



Setting the Gold  
Standard in Cyber  
Expertise



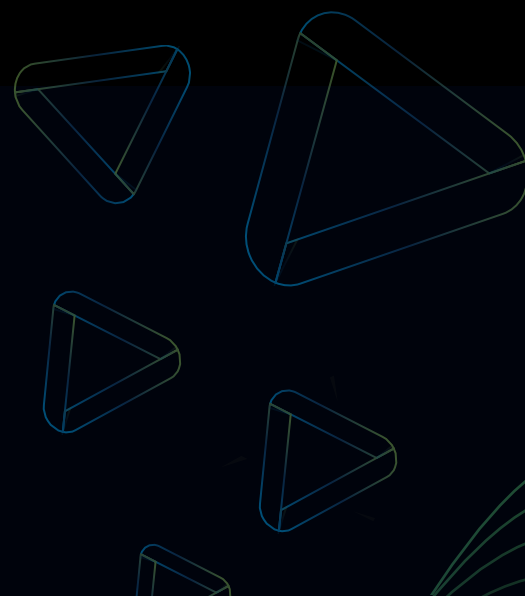
# ARTIFICIAL INTELLIGENCE **Security Expert**

EXAMINATION **OUTLINE**



**Certified Artificial Intelligence  
Security Expert**

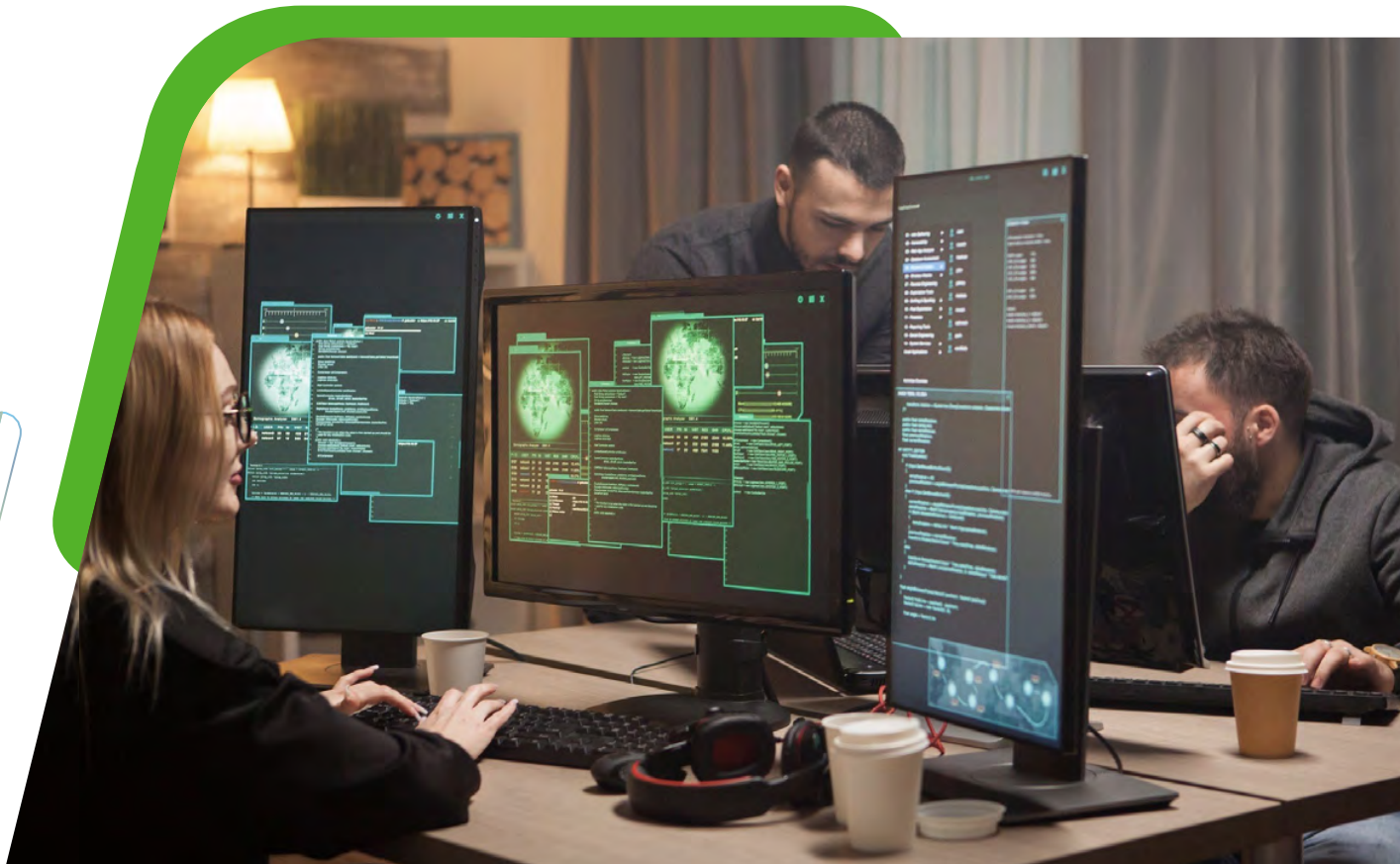
An IAISP Certification



## Certified Artificial Intelligence Security Expert (CAISE) Course Outline

### Introduction

The Certified Artificial Intelligence Security Expert (CAISE) certification is designed to bestow professionals with in-depth knowledge and proficiency in the complex intersection of artificial intelligence and information security. Through a systematically designed curriculum, candidates are prepared to excel in AI security.



## Domains and Weightages



The certification covers five core domains, each with its respective weightage, aiming to provide a comprehensive understanding of the subject. The domains and their weightages are as follows:



**1. Fundamentals of Cybersecurity and AI - 20%**

---



**2. AI for Threat Detection and Analysis - 30%**

---



**3. AI in Security Operations and Incident Response - 25%**

---



**4. Secure AI Development and Deployment - 15%**

---



**5. Ethical and Legal Aspects of AI Security - 10%**



## Detailed Examination Outline

Each domain encompasses specific learning lines, essential to grasp the intricate facets of AI security.



### 1. Fundamentals of Cybersecurity and AI - 20%

- Gain an overview of cybersecurity principles and practices, forming the foundation of secure AI landscapes.
- Explore the introduction to artificial intelligence and its dynamic applications within the realm of security.



### 2. AI for Threat Detection and Analysis

- Develop an in-depth understanding of leveraging AI for the detection and analysis of security threats.
- Acquire the skills needed for implementing AI-driven threat intelligence solutions that enhance risk assessment.





### 3. AI in Security Operations and Incident Response

- Seamlessly integrate AI technologies into security operations for heightened vigilance.
- Harness the power of AI for efficient incident detection, rigorous investigation, and swift response.



### 4. Secure AI Development and Deployment

- Explore best practices for the development of secure AI systems, ensuring resilience against evolving threats.
- Learn to safely deploy AI models within production environments, safeguarding their effectiveness and integrity.



### 5. Ethical and Legal Aspects of AI Security

- Navigate the ethical considerations intrinsic to AI security, emphasizing integrity and accountability.
- Comply with the complex web of legal and regulatory frameworks governing the ethical use of AI.

## Table Summary

Domain	Weightage	Learning Lines
Fundamentals of Cybersecurity and AI	20%	Overview of cybersecurity principles and practices. Introduction to AI and its security applications.
AI for Threat Detection and Analysis	30%	Understanding AI for threat detection and analysis. Implementing AI-driven threat intelligence solutions.
AI in Security Operations and Incident Response	25%	Integration of AI in security operations. Utilizing AI for incident detection, investigation, and response.
Secure AI Development & Deployment	15%	Best practices for developing secure AI systems. Safe deployment of AI models in production.
Ethical and Legal Aspects of AI Security	10%	Addressing ethical considerations in AI security. Compliance with legal and regulatory frameworks.

## Conclusion

The CAISE certification aids professionals in mastering the vast and dynamic realm of AI security. With a detailed examination of each domain, candidates are equipped to navigate and protect the digital world effectively.