Coincent
Learning Drives Excellence

# Coincent 3 Year Program Curriculum
# **Cyber Security Domain**

Partnered by

Microsoft

THREAT PRISM

*Empowering Learners,*
*Accelerating Careers.*

coincent.ai

## ABOUT COINCENT

Coincent offers a 3-Year Program that is a well-structured, career-focused initiative designed to equip students with practical skills, real-world experience, and strong placement support. The program is tailored to ensure progressive learning and career readiness across three year phases.

### Why It’s Unique

- Only one batch per year with limited seats (150 students) per Domain to maintain quality.
- Prepares students step-by-step to become job-ready by graduation.

## DETAILED ABOUT COINCENT 3 YEAR CYBER SECURITY AND ETHICAL HACKING PROGRAM

### “Cyber Security Program at Coincent – Learn by Doing”

Cybersecurity is the practice of protecting computers, networks, data, and systems from digital attacks, unauthorized access, and damage. It helps ensure privacy, safety, and trust in today's connected world.

**Key Points:**

1. It defends against threats like hacking, phishing, and malware.
2. It's essential for protecting personal data, business assets, and national security.
3. It helps organizations maintain trust, comply with regulations, and avoid financial losses.

# 3-Year Program Structure Breakdown

## TABLE OF CONTENTS

# Year 1 :- Industrial Training

## Module 1: Networking Basics

Objective: Understand how computer networks function, focusing on key terminology and protocols.

Topics:

- Types of Networks: LAN, WAN, MAN, PAN, CAN
- Basic Terminologies: IP, MAC, DNS, DHCP, Gateway, Subnet, VPN
- OSI Model: 7 layers (Physical to Application); responsibilities of each
- Protocols: TCP/IP, UDP, ICMP, HTTP/S, FTP, ARP, DNS, etc.

Common Protocols & Ports:

- HTTP (80), HTTPS (443)
- FTP (20/21), SSH (22), Telnet (23)
- SMTP (25), DNS (53), SNMP (161), RDP (3389)

### Benefits and Outcomes:

### Strong Technical Foundation:

Understand how data travels between devices and across the internet. Grasp the structure and logic behind how networks are designed and maintained.

### Better Cybersecurity Awareness:

Know how attacks exploit weaknesses in protocols and network layers. Learn how firewalls, VPNs, and gateways protect systems.

### Improved Troubleshooting Skills:

Identify and resolve issues like IP conflicts, DNS failures, or slow networks. Read logs and trace packet flows more confidently.

### Key Outcomes After Learning:

- You'll know how to differentiate between network types (LAN, WAN, etc.) and when to use them.
- You'll understand key terms like IP address, MAC address, DNS, and how they interact.
- You'll be able to explain the OSI Model and how data moves through each of the 7 layers.
- You'll recognize major protocols (HTTP, FTP, SSH, DNS, etc.) and their port numbers, which is crucial for firewall and traffic configuration.

## Module 2: Linux Fundamentals for Hackers

Objective: Use Linux for ethical hacking; master key commands and concepts.

Topics:

- Installing Kali Linux: On VM (VirtualBox/VMware) or dual boot
- Linux Basic Commands: ls, cd, pwd, cp, mv, mkdir, touch
- Intermediate Commands: grep, find, chmod, chown, tar, wget, curl, top
- Linux Directory & File Permissions: rwx, chown, chmod, SUID/SGID
- Linux Utilities: nmap, netstat, tcpdump, iptables, wireshark

## Benefits and Outcomes:

Industry-Standard for Ethical Hacking:

- Kali Linux is the go-to OS for ethical hackers, packed with pre-installed tools.
- Learning to set it up on a virtual machine or dual boot prepares you for real-world testing environments.

Command-Line Proficiency:

- Mastering basic and intermediate Linux commands helps automate tasks, manage files, and navigate systems efficiently — a must for any hacker or sysadmin.

Enhanced Security Understanding:

- Knowing file permissions (rwx) and how to use chmod, chown, and special permissions like SUID/SGID is key to securing Linux systems and exploiting misconfigurations.
-

## Key Outcomes After Learning:

- You can install and run Kali Linux in isolated environments like VMs for safe testing.
- You'll navigate and manage a Linux system confidently using terminal commands.
- You'll understand how Linux permissions work, which is crucial for both securing and exploiting systems.

## Module 3: Introduction to Ethical Hacking

Objective: Learn the foundational concepts of ethical hacking and information security.

Topics:

- Information Security Overview
- Cyber Kill Chain (Reconnaissance → Weaponization → Delivery → Exploitation → Installation → Command and Control → Actions)
- Hacking Concepts: Attack vectors, threat actors
- Ethical Hacking Concepts: Legal boundaries, white hat vs. black hat
- Information Security Controls: Physical, administrative, technical
- Information Security Laws and Standards: GDPR, HIPAA, ISO/IEC 27001

### Benefits:

Gain a solid understanding of how cyber attacks are structured and how to defend against them using ethical and legal practices. Develop critical awareness of security frameworks, threat models, and compliance standards used in real-world cybersecurity.

### Outcomes:

You'll be able to explain the stages of the cyber kill chain, distinguish between types of hackers, and identify key security controls. You'll also understand major global information security laws and how organizations stay compliant.

## Module 4: Footprinting and Reconnaissance

Objective: Gather information about targets using passive and active techniques.

Topics:

- Footprinting Methodology
- Search Engine Footprinting: Google dorking
- Web Services & WHOIS
- Social Media Footprinting
- DNS & Network Footprinting
- Email Tracking & Metadata Analysis

### Benefits:

Learning these modules equips you with essential reconnaissance techniques used in ethical hacking to identify potential vulnerabilities **before launching an attack**. You'll master both passive and active information-gathering strategies, making your penetration testing more targeted and efficient.

### Outcomes:

You'll be able to perform footprinting using tools like Google Dorks, WHOIS, and DNS lookup. You'll know how to trace email origins, analyze metadata, and gather intelligence from social media and web services. This foundation allows you to map a target's digital presence accurately and ethically as the first step in ethical hacking.

## Module 5: Scanning Networks

Objective: Detect live systems, open ports, services, and OS types.

Topics:

- Network Scanning Concepts
- Scanning Tools: Nmap, Netcat, Angry IP Scanner
- Host Discovery
- Port and Service Detection
- OS Fingerprinting
- Bypassing Firewalls/IDS Detection

### Benefits:

These modules help you understand how to identify live systems, open ports, and running services in a network — a crucial step in ethical hacking. Learning scanning techniques strengthens your ability to assess network security and uncover potential entry points.

### Outcomes:

You'll gain hands-on experience using tools like Nmap and Netcat to perform host discovery, port scanning, and OS fingerprinting. You'll also learn basic evasion techniques to bypass firewalls and intrusion detection systems (IDS), enhancing your penetration testing skills.

## Module 6: Enumeration

Objective: Extract more detailed info from discovered hosts.

Topics:

- NetBIOS Enumeration
- SNMP, LDAP Enumeration

- DNS, SMTP, NFS, NTP Enumeration
- Tools: enum4linux, snmpwalk, rpcclient, ldapsearch

**Benefits:**

These modules teach you how to gather in-depth information from identified systems and services, which is vital for understanding vulnerabilities and planning further penetration tests. Enumeration reveals usernames, shared resources, service versions, and network configurations.

**Outcomes:**

You'll be able to perform targeted enumeration using tools like enum4linux, snmpwalk, and ldapsearch to extract data from services like NetBIOS, SNMP, DNS, and LDAP. This skill helps in identifying misconfigurations and weaknesses that attackers commonly exploit.

## Module 7: System Hacking

Objective: Understand and simulate unauthorized access to systems.

Topics:

- System Hacking Concepts
- Password Cracking: Dictionary, Brute-force, Rainbow tables
- Vulnerability Exploitation: Using Metasploit
- Privilege Escalation Techniques
- Maintaining Access: Rootkits, keyloggers
- Covering Tracks

**Benefits:**

These modules help you understand how attackers gain, escalate, and maintain unauthorized access to systems, which is crucial for defending against real-world threats. You'll also learn how to think like a hacker to better protect your systems.

### Outcomes:

You'll gain hands-on skills in password cracking, exploiting vulnerabilities with tools like Metasploit, and performing privilege escalation. You'll also understand how attackers hide their presence, preparing you to detect and respond to advanced intrusions.

## Module 8: Denial of Service (DoS)

Objective: Learn DoS/DDoS attack vectors and protection techniques.

Topics:

- DoS/DDoS Techniques
- Botnets: Architecture and use in attacks
- Attack Tools: LOIC, HOIC, hping3
- Case Studies: GitHub DDoS, Dyn attack
- Countermeasures: Rate limiting, firewalls, CDN

### Benefits:

These modules help you understand how DoS and DDoS attacks are launched, the role of botnets, and the tools commonly used by attackers. This knowledge is essential for designing systems that can withstand high-volume attacks.

### Outcomes:

These modules help you understand how DoS and DDoS attacks are launched, the role of botnets, and the tools commonly used by attackers. This knowledge is essential for designing systems that can withstand high-volume attacks.

## Module 9: IDS, Firewalls, and Honeypots

Objective: Understand and bypass detection systems.

Topics:

- IDS/IPS/Firewall/Honeypot Concepts
- Evading IDS/Firewalls: Fragmentation, encryption, tunneling
- Detection Tools: Snort, Suricata, Wireshark
- Honeypot Types: Low-interaction vs. high-interaction
- Countermeasures

### Benefits:

You'll gain practical skills using tools like Snort and Wireshark to detect malicious activity, understand evasion techniques, and deploy honeypots for threat monitoring. This knowledge strengthens your ability to build resilient and secure network environments.

### Outcomes:

You'll gain practical skills using tools like Snort and Wireshark to detect malicious activity, understand evasion techniques, and deploy honeypots for threat monitoring. This knowledge strengthens your ability to build resilient and secure network environments.

## Module 10: Web Application Hacking

Objective: Exploit and protect web applications.

Topics:

- Web App Architecture
- Threats: SQLi, XSS, CSRF, LFI, RFI
- OWASP Top 10 Vulnerabilities
- Hacking Tools: Burp Suite, OWASP ZAP

- Footprinting & Vulnerability Detection

**Benefits:**

These modules provide a deep understanding of how web applications function and where they are most vulnerable. You'll learn to identify and test for common web threats like SQL injection and XSS using industry-standard tools.

**Outcomes:**

You'll be able to analyze web app vulnerabilities using tools like Burp Suite and OWASP ZAP, understand the OWASP Top 10 risks, and perform effective web footprinting and scanning — essential skills for any ethical hacker or web security analyst.

## Module 11: Wireless Network Hacking

Objective: Understand wireless technologies and exploit weaknesses.
Topics:

- Wireless Encryption Standards: WEP, WPA/WPA2/WPA3
- Attack Techniques: Evil twin, deauthentication, handshake cracking
- Tools: Aircrack-ng, Kismet, Wireshark
- Bluetooth Hacking
- Countermeasures

**Benefits:**

These modules teach you how wireless networks and Bluetooth devices can be secured and exploited, highlighting common vulnerabilities and attack methods. Understanding these helps in protecting wireless communications from unauthorized access.

### Outcomes:

You’ll gain hands-on experience using tools like Aircrack-ng and Kismet to perform attacks such as handshake cracking and evil twin setups, while also learning effective countermeasures to secure Wi-Fi and Bluetooth networks.

## Module 12: Mobile Platform Hacking

Objective: Target Android & iOS platforms.

Topics:

- Attack Vectors: App vulnerabilities, OS exploits, malware
- Android Attacks: APK reverse engineering, ADB access
- Tools: MobSF, Drozer, Frida
- Security Practices

### Benefits:

These modules help you understand the unique security challenges in mobile environments, including common attack vectors and vulnerabilities specific to Android devices. You'll learn how to analyze and secure mobile apps against threats.

### Outcomes:

You’ll gain practical skills in reverse engineering APKs, using tools like MobSF and Drozer to identify weaknesses, and applying security best practices to protect Android devices from exploits and malware.

## Module 13: Cryptography

Objective: Learn data encryption and cryptographic security.

Topics:

- Encryption Types: Symmetric (AES,DES), Asymmetric (RSA, ECC)
- Hashing: SHA, MD5, bcrypt
- Tools: GPG, OpenSSL, VeraCrypt
- Public Key Infrastructure (PKI)
- Email & Disk Encryption Techniques

### Benefits:

You'll be able to apply symmetric and asymmetric encryption, use tools like OpenSSL and GPG for secure communications, and understand PKI concepts along with practical email and disk encryption methods to safeguard digital assets.

### Outcomes:

These modules provide a strong foundation in encryption and hashing techniques essential for securing data and communications. Understanding cryptography helps protect sensitive information from unauthorized access and ensures data integrity.

## Year 2 :- Application & Project Phase:

– Year 2 is full of hands-on-experience on 8 live projects –

1. **Scanning using OWASP ZAP** involves identifying vulnerabilities in web applications through automated security testing. ZAP (Zed Attack Proxy) is an open-source tool developed by OWASP that helps in detecting issues like SQL injection, XSS, and insecure authentication. It performs both passive and active scanning by intercepting traffic between the client and server. ZAP is widely used by security analysts for penetration testing, vulnerability assessments, and ensuring compliance with secure coding practices.

2. **Scanning for open ports and attacking** them is a common technique in cybersecurity used to identify entry points into a system. Tools like Nmap scan a target machine to detect active ports and the services running on them. Once open ports are discovered, attackers may exploit known vulnerabilities in those services to gain unauthorized access. This method is often used in penetration testing to assess a system’s exposure to threats and to harden its defenses.

3. **Information Gathering tools** in cybersecurity are used to collect data about a target system, organization, or individual before launching a potential attack or penetration test. These tools help identify domains, IP addresses, subdomains, open ports, technologies used, and even leaked credentials. This phase, also known as reconnaissance, is crucial for mapping the target's surface area and planning further exploitation. It’s used by ethical hackers to detect weak points in security.

4. **Exploiting server vulnerabilities** in cybersecurity involves taking advantage of weaknesses in a server's software, configuration, or exposed services to gain unauthorized access or control. These vulnerabilities may include outdated software, misconfigured settings, or insecure services like FTP or SMB. Ethical hackers use this process during penetration testing to demonstrate real-world risks and help organizations patch flaws. Exploits can lead to data breaches, privilege escalation, or system takeover if left unaddressed

5. **OWASP Juice Shop** is a deliberately insecure web application developed for learning and practicing web application security. It simulates a real-world e-commerce platform filled with vulnerabilities such as XSS, SQL injection, insecure authentication, and broken access control. Security professionals and students use Juice Shop for hands-on training in ethical hacking and secure coding practices. It's widely used in Capture the Flag (CTF) challenges and cybersecurity education.

6. **System Hacking** in the cybersecurity domain refers to the process of gaining unauthorized access to computer systems to uncover vulnerabilities, test defenses, or demonstrate potential risks. It typically involves password cracking, privilege escalation, and accessing sensitive data. Attackers may exploit weak or reused passwords, open ports, or system misconfigurations. Tools like Hydra are used for brute-force attacks on login services, while Auxiliary Modules in Metasploit help in scanning and exploiting services. NSE Scripts in Nmap

automate vulnerability detection and exploitation tasks. John the Ripper is a fast password-cracking tool, and Crunch helps generate custom wordlists for brute-force attacks. These tools are essential for ethical hackers during penetration testing to assess and strengthen system security

- Tools Utilized:
- Hydra
- Auxiliary Module (Metasploit)
- NSE Scripts (Nmap)
- John the Ripper
- Crunch (Password list generator)

7. **Simulated Ransomware Attack and Defense** is a controlled cybersecurity exercise that mimics a real ransomware attack to test an organization’s detection and response capabilities. It involves encrypting files or restricting system access in a safe environment to evaluate how security teams react. Defensive measures such as backups, endpoint protection, and incident response are tested. This helps organizations strengthen preparedness and identify gaps in their defenses. It also raises awareness among staff and validates recovery procedures.

## Year 3 – Placement & Internship Phase:

### 1. Guaranteed Internship Phase

- In Year 3, Coincent guarantees an internship with partner companies for every student at no extra cost. The internship includes a formal Internship Offer Letter and a Completion Certificate upon successful completion.
- This is part of their "Industrial Training + Internship" model — training fees cover live classes, mentorship, and project work, but the internship phase itself is completely complimentary

### 2. Structured Placement Preparation

- Coincent supports students in portfolio-building with multiple completed projects (typically around 8) and Microsoft-aligned certifications .
- They provide mock interviews, resume reviews, and training for HR and technical rounds — all aimed at preparing you for real-world hiring.

### 3. Final Take

- Coincent's 3rd year transforms theory into practical experience through a guaranteed internship, builds a robust credentials portfolio, and equips you with placement-ready skills via mock interviews and resume prep. If you're in your 4th year, this phase sets you on a clear trajectory from "training" to "hired."

## Step Into Top Cyber Security and Ethical Hacker Domain Roles

The leading and high-demand roles in the Cyber Security & Ethical Hacking Field along with a brief description of each:

### Cybersecurity Analyst

Role:Monitor networks for threats, investigate security breaches, and implement protective measures.
Skills:SIEM tools, firewalls, IDS/IPS, incident response.

### Security Engineer

Role:Design and build secure network systems; ensure architecture is resistant to attacks.
Skills:Network security, scripting (Python, Bash), threat modeling, firewall configuration.

### Security Architect

Role:Create and maintain an organization's overall security structure.
Skills:Enterprise architecture, risk assessment, system design, zero-trust framework.

### Compliance & Risk Analyst

Role:Ensure security practices comply with regulations like GDPR, HIPAA, ISO 27001.
Skills:Risk management frameworks (NIST, ISO), documentation, audit readiness.

### Penetration Tester (Ethical Hacker)

Role:Simulate attacks to identify system vulnerabilities before real hackers do.
Skills:Kali Linux, Metasploit, Burp Suite, scripting.

### Incident Responder

Role:Act quickly to contain and eliminate active threats during a security breach.
Skills:Forensics, malware analysis, playbook creation, endpoint detection tools.

### Cloud Security Engineer

Role:Secure cloud infrastructures (AWS, Azure, GCP) against evolving threats.
Skills:IAM, encryption, DevSecOps, container security (Docker, Kubernetes).

### Security Operations Center (SOC) Analyst

Role:Front-line defenders, continuously monitoring security alerts and responding in real-time.
Skills:SIEM tools (Splunk, IBM QRadar), log analysis, threat detection.

### Cybersecurity Trainer / Awareness Officer

Role:Educate employees and users about best practices, phishing threats, and password hygiene.
Skills:Communication, instructional design, user behavior analysis.

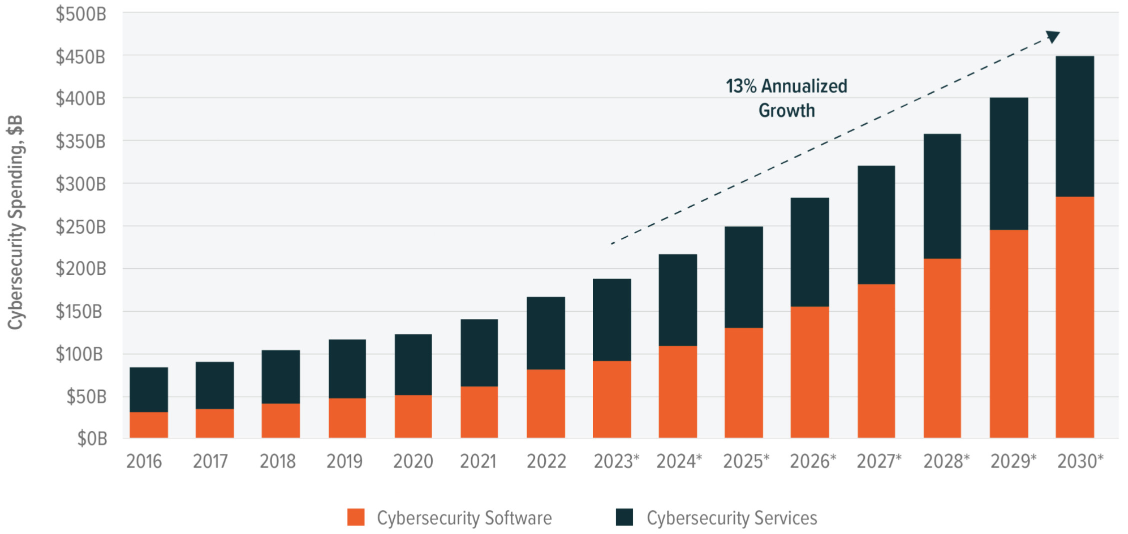
### Cyber Threat Intelligence Analyst

Role:Gather, analyze, and report on threat data to predict and prevent attacks.

Skills:OSINT, malware trends, threat actor profiling, MITRE ATT&CK framework.

GLOBAL CYBERSECURITY SPENDING FORECASTED TO GROW TO $450 BILLION BY 2030

Sources: Global X estimates with data from Gartner (2023, Sep 28) Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.



*Indicates Forecast