Stefan AppSec-DevSecOps-Aichinger

Senior Cyber Security Analyst / Tech Lead Detection

stefan.aichinger@example.de +49 69 5544 6677 Frankfurt am Main, Deutschland aichinger-cysec.dev

linkedin.com/in/stefan-aichinger-cysec github.com/aichinger-cysec

PROFIL

Senior Cyber Security Analyst mit M.Sc. IT-Sicherheit (RUB HGI Bochum, Note 1,3) und 8 Jahren SOC-Erfahrung bei Deutsche Bank Cyber Frankfurt und Munich Re Cyber. CISSP + GIAC GCIH + GCDA + GPEN + ISO 27001 Lead Auditor zertifiziert, Tech-Lead von 6 L2-Analysten und Owner von 38 Detection-Use-Cases nach MITRE ATT+CK. MTTD von 12 auf 3 Minuten reduziert, BAIT- und DORA-Audits 2024 + 2025 ohne Major Findings. Speaker auf Heise IT-Security 2024 + Troopers 2025.

BERUFSERFAHRUNG

Senior Cyber Security Analyst / Tech Lead Detection

10/2022 - heute

Deutsche Bank AG Cyber Defense Center — Frankfurt am Main, Deutschland

Tech-Lead von 6 L2-Analysten im 38-koepfigen Cyber Defense Center fuer 12 Konzerneinheiten in 28 Laendern

- Owner von 38 Detection-Use-Cases nach MITRE ATT+CK mit Detection-as-Code in GitLab und CI/CD-Test-Pipeline
- MTTD von 12 auf 3 Minuten und MTTR von 1,5 h auf 18 Minuten in 24 Monaten reduziert durch SOAR und Hunting
- Incident-Lead fuer 38 Major-Incidents (S1/S2) inkl. 4 Ransomware-Vorfaelle mit BaFin- und BSI-Meldung
- BAIT- und DORA-Audit 2024 + 2025 ohne Major Findings im Detection-Bereich, 124 Kontrollen dokumentiert
- Mentoring von 6 L2-Analysten mit 5 Beforderungen zu L3 / Detection Engineer in 24 Monaten
- Speaker auf Heise IT-Security Frankfurt 2024 und Troopers Heidelberg 2025

Cyber Security Analyst L2/L3

10/2018 - 09/2022

Munich Re Cyber / Munich Re Group — Muenchen, Deutschland

L2/L3-Analyst im 22-koepfigen Munich-Re Cyber Operations Center (BaFin- und VAIT-reguliert)

- Lead-Analyst fuer 24 Detection-Use-Cases mit Schwerpunkt auf APT-Aktoren (APT29, APT41, Lazarus)
- Aufbau eines SOAR-Stacks mit 48 Cortex-XSOAR-Playbooks, MTTR-Reduktion von 4 h auf 38 Minuten
- Co-Lead von 3 VAIT-Audits + 1 Solvency-II-Audit ohne Major Findings, 96 Kontrollen dokumentiert
- Pflege eines internen Threat-Intel-Streams mit MISP + OpenCTI + Mandiant Advantage, 4.800 IOCs pro Monat

Junior Cyber Security Analyst L1/L2

10/2016 - 09/2018

T-Systems International GmbH — Bonn, Deutschland

L1/L2-Analyst im Telekom-Cyber-Defense-Center fuer Bundesbehoerden

- Triage von durchschnittlich 124 SIEM-Alerts pro Schicht in IBM QRadar mit MITRE-ATT+CK-Mapping
- Aufbau von 18 Suricata-IDS-Regeln und 38 KQL-Hunting-Queries fuer Microsoft 365 Defender
- Eskalation und Dokumentation von 84 Incidents nach BSI-Grundschutz 200-2 + BSI 200-4

AUSBILDUNG

M.Sc. IT-Sicherheit

10/2014 - 09/2016

Ruhr-Universitaet Bochum (RUB) - Horst-Goertz-Institut — Bochum, Deutschland

IT-Sicherheit — 1,3

B.Sc. Informatik

10/2011 - 09/2014

Ruhr-Universitaet Bochum — Bochum, Deutschland

Informatik — GPA: 1,5

FÄHIGKEITEN

- Splunk ES + IBM QRadar + Sentinel (SIEM)
- CrowdStrike Falcon + Microsoft Defender XDR
- MITRE ATT+CK + D3FEND + Pyramid of Pain
- Splunk SOAR + Cortex XSOAR + IBM Resilient
- Threat-Hunting (KQL + SPL + EQL)
- MISP + OpenCTI + Mandiant Advantage
- Python + PowerShell + Go SecOps-Automation
- BSI IT-Grundschutz + ISO 27001 + BAIT/VAIT/DORA

PROJEKTE

purple-team-coverage (Open Source)

06/2023 - heute

Open-Source-Framework fuer MITRE-ATT+CK-Coverage-Audits mit 84 Atomic-Red-Team-Test-Cases, 1.840 GitHub-Stars, in 48 SOC-Pipelines produktiv.

Heise IT-Security Frankfurt 2024 - Speaker 09/2024

Vortrag 'MTTD-Reduktion durch Detection-as-Code in der BaFin-regulierten Bank', 380 Teilnehmer:innen, 4,8/5 Bewertung.

ZERTIFIKATE

ISO/IEC 27001 Lead Auditor (TUEV SUED) 11/2024

GIAC Continuous Monitoring + Detection (GCDA) 06/2023

GIAC Penetration Tester (GPEN) 11/2022

GIAC Certified Incident Handler (GCIH) 03/2021

(ISC)2 CISSP 09/2019

BSI IT-Sicherheits-Beauftragte BSI 200-2 (TUEV) 02/2018

SPRACHEN

Deutsch	Muttersprache
Englisch	C2
Franzoesisch	B2

PUBLIKATIONEN

09/2024

Konferenz-Vortrag bei Heise IT-Security mit 380 Teilnehmer:innen, Bewertung 4,8/5.

06/2025

Konferenz-Vortrag bei Troopers mit 220 Teilnehmer:innen, Bewertung 4,9/5.

STÄRKEN

Detection-as-Code

Behandle Detection wie Software: PR-Reviews, CI-Tests mit Atomic Red Team, Versions-Tracking pro Use-Case in Git.

Major-Incident-Lead

Habe 38 Major-Incidents (S1/S2) geleitet, davon 4 Ransomware-Vorfaelle mit BaFin- und BSI-Meldung.

Mentoring

5 von 6 L2-Analysten zu L3 / Detection Engineer befoerdert, woechentliche 1:1 mit Karriere-Roadmap.