Stefan Richter

Senior Security Analyst

München +49 170 82736451 stefan.richter@email.de linkedin.com/in/stefanrichter

PROFIL

Senior Security Analyst mit 9 Jahren Erfahrung in Security Operations, zuletzt im Cyber Defense Center einer Bank. Schwerpunkte sind Threat Hunting, Detection Engineering mit Sigma und Splunk Enterprise Security sowie die Leitung komplexer Incident Response Fälle. Mentoring von 5 Analysten und Umsetzung der DORA-Anforderungen an das Vorfallmanagement.

KENNTNISSE

- **Threat Hunting**
- **Detection Engineering**
- **Sigma**
- **Splunk Enterprise Security**
- **Incident Response**
- **CrowdStrike Falcon**
- **Malware-Analyse**
- **Purple Teaming**
- **DORA**
- **Mentoring**

BERUFSERFAHRUNG

Senior Security Analyst 04/2022 - heute
Münchner Handelsbank AG München

- Threat Hunting nach Hypothesen aus aktuellen Kampagnen, **11** unentdeckte Kompromittierungsversuche aufgedeckt
- Detection Engineering mit Sigma-Regeln für Splunk Enterprise Security, 80 Use Cases neu geschrieben und getestet
- Leitung von Incident Response bei schweren Vorfällen, Meldeprozess an die BaFin nach DORA mit aufgebaut
- Mentoring von 5 Analysten im Cyber Defense Center inklusive Einarbeitungsplan und Fallbesprechungen

Security Analyst 01/2019 - 03/2022
Oberland Cyber Defense GmbH Unterföhring

- Analyse von Vorfällen bei **20** Kunden aus Industrie und Versicherungen, 2nd- und 3rd-Level im SOC
- Malware-Analyse verdächtiger Dateien in isolierter Umgebung, Ergebnisse als IoC-Listen an alle Kunden verteilt
- Rollout von CrowdStrike Falcon bei 6 Kunden mit zusammen 14.000 Endpunkten und Feinjustierung der Richtlinien
- Purple Teaming mit dem Red Team, 3 Übungen pro Jahr und daraus abgeleitete Erkennungslücken geschlossen

Junior Security Analyst 10/2017 - 12/2018
Datenwerk Bayern GmbH Augsburg

- Überwachung von Alarmen im SIEM für das eigene Rechenzentrum mit 900 Servern
- Erstellung von Wochenberichten zur Sicherheitslage für die IT-Leitung und den Datenschutz
- Mitarbeit an 45 neuen Use Cases bei der Umstellung auf ein neues SIEM

AUSBILDUNG

Master of Science
Technische Universität München
Informatik
München
10/2015 - 09/2017

Bachelor of Science
Technische Universität München
Informatik
München
10/2012 - 09/2015

ZERTIFIKATE

Certified Information Systems Security Professional (CISSP) 10/2021
ISC2

GIAC Certified Incident Handler (GCIH) 04/2020
GIAC

SPRACHEN

Deutsch
Muttersprache

Englisch
C1