>> IT Security

Hacking: AI/KI-Security & AI-Augmented Pentesting

EGOS! the education company

Angriffe auf Netzwerke stellen eine ernstzunehmende Bedrohung für IT Netzwerke und damit das ganze Unternehmen dar. Systemadministratoren können ein Netzwerk nur mit fundierten Kenntnissen des "Hacking" sinnvoll schützen.

Ihr Nutzen

KI ist gleichzeitig Werkzeug und Angriffsfläche. Dieser Tag zeigt (1) wie Pentester KI verantwortungsvoll zur Beschleunigung von Recon, Triage und Reporting nutzen und (2) wie KI-Systeme über Eingaben, Daten und Integrationen kompromittiert oder fehlgesteuert werden können – inklusive Hardening und Re-Tests.

Voraussetzungen

TCP/IP-Basics, Windows-/Linux-Admin-Grundlagen

Preis pro Teilnehmer

EUR 950,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Hinweise

Version: N/A

Seminarinhalte

* Wie Pentester KI nutzen
- Scan-/Log-Outputs strukturieren
- Priorisierung
- Hypothesenbildung
- Testfall-Generierung
- Reporting-Qualität erhöhen
- Grenzen: Halluzinationen/Nachweisbarkeit/Datenschutz

* Wie KI ‚gehackt' wird (AI Threat Model)
- Prompt-/Context-Manipulation
- RAG-/Knowledge-Base-Poisoning
- Datenabfluss
- Tool-/Plugin-Missbrauch

* Labs
- ‚AI Assistant'-Lab: Prompt-/Context-Angriff ? Risiko-Nachweis ? Hardening ? Re-Test
- ‚RAG'-Lab: manipulierte Wissensquelle ? falsche Security-Empfehlung ? Governance/Fix
- Action-Safety: Least Privilege + Approval Gate als Designkontrolle

* Tools
- Kali + Webproxy (für Request/Response)
- einfache AI-Lab-Komponenten (lokal/isoliert)
- Logging/Policy-Checks

* Output
- AI Threat Model (kurz)
- Control-Liste (Hardening)
- Testfälle für wiederkehrende AI-Sicherheitsaudits
- Mini-Report