# cybersecurity whitepaper

Tensor Security Academy

tensorsecurityacademy.com

# Cyber Security Engineering With Generative AI

TENSOR SECURITY ACADEMY

## Beyond Traditional CYBERSECURITY

### The Playbook for Next GEN SECURITY PROFESSIONALS

This is where your cybersecurity career begins. Not with another generic course, but with a complete transformation. This is the program that bridges the gap between eager learner and in-demand expert, equipping you with the strategic mindset that defines the industry's elite.

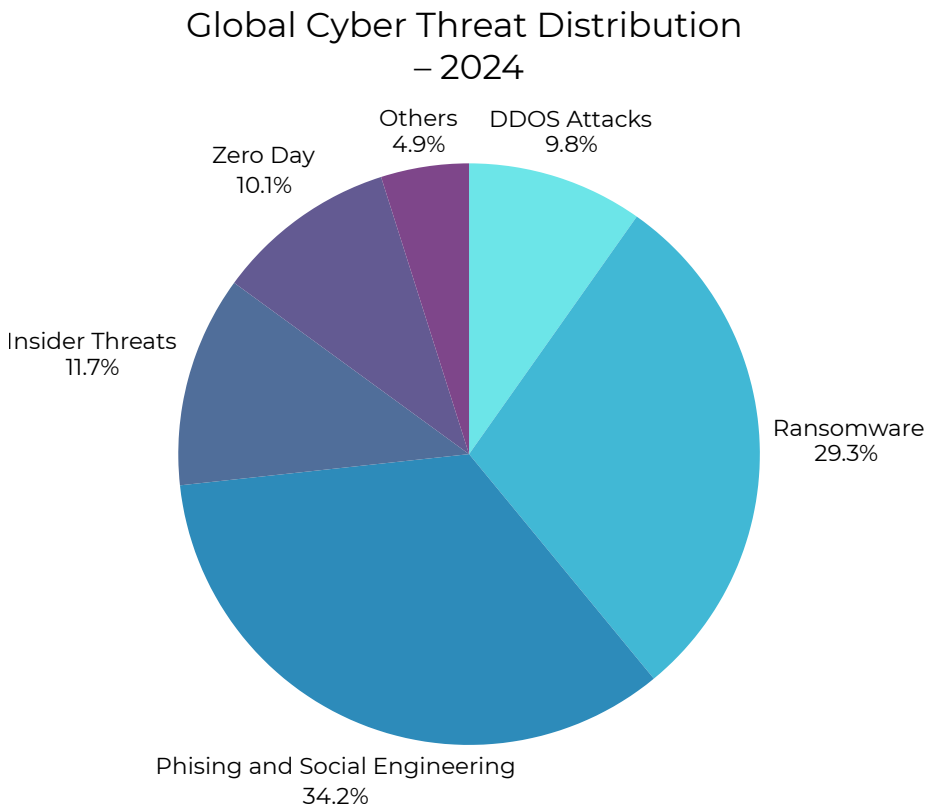
We provide more than knowledge; we forge capability. You will master the full spectrum, from defending critical networks to ethically probing their weaknesses, all while integrating the transformative power of **artificial intelligence.** This is holistic expertise for a complex digital world.

You will train with the tools that shape the field **Kali Linux, Wireshark, Metasploit, Burp Suite in hands-on simulations** that mirror real world threats. You will learn to think like both defender and adversary through red and blue team operations, and you will stay ahead of the curve with **AI driven security, OSINT investigations, and the competitive edge of bug bounty hunting.**

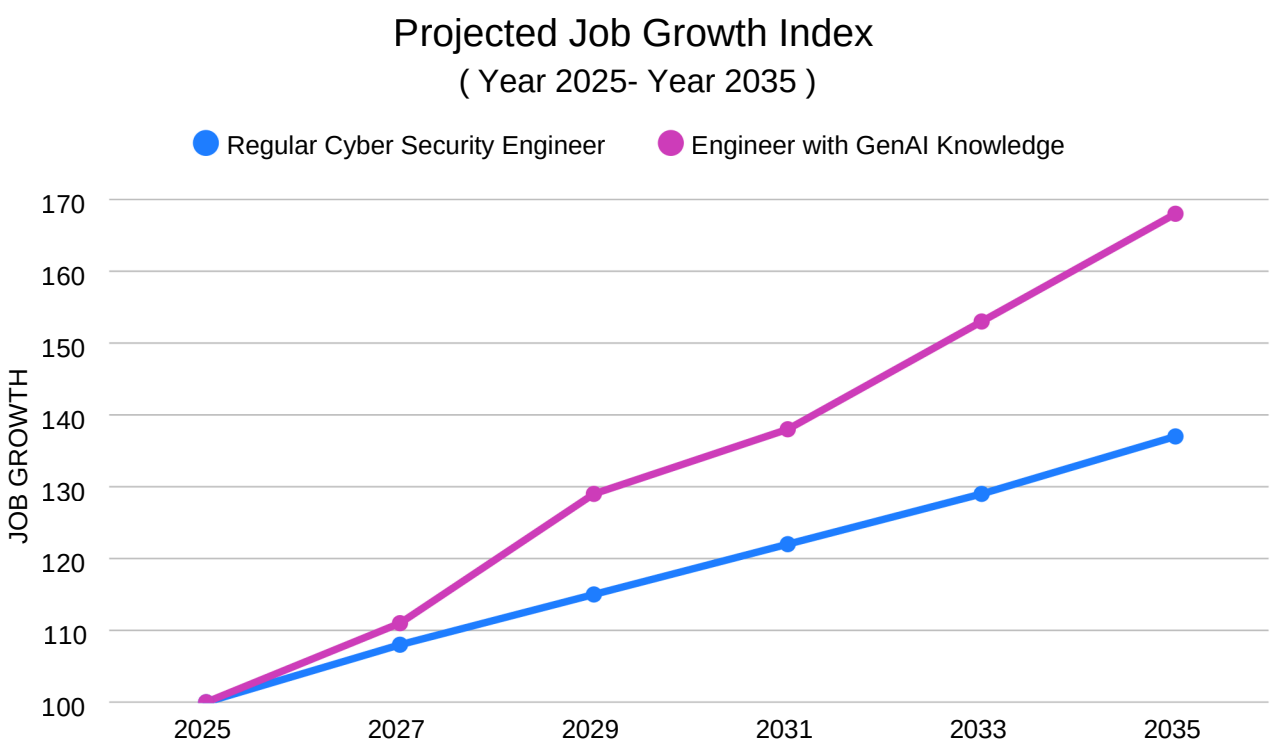
But we go beyond the lab. Your journey here is built for tangible success. You will build a professional portfolio of capstone projects that demonstrate your skill. You will prepare for global certifications that validate your expertise. You will gain the guidance to launch a freelance career or seize roles in SOC, Red Teaming, or Threat Intelligence

# The Era of Cyber Security with Gen AI

**Generative AI** has catalyzed a fundamental shift in **cybersecurity,** transforming the tools of both attackers and defenders. With the **integration of Generative AI** into both offensive and defensive cyber capabilities, the landscape is shifting rapidly. Organizations now face not only known threats but an entirely new class of AI-augmented attacks capable of morphing and adapting in real-time. This new age presents a critical challenge. To secure the future, organizations must proactively embrace these same technologies, leveraging AI to power next-generation protection, detection, and defense strategies.




The cyber threat landscape is evolving at a breakneck pace. **Phishing remains** the dominant threat, responsible for over **31% of breaches,** with **ransomware close behind at 28%** often targeting critical sectors like **healthcare** and **government**. **Zero-day exploits** and insider threats have surged by more than 20% year-over-year, many now powered by **AI tools and LLMs,** making detection and response more challenging than ever. Understanding these advanced, **AI-powered threats** is no longer optional it's the essential foundation of modern cybersecurity.




From **2025 to 2035,** demand for cybersecurity engineers is projected to **grow by 35%**, while roles requiring **Generative AI expertise** are expected to surge by **65%.** As AI reshapes cyber defense, professionals skilled in both **cybersecurity and GenAI** will lead the next wave of innovation and impact.

# Module 1

Cybersecurity Foundations & Principles

Master the core principles of cybersecurity strategy, mindset, and defense. Gain the essential knowledge to build secure systems, evaluate risks with precision, and deploy proactive protections that keep organizations one step ahead in an ever changing threat environment.

- **Developing the Cybersecurity Mindset**

Develop the sharp, forward-thinking mindset of elite cybersecurity professional. Train yourself to predict threats, think like an attacker, and deploy strong defenses early evolving from a reactive fixer to a proactive guardian.

- **The CIA Triad: Confidentiality, Integrity, and Availability**

Explore the cornerstone security model that shapes every secure system and policy. Understand how protecting confidentiality, integrity, and availability directly impacts data security and operational resilience.

- **Threats, Vulnerabilities, and Risk Assessment**

Clearly distinguish threat actors, vulnerabilities, and exploits. Master proven risk assessment frameworks to identify, prioritize, and strengthen defenses against real-world dangers.

- **Common Cybersecurity Attack Types**

Uncover today's most common and dangerous attack methods phishing, ransomware, DDoS, zero-day exploits, and more. Learn their tactics, indicators, and effective countermeasures to stay protected.

- **Cybersecurity Career Pathways**

Explore exciting career tracks in cybersecurity from Red and Blue Teaming to Governance, Risk & Compliance (GRC), penetration testing, and cutting edge roles in AI and cloud security.

- **Security Policies and Governance**

Discover how strong policies, standards, and procedures form the backbone of effective governance. Align security efforts with business objectives to create sustainable, organization wide protection.

- **Introduction to Virtualization and Cloud Security**

Explore the fundamentals of securing virtualized and cloud-based environments. Learn about shared responsibility models, hypervisor-level risks, and cloud-native security considerations.

- **Introduction to Virtualization and Cloud Security**

Grasp the essentials of securing virtual and cloud environments. Understand shared responsibility models, hypervisor risks, and modern cloud native security best practices.

- **Cybersecurity Terminologies and Acronyms**

Build fluency in the essential language of cybersecurity. Master key terms and acronyms to communicate confidently with teams, stakeholders, and technical experts.

- **Introduction to Compliance Frameworks (GDPR, HIPAA, ISO 27001)**

Get a clear overview of leading global standards and their requirements. Learn how compliance drives better data protection, risk management, and accountability across industries.

TENSOR SECURITY ACADEMY

# Module 2

## Operating Systems & System Security

Effective cybersecurity starts with mastering the operating systems that power modern infrastructure and the assets they protect. This module delivers practical, hands-on experience in both Linux and Windows environments, building essential skills in system auditing, automation, and asset management.

### Linux Operating System Fundamentals (Kali Linux)

Dive into a leading penetration-testing distribution widely used in professional cybersecurity labs. Gain real-world experience navigating, configuring, and hardening Kali Linux systems.

### Command Line Interface (CLI) Prof iciency

Develop fluency in the Linux and Windows CLI to efficiently manage files, directories, permissions, and system processes—critical for any cybersecurity professional.

### File Systems and Permission Structures

Build confidence and speed in both Linux and Windows command lines. Efficiently handle files, directories, permissions, processes, and system configurations—skills every cybersecurity professional relies on daily.

### System Logs and Monitoring Essentials

Learn to collect, analyze, and interpret system logs across platforms. Detect anomalies early, preserve evidence for forensics, and support faster incident response.

### User, Group, and Process Management

Effectively manage users, groups, and system processes to minimize vulnerabilities and ensure a secure operational environment.

### Bash Scripting for Security Automation

Create powerful Bash scripts to automate repetitive security tasks, including log parsing, patch management, configuration checks, and compliance scanning—saving time and reducing human error.

### Introduction to Windows System Security

Explore core Windows security features such as User Account Control (UAC), Group Policy Objects (GPOs), Windows Defender controls, and the advanced Windows Event Logging system for centralized monitoring and threat detection.

### Asset Discovery and Inventory Management

Use industry-standard tools (open-source and commercial) to scan networks, identify devices, and maintain an accurate asset inventory essential for compliance, risk assessment, and security audits.

TENSOR SECURITY ACADEMY

# Module 3

## Networking Fundamentals & Network Security

Strong networks form the backbone of any effective cybersecurity strategy. This module delivers essential networking foundations alongside practical tools and techniques to protect enterprise environments from evolving threats.

- **Introduction to Networking Concepts**

Explore key networking components—topologies, protocols, and the client-server model—from a cybersecurity perspective.

- **Understanding the OSI and TCP/IP Models**

Explore the layered architecture of modern networks. Learn how data moves through each layer and pinpoint the best places to deploy targeted security controls.

- **IP Addressing, Subnetting, and Routing**

Master IP addressing, subnetting techniques, and routing principles. Use them to segment networks securely, control traffic flow, and enforce strong security boundaries.

- **Network Scanning**

Harness powerful reconnaissance tools like Nmap and Zenmap to discover hosts, map open ports and services, and uncover hidden vulnerabilities before attackers do.

- **Traffic Analysis**

Capture and analyze live network packets. Spot anomalies, detect indicators of compromise, and trace attacker lateral movement with precision.

- **Intrusion Detection and Prevention Systems (IDS/IPS)**

Deploy and tune IDS/IPS solutions to monitor traffic in real time. Detect threats using signatures and behavioral analysis, then automatically block attacks before damage occurs.

- **Firewall Concepts and Implementation**

Build expertise in stateful firewalls, rule based access control, and next generation features that deliver robust perimeter and internal network defense.

- **VPNs and Secure Communication Protocols**

Understand VPN technologies, secure tunneling protocols, and encryption standards that safeguard sensitive data as it travels across untrusted networks.

- **Encryption and Encoding Fundamentals**

Grasp symmetric and asymmetric encryption, hashing algorithms, and common encoding methods essential for protecting data in transit and at rest.

- **Network Access Control (NAC)**

Implement identity based and role aware access policies. Ensure only trusted users and compliant devices gain entry to your network resources.

- **DNS and Network Protocol Analysis**

Examine DNS queries and other critical protocols. Identify misuse, detect command and control traffic, and reveal stealthy malicious activity.

TENSOR SECURITY ACADEMY

# Module 4

## Red Team Operations

Step into the mindset of a real-world attacker. This module immerses you in offensive security techniques, teaching you how to ethically discover, exploit, and report vulnerabilities through realistic, hands on simulations that mirror actual cyber threats.

- **Foundations of Ethical Hacking**

Master the principles, legal boundaries, and professional standards of ethical hacking, including frameworks like the Penetration Testing Execution Standard (PTES) and rules of engagement.

- **Web Application Security Basics**

Understand web application architecture and learn how attackers target common weaknesses such as poor input validation, broken authentication, and misconfigured security controls.

- **OWASP Top 10 Vulnerabilities**

Explore the world's most critical web risks as defined by OWASP. Perform guided exploitation exercises to fully grasp their impact and learn effective remediation techniques.

- **SQL Injection (SQLi) & Cross-Site Scripting (XSS)**

Identify and exploit flaws in input handling that let attackers steal data, hijack sessions, or manipulate databases then discover how to prevent these widespread attacks.

- **Hands-on Tools: Burp Suite, Dirb, Nikto, and More**

Gain proficiency with essential offensive tools for web interception, directory enumeration, vulnerability scanning, fuzzing, and traffic manipulation tools used daily by professional pentesters.

- **Command Injection & File Inclusion (LFI/RFI)**

Master advanced injection techniques that allow arbitrary command execution or the inclusion of malicious files, leading to full system compromise.

- **Vulnerability Scanning and Assessment**

Deploy automated scanners to detect, prioritize, and validate vulnerabilities across networks and applications, building a clear picture of an organization's risk exposure.

- **Exploitation with Metasploit Framework**

Harness the power of Metasploit for rapid vulnerability exploitation, payload delivery, privilege escalation, persistence, and lateral movement in simulated environments.

- **Penetration Testing Methodologies**

Follow industry-standard processes from initial scoping and reconnaissance through exploitation, post exploitation, and professional reporting with actionable recommendations.

- **Phishing and Social Engineering Techniques**

Design convincing phishing campaigns and social engineering scenarios to bypass even the strongest technical defenses by exploiting the human element.

TENSOR SECURITY ACADEMY

# Module 5

## Blue Team Operations

Step into the heart of cyber defense and master the art of protecting organizations from real world threats. This module focuses on building robust monitoring, rapid detection, and effective response capabilities, empowering you to create resilient security operations in modern enterprise environments.

### Log Management and Analysis

Build efficient logging pipelines and craft advanced search queries. Master correlation rules to uncover hidden anomalies, policy breaches, and indicators of compromise.

### Security Information and Event Management (SIEM)

Explore SIEM architecture in depth. Learn to ingest logs from diverse sources, perform real-time correlation, and maintain constant situational awareness to catch threats early.

### Threat Detection with Splunk

Get hands-on with Splunk: create custom dashboards, write precise SPL queries, visualize security trends, and turn raw data into actionable threat intelligence for faster investigations.

### Foundations of Digital Forensics

Learn professional forensic workflows: acquire evidence without contamination, build timelines, verify data integrity, and preserve findings for investigations and legal proceedings.

### Automation and AI in Defensive Security

Harness scripting, orchestration, and AI powered tools to automate alerts, reduce false positives, speed up triage, and scale your defensive operations efficiently.

### Security Monitoring Solutions

Deploy and manage endpoint detection and response (EDR), network security monitoring, and cloud-native tools to gain full visibility across on-premises, hybrid, and cloud environments.

### Malware Detection and Analysis

Master static and dynamic analysis techniques. Safely dissect malicious samples, identify malware behaviors and families, and extract high-value Indicators of Compromise (IOCs).

### Incident Response Planning and Execution

Create and execute detailed playbooks following the NIST Incident Response Lifecycle from preparation and identification through containment, eradication, recovery, and lessons learned.

### Threat Hunting Methodologies

Shift from reactive to proactive defense. Develop hypothesis-driven hunts, use behavioral analytics, and uncover advanced persistent threats that evade traditional detection.

### Applying the NIST Cybersecurity Framework

Implement the five core functions (Identify, Protect, Detect, Respond, Recover) to build a mature, risk-based security program that aligns with industry standards.

TENSOR SECURITY ACADEMY

# Module 6

## Generative AI for Cybersecurity

Harness the game-changing potential of generative AI to supercharge cybersecurity operations with greater speed, accuracy, and innovation. This module dives into practical, responsible ways to integrate large language models (LLMs) and other GenAI tools into both defensive and offensive security practices.

### Introduction to Generative AI and Security Applications

Grasp the core concepts of generative AI, including large language models and transformers. Explore their rapidly growing applications in cybersecurity from automation and analysis to advanced threat simulation.

### Prompt Engineering for Security Outcomes

Master the art of crafting precise, effective prompts to drive AI tools toward reliable, secure, and high-impact results in vulnerability assessment, threat hunting, and defensive scripting.

### Utilizing ChatGPT for Security Automation

Deploy ChatGPT to automate everyday security tasks like report drafting, code reviews, documentation, and alert prioritization dramatically increasing efficiency in SOCs and DevSecOps teams.

### Ethical Considerations and Responsible AI Use

Address critical risks like model bias, hallucinations, prompt injection vulnerabilities, and data privacy learning best practices for ethical and secure AI deployment in cybersecurity.

### Phishing Detection and Simulation with AI

Leverage AI to detect subtle phishing indicators in emails and messages, while generating realistic phishing simulations to strengthen employee awareness and training programs

### Hands-On with OpenAI Playground & APIs

Get practical experience with OpenAI's Playground and APIs to build custom integrations for automated threat detection, vulnerability scanning, and workflow enhancements.

### Integrating AI into Cybersecurity Workflows

Seamlessly embed generative AI into real-world pipelines for log analysis, incident enrichment, threat classification, and automated response orchestration.

### AI-Powered Reporting and Threat Intelligence

Create professional, compliant reports, executive briefs, and actionable threat intelligence faster than ever using AI-assisted generation and summarization techniques.

**Key Tools:** Chatgpt, Pentestergpt, Hackergpt, Deepseek

TENSOR SECURITY ACADEMY

# Module 7

## Web Application Security & Bug Bounty Hunting

Master the offensive side of web security and turn your skills into real-world rewards. This module dives deep into the bug bounty ecosystem, teaching you advanced web penetration testing techniques, responsible disclosure, and how to hunt high-impact vulnerabilities on live programs all while building a professional portfolio that opens doors to cybersecurity careers.

### Foundations of Web Technologies

Develop a rock-solid understanding of the modern web stack: HTTP/HTTPS protocols, cookies, sessions, authentication mechanisms, and client-server interactions essential knowledge for spotting and exploiting security flaws.

### Web Reconnaissance and Target Scoping

Master passive and active reconnaissance: OSINT gathering, subdomain enumeration, technology fingerprinting, and directory brute-forcing to map attack surfaces and uncover hidden entry points.

### Exploitation of Common Web Vulnerabilities

Get hands-on with exploiting prevalent issues like Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), and more complete with proof-of-concept demos and impact analysis.

- **Key Tools :** Gain expert-level proficiency with these industry-standard tools to intercept, modify, and analyze web traffic; automate vulnerability scans; and streamline your entire testing workflow.
- **Building a Professional Bug Bounty Portfolio :** Document your responsibly disclosed vulnerabilities effectively. Build public proof of your skills, establish credibility in the community, and create a powerful launchpad for bug bounty success and full-time security roles.

### Authentication & Authorization Bypass

Learn to identify and exploit flaws in session management, broken access controls, and insecure authentication flows that lead to account takeovers and privilege escalation

### Business Logic Vulnerabilities

Uncover subtle, non-technical flaws in application workflows—race conditions, payment manipulation, and process abuses—that often result in severe financial or data exposure.

### Manual Testing vs. Automated Scanning

Understand when and how to combine manual in-depth testing (perfect for logic and chained vulnerabilities) with fast automated scanners for broad coverage and efficiency.

### Bug Bounty Program Case Studies

Dissect real-world submissions from platforms like HackerOne and Bugcrowd. Learn winning techniques, communication strategies, triage interactions, and what turns good finds into high payouts.

### Effective Bug Report Writing

Craft clear, professional vulnerability reports with detailed reproduction steps, root cause analysis, business impact, and remediation recommendations reports that get accepted and rewarded.

TENSOR SECURITY ACADEMY

# Module 8

## Capture the Flag (CTF)

Put your cybersecurity skills to the ultimate test in fast-paced, gamified challenges that mirror real world hacking scenarios. This module focuses on experiential learning through immersive CTF exercises, virtual labs, and team-based competitions helping you sharpen your technical abilities, think creatively under pressure, and build the practical experience employers crave.

### Introduction to CTFs and Practice Platforms

Discover the different CTF formats Jeopardy-style, Attack-Defense, and Hybrid and dive straight into hands-on practice on industry-leading platforms like TryHackMe, Hack The Box, and PicoCTF.

### Cryptography Challenges (Caesar, XOR, AES)

Crack classical and modern ciphers head-on. Decrypt hidden messages, break weak implementations, and deepen your understanding of core cryptographic concepts through practical challenges.

**Core Platforms:** TryHackMe, Hack The Box, PicoCTF
Master CTF skills using leading cybersecurity training platforms designed to build real-world technical expertise.

### Building Your CTF Portfolio

Document your solved challenges, write-ups, techniques, and rankings. Create a standout professional portfolio packed with proof of your hands-on skills that impresses recruiters and hiring managers.

### Web Exploitation Labs

Hunt for and exploit vulnerabilities in deliberately vulnerable web applications. Practice everything from injection attacks to misconfigurations in safe, isolated environments.

### OSINT and Reconnaissance-Based CTFs

Leverage open-source intelligence to trace digital footprints, enumerate targets, gather intel, and turn publicly available information into powerful reconnaissance advantages.

### Forensics and Steganography Challenges

Recover digital evidence, analyze memory dumps, extract hidden data from images and files, and master steganography techniques to uncover secrets attackers try to conceal.

### Team-Based CTF Competitions

Join forces with peers in simulated red team vs. blue team scenarios. Compete in timed events to attack, defend, pivot, and collaborate—just like in real adversarial engagements.

TENSOR SECURITY ACADEMY

# Module 9

Open Source Intelligence (OSINT)

Unlock the power of publicly available data to fuel cyber investigations and threat hunting. This module equips you with proven techniques to systematically collect, analyze, and correlate open source information turning everyday digital traces into actionable intelligence for profiling targets, attributing attacks, and validating threats.

- **Introduction to OSINT and Its Role in Cybersecurity**

Build a solid foundation in OSINT principles, its critical applications in threat intelligence and cybercrime probes, plus essential ethical guidelines and legal considerations to ensure responsible use.

- **Types of OSINT: Technical, Human, Social, Geo, and Dark Web**

Explore diverse OSINT categories from technical infrastructure scans to human-centric social analysis, geolocation mapping, and safe navigation of dark web resources learning to integrate them for holistic insights.

- **OSINT Investigation Methodologies**

Master professional frameworks like the intelligence cycle (planning, collection, processing, analysis, dissemination) adopted by law enforcement, intelligence agencies, and security teams.

- **Real-World OSINT Case Studies**

Dissect high-profile examples where OSINT cracked cases: tracking cybercriminals, exposing state sponsored operations, and aiding investigations with open data alone.

- **Search Engine Intelligence and Google Dorking**

Harness advanced search operators (dorks) to expose sensitive data, misconfigurations, and unprotected assets that standard searches miss supercharging your reconnaissance efficiency.

- **Email, Username, and Phone Number Tracing**

Link fragmented digital identities across services, breach databases, and platforms. Trace emails, usernames, and phone numbers to build comprehensive profiles and uncover hidden connections.

- **Social Media Intelligence (SOCMINT)**

Extract valuable insights from public profiles, posts, and interactions. Map networks, identify behavioral patterns, and detect threat signals on platforms like X, LinkedIn, and beyond.

- **Domain, DNS, and WHOIS Investigations**

Conduct deep infrastructure reconnaissance: query WHOIS records, resolve DNS histories, spot anomalies in hosting setups, and map domain relationships to reveal ownership and potential vulnerabilities.

- **Metadata Analysis of Digital Files**

Dive into images, PDFs, videos, and documents to strip out embedded metadata revealing geolocations, creation timestamps, device fingerprints, and editing histories for forensic-level detail.

TENSOR SECURITY ACADEMY

# Module 10

## DevOps & Secure Infrastructure

Bridge the gap between development, operations, and security in modern cloud native environments. This module equips you with essential DevOps practices, infrastructure-as-code, container security, and CI/CD pipeline protection ensuring systems are scalable, resilient, and secure by design.

### Cloud Computing Fundamentals & Shared Responsibility Model

Understand IaaS, PaaS, SaaS models and the division of security responsibilities across AWS, Azure, and Google Cloud Platform.

### Identity & Access Management (IAM)

Master least-privilege policies, roles, multi-factor authentication, federated identity, and conditional access controls in cloud environments.

### Network Security in the Cloud

Configure VPCs, subnets, security groups, network ACLs, WAFs, and private endpoints to isolate and protect cloud workloads.

### CI/CD Pipelines with GitHub Actions & Jenkins

Design and implement automated build, test, and deployment pipelines. Integrate security scanning tools to catch vulnerabilities before production.

### Cloud Platforms Fundamentals (AWS, Azure, GCP)

Gain practical experience with major cloud providers: VPCs, IAM roles, security groups, and shared responsibility models for secure cloud deployments.

### Configuration Management with Ansible

Automate system configuration, patching, and hardening at scale using Ansible playbooks enforcing consistent, secure baselines across environments.

### Secrets Management & Secure Credential Handling

Implement secure storage and injection using tools like HashiCorp Vault, AWS Secrets Manager, and environment variables to eliminate hardcoded credentials.

### Monitoring, Logging, and Observability

Set up centralized logging (ELK Stack/Prometheus/Grafana) and alerting to maintain visibility, detect anomalies, and support rapid incident response.

### Security in DevOps (DevSecOps Practices)

Shift security left: integrate SAST/DAST/SCA scans, policy-as-code (OPA), and compliance checks directly into your pipelines and infrastructure.

### Automation Scripting with Python & Bash

Write reusable scripts to automate repetitive tasks, enforce security controls, and streamline operations in hybrid and multi-cloud setups.

TENSOR SECURITY ACADEMY

# Module 11

## Cloud Security & Architecture

Secure the future of infrastructure in the cloud era. This module provides hands-on mastery of major cloud platforms, teaching you to design, deploy, and defend cloud native environments while implementing security controls, compliance frameworks, and threat detection at scale.

### Cloud Computing Fundamentals & Shared Responsibility Model

Understand IaaS, PaaS, SaaS models and the division of security responsibilities across AWS, Azure, and Google Cloud Platform.

### Identity & Access Management (IAM)

Master least-privilege policies, roles, multi-factor authentication, federated identity, and conditional access controls in cloud environments.

### Network Security in the Cloud

Configure VPCs, subnets, security groups, network ACLs, WAFs, and private endpoints to isolate and protect cloud workloads.

### Data Protection & Encryption

Implement encryption at rest and in transit, key management services (KMS), secrets management, and data classification strategies.

### Cloud Security Monitoring & Logging

Set up centralized logging (CloudTrail, GuardDuty, Azure Monitor, Cloud Audit Logs), real-time alerting, and threat detection using native services.

### Compliance & Governance Frameworks

Align cloud deployments with standards like CIS Benchmarks, NIST, GDPR, and SOC 2 using policy as code and automated compliance scanning.

### Container & Serverless Security

Secure Docker containers, Kubernetes clusters (EKS/AKS/GKE), and serverless functions (Lambda, Azure Functions) against common risks.

### Cloud Incident Response & Forensics

Practice responding to cloud breaches: investigate compromised resources, preserve evidence, and perform forensics using cloud-native tools.

### Infrastructure as Code Security

Integrate security scanning into Terraform and CloudFormation templates to prevent misconfigurations from reaching production.

### Multi-Cloud & Hybrid Security Strategies

Design secure architectures across multiple providers and on-premises integrations, including zero-trust network access.

TENSOR SECURITY ACADEMY

# Module 12

## Machine Learning Security & MLOps Security (MLSecOps)

Protect the next frontier of technology: artificial intelligence and machine learning systems. This module dives into the unique security challenges of ML pipelines, teaching you to secure models, data, and deployments while integrating robust defenses into MLOps workflows for safe, reliable AI at scale.

### Introduction to ML Security & Adversarial Threats

Explore the ML lifecycle vulnerabilities from data poisoning and model theft to evasion attacks and inference time exploits.

### Adversarial Machine Learning Attacks

Hands-on crafting and defending against evasion (FGSM, PGD), poisoning, extraction, and inversion attacks on image, text, and tabular models.

### Secure Data Handling & Privacy in ML

Implement differential privacy, federated learning, encrypted computation (Homomorphic Encryption basics), and data anonymization techniques.

### Model Security & Integrity Checks

Detect backdoors, trojans, and supply-chain attacks in models using scanning tools, watermarking, and provenance tracking.

### MLOps Fundamentals with Security Integration

Build secure CI/CD pipelines for ML using tools like MLflow, Kubeflow, and GitHub Actions embedding security at every stage.

### Secure Model Deployment & Serving

Harden inference endpoints (TensorFlow Serving, TorchServe, Sagemaker) against extraction, inversion, and denial-of-service attacks.

### Threat Detection in ML Systems

Set up monitoring for drift, anomalies, and attacks using tools like Prometheus, Grafana, and specialized ML monitoring platforms.

### Supply Chain Security for ML

Secure dependencies (PyPI, Docker images), verify third party models/datasets, and implement SBOMs for ML artifacts.

### Compliance & Ethical AI Governance

Align ML systems with frameworks like NIST AI RMF, EU AI Act, and implement bias detection, explainability, and audit trails.

### Hands-on Tools: Adversarial Robustness Toolbox, TensorFlow Privacy, Hugging Face Security

Gain practical experience with leading libraries and platforms to test, harden, and deploy secure ML solutions.

TENSOR SECURITY ACADEMY

# Module 13

## Web3 & Blockchain Security

Enter the decentralized future securely. This module explores the unique security landscape of blockchain, cryptocurrencies, and Web3 applications teaching you to identify, exploit, and mitigate vulnerabilities in smart contracts, decentralized protocols, and blockchain infrastructure.

### Blockchain Fundamentals & Security Model

Understand consensus mechanisms, immutability, transparency, and the trustless model while examining how these introduce new attack vectors distinct from traditional systems.

### Smart Contract Security (Solidity & Vyper)

Write, audit, and secure Ethereum-compatible smart contracts. Master common vulnerabilities like reentrancy, integer overflows, access control flaws, and oracle manipulation.

### Common Web3 Vulnerabilities & Exploits

Hands-on exploration of real-world attacks: flash loan exploits, rug pulls, phishing in dApps, bridge hacks, and private key compromises.

### Smart Contract Auditing Tools

Use industry standard tools including Slither, MythX, Foundry, Hardhat, and Echidna for static analysis, fuzzing, and formal verification of contract code.

### DeFi Protocol Security

Analyze risks in decentralized finance: liquidity pools, lending platforms, yield farming, and governance tokens learning to spot price manipulation and economic attacks.

### Wallet & Transaction Security

Secure seed phrases, hardware wallets, multisig setups, and transaction signing. Detect phishing, malware, and front running attacks on the mempool.

### Layer 2 & Cross-Chain Security

Evaluate risks in rollups, sidechains, and bridges (Optimism, Arbitrum, Polygon, Wormhole) including sequencer failures and cross-chain replay attacks.

### Blockchain Forensics & Incident Response

Trace transactions on Etherscan and blockchain explorers, recover from exploits, and perform post mortem analysis of major hacks.

### Web3 Privacy & Zero-Knowledge Proofs

Explore privacy-enhancing technologies like zk-SNARKs, Tornado Cash alternatives, and privacy focused chains (Zcash, Aztec).

### Secure dApp Development Best Practices

Integrate secure front-end patterns (Web3.js, ethers.js), prevent client-side attacks, and implement proper signature verification.

TENSOR SECURITY ACADEMY

# Module 14

## Capstone Projects & Career Preparation

Tie it all together and kickstart your cybersecurity career. This capstone module blends hands-on projects with practical career guidance to solidify your skills, craft a compelling professional profile, and land your first role with confidence.

- **Project Planning and Documentation**

Master the art of scoping, executing, and documenting end-to-end cybersecurity projects. Produce professional grade reports and write-ups that clearly showcase your methodology, findings, and technical depth.

- **Red Team / Blue Team Final Simulation**

Experience the ultimate capstone challenge: a high stakes, full-scale Red Team vs. Blue Team simulation that mirrors real world cyber operations. Apply everything you've learned to plan, execute, and defend against sophisticated attacks in a safe, controlled environment.

- **AI-Driven Security Tool or Automation Development**

Design, develop, and deploy your own AI-enhanced cybersecurity tool or automation script integrating machine learning for threat detection, log analysis, or workflow efficiency to demonstrate cutting-edge innovation.

- **Cybersecurity Resume Development**

Craft a tailored, impactful resume optimized for cybersecurity roles. Highlight achievements, technical proficiencies, and projects using industry keywords to pass ATS filters and impress hiring managers.

- **LinkedIn Profile Enhancement and Personal Branding**

Transform your LinkedIn into a professional magnet: optimize your profile, share content, network strategically, and establish yourself as an emerging voice in the cybersecurity community.

- **GitHub Portfolio Management**

Build and curate a powerful public GitHub repository filled with your projects, scripts, tools, and detailed write-ups creating tangible proof of your skills that recruiters actively seek.

- **Interview Preparation: Technical and Behavioral**

Practice high-frequency technical questions, live coding challenges, and behavioral interviews. Build confidence and learn proven techniques to articulate your experience and stand out in competitive hiring processes.

- **Certification Pathways and Planning**

Map out your post-program certification journey prioritizing high-value credentials like CompTIA Security+, CEH, OSCP, CISSP, and others to accelerate career progression and validate expertise.

- **Career Strategy and Domain Entry Points**

Explore diverse paths in cybersecurity (SOC, pentesting, consulting, governance, and more). Develop personalized job search strategies, salary negotiation tactics, and long-term growth plans.

TENSOR SECURITY ACADEMY

# Potential Job Roles

Launch your cybersecurity career with the practical skills and hands-on experience employers demand. Tensr Security Academy prepares you for a wide range of entry-level and specialized roles across the industry.

Below is an important list of job roles you'll be qualified for upon graduation, including average entry-level salaries (US market, 2025 data) and key responsibilities.

| Job Role | Average Entry-Level Salary (US) | Key Responsibilities |
|---|---|---|
| Ethical Hacker | $85,000–$110,000 | Simulate real-world attacks |
| Vulnerability Assessment Analyst | $78,000–$100,000 | Scanning, prioritization, reporting |
| Penetration Tester (Junior) | $80,000–$105,000 | Ethical hacking, vulnerability testing |
| SOC Analyst (Tier 1) | $65,000–$85,000 | Alert monitoring, initial incident analysis |
| Cloud Engineer (Security Focus) | $95,000–$120,000 | Secure cloud architecture design |
| Web Application Penetration Tester | $85,000–$110,000 | Web app exploitation and testing |
| Smart Contract Auditor | $110,000–$160,000 | Smart contract code review |
| ML Security Engineer | $100,000–$140,000 | dApp and ecosystem protection |

TENSOR SECURITY ACADEMY

# cybersecurity whitepaper

Tensor Security Academy