CHHAVISHKA IT
LEARN | GROW | SUCCEED

CYBER SECURITY SYLLABUS

Scratch to advance Cyber Security Master Course: CVAPT, SOC, and GRC

Cybersecurity Professional plus designed by experts, blending theoretical learning with hands-on projects, so you can apply what you learn in real-world scenarios. With dedicated trainers, modern labs, and placement support, get it core helps you achieve your career goals. This course is mapped to the popular Cybersecurity Professional course today's increasingly interconnected world, protecting your organization's critical information and systems from cyber threats is more important than ever. This course is designed to give you a comprehensive understanding of cybersecurity concepts and practices, equipping you with the skills and knowledge necessary to defend against cyber attacks. You will learn about various types of threats, including malware, phishing, and social engineering, as well as the strategies and technologies used to detect, prevent, and respond to them right from risk management, to ethical hacking and penetration testing. Whether you are a network administrator or security professional, or simply interested in learning about cybersecurity, this course will provide you with the skills you need to help keep your systems and data secure.

Career JOB Opportunities after Cyber Security Certification

1. **Cybersecurity Analyst:** Monitor and secure networks against potential threats.
2. **Ethical Hacker:** Test systems for vulnerabilities and strengthen security.
3. **Information Security Manager:** Lead teams to protect sensitive data and implement security policies.
4. **Security Consultant:** Advise organizations on the best security practices and solutions.
5. **Incident Responder:** Act swiftly to detect and mitigate security breaches.
6. **Cloud Security Expert:** Secure cloud-based systems and data for organizations.
7. **Penetration Tester:** Simulate attacks to identify system weaknesses.

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056

CHHAVISHKA IT
LEARN | GROW | SUCCEED

When you enroll in a Cyber Security course, here's what you'll learn:

1. Fundamentals of Cybersecurity: Understand the basics of protecting systems and network
2. Ethical Hacking: Learn how to identify and fix vulnerabilities by simulating attacks.
3. Network Security: Secure networks from unauthorized access and threats.
4. Malware Analysis: Study how viruses, ransomware, and other threats operate and how to prevent them.
5. Data Encryption: Protect sensitive information using advanced encryption techniques.
6. Incident Response: Learn to handle and resolve security breaches quickly and effectively.
7. Cloud Security: Explore methods to secure cloud-based applications and data.
8. Compliance and Regulations: Understand legal and ethical standards in cybersecurity.

Course Overview

This comprehensive master course combines three critical areas of cybersecurity—Certified Vulnerability Assessment and Penetration Testing (CVAPT), Security Operations Center (SOC) Analysis, and Governance, Risk, and Compliance (GRC). It is designed for cybersecurity professionals, beginners, and organizations aiming to build or enhance their cybersecurity skillset.

A **Security Operations Center (SOC)** is a **centralized team and facility** that continuously **monitors, detects, analyzes, and responds to cyber security threats in an organization**.A Security Operations Center (SOC) is a centralized, 24/7 command center where dedicated cybersecurity professionals monitor, detect, analyze, and respond to threats across an organization's IT infrastructure

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056

CHHAVISHKA IT
LEARN | GROW | SUCCEED

Main Goal of a SOC

- Detect cyber attacks early
- Respond before damage happens
- Protect sensitive data
- Ensure business continuity
- Reduce security risks
- Network traffic
- Servers and endpoints
- Firewalls and IDS/IPS alerts
- User activities
- Logs from applications and devices
- Cloud infrastructure
- Emails and web traffic

Security Operations Center (SOC)

Module 1: Introduction to SOC

- Role of SOC in Cybersecurity
- SOC Models and Hierarchy
- Introduction to Cyber Security
- Network Fundamentals
- How The Web Works
- Linux Fundamentals
- Windows Fundamentals
- Blue Team Introduction
- SOC Team Internals
- ore SOC Solutions
- Cyber Defence Frameworks
- Phishing Analysis
- Network Traffic Analysis
- Network Security Monitoring
- Web Security Monitoring
- Windows Security Monitoring
- Linux Security Monitoring
- Malware Concepts for SOC
- Threat Analysis Tools
- SIEM Triage for SOC
- SOC Level 1 Capstone Challenges

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056

CHHAVISHKA IT
LEARN | GROW | SUCCEED

Module 2: Threat Landscape and Cyber Kill Chain

- Common Threat Actors
- MITRE ATT&CK Framework

Module 3: Networking for SOC Analysts

- Deep Dive into Network Protocols
- Packet Analysis using Wireshark

Module 4: Log Management and SIEM

- Understanding Logs
- SIEM Overview (Splunk, ELK)

Module 5: Incident Detection

- Indicators of Compromise (IOC)
- Use Case Development

Module 6: Threat Intelligence

- Intelligence Feeds
- Tools: MISP, ThreatConnect

Module 7: Malware Analysis Basics

- Static and Dynamic Analysis
- Tools: Any.Run, Cuckoo

Module 8: Real-Time Monitoring

- Use Cases in Splunk
- Dashboards and Alerts

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056

CHHAVISHKA IT
LEARN | GROW | SUCCEED

Module 9: Incident Response

- IR Lifecycle
- Containment, Eradication, Recovery

Module 10: SOC Reporting and Communication

- Alert Documentation
- Report Writing Skills

Governance, Risk, and Compliance (GRC)

Governance, Risk, and Compliance (GRC) in cyber security is a strategic framework aligning IT security with business goals by setting policies (Governance), identifying/mitigating threats (Risk), and ensuring adherence to laws/standards (Compliance), creating a holistic approach to protect digital assets, reduce uncertainty, and maintain integrity through integrated people, processes, and technology.

How They Work Together

Integrated Approach: GRC moves away from siloed IT efforts, creating a unified view of security, risk, and compliance.
Strategic Alignment: It connects cybersecurity to overall business strategy, making security a business enabler, not just a technical hurdle.
Proactive Posture: Helps organizations make informed decisions, reduce costs, and build resilience against sophisticated attacks, ensuring business continuity.
Governance, Risk, and Compliance (GRC) is a framework organizations use to run IT and business in a controlled, secure, and policy-driven way.

It ensures:

- You run the organization properly (Governance)
- You identify and handle threats (Risk)
- You follow laws and standards (Compliance)

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056

CHHAVISHKA IT
LEARN | GROW | SUCCEED

Governance, Risk, and Compliance (GRC)

Module 1: Introduction to GRC

- What is GRC?
- Importance of GRC in Cybersecurity

Module 2: Governance in Cybersecurity

- Policies, Procedures, and Frameworks
- Security Governance Models

Module 3: Risk Management Fundamentals

- Identifying and Assessing Risk
- Risk Mitigation Techniques

Module 4: Compliance and Legal Regulations

- GDPR, HIPAA, ISO 27001, PCI-DSS
- Compliance Audits

Module 5: Security Frameworks and Standards

- NIST, COBIT, ISO
- Framework Mapping

Module 6: Internal and External Auditing

- Audit Planning and Execution
- Tools and Best Practices

Module 7: Business Continuity and Disaster Recovery

- BCP and DRP Planning
- Crisis Management

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056

CHHAVISHKA IT
LEARN | GROW | SUCCEED

Module 8: GRC Tools and Technologies

- GRC Platforms Overview (RSA Archer, LogicGate)
- Integrating GRC with SIEM

Module 9: Reporting and Documentation

- GRC Dashboards and KPIs
- Executive Reports and Presentations

Module 10: Career Development and Certification

- Career Roles in GRC
- Certifications: CISA, CRISC, CGEIT
- Resume and Interview Preparation

Final Assessment & Certification

- Quizzes and Practical Labs per Module
- Final Exam (Theory + Practical)
- Certification of Completion for Each Track (CVAPT, SOC, GRC)

Certified Vulnerability Assessment and Penetration Testing (VAPT)

Certified Vulnerability Assessment and Penetration Testing (VAPT) is a professional cybersecurity program that teaches how to identify, analyze, and exploit security weaknesses in networks, systems, web apps, and servers — legally and ethically. Certified Vulnerability Assessment and Penetration Testing (VAPT) is a comprehensive, professional approach to identifying, analyzing, and exploiting security vulnerabilities in IT infrastructure to strengthen defenses against cyber threats. It combines automated scanning to identify gaps with manual exploitation (penetration testing) to evaluate real-world risks. Key certifications include EC-Council, CPENT, and various vendor-neutral certifications that validate skills in ethical hacking and network security.

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056

CHHAVISHKA IT
LEARN | GROW | SUCCEED

Key Components and Purpose

Vulnerability Assessment (VA): Systematically scans and categorizes, identifying potential security weaknesses.
Penetration Testing (PT): Simulates cyberattacks to validate if vulnerabilities are exploitable and to assess potential impact.
Purpose: To proactively secure networks, applications, and data from breaches, often meeting compliance standards like ISO 27001.

Certified Vulnerability Assessment and Penetration Testing (CVAPT)

Module 1: Introduction to VAPT

- What is Vulnerability Assessment?
- What is Penetration Testing?
- Differences Between VA and PT
- Importance of VAPT in Cybersecurity
- VAPT Methodologies (OWASP, PTES)

Module 2: Cybersecurity Fundamentals

- Information Security Concepts
- Threats and Attack Types
- CIA Triad and Security Principles
- Security Controls
- Cyber Kill Chain & MITRE ATT&CK

Module 3: Networking Essentials

- OSI and TCP/IP Models
- IP Addressing and Subnetting
- Ports, Protocols, and Devices
- Network Topologies and Communication

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056

CHHAVISHKA IT
LEARN | GROW | SUCCEED

Module 4: Kali Linux and Lab Setup

- Installing Kali Linux
- Lab Setup (DVWA, Metasploitable, etc.)
- VirtualBox/VMware Configuration

Module 5: Footprinting and Reconnaissance

- Passive vs Active Recon
- WHOIS, DNS, OSINT
- Tools: Recon-ng, Maltego, theHarvester

Module 6: Scanning and Enumeration

- Network Scanning with Nmap
- Banner Grabbing, Port Discovery
- Enumeration Techniques

Module 7: Vulnerability Assessment

- Using CVE/CVSS/NVD
- Tools: Nessus, Nikto
- Manual Techniques

Module 8: Exploitation Basics

- Exploit Development Intro
- Metasploit Basics
- Exploiting Common Services

Module 9: Web Application Security

- OWASP Top 10
- SQLi, XSS, CSRF, etc.
- Manual & Automated Testing

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056

CHHAVISHKA IT
LEARN | GROW | SUCCEED

Module 10: Wireless Network Testing

- Cracking WEP/WPA
- Rogue AP Attacks
- Tools: Aircrack-ng

Module 11: Social Engineering Attacks

- Phishing, Vishing
- SET Toolkit
- Awareness and Defense

Module 12: Privilege Escalation

- Windows & Linux Techniques
- LinPEAS, WinPEAS
- Kernel Exploits

Module 13: OS-Specific Testing

- Windows & Linux Enumeration
- AV Bypass, Persistence

Module 14: Report Writing

- VAPT Report Structure
- Executive & Technical Summary

Module 15: Case Studies

- Red vs Blue Team
- Industry-Specific Scenarios

Module 16: Certification Guidance

- CVPT Preparation
- Career Roadmap

+ 91 90593 72919
https://chhavishkait.com/
chhavishkait@gmail.com
Flat No 402, DV Town Ship, East Sudha Nagar, AS Rao Nagar, Secunderabad - 500056