AISECT LEARN
Better Education. Better Careers.

LIVE + SELF-PACED

CERTIFICATE IN SECURITY MANAGEMENT

COURSE OVERVIEW

The Certificate in Security Management is a specialized professional course designed to provide participants with a comprehensive understanding of security management principles, practices, and strategies. This course aims to equip individuals with the knowledge and skills necessary to effectively manage security risks, protect assets, and maintain a secure environment within organizations.

COURSE OBJECTIVE

Gain a comprehensive understanding of security management principles and practices to protect information and assets effectively.

WHAT YOU WILL LEARN

The Certified Security Management course covers a broad range of security management principles and practices. Participants will learn how to assess security risks, develop and implement security strategies, and establish security policies and procedures. They will delve into physical security management, understanding concepts such as access control, surveillance systems, and emergency response planning. In the realm of information security management, participants will gain insights into data protection, network security, incident response planning, and compliance with regulations. The course also focuses on crisis management and business continuity, security compliance and regulations, security technology, and effective security leadership and communication. Upon completion, participants will have a comprehensive understanding of security management, enabling them to contribute to creating a secure environment within organizations and effectively managing security risks.

COURSE COURSE

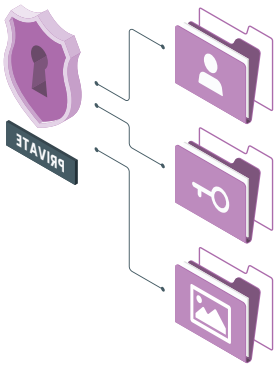
- Cybersecurity fundamentals
- Knowledge of common threat actors and attack methods
- Implementation of mitigation strategies
- Development of security policies and procedures
- Designing secure architectures for systems and networks
- Securing wireless networks

- Understanding and implementing network security controls
- Conducting penetration testing and vulnerability assessments
- Incident management and response
- Understanding and implementing governance, risk, and compliance measures
- Familiarity with cybersecurity frameworks and standards
- Proficiency in the Linux operating system and command line
- Programming skills, particularly in Python scripting
- Understanding of computer forensics principles and investigation techniques
- Knowledge of firewall technologies and their configuration.

Instructor - **Ajay Gautam | Cyber Security Expert**
Instructor - **Aman Roy | Cyber Security Expert**
Duration - 2 Months
Eligibility - Any graduate with a Science stream
No. of Modules – 16 Modules
Language - English
Shareable certificate - Yes

PROGRAM SYLLABUS

Module 1	Introduction to Cybersecurity
Session 1.1	Introduction
Session 1.2	Why Cyber Security is Important?
Session 1.3	Role of cyber security engineer
Session 1.4	CIA Triad
Session 1.5	The Hacking Methodology
Session 1.6	The Who IS Query
Session 1.7	Social Engineering
Session 1.8	Brute Force Attacks
Session 1.9	Phishing
Session 1.10	Bots and Botnets
Session 1.11	DoS and DDoS
Session 1.12	Pings
Session 1.13	Man, in the Middle Attacks (MITM)



Module 2 Cyber Security Building blocks
Session 2.1 Malicious Codes and Terminologies
Session 2.2 Cybersecurity Breaches
Session 2.3 Penetration Testing and Methodologies
Session 2.4 Frameworks and Standards for Cybersecurity
Session 2.5 Hardware and Software Elements of Computer Systems
Session 2.6 Introduction to Networks and Reference Models
Session 2.7 OSI layers
Session 2.8 Network Protocol
Session 2.9 IP Address and Subnet Classes
Session 2.10 Network Devices

Module 3 Security Basics
Session 3.1 Attacks & Threats
Session 3.2 Architecture & Design
Session 3.3 Implementation
Session 3.4 Operations & Incident Response
Session 3.5 Governance, Risk & Compliance
Session 3.6 What is Cyber Kill Chain?
Session 3.7 Reconnaissance & Weaponization
Session 3.8 Delivery & Exploitation
Session 3.9 Installation, Command and control (C2) & Actions on Objectives

Module 4 Linux Basics
Session 4.1 Overview of Operating System
Session 4.2 Working with Linux
Session 4.3 Linux Command Line Structure
Session 4.4 Sample Command Application
Session 4.5 Linux Directory Structure
Session 4.6 Flavours of Linux OS

Module 5 Python Scripting
Session 5.1 Introduction to Python
Session 5.2 Python execution and installation
Session 5.3 Identifiers, variables and Datatypes
Session 5.4 Operators
Session 5.5 Python-Flow Controls
Session 5.6 Functions
Session 5.7 Python Classes
Session 5.8 Inheritance, Files

Module 6 Blue Teaming & Cyber SOC
Session 6.1 Incident Management Process
Session 6.2 Lifecycle of an Incident
Session 6.3 Incident Response Team & Benefits
Session 6.4 Incident Response Plan
Session 6.5 How does Log Management help?
Session 6.6 Prevention, Detection & Investigation through Logs
Session 6.7 System Logs

Module 7 Attacks, Threats, and Vulnerabilities
Session 7.1 Compare and Contrast Information Security Roles
Session 7.2 Compare and Contrast Security Control and Framework Types
Session 7.3 Type of Threat Actors and Attack vectors
Session 7.4 Threat Intelligent Sources
Session 7.5 Assess Organizational Security with Network Re connaissance Tools
Session 7.6 Security Concerns with General Vulnerability Types
Session 7.7 Vulnerability Scanning Techniques
Session 7.8 Penetration Testing Concepts
Session 7.9 Classify Contrast Social Engineering Techniques
Session 7.10 Indicators of Malware-Based Attacks

Module 8 Governance Risk and Compliance
Session 8.1 Part 1 Risk Management Processes and Concepts
Session 8.1 Part 2 Risk Management Processes and Concepts
Session 8.1 Part 3 Risk Management Processes and Concepts
Session 8.2 Business Impact Analysis Concepts
Session 8.3 Redundancy Strategies
Session 8.4 Backup Strategies
Session 8.5 Cybersecurity Resiliency Strategies
Session 8.6 Importance of Physical Site Security Controls
Session 8.7 Importance of Physical Host Security Controls

Module 9 Cyber Security Frameworks
Session 9.1 Introduction to NIST Framework
Session 9.2 Using NIST Framework
Session 9.3 Real World Case Studies
Session 9.4 Introduction to Cobit Framework

Session 12.11 History, Cookies, and Supercookies
Session 12.12 HTTP Referer
Session 12.13 Browser Fingerprinting
Session 12.14 Certificates and Encryption
Session 12.15 Firefox Hardening

Module 13 e-Asset Security
Session 13.1 The Information Life Cycle
Session 13.2 Data Classification and Clearance
Session 13.3 The 3 States of Data (data at rest, data in motion, and data in use)
Session 13.4 Data Handling, Data Storage, and Data Retention
Session 13.5 Business owners, Information owners, data custodians and system owner
Session 13.6 Memory and Data Remanence
Session 13.7 Data remanence and destruction
Session 13.8 Data Security Frameworks
Session 13.9 Data Protection

Module 14 HTML Injection
Session 14.1 HTML Injection - Theory
Session 14.2 HTML Injection 1 on TryHackMe
Session 14.3 HTML Injection 2 - Injecting User-Agent Header
Session 14.4 Injecting Cookie Field and Redirecting The Page
Session 14.5 Advance Example of HTML Injection

Module 15 Cross site scripting (XSS)
Session 15.1 XSS Theory
Session 15.2 Changing Page Content With XSS
Session 15.3 Bypassing Simple Filter
Session 15.4 Downloading a File With XSS Vulnerability
Session 15.5 DOM XSS Password Generator
Session 15.6 JSON XSS
Session 15.7 Old Vulnerable Real Applications

Module 16 Job roles
Session 16.1 Analyst
Session 16.2 Analyst Application Security
Session 16.3 Engineer Trainee
Session 16.4 Penetration Tester
Session 16.5 Security Analyst

Session 9.5 Principles
Session 9.6 Cobit - Governance and Managing Objectives
Session 9.7 Business cases
Session 9.8 ISO Standard
Session 9.9 Implementation Over IT
Session 9.10 Fundamentals of PCI-DSS
Session 9.11 PCI DSS History
Session 9.12 Anatomy Of Payment Flow
Session 9.13 Payment Attacks - Indian Perspective

Module 10 Computer Forensics
Session 10.1 Computer Forensics investigation process
Session 10.2 Data Acquisition & Duplication
Session 10.3 Introduction to Windows Forensics
Session 10.4 Lab: Capturing Windows Memory
Session 10.5 Browser Forensics using Encase
Session 10.6 Lab: Web Historian
Session 10.7 Memory Forensics
Session 10.8 Lab: Analysing USB data
Session 10.9 Lab: Analysing Malware using Volatility
Session 10.10 Introduction to Indian Cyber Law

Module 11 Firewalls
Session 11.1 Firewalls – Host-based, network-based, and virtual
Session 11.2 Windows - Host Based Firewalls - Windows Firewall

Module 12 Browser security and tracking prevention
Session 12.1 Choosing the Right Browser
Session 12.2 Reducing the Browser Attack Surface
Session 12.3 Demo on Browser hacking
Session 12.4 Browser Isolation and Compartmentalization
Session 12.5 Firefox Security, Privacy, and Tracking
Session 12.6 uBlock origin - HTTP Filters, ad, and track blockers
Session 12.7 uMatrix - HTTP Filters, ad and track blockers
Session 12.8 Disconnect and Ghostery - HTTP Filters, ad and track blockers
Session 12.9 ABP, Privacy badger, WOT - HTTP Filters, ad and track blockers
Session 12.10 No-script - HTTP Filters, ad and track blockers

AISECT LEARN
Better Education. Better Careers.

Sign up for

Webinars, Free courses and Paid Courses

starting from ₹**499/-** onwards only

Contact Us

+91 9111177800

learn@aisectlearn.com

www.courses.aisectlearn.com