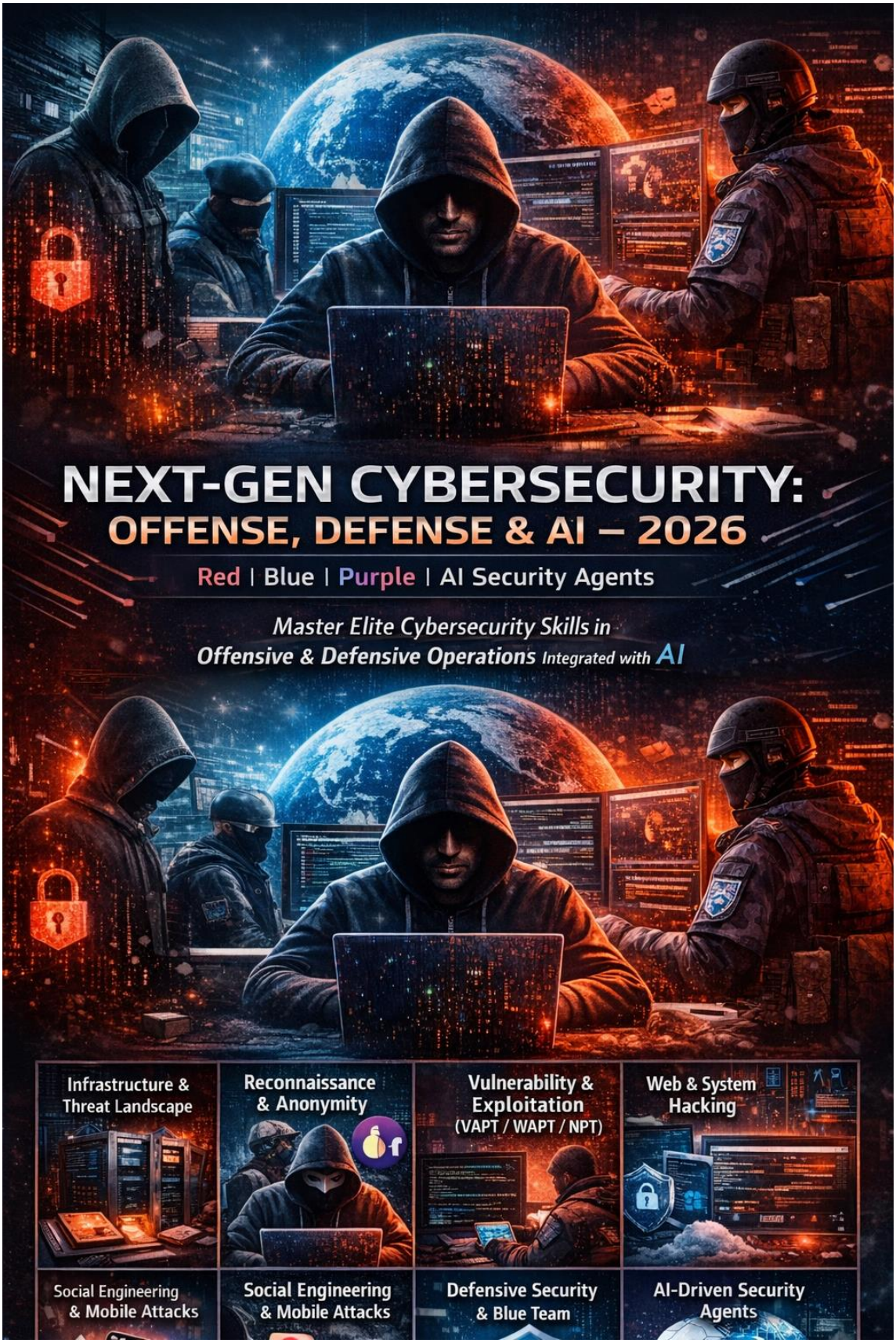
NEXT-GEN CYBERSECURITY: OFFENSE, DÉFENSE & AI – 2026

Red | Blue | Purple | AI Security Agents



Course Highlights

🚀 Advanced, Enterprise-Grade Curriculum

Designed for **working professionals and security teams**, this course goes far beyond basics—focusing on **real enterprise security operations**, not just tools or theory.

🧠 Offense + Defense + AI (End-to-End Security View)

Learners gain a **complete cybersecurity mindset**:

- How attackers **think, plan, and execute**
- How defenders **detect, respond, and mitigate**
- How **AI enhances modern security operations**

🛡️ Comprehensive VAPT Coverage

Hands-on exposure to:

- **VAPT** – Vulnerability Assessment & Penetration Testing
- **WAPT** – Web Application Penetration Testing
- **NPT** – Network Penetration Testing

All mapped to **real consulting-style workflows used in MNCs**.

🔍 Real-World Reconnaissance & Threat Intelligence

Learn how modern attackers and defenders:

- Perform **OSINT & asset discovery**
- Understand **Surface, Deep & Dark Web**

⚔️ Red Team | Blue Team | Purple Team Approach

Simulates **real enterprise security roles**:

- **Red Team:** Attack simulation & reporting
- **Blue Team:** Detection, monitoring & response
- **Purple Team:** Collaboration & security improvement

🤖 AI-Integrated Cybersecurity (Future-Ready)

Exclusive coverage of **AI-driven cybersecurity agents**:

- Automated log analysis ,Phishing detection, Vulnerability prioritization, Threat prediction & correlation

Built using **Amazon Bedrock**, aligned with **enterprise AI governance**.

💎 Why This Course Is Valuable

Not a tool demo. Not a beginner course.
This is a **serious, advanced cybersecurity journey** aligned with how **real organizations secure real systems—today and in the AI-driven future**.

NEXT-GEN CYBERSECURITY: OFFENSE, DÉFENSE & AI – 2026

Red | Blue | Purple | AI Security Agents

🎯 Objective

To develop **enterprise-ready cybersecurity professionals** capable of executing **VAPT, WAPT, and NPT**, conducting realistic threat simulations, supporting defensive and SOC operations, and leveraging **AI-assisted security automation**, aligned with **real-world MNC security architectures, governance, and compliance expectations**.

📦 DOMAIN 1: Core Infrastructure & Security Foundations

Module 1: Networking & Infrastructure Fundamentals

Key Topics (with Tools)

- OSI & TCP/IP Models *(Wireshark)*
- Routing, Switching & VLANs *(Cisco Packet Tracer)*
- IP Addressing & Subnetting *(ipcalc)*
- Network Topologies & Traffic Flow Analysis *(Wireshark)*

📌 *Foundation for NPT, SOC, and Blue Team roles*

Module 2: Server, OS & Virtualization Security

Key Topics (with Tools)

- Windows & Linux Server Architecture *(Windows Server, Ubuntu)*
- IIS vs Apache Configuration & Hardening *(IIS Manager, Apache2)*
- Virtualization & Secure Lab Setup *(VirtualBox, VMware)*

📌 *Attackers exploit misconfigurations — defenders must master them*

📦 DOMAIN 2: Cybersecurity Core & Threat Landscape

Module 3: Cybersecurity Fundamentals & Attack Lifecycle

Key Topics

- CIA Triad & Core Security Principles
- Cyber Kill Chain & MITRE ATT&CK Overview
- Vulnerability Assessment vs Penetration Testing vs Red Teaming *(Nmap, Manual Validation)*

📌 *Builds the offensive and defensive security mindset*

📦 DOMAIN 3: Reconnaissance, Anonymity & Vulnerability Assessment (VA)

Module 4: Reconnaissance & OSINT (Passive & Active)

Key Topics (with Tools)

- Passive Reconnaissance *(Google Dorks, Public Intelligence Sources)*
- Active Reconnaissance *(recon-ng, theHarvester)*
- DNS & Subdomain Enumeration *(dnsenum, sublist3r)*
- Metadata & Historical Intelligence *(ExifTool, Wayback Machine)*
- Internet-Exposed Asset Discovery *(Shodan)*

📌 *VAPT Phase: Reconnaissance*

Module 4.1: Anonymity, Evasion & Internet Layers

Key Topics (with Tools)

- Surface Web vs Deep Web vs Dark Web *(Conceptual with controlled TOR demonstration)*
- TOR Architecture, Use-Cases & Risks *(Tor Browser – awareness & testing)*
- VPN Technologies, Capabilities & Limitations *(OpenVPN, ProtonVPN – demo)*
- Proxy Chains & Traffic Routing *(proxychains)*
- Legal, Ethical & Compliance Boundaries of Anonymity

📌 *Used by attackers and defenders for threat research and analysis*

Module 4.2: Identity & Network Spoofing Techniques

Key Topics (with Tools)

- MAC Address Spoofing *(macchanger)*
- IP Spoofing Concepts *(hping3 – controlled lab)*
- ARP Cache Poisoning *(Ettercap)*
- Detection, Monitoring & Prevention Techniques

📌 *Bridges reconnaissance into network-level attack understanding*

Module 5: Network & Host Scanning (VA Phase)

Key Topics (with Tools)

- Host Discovery *(Nmap, ping)*
- Port Scanning *(Nmap –sS, –p-)*
- Service & Version Detection *(Nmap –sV)*
- OS Fingerprinting *(Nmap –O)*
- Vulnerability Scanning *(Nessus, Nikto)*

📌 *Outcome: Vulnerability identification without exploitation*

Module 6: Vulnerability Analysis & Risk Management

Key Topics (with Tools)

- CVE & CVSS Scoring *(NVD, CVSS Calculator)*
- False Positive Validation *(Manual Verification)*
- Risk vs Impact Assessment *(OWASP Risk Rating)*
- VA → PT Target Mapping *(Attack Surface Mapping)*

📦 DOMAIN 4: Penetration Testing (PT – Controlled Exploitation)

Module 7: Network Penetration Testing (NPT)

Key Topics (with Tools)

- Passive Network Sniffing *(Wireshark)*
- Active Sniffing & MITM Attacks *(Ettercap, Bettercap)*
- ARP Poisoning *(dsniff, Ettercap)*
- DNS Spoofing *(Ettercap)*
- Credential Interception & Analysis *(Wireshark Filters)*

📌 *Enterprise-safe, isolated lab simulations*

Module 7.1: Denial-of-Service (DoS & DDoS) Attacks

Key Topics (with Tools)

- DoS vs DDoS Architecture & Impact
- Network-Level Flooding *(hping3 – demonstration)*
- Application-Layer Attacks *(Slowloris – awareness)*
- Botnets, Reflection & Amplification Attacks *(Conceptual)*

📌 *Focused on impact analysis and defensive strategy*

Module 8: Web Application Penetration Testing (WAPT)

Key Topics (with Tools)

- OWASP Top 10
- SQL Injection – Authentication Bypass & Data Extraction *(Browser, sqlmap)*
- Cross-Site Scripting (Reflected & Stored) *(Browser, Burp Suite)*
- Directory & Resource Enumeration *(DIRB, Gobuster)*

Module 9: System Hacking & Privilege Escalation

Key Topics (with Tools)

- Password Attacks *(Hydra, John the Ripper)*
- Privilege Escalation Techniques *(Conceptual & lab-safe)*
- Post-Exploitation Concepts *(Metasploit – controlled usage)*

Module 10: Malware, Steganography & Persistence

Key Topics

- Malware Types & Attack Kill Chain *(Static analysis concepts)*
- Capability Demonstrations: screen capture, webcam, live feed *(controlled lab)*
- Steganography Techniques *(Steghide, OpenStego)*
- Detection, Mitigation & Prevention Strategies

📌 *Defensive understanding emphasized*

📦 DOMAIN 5: Human, Mobile & Social Attack Vectors

Module 11: Social Engineering & Human-Centric Attacks

Key Topics (with Tools)

- Phishing Types: Email, SMS, QR, Voice
- OSINT-Based Target Profiling *(Sherlock)*
- Phishing Simulation & Awareness *(Zphisher, PyPhish – lab use)*
- Psychological Triggers, User Awareness & Defense

📌 *Mapped to real-world enterprise breaches*

Module 12: Mobile Application Security (Threats & Abuse)

Key Topics (with Tools)

- Mobile Threat Landscape & Attack Surface
- Location, Camera & Sensor Abuse *(CamPhish – demo)*
- Credential & Information Harvesting *(Storm-Breaker – awareness)*
- Secure Configuration, Permissions & Defense

📌 *Security awareness with defensive emphasis*

📦 DOMAIN 6: Defensive Security, Cloud & Security Teams

Module 13: Network, Cloud & Blue Team Security

Key Topics (with Tools)

- Firewall, IDS & IPS Concepts *(pfSense)*
- Cloud Network Security *(Azure NSG & Firewall – Azure Portal)*
- Log Monitoring & Alerting *(SIEM Concepts)*
- Incident Response Lifecycle *(NIST IR Framework)*

Module 14: Red Team, Blue Team & Purple Team Operations

Key Topics

- Red Team: Attack Simulation & Reporting
- Blue Team: Detection, Response & Hardening
- Purple Team: Collaboration, Validation & Continuous Improvement
- Executive, Technical & Compliance Reporting

📦 DOMAIN 7: AI-Driven Cybersecurity & Security Agents

Module 15: AI-Driven Cybersecurity Agents

(Adversary-Aware, Ethical Gray-Hat Perspective)

Key Topics (with Tools)

- AI-Driven Security Agents using **Amazon Bedrock**
- Practical Use-Cases:
  - Automated log analysis, Phishing detection, Vulnerability prioritization & triage,Threat prediction & correlation
- Responsible AI, Ethics, Governance & Compliance

📌 *"Think like an attacker — defend like an enterprise."*