Certified AI-SECURITY PROFESSIONAL 2025

Empowering Cyber Security with AI-Driven Intelligence

5-7 November 2025 | Parkroyal Collection Hotel Kuala Lumpur

As the capabilities of AI continue to advance, so too do the potential risks, posing significant threats to data integrity, system security, and decision-making processes. Defend against AI-driven threats with Encipher's CAISP, the premier certification for experienced IT professionals to master AI security. You will learn how to protect your enterprise from the rapidly evolving risks posed by AI and ensure responsible, secure AI adoption across the organization.

With CAISP's hands-on, real-world training, you will become a leading authority on AI-driven threat detection, mitigation, and prevention strategies in modern cloud environments, preparing organizations to stay ahead in an evolving threat landscape.

Abhinav Mishra is an Application Security Researcher with over 13 years of experience in penetration testing across web, mobile, and infrastructure. He is the founder of ENCIPHERS, where he leads offensive security projects, including penetration testing, red teaming, and specialized training programs. Abhinav has trained security professionals globally on web, mobile, infrastructure, and AI-driven application hacking, bringing real-world insights and hands-on experience to his sessions.

Why You Should Attend #CAISP2025 Workshop:

- **Become The Master:** Learn how to use AI-powered threat detection, automated vulnerability discovery & cyber defence strategies
- **State-Of-The-Art Training Lab:** Gain hands-on experience with our state-of-the-art training lab environment
- **Certified Expertise:** Earn a prestigious certification that validates your expertise and positions you as a top-tier professional in AI-Security

Certification For Future-Ready Security Teams:

The CAISP program delivers an advanced, real-world training experience that blends insights, real-world case studies & hand-on labs. Participants will gain a robust skill set essential for harnessing AI for offensive & defensive cybersecurity

Exclusively by:

THOMVELL international

Supporting Partner:

ENCIPHERS

Overview :

Cybersecurity is moving fast, and AI is changing the game. That is why we created the Certified AI-Security Professional (CAISP) program. It's not just another training - it's a hands-on, real-world experience that helps your team use AI to detect threats faster, automate defenses, and even uncover vulnerabilities before attackers do. Whether it is securing your code, testing your AI apps, or strengthening your red/blue teams - we help your people become future-ready. Participants will leave with practical, job-ready AI-cybersecurity skills that can be applied immediately in offensive, defensive, and secure development roles.

Moreover, the best part? Everything we teach is practical, privacy-focused, and built for real environments, not just theory.

Upon Completing CAISP - You Will Be Able To:

- Deploy and manage self-hosted LLMs (eg: LLaMA) for secure, private AI applications
- Use AI tools for Threat detection and hunting, Anomaly detection and log analysis & Automated vulnerability discovery
- Perform AI-assisted offensive operations, including: Reconnaissance | Payload generation | Fuzzing and exploit customization
- Prompt engineering for malicious inputs
- Conduct AI Red Teaming, including: Prompt injection and LLM jailbreaking | Exploiting flaws in AI-powered applications (e.g., chatbots, code assistants) | Enhance secure development workflows using AI-assisted secure coding
- Gain competitive edge with practical, technical-ready AI-cybersecurity skills that can be applied immediately in offensive, defensive, and secure development roles.

This training covers everything from setting up a locally hosted, privacy-friendly LLM to leveraging its full potential for AI-driven cybersecurity applications. You'll learn how to use a self-hosted LLM for:

- **Threat Hunting with AI** - Using ML models to detect anomalies and uncover hidden threats.
- **Automated Secure Coding with AI** - AI-assisted real-time secure coding suggestions.
- **AI-Assisted Exploitation** - Using LLMs for automated reconnaissance, payload generation and exploit customization.