



Certified  
AI Security  
Specialist



# The Future Of Security With Certified AI Security Specialist (CAISS)

Certified AI Security Specialist (CAISS) Workshop shapes experts to lead the future of security by mastering AI-driven defense against evolving cyber threats.

[REGISTER NOW](#)



[WEBSITE](#)

BATCH 1

ASIA & MIDDLE EAST


 19<sup>th</sup> FEB – 22<sup>nd</sup> FEB, 2024

 6:00 am – 10:00 am GMT

BATCH 2

AMERICA & EUROPE

 26<sup>th</sup> FEB – 29<sup>th</sup> FEB, 2024

 3:00 pm – 7:00 pm GMT

16 Hours of Live Interactive Training  
(4 Days 4 Hours)

COURSE FEE:

\$ 130 REGULAR  
PARTICIPANTS

\$ 100 ISACA &  
ISC2 MEMBER

In partnership with





# Introduction of AI Security:

The Certified AI Security Specialist (CAISS) training is a cutting-edge program designed to bridge the gap between cybersecurity and the revolutionary world of Artificial Intelligence. This comprehensive training equips professionals with the skills and knowledge to navigate the evolving landscape of security, combining the power of AI with robust cybersecurity practices. The thoroughness of this training guarantees that experts can not only comprehend the complexity of security in the AI era, but also handle them with skill. Through the integration of artificial intelligence (AI) and strong cybersecurity protocols, CAISS enables people to remain ahead of the constantly evolving field of digital security. The objective is to produce experts who can protect against new risks and weaknesses while utilizing AI to its fullest.





# Why attend CAISS?



1

## STAY RELEVANT

In a rapidly changing digital landscape, staying updated on the latest security trends is crucial.

2

## PRACTICAL LEARNING

Hands-on workshops and real-world case studies ensure practical application of AI in cybersecurity.

3

## NETWORKING OPPURTUNITIES

Connect with industry experts and peers to exchange insights and best practices.

4

## CAREER ADVANCEMENT

Earn a prestigious certification that demonstrates your expertise in the intersection of AI and cybersecurity.



# What to Expect?

## COMPREHENSIVE CURRICULUM

Covering AI fundamentals, practical applications, and future trends.

## INTERACTIVE WORKSHOPS

Engage in hands-on sessions to implement AI in cybersecurity scenarios.

## REAL-WORLD INSIGHTS

Learn from successful AI integration case studies and industry experts.

## CERTIFICATION EXAM

Validate your skills with a recognized certification in AI Security.



# Key Topics Covered

1. AI Basics and Business Applications

---

2. AI in Vulnerability Assessment and Penetration Testing

---

3. Governance, Risk, and Compliance with AI

---

4. Managed Detection and Response (MDR) with AI

---

5. Building a Secure AI Environment

---

6. Threat Intelligence and Threat Hunting with AI

---

7. Privacy Impact Assessment (PIA) with AI

---

# Table Of Contents:



## Day 1. Introduction to AI in Business & Security

### Session 1: Understanding AI Basics

- Overview of Artificial Intelligence
- Machine Learning vs. Traditional Programming
- Types of Machine Learning: Supervised, Unsupervised, Reinforcement Learning
- Common AI Terminology

### Session 2: Applications of AI in Business

- AI in Business Processes
- Automation and Efficiency Gains
- Case Studies: Successful AI Implementations in Business

### Session 3: AI and Cybersecurity Landscape

- The Intersection of AI and Cybersecurity
- Current Challenges in Cybersecurity
- Role of AI in Enhancing Cybersecurity

### Session 4: Regulatory and Ethical Considerations

- AI and Privacy Regulations
- Ethical Use of AI in Security
- Responsible AI Practices

## Day 2. AI Integration in Cybersecurity Domains

### Session 5: Vulnerability Assessment & Pen Testing (VAPT) with AI

- Overview of VAPT
- How AI Enhances VAPT
- Hands-on: AI-driven VAPT tools and techniques

### Session 6: Governance, Risk, and Compliance (GRC) with AI

- Importance of GRC in Cybersecurity
- AI for Risk Assessment and Compliance
- Data Protection Impact Assessment (DPIA) with AI
- Real-world GRC use cases with AI

### Session 7: AI in Managed Detection and Response (MDR)

- Introduction to MDR
- Leveraging AI for Threat Detection
- Incident Response with AI



# Table Of Contents:



## Day 3. AI in Security Operations Center (SOC)

### Session 8: Building a Secure AI Environment

- Securing AI Systems
- Adversarial Attacks on AI
- Best Practices for Secure AI Implementation

### Session 9: AI for Threat Intelligence

- Threat Intelligence Basics
- Role of AI in Threat Intelligence
- Threat Hunting with AI

### Session 10: AI in Security Analytics

- Log Analysis and Security Analytics
- Using AI for Anomaly Detection
- Case Studies on AI-driven Security Analytics

## Day 4. Practical Implementation & Future Trends

### Session 11: Real-world Case Studies

- Examining Successful AI Integration in Cybersecurity
- Learning from Failures: Challenges and Solutions
- Industry Trends and Emerging Technologies

### Session 12: AI Threats, Risks, and Privacy Considerations

- Assessing Risks in AI Applications
- Privacy Impact Assessment (PIA) with AI
- Addressing AI-specific Threats and Risks

### Session 13: Future Trends in AI and Cybersecurity

- Advances in AI for Cybersecurity
- The Role of AI in Shaping the Future of Security
- Preparing for Tomorrow's Threats

### Session 14: Q&A and Certification

- Open Floor for Questions and Discussions
- Certification Exam for AI in Cybersecurity



## Prajwal Gowda

VP Delivery and Trainings

CISA, CISM, PCI QSA, PCI P2PE QSA,  
PCI 3DS QSA, SWIFT CSP, PCI TSP, ISO  
27001 LA, ISO 27001 LI, CPISI – S  
Master Trainer

Prajwal Gowda, a seasoned cybersecurity professional with 10+ years' expertise, specializes in AI Security and safeguarding organizations from evolving threats. As Chief Technology Officer (CTO) at Ampcus Cyber, he draws on a rich background as a Business Unit Head, excelling in Compliance and Testing services. His proficiency spans PCI, ISO 27001, Software Security Framework, ISMS, Risk Analysis, and more, reflecting a comprehensive grasp of the cybersecurity landscape. Prajwal is a Master Trainer, having conducted 100+ cybersecurity and AI Security sessions globally, training over 1000 professionals.



## Deep Chanda

Chief Officer

CISA, CISM, PCI QSA, CAISP,  
CASE, CPISI

Deep Chanda, is an industry veteran with 20+ years of experience in the cybersecurity space. Deep is currently the Chief Officer of Ampcus Cyber, where he specializes in assisting clients in improving their security posture against emerging threats. He directs the company's technological strategy, He leads the company's technology strategy, drives innovation in cybersecurity solutions, and envisions a secure digital future for organizations. Deep is a well-respected trainer and speaker who is well-versed in the necessity of AI security and the scrutiny that surrounds this growing technology.

[REGISTER NOW](#)

