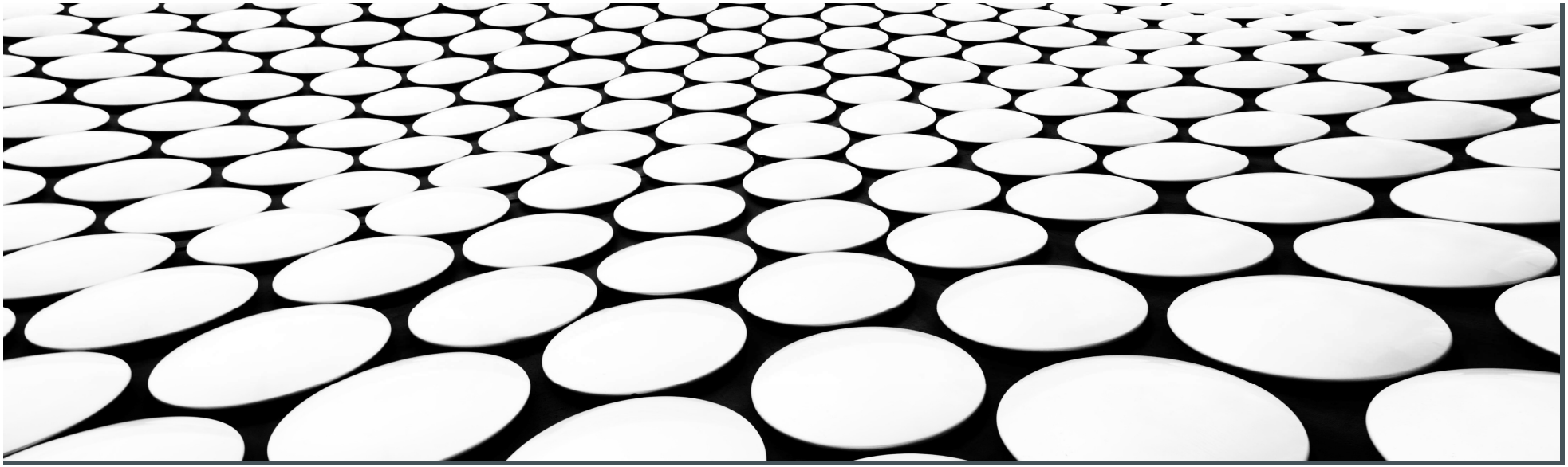
CERTIFIED AI SECURITY FUNDAMENTALS™ (CAISF™)



COURSE INSTRUCTORS

- Charles Alexi
  - Senior Consultant and Instructor
  - Charlesalexi@tonex.com
- Kevin Krautwald
  - Senior Consultant and Instructor
  - kkrautwald@tonex.com
- George Jackson
  - Senior Consultant and Instructor
  - gjackson@tonex.com

CERTIFIED AI SECURITY FUNDAMENTALS™ (CAISF™)

- The Certified AI Security Fundamentals™ (CAISF™) Certification Course by Tonex provides comprehensive training in the critical domain of AI security. This program equips participants with essential knowledge and skills to safeguard AI systems and data against evolving cyber threats.

- Tonex's Certified AI Security Fundamentals™ certification course is designed for IT professionals and cybersecurity specialists to understand and apply AI security principles. It covers risk assessment, secure development practices, resilience strategies, compliance, and real-world case studies, ensuring data confidentiality and resilience.

LEARNING OBJECTIVES

- Understand the fundamentals of AI security.
- Identify and mitigate potential risks in AI applications.
- Implement secure AI development practices.
- Gain proficiency in assessing and enhancing AI system resilience.
- Learn best practices for securing AI models and data.
- Acquire knowledge on compliance and regulatory considerations in AI security.

AUDIENCE

The Certified AI Security Fundamentals™ (CAISF™) certification is designed for individuals who work in roles related to artificial intelligence (AI) security, including:

- **AI Developers**: Those who develop AI systems or algorithms need to ensure that their creations are secure and resilient against potential attacks.
- **AI Engineers**: Professionals responsible for designing and implementing AI solutions should understand the security implications of their work to mitigate risks effectively.
- **Cybersecurity Professionals**: Individuals working in cybersecurity roles may need specialized knowledge and skills to secure AI systems and data against cyber threats.
- **Data Scientists**: Data scientists who work with AI technologies should be aware of security best practices to protect sensitive data and ensure the integrity of AI models.
- **Ethical AI Practitioners**: Professionals involved in ethical AI practices need to consider security as an essential aspect of responsible AI development and deployment.
- **Compliance Officers**: Compliance officers ensure that AI systems adhere to relevant regulations and standards, including security requirements.
- **Risk Managers**: Professionals responsible for managing risks within organizations should understand the security risks associated with AI technologies and how to mitigate them effectively.

COURSE STRUCTURE (PARTS)

Day 1

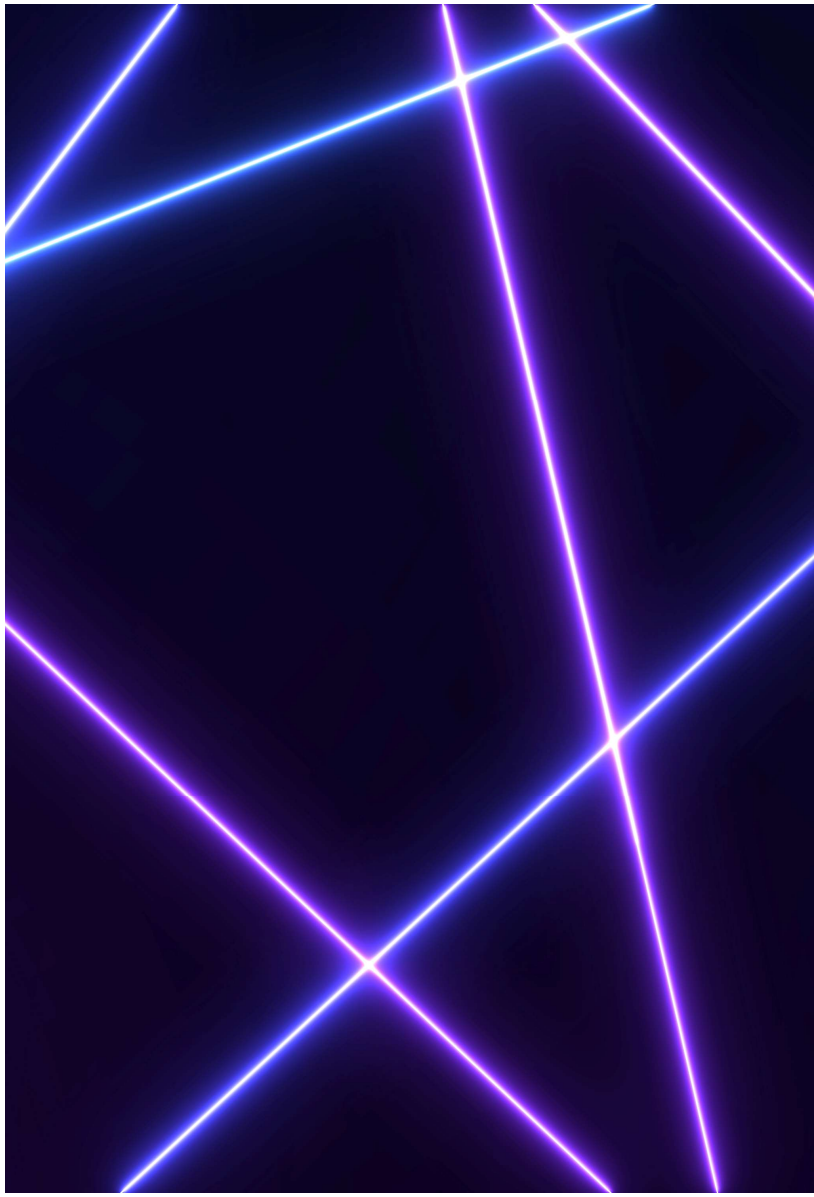
- Part 1: Introduction
- Part 2: Main Modules:
  - Module 1: Introduction to AI Security
  - Module 2: Risk Assessment in AI
  - Module 3: Secure AI Development Practices
  - Module 4: Resilience in AI Systems
  - Module 5: Securing AI Models and Data
  - Module 6: Compliance and Regulatory Considerations

Day 2

- Other Key Topics and Workshops:
  - Part 3: Security, threat modeling, frameworks and Mitigating Risks in AI and LLM/GenAI
  - Part 4: More on Threat Modeling Frameworks
  - Part 5: workshops, Hands-on Practical Exercises

ABOUT THE EXAM

- Exam Domains
  - AI Security Basics: Introduction to AI concepts and their security implications.
  - Data Privacy and Protection: Key practices in securing data used in AI systems.
  - Threat Models in AI: Understanding potential threats specific to AI and machine learning models.
  - Secure AI Development Lifecycle: Best practices in developing, testing, and deploying secure AI applications.
  - Ethical and Compliance Issues: Overview of ethical concerns and compliance with regulations relevant to AI security.
- Number of Questions
  - Total No of Questions: 40 questions.
  - Question Database 240 Questions
- Type of Questions
  - Multiple-Choice Questions (MCQs): These would assess understanding of theoretical knowledge and practical application.
  - True/False Questions: To quickly verify understanding of basic AI security principles.



ADDITIONAL EXAM DETAILS

- Exam Duration
  - Duration: 90 minutes.
- A passing score might be set at around 65% to ensure a basic yet solid understanding of AI security fundamentals.
- The exam could be offered online for accessibility to a global audience.
- This proposed certification exam aims to equip professionals with the foundational knowledge necessary to contribute to the security aspects of AI projects and initiatives, ensuring they understand the unique challenges and solutions in the field of AI security.

WORKSHOP 1: OBJECTIVE AND DETAILED EXPLANATION

- **Objective:** To apply the knowledge gained in the sessions by conducting threat modeling on hypothetical AI/ML systems. This involves identifying potential security threats and vulnerabilities within these systems. **Duration:** 1 hour
- Steps:

1. Introduction to the Hypothetical Business Scenario:
    1. Present a business scenario where a platform connects consumers with repair contractors for home services, such as plumbing, electrical work, HVAC maintenance etc..
2. Importance of Threat Modeling:
    1. **Identifying Security Risks:** Explain that threat modeling is crucial for pinpointing security threats and vulnerabilities within AI/ML systems, particularly those that utilize large language models (LLMs) and generative AI (GENAI) technologies.
    2. **Mitigating Risks:** Emphasize how threat modeling helps in developing strategies to mitigate these risks, ensuring the platform remains secure and reliable.
    3. **Enhancing Security Posture:** Discuss how regular threat modeling can improve the overall security posture of the platform, making it resilient against potential cyberattacks.

- Detailed Steps for the Session:

1. Objective Clarification:
    1. The goal is to apply theoretical knowledge to a practical scenario, enhancing understanding through hands-on threat modeling.
2. Hypothetical Business Scenario:
    1. Introduce a fictitious platform that matches consumers with home repair contractors.
    2. The platform uses AI/ML to optimize matching, schedule appointments, and manage communications.
3. Threat Modeling Process:
    1. **System Overview:** Begin with an overview of the AI/ML system architecture, including data flow, key components, and user interactions.
    2. **Threat Identification:** Identify potential security threats, such as data breaches, unauthorized access, and adversarial attacks on AI models.
    3. **Vulnerability Analysis:** Analyze vulnerabilities within the system, focusing on areas where LLM and GENAI technologies are implemented.
    4. **Risk Assessment:** Assess the potential impact and likelihood of identified threats, prioritizing them based on severity.
    5. **Mitigation Strategies:** Develop strategies to mitigate identified risks, such as implementing stronger authentication, encrypting sensitive data, and conducting regular security audits.

WORKSHOP 1: CONCLUSION AND DISCUSSION:

1. Summarize the key findings from the threat modeling exercise.

2. Discuss the importance of ongoing threat modeling and risk management in maintaining a secure AI/ML platform.

QUESTION AND ANSWER