SISA

certin
Enhancing Cyber Security in India

CERTIFIED SECURITY PROFESSIONAL IN ARTIFICIAL INTELLIGENCE PROGRAM - CSPAI

Did You Know?

The AI market size is expected to reach USD 60.24 billion by 2029, growing at a CAGR of 19.02% during this period.

As organizations increasingly integrate AI solutions, this increase in spend will lead to pronounced challenges.

77%
Companies faced AI breaches last year.

89%
Express concerns over security vulnerabilities linked to third-party AI integration.

US$ 3.5 Trillion
Cost of a potential major cyberattack to the global economy.

US$ 12 Billion
Losses in the financial sector over the past 20 years with over 20,000 cyberattacks.

THE KEY TO BALANCING AI INNOVATION AND SECURITY?

A TRAINED WORKFORCE IS YOUR BEST DEFENSE.

CSPAI: The solution to secure AI innovation

The Certified Security Professional in Artificial Intelligence (CSPAI) program is the answer to empowering security professionals with the knowledge they need. CSPAI is tailored to educate on the integration of AI and ML in organizations, highlighting potential vulnerabilities and providing strategies to mitigate risks. With CSPAI, organizations can foster innovation while maintaining robust security frameworks, ensuring that AI is implemented securely and compliantly, without compromising on safety or regulatory standards.

Comprehensive AI Security Program

A comprehensive, structured program that combines both theoretical knowledge and practical skills specific to cybersecurity in AI contexts.

Actionable Insights on Emerging Threats

A program designed to address the latest threats and regulations, providing participants with up-to-date, actionable insights.

Global Security Framework Alignment

Emphasizes adherence to global security frameworks like ISO and NIST, ensuring your AI applications meet international security standards.

Advanced Risk Management Skills

Develop advanced risk management capabilities to identify and mitigate AI-related vulnerabilities effectively.

Combat Sophisticated AI Threats

Gain insights into defending against sophisticated cyber threats specifically targeting AI models.

Up-to-date Global AI Compliance

The certification ensures adherence to the latest AI regulations and global compliance laws, maintaining the integrity and security of your AI applications.

Continuous Learning & Certification Maintenance

Our curriculum is regularly updated to reflect the latest AI advancements and threats, with a three-year recertification ensuring professionals stay current with new developments and best practices.

Hands-On Learning Experience

The workshop features practical exercises and case studies, allowing participants to apply concepts in real-world scenarios, enhancing both understanding and retention.

Why CSPAI with SISA Institute?

ANAB Accreditation

Achieve certification from the world's first ANAB-accredited certification program for AI security, ensuring the highest standards of quality and credibility.

Access to Industry Veterans

Gain access to a pool of experts with over 20 years of experience in cybersecurity, guiding your AI integration.

Collaboration with CERT-IN

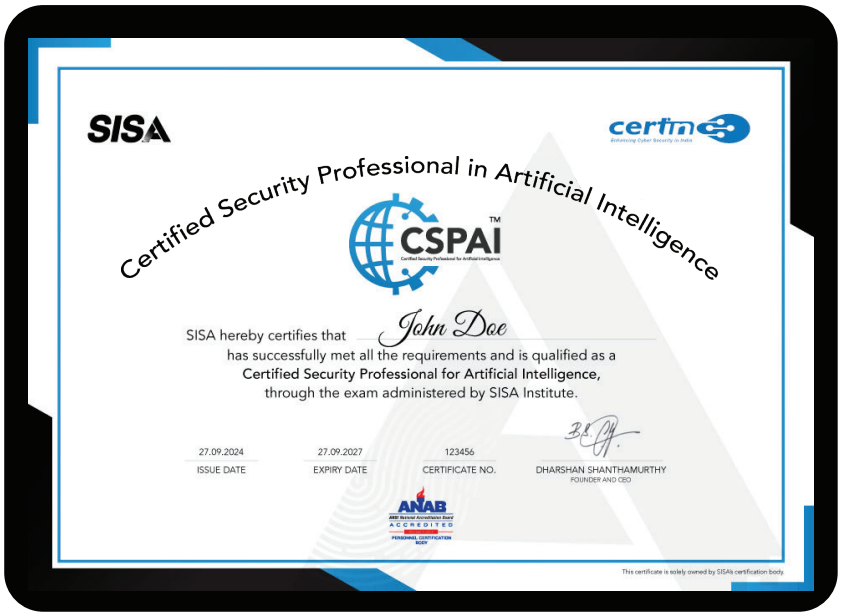
Benefit from a strategic partnership with a leading industry body, ensuring your organization stays aligned with national AI security standards.

Alumni Portal Access

Connect with a global network of AI security professionals through an exclusive alumni portal, fostering knowledge sharing and collaboration.

ANAB-accredited CSPAI Certificate

A SISA & Cert-In Collaboration



(A Sample Certificate for Illustration Purpose)

About ANAB

ANAB (ANSI National Accreditation Board) is a member of the International Laboratory Accreditation Cooperation (ILAC) and the International Accreditation Forum (IAF) and has signed the ILAC and IAF multilateral recognition agreements. The ANSI/ISO/IEC Standard 17024 accreditation holds international relevance as it is a global standard. The ANAB accreditation ensures that the CSPAI certification program was designed and will be maintained to stringent criteria for existing and future certification holders.

Curriculum of CSPAI

Topic 1 Evolution of AI

1.1 Evolution of AI

1.2 Concepts of AI

1.4 List of all GenAI

1.3 What is Generative AI

Topic 2 Concepts Behind Developing GenAI

2.1 Concepts behind developing a GenAI LLM model (covering the entire transformer model)

2.2 Various deployments of LLM's in live production

Topic 3 Concepts Behind Training of LLM Models

3.1 Training of LLM models

3.2 Fine-tuning of LLM models

3.4 Measures to be taken for developing Responsible AI

3.3 Basic concepts behind every AI standard and Regulation – Responsible AI

Topic 4 LLM Usage Within the Application

4.1 In-detail review and scenarios on how LLM's are incorporated into applications

4.2 In-detail review on how ML's are incorporated into applications

Topic 5 Future of AI/ML

5.1 Expected evolution of AI / ML

5.2 New upcoming concepts in AI / ML

5.3 Anticipated changes to business and applications

Topic 6 LLM Vulnerabilities and Exploits

6.1 Detailed in-depth review of various LLM vulnerabilities and exploits

6.2 OWASP Top 10 LLM vulnerabilities

6.3 Mitre ATLAS

Topic 7 Usage of GenAI in BAU Security Functions/Teams

7.1 Various scenarios on how GenAI can be used in the day-to-day functions of various security teams

7.2 How to use AI to fight intruders using AI

Topic 8 AI Risk Assessment, AI Regulations, and Overview of ISO Standards Covering Cybersecurity for AI

8.1 Detailed overview on how to do AI risk assessment covering multiple standards and regulations

8.2 In-depth dive into various AI regulations, especially EU AI Act

8.3 Overview on the various ISO standards covering cybersecurity for AI, and how to go about implementing the same

About SISA

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry. As a Global Payment Forensic Investigator of the PCI Security Standards Council, we leverage forensics insights into preventive, detective, and corrective security solutions, protecting 1,000+ organizations across 40+ countries from evolving cyberthreats. Our suite of solutions from AI-driven compliance, advanced security testing, agentic detection/ response and learner focused-training has been honored with prestigious awards, including from Financial Express, DSCI-NASSCOM and The Economic Times. With commitment to innovation, and pioneering advancements in Quantum Security, Hardware Security, and Cybersecurity for AI, SISA is shaping the future of cybersecurity through cutting-edge forensics research.

Compliance

Payment Data Security
- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance
- SWIFT

Strategy and Risk
- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security
- HITRUST

Unified Audits

Managed Compliance

Security Testing

Application Security
- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Security Testing
- Secure Code Review

Network Security
- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Firewall Rule Review
- PCI ASV Scan

Phishing Simulation

Red Teaming Exercise
- Layer Security Testing

Cyber Defense

Managed Extended Detection and Response Solution - SISA ProACT
- 24x7 Monitoring
- UEBA
- Threat Intel
- Advanced Threat Hunting
- Breach & Attack Simulation
- SOAR
- Use-case Factory

Digital Forensics and Incident Response
- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- PCI Forensic Investigation (PCI)
- Internal Forensic Investigation (IFI)
- Ransomware Simulation

Data Protection & Governance

Data Discovery and Classification
- PCI/PII/PHI Data Discovery
- Data Classification in Endpoint (Windows, Linux)
- Data Classification in O365, Metadata
- Dynamic Masking, Redact, Truncation
- Integration to DRM, DLP, SIEM

Data Privacy Professional Services
- Assessments (Unified Privacy Maturity, DPIA, 3rd Party Risk)
- Data Inventory, Mapping and Process flow, RoPA
- Data Privacy Framework - Policy, Notice, SoPs
- Consent and Notice Management framework
- Data Breach and Management
- Principal management
- Privacy by Design implementation guide
- Define Data Retention Guidelines and processes
- Technical/Organization measures
- Privacy Training/Awareness

Trainings & Certifications

Payment Data Security Training and ANSI Accredited Certification
- CPISI (2 Day Program
- CPISI (3 Day Program)
- CPISI- Advanced (3 Day Program)
- CPISI-D (Developers)
- CPISI Hybrid (4 Weeks)

Certification Program in Cybersecurity for AI – CSPAI
- CSPAI

Forensic Briefing Sessions for Senior Management

Leading Tech Security

AI PRISM
- AI PRISM LLM Vulnerability Scanner Solution
- AI Risk Management and Governance Solution Framework
- AI Compliance and Governance Consulting Service

Hardware and IoT Security Testing
- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing
- MPOC/ PCI PTS

Quantum Security
- Quantum Cryptographic Consulting
- Quantum Security Risk Assessment
- Quantum Security Standards Compliance

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia

To learn more about SISA's offerings visit us at **www.sisainfosec.com** or
Contact your SISA sales representative at **contact@sisainfosec.com**