(AISSP)

AI Security Professional(AISSP)

Training and Certification

Cyber Security Educational Courses Professional Sessions

ABOUT US

We offer Cyber Security and Information Security training and Certification in Delhi for Cyber Security and Information Technology aspirants. Since Decade, we have been in the Information Technology and Cybersecurity industry. You can learn more about cybersecurity, Techniques, and Tools to choose a better career path.

DESCRIPTION

AI Security Professional Certification (AISSP) is a specialized cybersecurity training program designed to help professionals secure AI systems, Large Language Models (LLMs), and intelligent applications against modern cyber threats. It focuses on AI security testing, prompt injection prevention, adversarial attacks, model protection, governance, and secure AI deployment while enabling learners to identify vulnerabilities, strengthen AI infrastructures, and build resilient AI-driven environments for enterprise and real-world applications.

Duration - 40Hrs

Language - Hindi & English

Mode - Online & Offline

BENEFITS

1. Basic to Advanced Courses
2. Interview Cracking and Proposal-Making Sessions
3. Transparent Syllabus
4. Career-Oriented Courses and Certifications
5. International Accreditation




CRAW ACADEMY

SAKET ADDRESS

1st Floor, Plot no. 4, Lane no. 2,
Kehar Singh Estate, Westend Marg,
Behind Saket Metro Station,
Saidulajab New Delhi - 110030

LAXMI NAGAR ADDRESS

R31/ 32, 2nd floor Jandu Tower,
Vikas marg, Shakarpur,
New Delhi -110092

www.craw.in

+91 951 380 5401

(AISSP)

AI Security Professional(AISSP)

Training and Certification

Cyber Security Educational Courses Professional Sessions

AI SECURITY PROFESSIONAL(AISSP) COURSE MODULE

Module 1: AI Attack Foundations

- Core AI cybersecurity concepts & attack surfaces
- MITRE ATLAS & OWASP LLM Top 10
- Red team lifecycle: Scoping, methodology, and risk classification

Module 2: Reconnaissance & Threat Modeling

- AI-focused OSINT: Identifying APIs & data pipelines
- Model fingerprinting & inference probing
- Mapping trust boundaries and attack paths

Module 3: Prompt Injection & LLM Attacks

- Direct & indirect prompt injection exploitation
- Jailbreaking techniques (PAIR, TAP, GCG)
- System prompt extraction & sensitive data leakage

Module 4: Agentic AI & Multi-Agent Attacks

- Attacking autonomous agents: Memory & tool abuse
- Multi-agent trust exploitation & impersonation
- Denial-of-wallet & resource abuse attacks

Module 5: Adversarial ML & Model Privacy

- Adversarial inputs (FGSM, PGD) on images & NLP
- Model extraction & inversion attacks
- Embedding inversion to recover sensitive data

Module 6: Data Poisoning & RAG Attacks

- Training data poisoning & backdoor insertion
- RAG pipeline exploitation & retrieval manipulation
- Supply chain attacks on datasets and weights

Module 7: Infrastructure & Tool Surface Attacks

- Exploiting cloud AI platforms & model servers
- MCP & tool integration abuse for privilege escalation
- NL2SQL injection & RCE in ML pipelines (MLflow)

Module 8: Hardening, IR & Capstone

- AI security hardening: Guardrails, sandboxing, monitoring
- AI incident response & forensics
- Capstone: Full-spectrum red team engagement

CRAW SECURITY

LEARN | RESEARCH | INNOVATE

SAKET ADDRESS

1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station, Saidulajab New Delhi - 110030

LAXMI NAGAR ADDRESS

R31/ 32, 2nd floor Jandu Tower, Vikas marg, Shakarpur, New Delhi -110092

www.craw.in

+91 951 380 5401

@crawsec