Practical DevSecOps AI Security Training Program Surpasses 1,000 Certified Professionals, Addressing Critical Skills Gap

Milestone for Flagship AI Security Certification Underscores Urgent Demand for Skills in AI Red Teaming and Combating LLM Threats

SAN FRANCISCO, CA, UNITED STATES, October 22, 2025 /EINPresswire.com/ -- Practical DevSecOps today announced a significant milestone in AI security training, having now trained over 1,000 professionals through its flagship AI security certification, the Certified AI Security Professional (CAISP) program. This achievement addresses the urgent need to secure artificial intelligence systems against emerging threats.

This achievement comes at a critical juncture as organizations grapple with a new class of vulnerabilities inherent to AI and machine learning models. Threats such as prompt injection, data poisoning, and model inversion attacks are evolving faster than traditional security defenses, creating an urgent demand for professionals with specialized expertise derived from practical AI security courses.

"When we launched Certified AI Security Professional (CAISP), we anticipated the growing importance of AI security, but the pace at which it has become a critical business imperative has been remarkable," said Mohammed A. Imran, CEO at Practical DevSecOps. "Training 1,000 professionals is not merely a number; it represents a growing cohort of defenders equipped with the practical skills needed to identify and mitigate threats that most conventional security tools are not designed to address."

Traditional cybersecurity training curricula have not kept pace with the rapid evolution of AI, leaving a significant skills gap. The Certified AI Security Professional (CAISP) program is specifically designed to bridge this divide by addressing core challenges unique to the AI domain, including:

- AI Red Teaming and Defending techniques, including the OWASP Top 10 for Large Language Models (LLMs).
- Threat Modeling AI Specific Systems and Models.
- Applying security frameworks like MITRE ATLAS.
- Understanding and mitigating AI Supply Chain Attacks.
- Securing the AI development and deployment pipeline (MLOps).

- Navigating complex governance and compliance frameworks, including the NIST AI RMF and the EU AI Act.

Check out the complete curriculum here. https://www.practical-devsecops.com/certified-ai-security-professional/

The Certified AI Security Professional (CAISP) program distinguishes itself with a curriculum where approximately 70% of the training is conducted in hands-on laboratory environments. Participants engage directly with AI systems, executing attacks and implementing defenses in real-world scenarios.

Validation of skills is conducted through a rigorous 6-hour practical examination consisting of five unique challenges. The exam is entirely performance-based, requiring candidates to demonstrate their applied knowledge without the use of multiple-choice questions.

"The difficulty of the exam is a direct reflection of the complexity of the threats our graduates will face," a company spokesperson noted. "A certification's value is tied to its rigor. This program's hands-on validation of attacking and defending AI systems provides the high standard expected from a specialized AI Security Certification, and we are committed to upholding that standard to signify true competence."

As one of the industry's leading AI security courses, the certification program provides participants with a comprehensive learning package, including:

- 60-Day Lab Access: Flexible, on-demand access to practical, browser-based labs.
- 40+ practical labs: break things, fix them, learn what actually happens in the field
- Dedicated Support: 24/7 support via a dedicated chat channel.
- Hands-on Examination: 6-hour task-oriented examination to validate your learning.

The rapid integration of AI systems into business operations has outpaced the development of corresponding security protocols. Many organizations rely on third-party models and libraries that may contain vulnerabilities or lack sufficient security controls. Certified AI Security Professional (CAISP)-certified professionals are trained to identify these risks and implement robust security measures, preventing incidents that could otherwise go undetected by traditional monitoring systems.

About Practical DevSecOps
Practical DevSecOps (part of Hysn Technologies Inc.) runs vendor-neutral, hands-on security certifications. Besides AI security, they offer courses in DevSecOps, cloud-native security, container security, threat modeling, API security, and software supply chain security.
Their certifications require passing practical exams that run anywhere from 6 to 24 hours—no multiple choice tests here. The company's training is used by security professionals at organizations worldwide.

Learn more about the Certified AI Security Professional course or enroll today.
https://www.practical-devsecops.com/certified-ai-security-professional/

Raja Shekar
Practical DevSecOps
+1 415-684-1697
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
