Magdalena Threat-Intel-Brammer

Junior SOC Analyst

Junior SOC Analyst mit B.Sc. IT-Sicherheit (RUB HGI Bochum, Note 1,5) und 22 Monaten Werkstudent-Erfahrung bei secunet AG und T-Systems International. CompTIA Security+ und CySA+ plus GIAC GSEC bereits im 1. Berufsjahr abgeschlossen, taeglich 96 SIEM-Alerts in Splunk Enterprise Security triagiert mit dokumentiertem MITRE-ATT+CK-Mapping. Co-Maintainer einer Open-Source-Detection-Library mit 740 GitHub-Stars.

magdalena.brammer@example.de
+49 201 4567 8910
Essen, Deutschland
brammer-cysec.dev
linkedin.com/in/magdalena-brammer-soc
github.com/brammer-cysec

Berufserfahrung

Junior SOC L1/L2 Analyst

secunet Security Networks AG • Essen, Deutschland • 10/2024 - heute

Vollzeit im 18-koepfigen Security Operations Center fuer 14 Bundesbehoerden- und KRITIS-Kunden

- Triage von durchschnittlich 96 SIEM-Alerts pro 8-h-Schicht in Splunk Enterprise Security mit MITRE-ATT+CK-Mapping
- Entwicklung von 38 Sigma-Regeln gegen Atomic Red Team T1059 + T1071 + T1027 mit dokumentierten Test-Cases
- MTTD von 24 auf 8 Minuten und MTTR von 4 h auf 48 Minuten in 12 Monaten reduziert durch Playbook-Standardisierung
- Phishing-Mail-Analyse mit URLScan, VirusTotal, Any.Run und MISP, 480 verifizierte Faelle in 9 Monaten
- Eskalation und Dokumentation von 28 Incidents nach BSI-Grundschutz 200-2 + BSI 200-4 inkl. Forensik-Triage
- Co-Author von 4 internen Threat-Intel-Briefings zu LockBit + Akira + BlackCat fuer KRITIS-Sektor

Werkstudent SOC L1 Analyst

T-Systems International GmbH • Frankfurt am Main, Deutschland

03/2023 - 09/2024

Werkstudent im Telekom-Cyber-Defense-Center fuer Konzern- und Bundeskunden

- Mitwirkung an 24/7-SOC-Schicht-Rotation mit durchschnittlich 84 Alerts pro Schicht in IBM QRadar
- Aufbau eines KQL-Hunting-Playbooks mit 38 Queries fuer Microsoft 365 Defender und Sentinel
- Wochenreport an SOC-Schichtleitung mit MTTD/MTTR-Trends und False-Positive-Rate pro Use-Case
- Mitarbeit an internem MITRE-ATT+CK-Coverage-Audit, Coverage von 42% auf 68% gesteigert

Projekte

sigma-detection-lab (Open Source)

- 05/2024 - heute

Open-Source-Library mit 184 Sigma-Regeln fuer T1059 + T1071 + T1027 + T1078, 740 GitHub-Stars, in 24 SOC-Pipelines produktiv eingesetzt.

Bachelorarbeit: ML-basierte UEBA-Detektion

- 03/2024 - 07/2024

Vergleich von 4 Algorithmen (Isolation Forest, Autoencoder, BERT, XGBoost) auf CERT R4.2 + UNSW-NB15 Datensatz, F1-Score 0,89, Note 1,2.

Ausbildung

B.Sc. IT-Sicherheit

Ruhr-Universitaet Bochum (RUB) - Horst-Goertz-Institut

Bochum, Deutschland

10/2020 - 09/2024

IT-Sicherheit • GPA: 1,5

Fähigkeiten

Splunk Enterprise Security, Microsoft Sentinel + KQL, CrowdStrike Falcon EDR, Suricata + Zeek IDS, Python + PowerShell SOC-Automation, MISP + OpenCTI Threat-Intel, Wireshark + tcpdump + Zeek, MITRE ATT+CK + D3FEND + CTI

Sprachen

Deutsch, Muttersprache

Englisch, C1

Stärken

Strukturierte Triage

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

Detection-Engineering

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

Zertifikate

GIAC Security Essentials (GSEC)

- 04/2025

CompTIA CySA+ (CS0-003)

- 11/2024

CompTIA Security+ (SY0-701)

- 06/2024

BSI IT-Sicherheits-Beauftragte BSI 200-2 (TUEV)

- 03/2024

Klarheit unter Druck

Behalte Ueberblick im Schicht-Betrieb, deeskaliere ruhig und uebergebe sauber an L2/L3 mit reproduzierbarem Playbook.