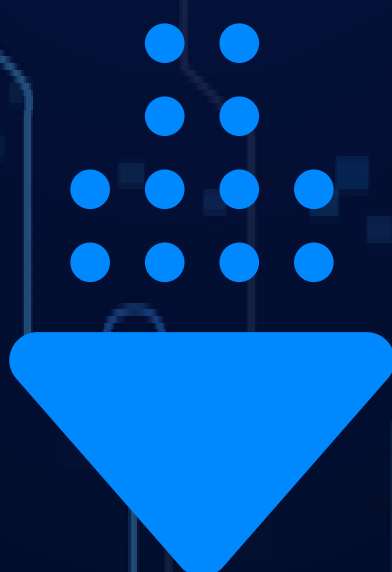
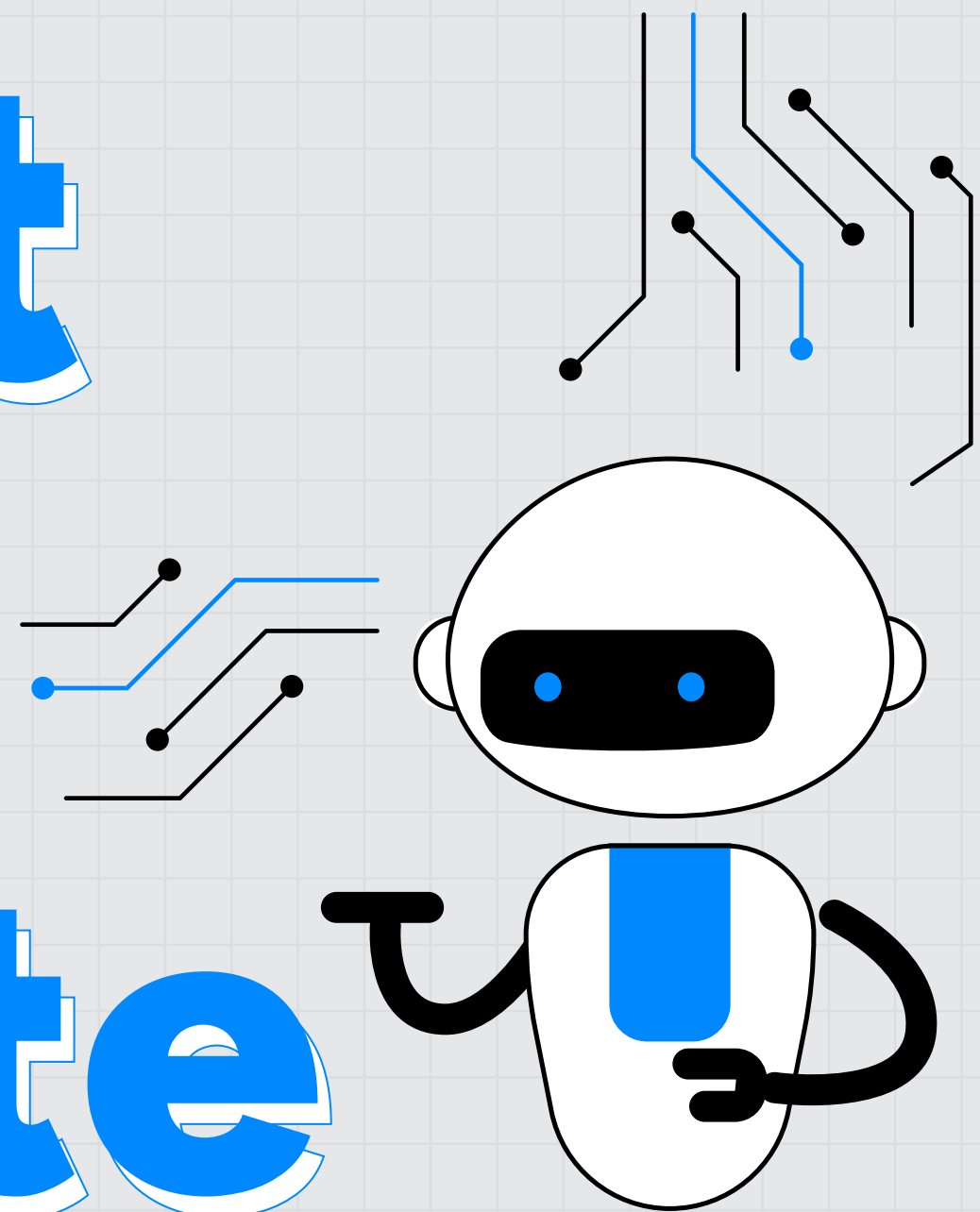




# INDUSTRY READINESS PROGRAM AI-POWERED CYBERSECURITY



# About Entri Elevate

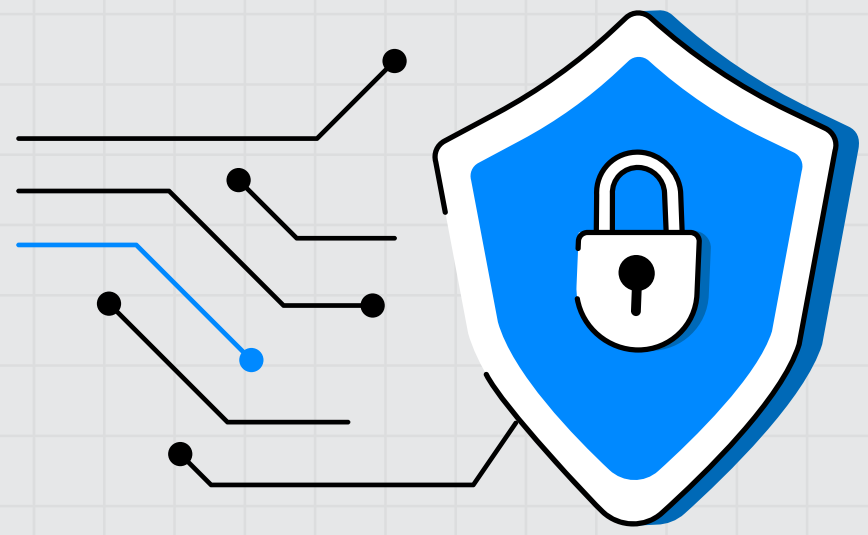


**Entri Elevate is an immersive training program meticulously crafted to enhance your skill set and transform you into a job-ready candidate.** This program is meticulously designed and led by seasoned trainers who provide comprehensive guidance throughout your journey. With access to expert mentors from diverse top industries, Entri Elevate ensures you gain invaluable industry exposure essential for success in your chosen field.

In addition to technical classes, Entri Elevate offers soft skills sessions to equip you with the essential interpersonal and communication skills vital for succeeding in today's competitive job market. Through Entri Elevate, you'll not only gain proficiency in your chosen field but also develop the holistic skills necessary to excel in interviews and beyond.

# Elevate

# AI-Powered Cybersecurity Program



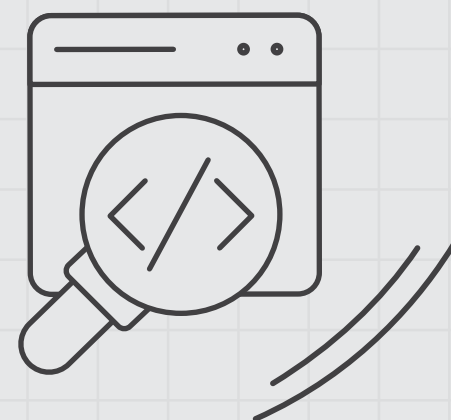
## About

This course provides a foundational understanding of cybersecurity, focusing on both defensive and offensive techniques. Learners will explore how to protect systems, networks, and data from evolving cyber threats. At the same time, the course covers ethical hacking and penetration testing to simulate attacks and identify vulnerabilities. By the end of the course, learners will be equipped with the skills to build and test secure systems from both attacker and defender perspectives. Learners registering for CH exams will receive dedicated guidance from our mentors.

Learners will receive industry internship opportunities along with certification.



## Format



Hybrid (Recorded Video Lectures + Online and Offline  
Interactive Mentored Learning)



## Time Commitment

12-15 Hrs/Week



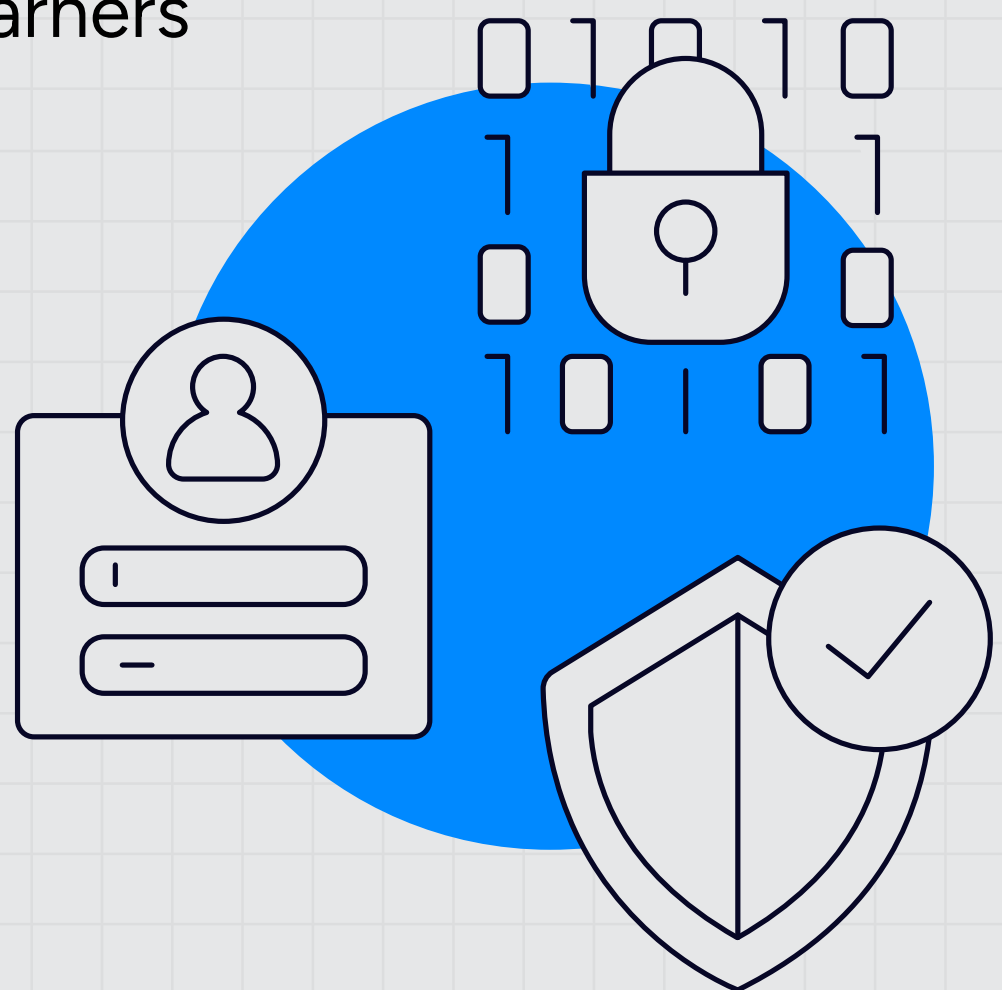
## Duration

- ✧ Batch Duration - 9 Months + 1 Month Industry Internship
- ✧ 15-20 days of offline Sessions

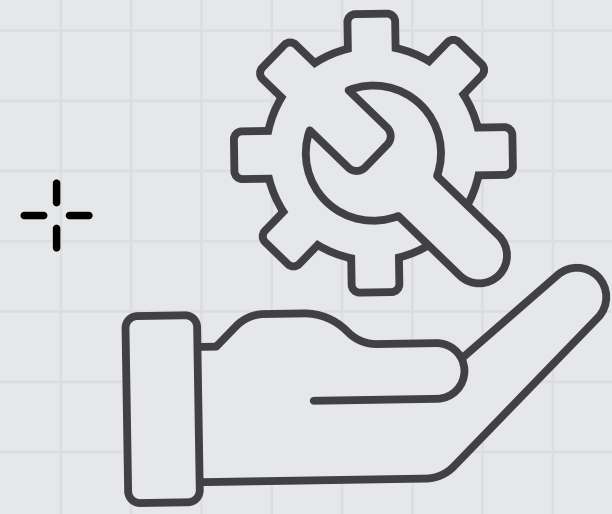


## Program Highlights

- ✧ Tailored Curriculum aligned with Industry Standards
- ✧ Inclusive & Immersive Hybrid Training Sessions
  - ✧ Tailored Curriculum aligned with Industry Standards
  - ✧ Inclusive & Immersive Hybrid Training Sessions
- ✧ Mentor-Led Live Core Sessions
- ✧ Self-Paced Learning Contents in Native Language (Malayalam)
- ✧ Placement Assistance for Eligible Learners
- ✧ Free Soft Skills Training
- ✧ Industry Expert Sessions
- ✧ 80% Hands on Experience
- ✧ Community Linking
- ✧ Certifications



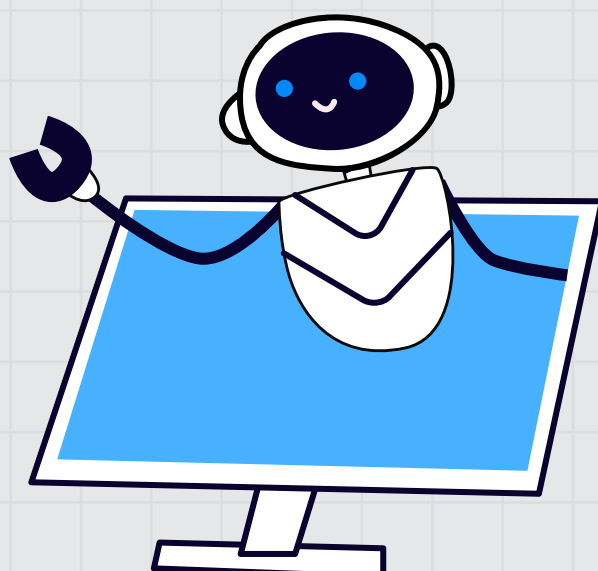
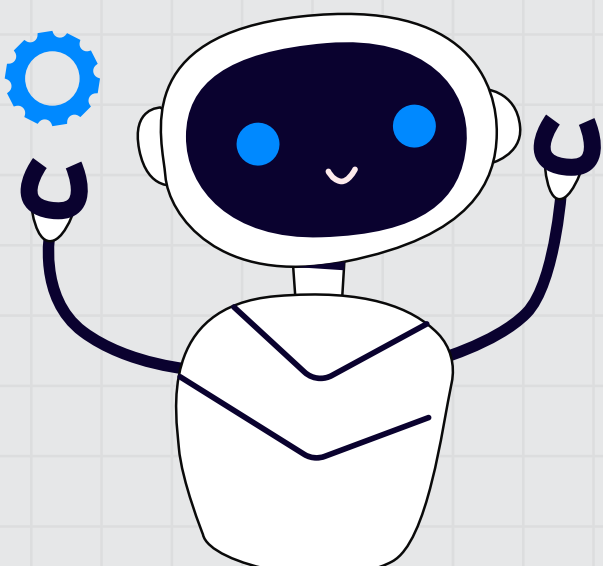
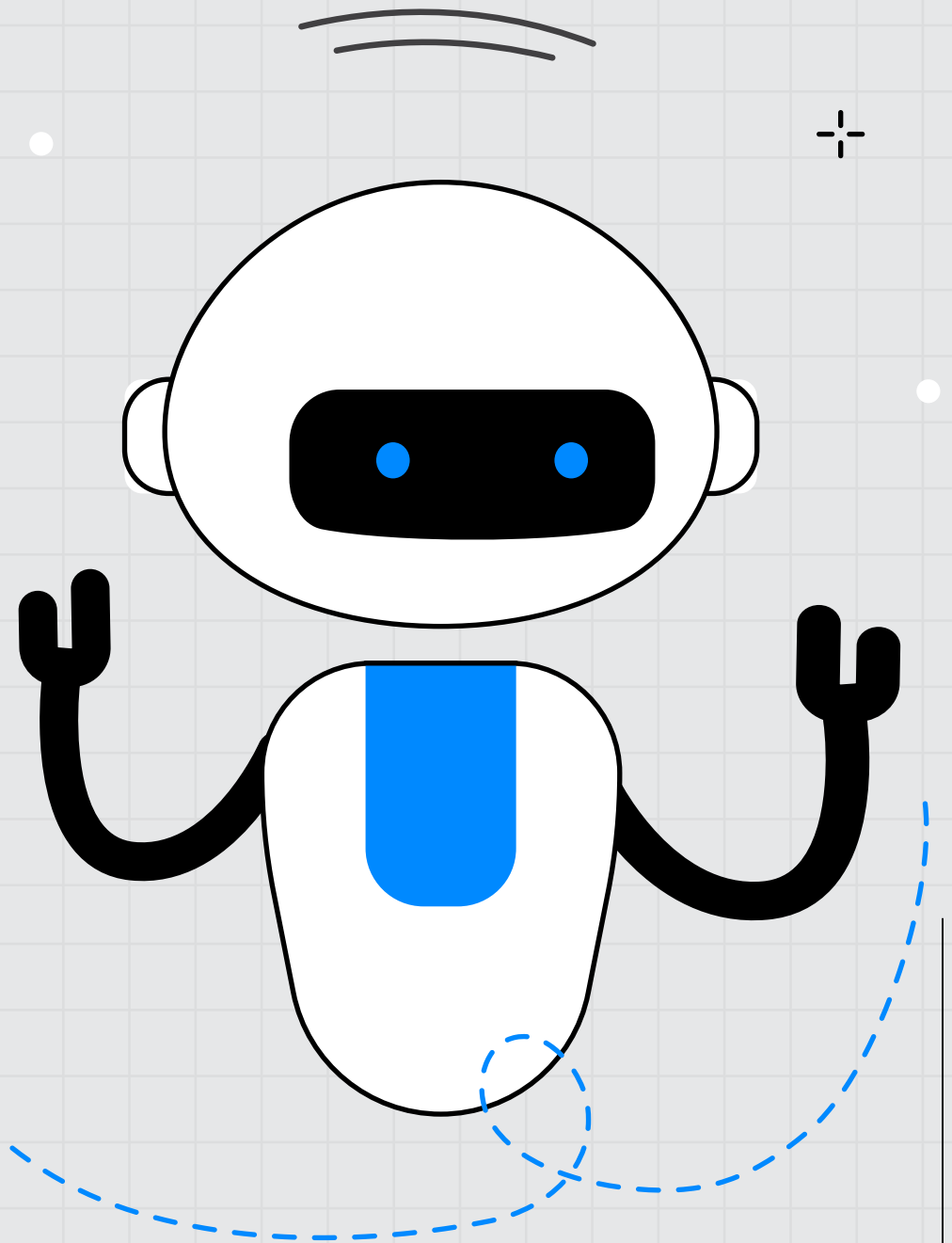
- ◆ Mid Level Certification
- ◆ Entri Course Certification
- ◆ NSDC Certification - National
- ◆ Illinois Certification - International
- ◆ Internship Certification



# AI-Powered Cybersecurity

## Learning Path

- ◆ Pre-Learning Module
- ◆ Cybersecurity & Networking Fundamentals
- ◆ Penetration Testing
- ◆ Conduct Attacks
- ◆ Web Application & Wireless Pentesting
- ◆ Cloud Pentesting
- ◆ Mobile Application Pentesting
- ◆ Reporting & Compliance
- ◆ SOC and Implementation
- ◆ Scripting
- ◆ Placement Training & Soft Skills

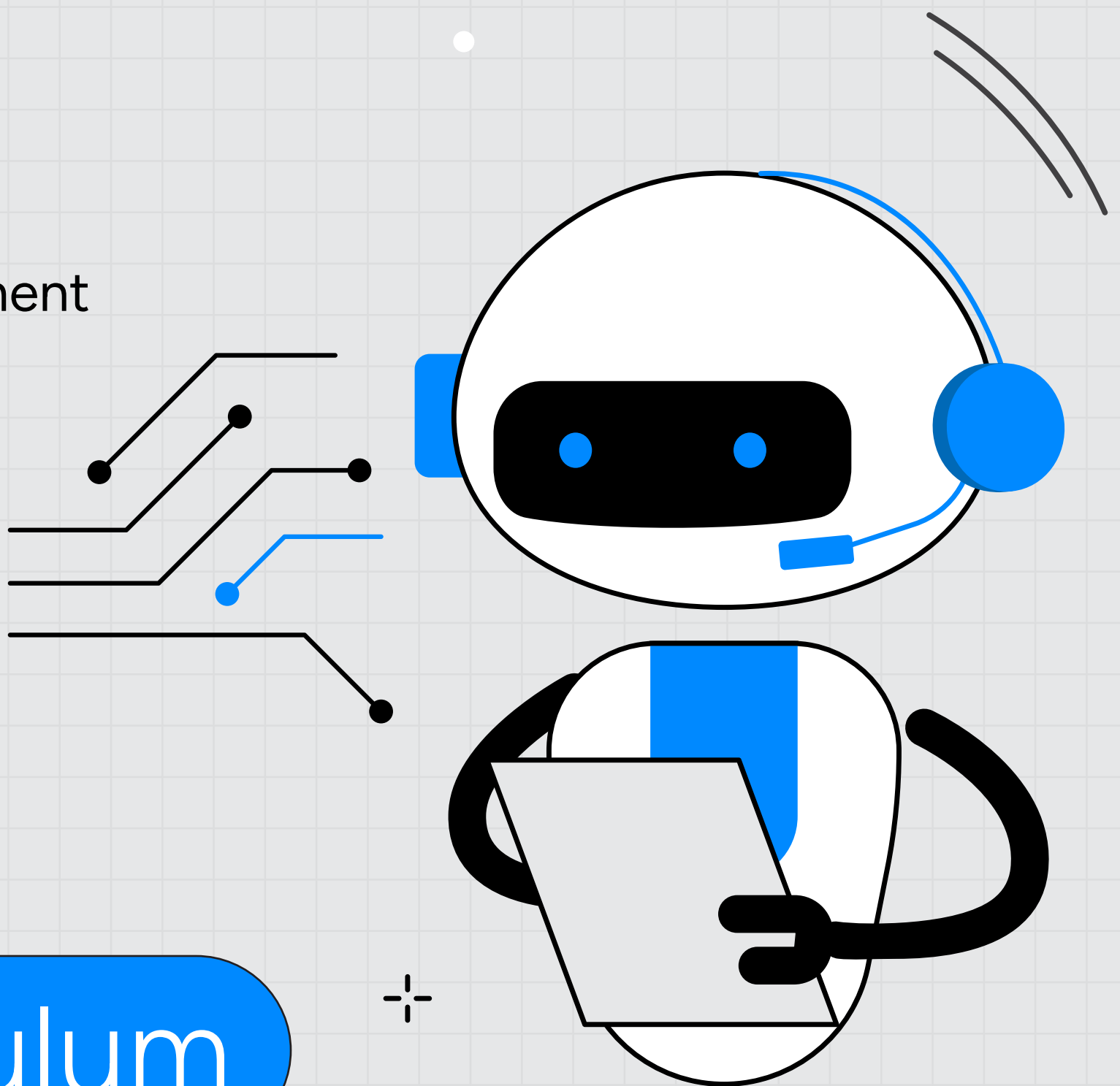






# Assessments & Tasks

- ✧ Formative Assessment
- ✧ Topic based Assignments
- ✧ Comprehensive Assessment
- ✧ Module End Assignments
- ✧ Mini Project
- ✧ Industry Internship
- ✧ Summative Assessment
- ✧ MCQ
- ✧ Coding
- ✧ Competitive Tasks



## Curriculum

### ▶ Module 1

- ▶ "Fundamentals of Cybersecurity & Information Security; The CIA Triad (Confidentiality, Integrity, Availability); Authentication, Authorization, and Accounting "
- ▶ Hacker types, Cybersecurity Domains & Career Paths; Hacking phase, Penetration testing, Penetration testing phases, types, EH

Cyber Threats & Attack Vectors (Malware, Phishing, Ransomware, etc.); Threat Intelligence Frameworks (MITRE ATT&CK, Cyber Kill Chain)

- ▶ Introduction to AI: AI, Machine learning, Deep learning
- ▶ OS: Windows: Windows commands, OS: lab configuration, LINUX: Linux file structure, commands. Security Logging & Monitoring Basics
- ▶ Networking Basics: Types of Networks, Topologies, and Devices-SWITCH(MAC,ARP); Devices: ROUTER (), FIREWALL , DNS; IP: header, addressing, subnetmask; Subnetting, DHCP; Ports, Protocols, UDP,TCP Secure Protocols(TLS, HTTPS, SSH, SFTP, DNSSEC, S/MIME, SMTPS, POP3S, and IMAPS, SNMP); OSI & TCP/IP Model (Layer-by-Layer Breakdown); Network Traffic Analysis & wireshark; VPN, NAT, PAT, VLAN, port forwarding
- ▶ Network lab configuration; Network Design: switching, routing; Algorithm(Cipher), Cipher text, Work Factor, crypt analysis, Cryptosystem
- ▶ Public Key Infrastructure (PKI), Digital Signatures & Certificates; Cryptographic Attacks (John the Ripper, Hashcat) & Mitigations; Implementing Cryptography in Real-world Scenarios  
TOR Networks, TOR browser Installation and Dark Web, Secure

- ▶ communication in dark and deep web; Anonymizing Kali linux ; Tails OS; Creating fake id ; Anonymity Using proxy, Securing using vpn

## ▶ Module 2

---

- ▶ Pentesting Methodologies: NIST,ISSAF,OWASP; Planning & Discovery(Identify purpose,Scoping,Resources,ROE,SLA) ; Information Gathering(Active, Passive, OSINT) OSINT framework
- ▶ Google Dorking, Whois,Netcraft,shodan; Nslookup,Dig,HOST , Maltego; sherlock,recon-ng; tracelab, phoneinfoga, raccoon; Anonymous and Information gathering
- ▶ Scanning: Nmap: Different type of scanning, Os detection (wireshark), Firewall evasion scanning, Script scanning. scanning with Ai; Scanning with GUI tools; Enumeration concept , Metasploitable2 machine installation; Metasploitable2: scanning, Enumeration
- ▶ TELNET , SSH ,NFS; FTP ,smb , SMTP
- ▶ Introduction to vulnerability scanning , Vulnerability scanning types , cve, CVSS, CWE(NIST); Vulnerability scanning using Nessus; Vulnerability Scanning tools, Vulnerability scanning using AI; Types:Automatic, Manual, Metasploit Framework; Sunset



(vulnhub machine) ; BruteForce Attack (Hydra)  
METASPLOITABLE2; "Machine hacking: Exploiting Port 3306  
(MYSQL) ,Apache, Blue -WINDOWS HACKING ;ICE WINDOWS  
HACKING"

- ▶ HF 2019 -machine; Basic Pentesting -machine; Reverse Shell;  
COWboy hackers-machine; Vegeta -machine
- ▶ Exploitation With AI; Active Directory Introduction,  
Kerberos-authentication; ATTACKTIVE DIRECTORY(AD  
enumeration and attack) TGT,TGS Asreproasting,DCsync  
Attack,golden ticket, silverticket, trust relationship;  
Vulnroast-kerberoasting ,BloodhoundAD, Post exploitation:  
windows: evilwinrm

### ▶ Module 3

---

- ▶ Stenography : hiding data in a file , Stenography with AI;  
Network sniffing attacks; DOS & DDOS attack; Slowloris Attack,  
LOIC & HOIC
- ▶ Social Eng, Types Of Social Engineering, Setool Kit; Social  
Engineering Attacks
- ▶ Malware , History of Malware; Malware Creation(msfvenom..) ,  
Malware attack; Malware analysis

### ▶ Module 3

---

- ▶ Stenography : hiding data in a file , Stenography with AI; Network sniffing attacks; DOS & DDOS attack; Slowloris Attack, LOIC & HOIC
- ▶ Social Eng, Types Of Social Engineering, Setool Kit; Social Engineering Attacks
- ▶ Malware , History of Malware; Malware Creation(msfvenom..) , Malware attack; Malware analysis

### ▶ Module 4

---

- ▶ Website & web application, URI, Understanding http,ssl/tls.https, WEB SERVER; Web pentesting intro: Scope and Domain,web information gathering
- ▶ Burp Suite basics(Burp Suite pro installation,usage of Burp Suite tabs and proxy configuration; Owasp top 10 THEORY, Lab setup ; Sqlinjection, xss, lfi,rfi,bruteforce, csrf
- ▶ Advanced web application testing: CSRF & SSRF; SSTI, LLM-Ai chatbot Exploitation
- ▶ Owasp juice shop SQL Injection attack PRACTICAL; Owasp juice shop SQL Broken authentication PRACTICAL; Owasp juice shop SQL XSS attack PRACTICAL

- ▶ Bug Bounty Platforms; CORS, X-FRAME,CSP; Web pentesting with AI
- ▶ Introduction API-Types of APIs (REST, SOAP, GraphQL); API Threats,API Endpoints, Api Lab Configuration; Enumerating API Endpoints Using Tools (Postman, Burp Suite),Exploiting Authentication and Authorization FlawsExploiting Injection Vulnerabilities
- ▶ CMS Exploitation Drupal,wordpress,Joomla; Real time web pentest; INTRODUCTION, WIRELESS ATTACKS; Wireless cracking, airgeddon, Evil Twin attack

## ▶ Module 5

---

- ▶ Cloud computing Intro, Service model, Deployment model; Cloud security: shared response model, cloud pentesting; Cloud services(Bucket,ec2,lambda,..); Cloud data security
- ▶ iAM ENUMERATION; S3 bucket enumeration; Azure pentest lab; Google cloud platform pentest lab

## ▶ Module 6

---

- ▶ Introduction Android,Android Architecture; Lab Setup, tools installation
- ▶ Android Pentesting, thick client v/s thin client applications
- ▶ Static analysis: Reverse Engineering; Dynamic analysis tools; Android Pentesting (DIVA)

## ▶ Module 7

---

- ▶ ISO/IEC 27001,27002
- ▶ PCI-DSS,HIPAA. GDPR, SOX, NIST Framework, IT ACTS
- ▶ Pentest Report writing

## ▶ Module 8

---

- ▶ Introduction to defensive security & Blue team, (THM); SOC fundamentals
- ▶ Deep packet inspection: Malware, Bruteforce, phishing analysis, webshell; Asset Inventory(Information Assets and Tools) ; Security Baselines,Standard Operating Procedures(SOP)
- ▶ Preparation and preventive Maintenance; Blacklisting and Whitelisting, Honeypots and Honeynets; Firewalls : LINUX,WINDOWS; IDS&IPS; Logging and Monitoring
- ▶ Patch Management , SOC2; Data leak Prevention(DLP) ; Soc team Introduction , Organization structure , SOC vs NOC
- ▶ Intro to SIEM; What is an event,incident,logs; Security orchestration,Automation and and Response (SOAR); Incident Management
- ▶ Cyber threat Intelligence(CTI) , Threat hunting; Defensive Security with AI

- ▶ SOC implementation: enterprise, forward setup, log analysis, correlation, SPL; Alert, table, dashboard creation. EDR : wazuh installation

## ▶ Module 9

---

- ▶ Bash script: intro coding; Bash script: Developing a cybersecurity tools; Powershell coding
- ▶ Python Basics; Python Cybersecurity

## ▶ Industry Internship

---

- ▶ Learn through industry projects
- ▶ Learn how to apply AI-Powered Cybersecurity concepts through this exciting Industry Internship spanning 1 Month.



## Career Support

- ✧ Benefit from Comprehensive Placement Assistance: Gain Access to Diverse Job Opportunities Across Various Industries.
- ✧ Experience Industry Mentorship: Receive Guidance from Seasoned Mentors at Leading Companies such as Tesla, Google, Samsung, and Zeta to Propel Your Career Forward.
- ✧ Resume Review Obtain specific, personalized inputs on your resume structure and content





# Placement Partners



**LOYAL**  
IT SOLUTIONS PVT LTD

**Qntash**

**euclidz.ai**

**Nav** technologies  
thought matters...

**experion**  
technologies

**DESCPRO**  
TECHNOLOGIES PVT. LTD.

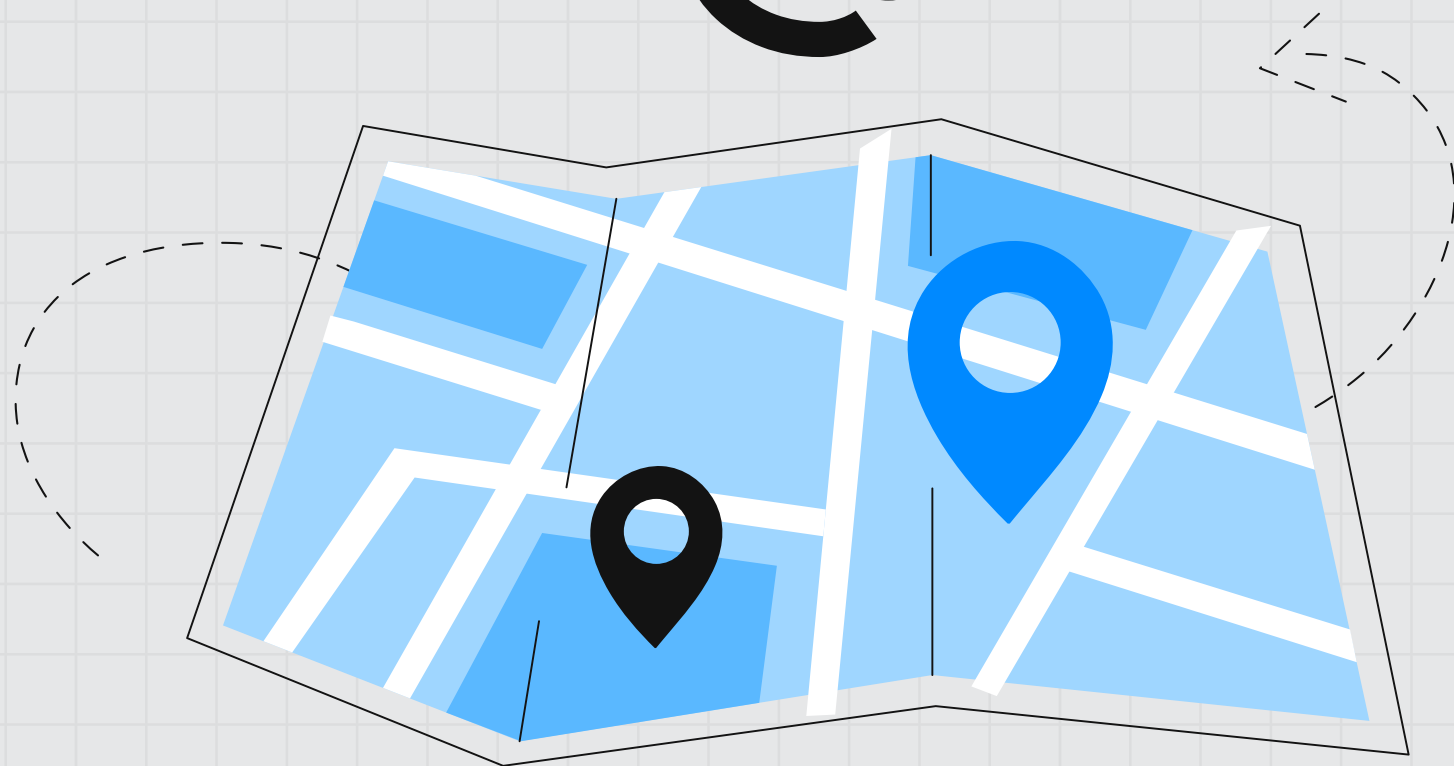


**ZENNODE**  
Technologies

**ENNEXA**  
TECHNOLOGIES



# We are located



## ***Entri HQ***

Maleppalli Road, Kakkanad, Thrikkakara, Ernakulam, Kerala - 682021

---

## ***Entri Business Development Center***

No. 32, 2nd cross, Nanjappa Reddy Layout, opp. Ganga Sagar Hotel  
Koramangala 8th Block, Koramangala. Bengaluru, Karnataka - 560095

---

D.No. 77-1, Vivekananda Rd, Ram Nagar, Coimbatore,  
Tamil Nadu - 641018

---

B-87 Defence Colony, S-4, 2nd floor, New Delhi-110024

---

## ***Entri Inc***

281 Summer St, Boston, MA, 2nd Floor, Boston, MA 02210  
United States

# THANK YOU

4.8 ★



**Download**  
the app now