AUSBILDUNG

B.Sc. IT-Sicherheit (5. Semester)

10/2022 - heute

Universitaet des Saarlandes - CISPA Helmholtz-Zentrum

Saarbruecken, Deutschland

IT-Sicherheit GPA: 1,5

FÄHIGKEITEN

- Splunk Enterprise Security
- Microsoft Sentinel
- Wazuh + Elastic Security
- Suricata + Zeek IDS
- Python fuer SOC-Automation
- Linux + Bash Scripting
- Wireshark + tcpdump
- MITRE ATT+CK + D3FEND

ZERTIFIKATE

CompTIA CySA+ (CS0-003)

02/2025

CompTIA Security+ (SY0-701)

08/2024

BSI-Grundschutz-Praktiker (Selbststudium)

05/2024

TryHackMe SOC Level 1 Path Certificate

02/2024

SPRACHEN

Deutsch Muttersprache

Englisch C1

PROFIL

Werkstudent Cyber Security im 5. Semester B.Sc. IT-Sicherheit am CISPA Helmholtz-Zentrum Saarbruecken mit Schwerpunkt Detection-Engineering. 16 Monate Werkstudent-Erfahrung im SOC bei Hornetsecurity Hannover und im Blue-Team von genua GmbH Kirchheim. CompTIA Security+ und CySA+ zertifiziert, aktiver CTF-Player bei saarsec mit Top-30-Platzierung auf CTFtime.org.

BERUFSERFAHRUNG

Werkstudent SOC L1 Detection Engineer

10/2024 - heute

Hornetsecurity GmbH Hannover, Deutschland

Werkstudent (20h/Woche) im 14-koepfigen Managed-SOC-Team fuer 8.400 KMU- und Mittelstand-Kunden

- Triage von durchschnittlich 92 SIEM-Alerts pro Schicht in Microsoft Sentinel mit dokumentiertem MITRE-ATT+CK-Mapping
- Entwicklung von 24 Sigma-Regeln gegen Atomic Red Team T1059 + T1071 + T1027, False-Positive-Rate von 14% auf 3,8% reduziert
- Phishing-URL-Analyse mit URLScan, VirusTotal, Any.Run und Hornetsecurity ATP, 380 verifizierte Faelle in 6 Monaten
- Pflege von 28 Suricata-IDS-Regeln und Beitrag von 6 neuen Regeln nach MITRE ATT+CK Initial Access
- Wochenreport an SOC-Schichtleitung mit MTTD-Trends und KQL-Hunting-Queries

Werkstudent Blue Team Defensive Security

04/2024 - 09/2024

genua GmbH Kirchheim bei Muenchen, Deutschland

Werkstudent im Blue-Team fuer Hochsicherheits-Netzwerke fuer Bundesbehoerden

- Aufbau von 12 Wazuh-Detektionen fuer LSA-Dumping (Mimikatz, ProcDump) und Lateral Movement nach MITRE ATT+CK
- Pflege eines internen Lab-Setups mit FLARE-VM, REMnux und Caldera fuer Purple-Team-Uebungen
- Mitarbeit an BSI-Grundschutz-Audit-Vorbereitung mit 28 dokumentierten Kontrollen nach BSI 200-2
- Erstellung eines KQL-Hunting-Playbooks mit 42 Queries fuer Microsoft 365 Defender Endpoint-Telemetrie

PROJEKTE

CTF-Team saarsec (CISPA)

11/2024 - heute

Aktives Mitglied im saarsec-Team, Rang 28 weltweit auf CTFtime.org im Maerz 2026, Schwerpunkt Forensik und Crypto.

STÄRKEN

Strukturierte Analyse

Folge dem MITRE ATT+CK Kill-Chain-Schema bei jedem Alert und dokumentiere IOCs reproduzierbar in MISP.

Detection-Engineering

Schreibe Sigma- und KQL-Regeln mit Test-Cases in Atomic Red Team und reduziere False-Positives systematisch.

Lernbereitschaft

Loese woechentlich 3-4 HackTheBox-Maschinen und nehme an internen Purple-Team-Uebungen aktiv teil.

Studienarbeit: Detection-Engineering mit Sigma-Regeln

04/2024 - 09/2024

Implementierung und Evaluierung von 84 Sigma-Regeln auf Wazuh + Elastic Security gegen Atomic Red Team T1059 + T1071, Recall 0,92, Note 1,3.