

AI-Enabled Cybersecurity, Ethical Hacking & GRC Master Program (12-Weeks)

About Armour1X

Armour1X is an AI-powered cybersecurity and digital security ecosystem focused on helping organizations, professionals and institutions navigate the rapidly evolving security landscape across **Cybersecurity, AI, Web3, Cloud, Digital Infrastructure and Cyber-Physical Systems**.

Armour1X combines **industry experience, cybersecurity expertise, AI-enabled security practices, technology partnerships and practical learning** to develop security capabilities that are relevant to today's increasingly AI-driven threat environment.

The Armour1X approach is built around **Learn. Defend. Assess. Govern. Secure.** — combining cybersecurity fundamentals with hands-on exposure to Security Operations, Ethical Hacking, VAPT, Threat Intelligence, GRC, AI Security, Cloud Security and emerging cyber threats.

The organization's focus is not only on technical knowledge, but also on developing **industry-ready cybersecurity professionals and security-aware leaders** capable of understanding technology, risk, governance and business impact.

Why Choose Armour1X for Cybersecurity Training?

Armour1X focuses on building **practical, industry-oriented cybersecurity capabilities** through structured learning, hands-on labs, real-world scenarios, attack and defence simulations, security investigations and AI-enabled security practices.

The **AI-Enabled Cybersecurity, Ethical Hacking & GRC Master Program** brings together:

- Cybersecurity Fundamentals
- Ethical Hacking
- Security Operations Centre (SOC)
- SIEM and Threat Detection
- Incident Response

- Threat Intelligence
- Threat Hunting
- Vulnerability Assessment & Penetration Testing (VAPT)
- MITRE ATT&CK
- Cyber Kill Chain
- Cloud Security
- Governance, Risk & Compliance (GRC)
- AI Security
- AI Governance and Responsible AI
- Generative AI for Cybersecurity
- LLM Security and Prompt Injection Awareness
- Deepfake and AI-enabled Social Engineering Awareness
- Malware and Endpoint Security
- Web and API Security
- Security Automation

The program uses practical exercises and industry-relevant tools and platforms including **Wireshark, Splunk, Wazuh, ELK, Burp Suite, Metasploit, Nmap, OSINT tools, Microsoft Security Copilot and GenAI-powered security workflows**, wherever appropriate.

Learners are exposed to both **defensive and offensive security perspectives**, while also developing an understanding of governance, risk, compliance and the emerging security challenges created by AI.

This approach is designed to help learners move beyond theoretical cybersecurity knowledge and develop the ability to **identify, assess, investigate, respond to and communicate cybersecurity risks**.

About the Founder / Program Director – Srinivas Mahankali, Armour1X

Email: srini@armour1x.com

Website: www.armour1x.com, LinkedIn: linkedin.com/in/srinivasindia

Srinivas Mahankali is a senior technology and business leader with **34+ years of**

experience spanning business leadership, sales and marketing, technology strategy, digital transformation, cloud, AI, blockchain, Web3 and cybersecurity.

He has held senior leadership and CXO positions across Indian and multinational business environments, including leadership roles with **BSE-listed technology companies**. His experience includes serving as **MD of Virinchi Technologies Ltd., Director/CXO of SecureKloud Technologies Ltd., and CIO & Chief Strategy Officer at Apollo Logi Solutions Ltd.**

He has also served as **Head of Blockchain Centre of Excellence at NISG (Government of India/NASSCOM ecosystem)**.

Armour1X Cybersecurity Training Philosophy

The Armour1X training philosophy is built around five dimensions:

1. Learn

Build strong foundations in cybersecurity, networking, cloud, AI, ethical hacking, GRC and emerging technologies.

2. Defend

Develop practical defensive capabilities covering SOC operations, SIEM, threat detection, incident response, threat hunting and security monitoring.

3. Assess

Learn to identify vulnerabilities, conduct reconnaissance, perform security assessments and understand penetration-testing methodologies.

4. Govern

Develop capabilities in cybersecurity governance, risk management, compliance, AI governance, security policies and regulatory frameworks.

5. Secure

Apply cybersecurity knowledge to modern environments involving **AI, Cloud, Web3, applications, data and digital infrastructure**.

Why Armour1X Brings a Different Perspective

The Armour1X program combines **technical cybersecurity with business and leadership perspectives**.

Participants are encouraged to understand not only:

“How does a cyberattack happen?”

but also:

“What does the attack mean for the business, its customers, data, operations, reputation and regulatory obligations?”

This approach reflects Srinivas Mahankali's experience across **technology leadership, business transformation, digital strategy, cybersecurity, AI, blockchain and enterprise ecosystems.**

The attached program already follows this broader approach by combining **SOC, Ethical Hacking, Threat Intelligence, VAPT, GRC, AI Security and AI Governance** within a single 12-week learning pathway.

About Cybersecurity Trainer:

<https://www.linkedin.com/in/12cn/>

Chandrasekhar Nemmani is a highly experienced cybersecurity professional specializing in AI-powered cybersecurity, threat detection engineering, vulnerability management, SIEM development, and cloud security architecture. With a strong blend of technical expertise and business leadership, he brings real-world industry experience in building intelligent security solutions that help organizations proactively defend against evolving cyber threats.

Specialized in AI-driven security operations, advanced threat detection, automated security analytics, behavioral monitoring, and the integration of Artificial Intelligence into enterprise cybersecurity environments.

Master Cybersecurity with AI-Augmented Security Operations, Ethical Hacking, and Governance

12-Week AI-Enabled Cybersecurity Curriculum from HAC

Duration: 3 Months (100+ Hours)

Mode: 60% Theory | 40% Hands-On Labs

Target Roles: SOC Analyst, Security Analyst, GRC Analyst, Ethical Hacker, Threat Hunter, Compliance Analyst, Junior AI Security Analyst

Week	Theory Topics	AI Integration	Hands-On Labs
Week 1	Cybersecurity Fundamentals, Threat Landscape, Security Domains, NIST Cybersecurity Framework (CSF), Introduction to AI in Cybersecurity	Understanding AI use cases in SOC operations and security research	Breach Analysis Case Study, Using ChatGPT/Gemini for Threat Research, Security Prompting Exercises
Week 2	GDPR, HIPAA, PCI DSS, ISO 27001 Fundamentals, Governance, Risk & Compliance (GRC) Foundations	Introduction to AI Governance and ethical considerations in AI adoption	Compliance Mapping Exercises, GRC Policy Drafting, AI Governance Discussion Workshop
Week 3	Risk Management, Business Impact Analysis (BIA), Risk Treatment Strategies, NIST AI RMF, Responsible AI Principles, EU AI Act	AI Risk Management and third-party AI risk considerations	Risk Assessment Case Study, Risk Register Creation, AI Risk Assessment Exercise
Week 4	Networking Fundamentals, OSI Model, TCP/IP, Ports & Protocols, Wireshark Introduction	AI-assisted network anomaly detection concepts	Packet Capture with Wireshark, TCP 3-Way Handshake Analysis, Protocol Investigation

Week 5	SOC Concepts, SIEM Architecture, Incident Response Lifecycle, Threat Detection Fundamentals	AI-assisted threat detection, User & Entity Behavior Analytics (UEBA) awareness	Splunk/ELK Labs, Alert Investigation, Log Analysis, AI-assisted Incident Triage Demonstration
Week 6	Cyber Kill Chain, MITRE ATT&CK Framework, Threat Intelligence Fundamentals, IOC Concepts	Introduction to MITRE ATLAS and AI-related attack techniques	ATT&CK Mapping Exercise, IOC Investigation, Threat Intelligence Analysis
Week 7	Passive Reconnaissance, OSINT Methodologies, Footprinting, Attack Surface Discovery	AI-generated threat intelligence awareness and validation	Google Dorking, Shodan, SpiderFoot, theHarvester, Amass, Subfinder Labs
Week 8	Active Reconnaissance, Host Discovery, Service Enumeration, Vulnerability Assessment Methodologies	AI-driven vulnerability prioritization concepts	Nmap Scanning, Banner Grabbing, Netdiscover, Exposure Identification Exercises
Week 9	Social Engineering, Phishing Techniques, Business Email Compromise (BEC), Human Factors in Security	Deepfake awareness, AI-enabled phishing campaigns, AI-driven fraud techniques	SEToolkit Demonstrations, Phishing Analysis, Deepfake Identification Exercises
Week 10	Malware Fundamentals, Reverse Shell Concepts, Endpoint Security, System Hardening, CIS Benchmarks	Understanding AI-assisted malware evolution and detection approaches	Metasploit Labs, CIS Benchmarking, Log Investigation, Detection Engineering Exercises
Week 11	Web Application Security, OWASP Top	OWASP Top 10 for LLM Applications,	DVWA/Juice Shop Labs, Burp Suite

	10, Secure Development Concepts, API Security	Prompt Injection Awareness, GenAI Security Risks	Testing, SQL Injection, XSS, Prompt Injection Demonstrations
Week 12	Cloud Security Fundamentals, Shared Responsibility Model, Security Career Roadmap, Emerging Threat Trends	Risks of Enterprise GenAI Adoption and Secure AI Implementation Practices	Final Capture the Flag (CTF), Documentation & Presentation, AI-assisted Report Generation

AI Security Topics Integrated Throughout the Program

Topic	Coverage
Introduction to AI in Cybersecurity	Week 1
Using Generative AI for Threat Research	Week 1
AI Governance & Responsible AI	Week 2
NIST AI RMF	Week 3
EU AI Act Overview	Week 3
AI Risk Assessment	Week 3
AI-Assisted Threat Detection	Week 5
MITRE ATLAS Awareness	Week 6
AI-enhanced Threat Intelligence	Week 7
Deepfakes & AI-enabled Social Engineering	Week 9
AI-assisted Malware Evolution Awareness	Week 10
OWASP Top 10 for LLM Applications	Week 11
Prompt Injection Awareness	Week 11
Risks of Enterprise GenAI Adoption	Week 12
AI-assisted Security Reporting	Throughout Program

Enhanced Hands-On Labs

Governance & Compliance Labs

- Compliance mapping exercises (GDPR, HIPAA, PCI DSS)
- AI Governance workshops
- NIST AI RMF implementation scenarios
- Risk register creation

Defensive Security Labs

- Wireshark packet analysis
- Splunk/ELK log analysis
- MITRE ATT&CK mapping
- Incident response tabletop exercises
- Threat hunting fundamentals

Offensive Security Labs

- Nmap enumeration
- OSINT investigations
- Subdomain discovery
- Burp Suite testing
- SQL Injection and XSS
- Metasploit demonstrations
- CIS-based system hardening

AI Security Awareness Labs

- Prompt engineering for threat research
- Security use cases for ChatGPT
- Deepfake detection exercises
- Prompt injection demonstrations
- AI-generated phishing analysis
- AI-assisted report generation

Capstone Project

AI-Enabled Security Operations Simulation

Students will perform an end-to-end security exercise involving:

1. Threat Intelligence Collection
2. Reconnaissance Activities
3. Vulnerability Assessment
4. Detection using SIEM
5. Incident Investigation
6. MITRE ATT&CK Mapping
7. Risk Assessment and Governance Review
8. AI-assisted Executive Reporting
9. Final Presentation to a simulated management board

Certification Roadmap Alignment

Certification	Coverage
ISC2 Certified in Cybersecurity (CC)	
CompTIA Security+	
EC-Council CEH	
Cisco Ethical Hacker	
ISO 27001 Foundation	
NIST Cybersecurity Framework	
NIST AI RMF Awareness	
Microsoft SC-900	Partial
Splunk Core User	Partial

Program Outcomes

Upon completion, participants will be able to:

- Understand modern cyber threats and AI-enabled attack techniques.
- Conduct reconnaissance and vulnerability assessments ethically.
- Investigate incidents using SIEM platforms.
- Apply MITRE ATT&CK techniques for threat analysis.
- Perform risk assessments and develop GRC documentation.
- Understand how organizations govern and secure AI systems.
- Recognize and defend against prompt injection, deepfakes, and AI-driven phishing attacks.
- Use generative AI responsibly for cybersecurity research and reporting.
- Prepare for entry-level cybersecurity roles with practical experience.

AI-Enabled Cybersecurity, Ethical Hacking & GRC Master Program

Master Modern Cybersecurity with Ethical Hacking, Governance, and AI Security Awareness

This approach keeps the course:

- **Job-oriented**
- **Beginner-friendly**
- **Hands-on and practical**
- **Aligned with current industry needs**
- **Suitable for a 100-hour / 3-month format**
- **Focused on how cybersecurity professionals use and secure AI, rather than building AI models**

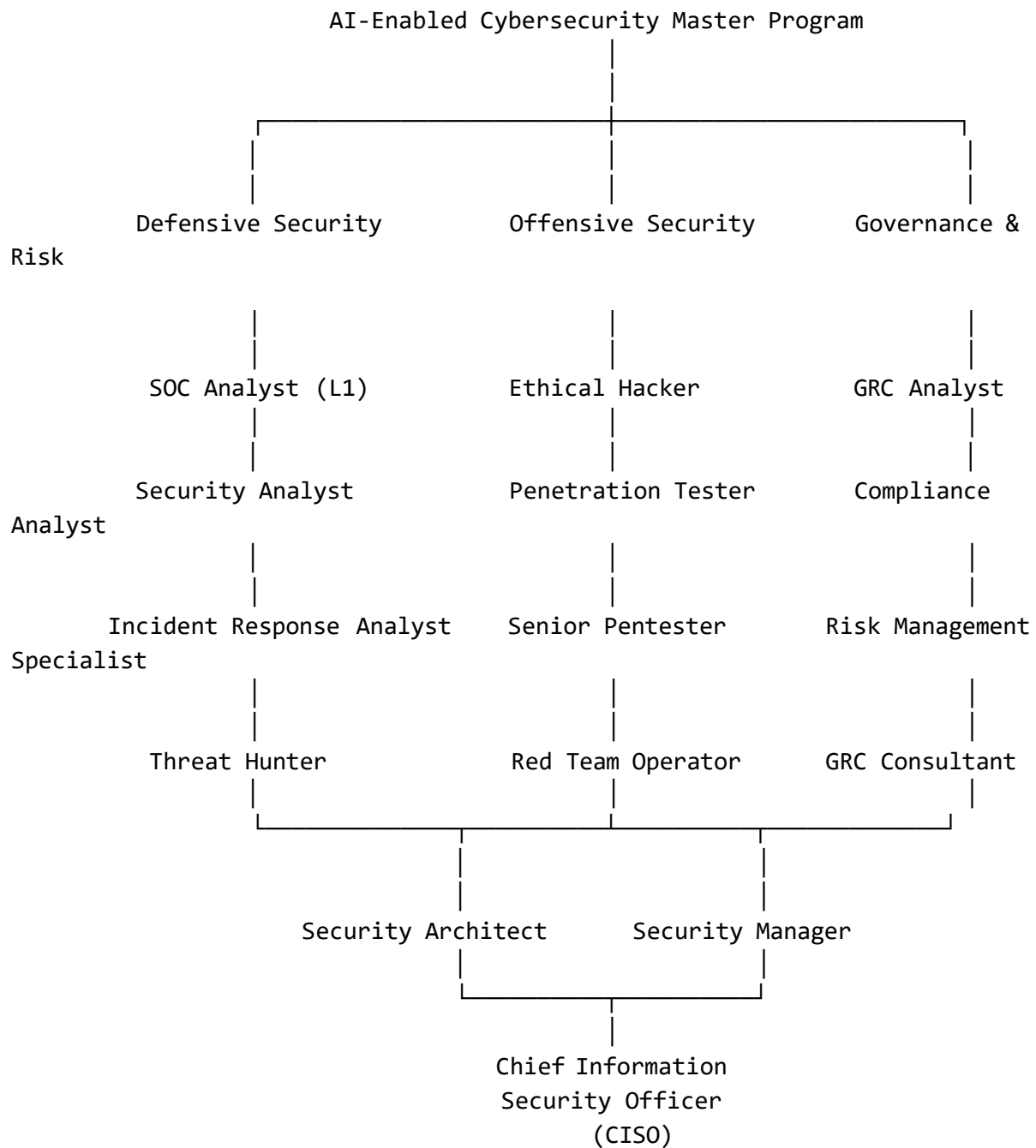
Career Roadmap – AI-Enabled Cybersecurity, Ethical Hacking & GRC Master Program

The curriculum is designed to support **multiple cybersecurity career pathways**, allowing participants to specialize based on their interests and strengths.

Career Path	Primary Responsibilities	Course Modules Covered	Suggested Certifications	Average Experience Level
SOC Analyst (L1/L2)	Monitor security events, investigate alerts, escalate incidents	SIEM, Incident Response, MITRE ATT&CK, Threat Intelligence, Log Analysis	ISC2 CC, CompTIA Security+, Splunk Core User	Entry Level
Security Analyst	Analyze threats, perform investigations, improve security controls	Threat Landscape, SIEM, Risk Management, Incident Response	Security+, CySA+	Entry–Mid
GRC Analyst	Manage policies, risk assessments, compliance activities	GDPR, HIPAA, PCI DSS, ISO 27001, NIST, Risk Management	ISO 27001 Foundation, CRISC (later)	Entry–Mid
Compliance Analyst	Ensure regulatory adherence and audit readiness	GRC Foundations, Compliance Mapping, Policy Development	ISO 27001, CISA (later)	Entry Level
Ethical Hacker / Junior Penetration Tester	Conduct vulnerability assessments and penetration testing	Reconnaissance, Enumeration, Web Security, Metasploit, Burp Suite	CEH, eJPT, PNPT	Entry–Mid
Vulnerability Management Analyst	Identify, prioritize, and track remediation of	Vulnerability Assessment, Nmap, System Hardening, Risk	Security+, Qualys VMDR	Entry Level

	vulnerabilities	Assessment		
Threat Intelligence Analyst	Research adversaries, IOCs, TTPs, emerging threats	MITRE ATT&CK, Cyber Kill Chain, Threat Intelligence, OSINT	CTIA (later), Security+	Mid Level
Threat Hunter (Junior)	Proactively search for malicious activity across environments	ATT&CK, SIEM, IOC Analysis, Incident Response	CySA+, GCFA (advanced)	Mid Level
Incident Response Analyst	Investigate and coordinate responses to security incidents	Incident Response Lifecycle, Log Analysis, SIEM, Threat Analysis	CySA+, GCIH (advanced)	Mid Level
AI Security Governance Analyst	Assess AI-related risks and support AI governance initiatives	NIST AI RMF, Responsible AI, EU AI Act, AI Governance	NIST AI RMF Training, ISO 42001 Foundation	Emerging Role
AI Security Awareness Specialist	Support secure adoption of AI technologies within organizations	Prompt Injection, Deepfakes, AI Risks, Enterprise AI Security	Vendor-specific AI Security Training	Emerging Role
Bug hunter	Bug bounty specialist	""	Ethical Hacking	Emerging Role

Career Progression Map



AI Security Career Extensions

As organizations increasingly adopt AI technologies, traditional cybersecurity professionals can transition into emerging AI-focused security roles.

SOC Analyst

|

└─▶ AI-Assisted SOC Analyst

|

└─▶ Security Automation Specialist

GRC Analyst

|

└─▶ AI Governance Analyst

|

└─▶ Responsible AI Consultant

Security Analyst

|

└─▶ AI Security Analyst

|

└─▶ AI Risk Specialist

Suggested Certification Path

Career Goal	0–1 Year	1–3 Years	3–5 Years
SOC / Blue Team	ISC2 CC, Security+	CySA+, Splunk	GCIH, GCFA
Ethical Hacking	Security+, CEH	eJPT, PNPT	OSCP
GRC & Compliance	ISO 27001 Foundation	CRISC, CISA	CISM
Threat Intelligence	Security+	CTIA	GCTI
Leadership Track	Security+	CISSP Associate	CISSP, CISM
AI Governance	NIST AI RMF Training	ISO 42001 Foundation	AI Governance Specialist

Recommended Entry Path for Students

Student Background	Recommended Career Track
Freshers / Graduates	SOC Analyst → Security Analyst
Network / System Administrators	Security Analyst → Incident Response
Developers	Application Security → Penetration Testing
Auditors / Compliance Professionals	GRC Analyst → Risk Consultant
IT Support Professionals	SOC Analyst → Threat Hunter
Existing Cybersecurity Professionals	AI Security Governance → Security Leadership

Program Outcome

By the end of this **AI-Enabled Cybersecurity, Ethical Hacking & GRC Master Program**, learners will have a clear pathway into one or more of the following domains:

- **Blue Team (SOC & Incident Response)**
- **Red Team (Ethical Hacking & Penetration Testing)**
- **Governance, Risk & Compliance (GRC)**
- **Threat Intelligence & Threat Hunting**
- **Emerging AI Security & AI Governance**

"Learn. Defend. Assess. Govern. Secure the Future with AI-Enabled Cybersecurity."

Trainer Core Expertise

- AI Powered Cybersecurity
- Security Operations Center (SOC)
- SIEM Engineering & Threat Detection
- Vulnerability Assessment & Penetration Testing (VAPT)
- AI Threat Hunting & Detection Engineering
- Cloud Infrastructure Security
- Governance, Risk & Compliance (GRC)
- Dark Web Monitoring & Threat Intelligence
- MITRE ATT&CK & Cyber Kill Chain Mapping
- Incident Response & Security Monitoring
- AI Governance & Responsible AI Security

Key Achievements

- Built and deployed an AI-enabled Vulnerability Assessment & Penetration Testing (VAPT) platform supporting 60+ advanced security checks across:
 - Web Applications
 - Mobile Applications
 - AI/LLM Models
 - Cloud Infrastructure
 - Network Security
- Designed and implemented a custom SIEM platform using:
 - HELK
 - Suricata
 - Wazuh
 - Real-time Threat Intelligence Integration
 - MITRE ATT&CK Enrichment
 - Automated Detection & Correlation
- Developed cloud security architectures focused on:
 - Infrastructure Hardening
 - Compliance Mapping
 - Threat Monitoring
 - Security Visibility

- Risk Reduction
- Hands-on experience in:
 - AI Security Operations
 - Detection Engineering
 - Threat Intelligence Automation
 - Security Analytics
 - AI-assisted Pentesting
 - AI Governance & Risk Management

Leadership & Industry Experience

In addition to deep technical expertise, the trainer has extensive experience leading:

- Security consulting engagements
- Client acquisition strategies
- Enterprise security transformation initiatives
- Technical solution architecture
- Security awareness and workforce enablement

Known for translating complex cybersecurity concepts into practical, business-focused outcomes for both technical teams and executive leadership.

Training Approach

The training methodology focuses heavily on:

- Real-world attack simulations
- Hands-on labs
- AI-powered security operations
- N8n pipeline
- Enterprise use cases
- SOC-driven workflows
- Practical implementation experience
- Industry-ready skills development

The objective is to help learners build modern cybersecurity capabilities aligned with current and future industry demands, including AI-driven security operations, threat hunting, cloud security, and intelligent defense automation.

Passionate about building scalable, intelligent, and proactive cybersecurity solutions that help organizations strengthen resilience, reduce detection gaps, and confidently modernize their security posture.