

# **CERTIFIED ARTIFICIAL INTELLIGENCE SECURITY EXPERT (L1)**



Website: [www.virtualcyberlabs.com](http://www.virtualcyberlabs.com)

Contact: +91 9324078256

Email: [support@virtualcyberlabs.com](mailto:support@virtualcyberlabs.com)

Instagram: [virtualcyberlabs](https://www.instagram.com/virtualcyberlabs)



# WHY WE ARE TOP 1%

Virtual Cyber Labs, is a leading EdTech firm in Cybersecurity, having expertise in delivering upskilling courses, sessions which are industry-oriented.

- ✓ 30+ industry ready programs
- ✓ trained 20,000+ students on cybersecurity

Enabling learners around the globe with rigorous and highly specialised cybersecurity trainings with industry mentors. In a collaborative learning environment, we are focused on implementing cybersecurity skills in fundamental stages of education.



Signed MoU with AICTE under National Education Alliance for Technology



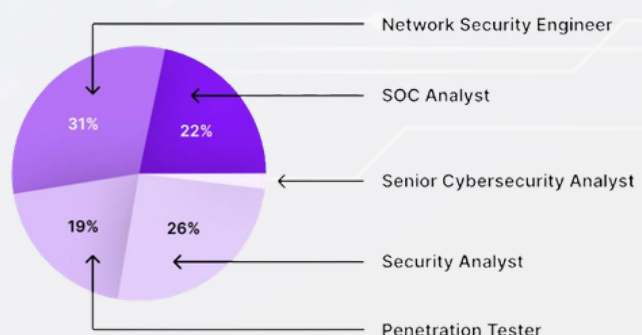
Affiliated & Approved by All India Council for Technical Education (AICTE), Government of India.

## Student report & portfolio

Our students have been placed in MNCs and are excelling in their security careers.



### Domains



# About CAISE (L1) Program

CAISE Level I by Virtual Cyber Labs is India's first hands-on certification merging **Artificial Intelligence and Cybersecurity**. It transforms learners into specialists capable of leveraging AI to detect, defend, and automate security operations. From red teaming and forensics to SOC automation and GRC compliance, CAISE is your gateway to the next era of cyber intelligence.

20+ Hours of  
Practical AI  
Hacks

30+ tools and  
custom scripts

VAPT, SOC and  
GRC using AI

Exclusive AI  
Integrations  
coverage

## You'll Learn To

- ✓ Integrate AI into red and blue team operations
- ✓ Automate reconnaissance, detection, and response workflows
- ✓ Secure AI pipelines, APIs, and autonomous systems
- ✓ Use machine learning for threat intelligence and anomaly detection
- ✓ Design AI-driven compliance frameworks
- ✓ Governance, Ethics & Real-World Labs

## Careers in AI & Machine Learning

**2.9 million**

jobs globally (2025)

**4 out of 5**

companies use AI

**\$985 billion**

global market value

**Up to \$137K**

global avg salary

### Careers in AI & ML

Here are the ideal job roles in AI sought after by companies in India

- AI Security Engineers
- Secure MLOps Engineer
- Big Data Engineer
- Machine Learning engineer
- Cybersecurity Analyst
- AI Threat Researcher
- Autonomous AI Security Consultant
- GenAI developer
- AI Governance Specialist



# MODULES

## TOPICS AS PER EACH MODULE

- **Module 1: Foundations of AI Security**

- Introduction to Model Context Protocols
- MCP Architecture and Security: Design principles
- JSON RPC communication Protocols
- Security considerations in MCP deployments
- Machine-to-Machine security orchestration

- **Module 2: Autonomous Red Teaming with AI**

- Red teaming frameworks and adversarial simulation
- Automated reconnaissance and scanning with AI
- Web application exploitation using AI-driven techniques
- Dynamic payload generation using ML
- Ethical and regulatory compliance
- External Reconnaissance and Asset Discovery

- **Module 3: AI Powered OSINT & Threat Intelligence**

- AI-powered social media and open-source monitoring
- Dark web intelligence gathering with AI
- Geospatial and attribution analysis
- Automated IOC extraction from unstructured data
- Multi-source threat intelligence correlation using AI
- AI for deception detection and disinformation analysis

# MODULES

## TOPICS AS PER EACH MODULE

- **Module 4: Mobile and Application Security Automation**
  - Mobile application threat landscape
  - AI Assisted reverse engineering and classification
  - Static and Dynamic Apk Analysis Automation
  - Comprehensive mobile security testing pipelines
  - AI Powered API and Endpoint Testing
- **Module 5: Network Forensics Intelligence**
  - Network forensics fundamentals and evidence handling
  - AI-assisted packet analysis and anomaly detection
  - Automated timeline reconstruction of incidents
  - Traffic classification using machine learning
  - AI attribution analysis in network forensics
  - Legal considerations for AI-generated forensic evidence
- **Module 6: Intelligent SOC Automation**
  - Blue team fundamentals and defensive strategies
  - MITRE ATT&CK integration with MCP
  - AI-enhanced alert triage and prioritization
  - Automation of detection and response workflows
  - RAG-powered threat intelligence - semantic search
  - Real time Threat Monitoring with AI Powered IDS

# MODULES

## TOPICS AS PER EACH MODULE

- Dual-agent architecture - Initial Triage vs Threat Hunting
- Dual-agent architectures for investigation and hunting
- End-to-end SOC automation and decision-making

- **Module 7: AI Powered Governance, Risk, and Compliance**

- Challenges in compliance and audit processes
- AI solutions for policy monitoring and evidence collection
- Automated assessment for regulatory frameworks (GDPR, DORA, SOC 2, etc.)
- Policy-as-code frameworks for real-time compliance
- Executive dashboarding and AI-driven reporting
- Security and governance considerations in AI GRC
- Building explainable AI systems for regulatory trust

- **Module 8: Securing AI & MCP Deployments**

- Security-first architecture principles
- Common vulnerabilities in AI/MCP systems
- Authentication, authorization, and access control in MCP
- Logging, monitoring, and auditing best practices
- TLS, key rotation, and secure credential management
- Incident response planning for MCP environments



## CONTACT US

[support@virtualcyberlabs.com](mailto:support@virtualcyberlabs.com)

+91 9324078256

[www.virtualcyberlabs.com](http://www.virtualcyberlabs.com)