN

Modules	Objectives
Module 6—Intrusion Detection System continued	Detection Models – Anomaly detection – Misuse/Signature Detection Anomaly Classification Detection Approaches – Statistical Approach – Knowledge Base Approach – Machine Learning Intruder Detection Approaches – Anomaly Detection – Limitations Misuse or Signature Detection Approaches – Signature Detection Approaches – Rules-Based Approach – Misuse Signature Detection – Example Deployment of IDS – Network-Based IDS (NIDS) – Host IDS Sensors – Inline Sensor – Passive Sensors – Firewall vs. Network IDS – NIDS Sensor Deployment SNORT – SNORT – Features – SNORT – Architecture – SNORT – Rules – SNORT – Fixed Header and Rule Options – SNORT Header – Action – SNORT Rule – Format – SNORT – Example Honeypots – Honeypot systems – Features – Honeypot systems – Classification – Honeypot Deployment Evaluating IDS Honeypot systems – Features Eluding Network IDS – Insertion Attack – Evasion Attack – Denial of Service Attack Intrusion Prevention System
Module 7—Introduction to Cryptography	Encryption/Decryption – Encryption/Decryption Definition – Encryption History – Encryption Basics Types of Cryptography

WHAT WILL YOU LEARN

Module 7—Introduction to Cryptography continued	Hash Functions – Hash Function – Properties – Hash Function – Example Symmetric Encryption Asymmetric Encryption Attacks on Encryption
Module 8—Web Security using Micro Focus Fortify Web Inspect	How the Web Works – Cookies – The Web and Security Attacks on Web – Cross Site Scripting (XSS) – Cross Site Scripting – Example – XSS Consequences – XSRF Cross Site Request Forgery – XSRF – Example – XSS vs XSRF – Structured Query Language – SQL Injection Attacks Web Application Scanner – Using Micro Focus Fortify Web Inspect
Module 9—Security Protocols	Why Security Protocols? Authentication Protocols – Mutual Authentication – Shared Secret – Mutual Authentication – Simplified – Mutual Authentication – Reflection Attack Key Exchange Protocols – Session Keys – Key Distribution Centre – Exchanging Public Key Certificate Kerberos PGP (Pretty Good Privacy) SSL (Secure Sockets Layer) SSH (Secure Shell) SCP (Secure CoPy) and SFTP (Secure File Transfer Protocol) – IPSec (Internet Protocol Security) Describe the basics of Hive Programming
Module 10—Types of Attacks	OS Attacks Ping Flood Ping of Death Port Scanning ARP Spoofing ACK Flood FTP Bounce Attack TCP Session Hijacking Man-In-The-Middle Attack Social Engineering Attacks OS Finger Printing Stealth Scan Key-Loggers

WHAT WILL YOU LEARN

Module 10—Types of Attacks continued	ICMP Tunneling LOKI Attack TCP Sequence Attack CAM Table Overflow
Module 11—End-to-End Security Management Platform using Micro Focus ArcSight	What Is the ArcSight Portfolio? Importance of the ArcSight Portfolio in Corporations ESM and Logger Management Center Security Information and Event Management Concepts User Behavior Analysis (UBA) Features DNS Malware Analytics (DMA) Features Reporting ▪ Because Micro Focus ArcSight requires a high-end hardware configuration, some of the Features will be shown in a demo mode due to limitations.

In addition to the Micro Focus software tools, this course also covers demonstrations and labs using the following freeware:

- CentOS GUI
- LAMP stack – Linux/Apache/Mysql/PHP
- Burpsuite portswigger
- DVWA tool
- XVWA tool
- NMAP on Linux
- NJRAT (Trojan)
- CRYTTOOLS

Certification in Cyber Security (C - CS)

Email Us:

rajat@aisect.org

anandkarajagi@aisect.org

Apply Now