FLORIAN RICHTER

AI SECURITY ENGINEER

CONTACT

florian.richter@email.de

+49 160 28495031

Bonn

linkedin.com/in/florianrichter

KENNTNISSE

- Red Teaming
- Prompt Injection
- Threat Modeling
- OWASP Top 10 for LLM
- MITRE ATLAS
- Guardrails
- EU AI Act
- ISO 27001
- Penetrationstests
- Python

AUSBILDUNG

Master of Science IT-Sicherheit

10/2016 - 09/2018

Ruhr-Universität Bochum

Bochum

Netze und Systeme

Bachelor of Science Informatik

10/2013 - 09/2016

Hochschule Bonn-Rhein-Sieg

Sankt Augustin

Informatik

SPRACHEN

Deutsch	Muttersprache
Englisch	C1

PROFIL

AI Security Engineer mit 8 Jahren Erfahrung in der IT-Sicherheit, davon 3 Jahre mit Schwerpunkt auf der Absicherung von KI- und LLM-Anwendungen. Red Teaming gegen Prompt Injection und Datenabfluss, Threat Modeling nach OWASP Top 10 for LLM und Umsetzung von Anforderungen aus EU AI Act und ISO 27001.

BERUFSERFAHRUNG

AI Security Engineer

09/2023 - heute

Rheinische Sicherheitsberatung GmbH — Bonn

- Red Teaming von **22** LLM-Anwendungen, über 140 Schwachstellen dokumentiert und mit Entwicklern behoben
- Threat Modeling für RAG- und Agenten-Systeme nach OWASP Top 10 for LLM und MITRE ATLAS
- Guardrails gegen Prompt Injection und Datenabfluss, Erfolgsquote von Angriffen im Test von 31 % auf 4 %
- Sicherheitsanforderungen nach EU AI Act und ISO 27001 in 5 Kundenprojekten umgesetzt

Penetrationstester

04/2020 - 08/2023

Siebengebirge Cyber Defense GmbH — Königswinter

- Penetrationstests von Webanwendungen und APIs, rund 35 Projekte pro Jahr
- Automatisierung von Scans mit Python, Prüfdauer je Projekt um 20 % verkürzt
- Erste Bewertungen von ML-Modellen gegen Model Extraction und Adversarial Examples

IT-Sicherheitsanalyst

10/2018 - 03/2020

Kommunale Datenzentrale Rhein-Sieg — Siegburg

- Auswertung von SIEM-Alarmen im Security Operations Center für 40 Kommunen
- Schwachstellenmanagement für 2.500 Systeme mit monatlichem Bericht an die Leitung
- Mitarbeit an der Notfallplanung nach BSI IT-Grundschutz

ZERTIFIKATE

Offensive Security Certified Professional (OSCP)

06/2021

OffSec

ISO/IEC 27001 Lead Implementer

02/2024

PECB