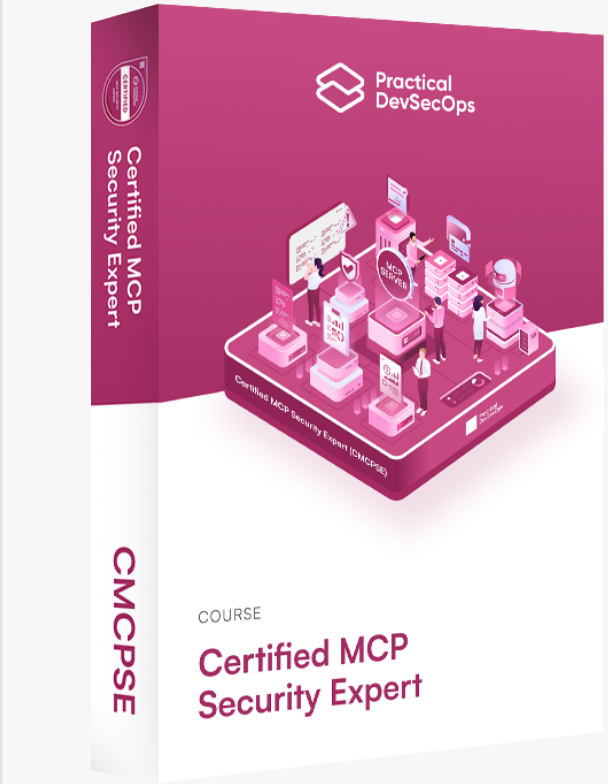
Practical DevSecOps Launches Certified MCP Security Expert (CMCPSE), First Dedicated Hands-On MCP Security Certification

Certified MCP Security Expert (CMCPSE), the first-of-its-kind credential built for security professionals attacking and defending MCP infrastructure.



Attack, assess, & harden MCP servers: tool poisoning, prompt injection, supply chain security, & agentic AI defenses.

SAN FRANCISCO, CA, UNITED STATES, June 15, 2026 /EINPresswire.com/ -- The 10th program in the Practical DevSecOps certification portfolio, Certified MCP Security Expert (CMCPSE), is the first credential built specifically for security professionals attacking and defending MCP infrastructure.

Practical DevSecOps, a global cybersecurity certification and training organization, today launched the Certified MCP Security Expert (CMCPSE). It is a hands-on practitioner certification for security professionals who need to attack, audit, and defend Model Context Protocol (MCP) implementations.

Certified MCP Security Expert (CMCPSE) is the 10th certification in the Practical DevSecOps portfolio. It extends the company's existing AI security training track, which includes the Certified AI Security Professional (CAISP), into the MCP threat surface.

MCP was introduced by Anthropic in late 2024 and has since been adopted by OpenAI, Google, Microsoft, and Block. It is now the dominant protocol for connecting AI agents to external tools, databases, APIs, and production systems. With adoption came risk. Between January and February 2026, researchers filed over 30 CVEs against MCP servers, clients, and tooling. In September 2025, the first confirmed malicious MCP package operated undetected for two weeks while exfiltrating email data. In May 2026, the NSA published a dedicated advisory on MCP security design considerations.

MCP attacks do not behave like conventional vulnerabilities. They operate at the semantic layer, through tool poisoning, prompt injection, rug pulls, and supply chain compromise. Signature-based detection misses them entirely. Existing AI governance frameworks like NIST AI RMF and ISO/IEC 42001 do not yet cover MCP-specific threats in detail.

Every major training platform has responded to MCP's rise with developer-focused courses. All of them teach developers how to ship servers faster. None of them trains security professionals to break and defend them. Certified MCP Security Expert (CMCPSE) fills that gap.

The program is built for security engineers, AppSec leads, red teamers, and platform engineers deploying or evaluating AI agent infrastructure. It covers:

1. MCP threat modeling and attack surface analysis
2. OWASP MCP Top 10, the first industry-standard framework for classifying MCP risks
3. Tool poisoning detection and prompt injection defense
4. Authentication and authorization patterns, including OAuth 2.1
5. MCP gateway architecture and sandboxing
6. Supply chain security for MCP servers and packages
7. Secure MCP server build practices
8. Hands-on adversarial labs against live MCP server environments

The certification includes 60 days of lab access, 30+ hands-on exercises, and a 6-hour practical exam. All labs run in-browser against live MCP server environments with no local setup required.

"MCP is now the connective tissue of enterprise AI. It touches databases, source code, cloud APIs, and production systems. The CVEs are real. Government agencies have issued formal guidance. Security teams need a credential built for this threat, not borrowed from adjacent domains. Certified MCP Security Expert (CMCPSE) is that credential." -- Mohammed A. Imran, CEO, Practical DevSecOps

The Certified MCP Security Expert (CMCPSE) is available starting June 15, 2026, at $599. The course is self-paced with on-demand access. Learners can enroll now and begin on their own schedule.

Enroll at: www.practical-devsecops.com/certified-mcp-security-expert/

About Practical DevSecOps
Practical DevSecOps (a Hysn Technologies Inc. company) is a global cybersecurity certification and training organization. Its 10 practitioner certifications are trusted by security teams at enterprises, including Roche, Accenture, IBM, PwC, and Booz Allen Hamilton. The company's programs cover DevSecOps, AI security, cloud-native security, application security, and threat modeling.

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