# With 88% of Orgs. Hit by AI Agent Security Incidents, Practical DevSecOps Launches Certification to Close the Skills Gap

*The Certified Agentic AI Security Expert (CAASE) trains defenders to secure AI agents that act on real systems with real credentials*



Certified Agentic AI Security Expert (CAASE)

SAN FRANCISCO, CA, UNITED STATES, October 1, 2026 /EINPresswire.com/ -- AI agents have moved from pilots to production faster than security teams can keep up. Nearly nine in ten organizations confirmed or suspected an AI agent security incident in the past year, according to Gravitee's State of AI Agent Security 2026 Report, a survey of 750 executives. In healthcare, the figure reached 92.7%.

To help close that gap, Practical DevSecOps today launched the Certified Agentic AI Security Expert (CAASE), a hands-on certification that teaches security professionals to attack and defend AI agents end-to-end. Pre-booking is open now.

Unlike a chatbot, an agent plans, remembers, calls tools, runs code, and hands tasks to other agents. Each of those abilities opens a path that standard threat models and trust diagrams were not built to see. CAASE is designed around those paths.

Across seven chapters, learners practice both sides of the fight. They hijack an agent's goal mid-task and learn to detect it. They poison long-term memory and RAG sources, then harden against it.

They escape a coding agent's workspace, spoof agent-to-agent messages and exploit confused-

deputy chains, then apply container sandboxing, scoped delegation tokens and skill vetting to shut those routes down. The course closes with threat modeling in MITRE ATLAS, AI agent bills of materials and mapping controls to the NIST AI RMF and EU AI Act, plus security for the A2A, ACP and UCP agent protocols.

The training is roughly 70% hands-on. Learners get 60 days of browser-based lab access, more than 30 guided exercises, and 24/7 instructor support. Certification requires passing a six-hour practical exam of five challenges with a score of 80% or higher.

The skills are in demand. According to Infosec. QA's 2026 salary data, specialists who add agentic red-teaming or multi-agent security skills earn 20–30% more than standard AI security pay.

CAASE is aimed at AI and agentic security architects, application and information security engineers, applied AI security engineers, and penetration testers. Participants need basic Linux skills; scripting experience helps, and the Certified AI Security Professional (CAISP) course is recommended first.

CAASE is available now at practical-devsecops.com. Organizations can train teams through the enterprise program, and certification bundles save a minimum of USD 270.

About Practical DevSecOps
Practical DevSecOps, a Hysn Technologies Inc. company, offers vendor-neutral, practical, and hands-on training and certification programs for IT and security professionals. The company's curriculum focuses on modern areas of information security, including DevOps Security, AI Security, MCP Security, Agentic AI Security, Cloud-Native Security, API Security, Container Security, Threat Modeling, and Software Supply Chain Security. Certifications from Practical DevSecOps are achieved after rigorous, skill-based exams ranging from 06 to 24 hours and are considered among the most valuable in the information security field.

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

This press release can be viewed online at: https://www.einpresswire.com/article/946639634

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.