careerpedia®

Hyderabad's Top 10
Startups Recognition 2024

Cybersecurity with AI Tools

Build practical security skills across networking, Linux, web security, SOC workflows, incident response, and AI-assisted analysis.

PROGRAM SNAPSHOT

4 Months Live Training	**1 Year** LMS Access	**Recorded** Sessions	**Capstone** Project	**90%** Attendance Expected	**80%** Projects Completion

PROGRAM OVERVIEW

The Cybersecurity with AI Tools program is a 4-month online live training program designed to help learners build practical understanding of cybersecurity fundamentals, networking, Linux, web security, security tools, SOC basics, SIEM, incident response, and AI-assisted security workflows. The program focuses on ethical, defensive, and lab-based cybersecurity learning.

Program Highlights

- 4 months online live training
- LMS access for 1 year with class recordings
- Assignments, case studies, and mentor feedback
- AI tools integrated into the learning workflow
- Capstone project in the final phase
- Certificate eligibility based on attendance, assignment completion, fee clearance, and policy compliance
- Cybersecurity labs and report writing
- Defensive security, SOC fundamentals, and AI-assisted security documentation

Key Skills You Will Master

- Cybersecurity fundamentals	- Networking basics
- Linux basics	- Web application security
- Vulnerability analysis	- Security monitoring
- Log analysis	- Incident response
- Security reporting	- AI-assisted threat analysis
- Security documentation	- Ethical security practice

Tools You Will Work With

Linux	**Windows security basics**	**VirtualBox/VMware**	**Kali Linux basics**
Wireshark	**Nmap**	**Burp Suite Community**	**OWASP ZAP**
Metasploit basics for lab use only	**Splunk/ELK basics**	**GitHub**	**ChatGPT**

Gemini	**Claude**	**AI-assisted log analysis tools**	**Security documentation tools**

What You Will Build

Lab Reports Document hands-on security practice.	**Traffic Analysis** Inspect and interpret network traffic.	**Incident Reports** Prepare clear incident summaries.	**Security Documentation** Create checklists and security reports.	**Capstone Portfolio** Present a defensive security project.

Learn by doing with live classes, assignments, projects, capstone work, LMS recordings, and mentor feedback.

Important Note: Careerpedia does not guarantee placements, employment, job offers, interview calls, salary outcomes, or employer selection. The program focuses on training, skill building, projects, assessments, and structured learning support.

DETAILED COURSE CURRICULUM

Cybersecurity with AI Tools

The curriculum below is structured module-wise so learners can clearly understand exactly what is covered, what tools are used, and what practical work is expected.

Module 1: Cybersecurity Foundations

This module introduces cybersecurity concepts, ethical boundaries, and defensive security thinking.

Topics Covered

- What is cybersecurity?
- Importance of cybersecurity
- Cybersecurity career paths
- CIA triad: confidentiality, integrity, availability
- Threats, vulnerabilities, and risks
- Types of cyber attacks
- Malware overview
- Phishing overview
- Social engineering basics
- Security controls
- Ethical boundaries
- Legal and responsible security learning
- Defensive vs offensive security
- Cybersecurity terminology

Practical Activities

- Cybersecurity fundamentals quiz
- Threat identification assignment
- Security awareness report

Module 2: Networking Fundamentals

This module builds networking foundations required for cybersecurity analysis and monitoring.

Topics Covered

- Computer network basics
- IP address
- MAC address
- DNS
- DHCP
- HTTP and HTTPS
- TCP and UDP
- Ports and protocols
- OSI model
- TCP/IP model
- Routers, switches, firewalls
- VPN basics
- Network traffic flow
- Common network services
- Network troubleshooting basics

Practical Activities

- Network diagram
- Protocol identification worksheet
- Port and service mapping task

Module 3: Linux and Windows Security Basics

This module introduces operating system basics used in security work.

Topics Covered

- Linux introduction

- Linux file system
- Basic Linux commands
- File permissions
- Users and groups
- Process management
- Package management basics
- Logs in Linux
- Windows security basics
- User accounts
- Password policies
- Access control
- Security settings
- Basic system hardening

Practical Activities

- Linux command assignment
- File permission practice
- Basic hardening checklist

Module 4: Cybersecurity Lab Setup and Tools

This module helps learners set up safe lab environments and become familiar with basic security tools.

Topics Covered

- Virtualization basics
- VirtualBox/VMware setup
- Kali Linux overview
- Safe lab environment
- Legal usage of security tools
- Wireshark introduction
- Nmap introduction
- OWASP ZAP introduction
- Burp Suite Community introduction
- Security documentation basics

Practical Activities

- Cyber lab setup
- Wireshark traffic capture
- Basic tool familiarization report

Module 5: Network Security and Traffic Analysis

This module teaches network observation, scanning concepts, and traffic interpretation in safe lab environments.

Topics Covered

- Network scanning concepts
- Service identification
- Vulnerability identification basics
- Wireshark packet analysis
- HTTP traffic inspection
- DNS traffic observation
- Suspicious traffic indicators
- Network security best practices
- Firewall basics
- Secure network configuration basics

Practical Activities

- Network scan report in lab environment
- Wireshark packet analysis report
- Suspicious traffic observation task

Module 6: Web Application Security

This module introduces common web application security concepts and safe lab-based vulnerability observation.

Topics Covered

- Web application architecture
- Client-side and server-side basics
- OWASP Top 10 overview
- Authentication issues
- Authorization issues
- Input validation
- SQL injection concept
- Cross-site scripting concept
- Security misconfiguration
- Sensitive data exposure
- Broken access control
- API security basics
- Secure coding awareness

Practical Activities

- OWASP Top 10 mapping
- Web security checklist
- Lab-based vulnerability observation report

Module 7: Burp Suite and OWASP ZAP Basics

This module introduces web request/response inspection and safe vulnerability documentation.

Topics Covered

- Proxy setup
- Request and response analysis
- Intercepting traffic in lab environment
- Repeater basics
- Scanner basics in safe environment
- Parameter testing basics
- Report generation
- Responsible vulnerability documentation
- False positive understanding

Practical Activities

- Web request analysis
- Lab vulnerability report
- Security testing documentation

Module 8: SOC, SIEM, and Log Analysis

This module introduces SOC workflows, SIEM thinking, and log analysis foundations.

Topics Covered

- What is SOC?
- SOC roles and workflow
- Security alerts
- Event logs
- Log sources
- SIEM introduction
- Splunk/ELK basics
- Alert investigation
- Log correlation basics
- Dashboard creation basics
- Incident ticketing basics
- Escalation process
- Reporting structure

Practical Activities

- Log analysis assignment

- SOC alert investigation
- SIEM dashboard mini-task

Module 9: Incident Response and AI for Cybersecurity

This module teaches structured incident response and how to use AI responsibly for security analysis and documentation.

Topics Covered

- Incident response lifecycle
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learned
- Evidence handling basics
- Incident report writing
- AI-assisted log summarization
- AI-assisted threat research
- AI-assisted phishing analysis
- AI-assisted security report drafting
- Risks of using AI in cybersecurity
- Data privacy while using AI tools

Practical Activities

- Incident response report
- AI-assisted log analysis
- Phishing email analysis
- Security report writing

Module 10: Capstone Project

This module helps learners apply cybersecurity concepts to a complete, safe, defensive security project.

Topics Covered

- Problem selection
- Lab setup or dataset selection
- Security observation or monitoring
- Evidence collection
- Analysis and reporting
- Recommendations and mitigation notes
- Final presentation
- Portfolio documentation

Practical Activities

- SOC alert investigation report
- Web application security assessment in a lab environment
- Phishing analysis and awareness report
- Network traffic analysis project
- Basic system hardening audit
- AI-assisted log analysis report
- Incident response simulation report

ASSESSMENTS THROUGHOUT THE PROGRAM

Networking Assessment	Linux Command Assessment	Wireshark Lab	Nmap Lab Report	Web Security Lab Report	SIEM/Log Analysis Assignment	Incident Response Report	Final Cybersecurity Capstone

CAPSTONE PROJECT EXAMPLES

SOC Alert Investigation Analyze logs and alerts and document findings.	**Web Security Assessment** Assess a lab web app and prepare a safe report.	**Phishing Email Analysis** Identify indicators and write awareness notes.	**Network Traffic Analysis** Capture and interpret network traffic.

Certificate Eligibility

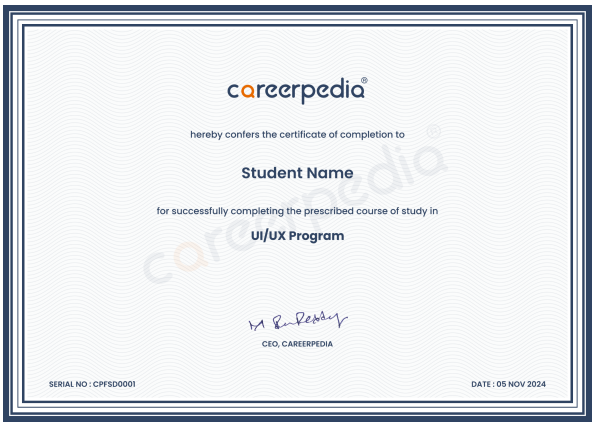
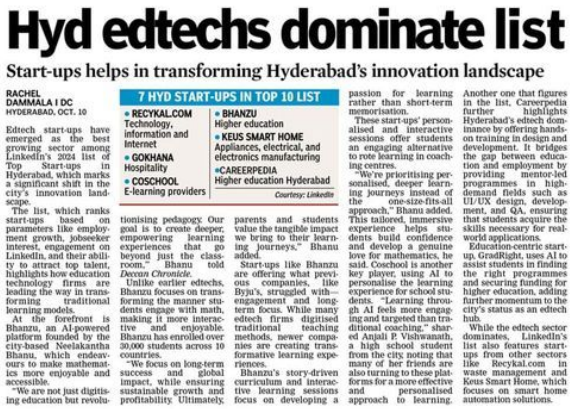
- Minimum 90% live-class attendance expected
- Minimum 80% assignment/project completion expected
- No pending course fee dues
- Compliance with LMS usage rules and program policies
- Final capstone/project submission and review, wherever applicable

OUR PARTNERS & ECOSYSTEM

t-hub · TASK · IMPACT HUB · HYSEA Hyderabad Software Enterprises Association · Qual Score

RECOGNITION, CERTIFICATE & ECOSYSTEM

The following page can be used as a credibility page in the candidate-facing brochure. It includes the sample certificate format, the startup recognition article, and the partner ecosystem references shared for Careerpedia.

Certificate Preview	News Article / Recognition
	

OUR PARTNERS & ECOSYSTEM

t-hub · TASK · IMPACT HUB · HYSEA Hyderabad Software Enterprises Association · Qual Score

Final Program Notes

- The course duration is 4 months of online live training.
- LMS access may be provided for up to 1 year for recordings, assignments, notices, and selected learning resources.
- Certificates are issued subject to attendance, assignment/project completion, fee clearance, and compliance with program rules.
- Careerpedia is an edtech and upskilling platform. It does not guarantee placement, employment, internship, interview calls, or salary outcome.