Magdalena Threat-Intel-Brammer

Senior Threat Intelligence Analyst

Threat Intelligence Analyst mit M.Sc. IT-Sicherheit (CISPA Saarland, Note 1,3) und 6 Jahren CTI-Erfahrung bei Mandiant Google DACH und IBM X-Force DACH. CTIA + GIAC GCTI + SANS FOR578 zertifiziert, Lead-Analyst fuer 18 APT-Profile (APT28, APT29, APT41, Lazarus, FIN7, BlackCat). 84 Threat-Intel-Briefings pro Jahr fuer DAX-Konzerne und Bundesbehoerden. Co-Author von 4 Mandiant-M-Trends-Reports 2023-2025.

magdalena.cti@example.de

+49 89 4455 6677

Muenchen, Deutschland

brammer-cti.dev

linkedin.com/in/magdalena-brammer-cti

github.com/brammer-cti

Experience

Senior Threat Intelligence Analyst (CTI)

10/2022 - heute

Mandiant (Google Cloud) DACH — Muenchen, Deutschland

Lead-CTI-Analyst im 18-koepfigen Mandiant Intelligence Team fuer DACH-Konzerne und Bundesbehoerden

- Lead-Analyst fuer 18 APT- und Ransomware-Profile (APT28/29/41, Lazarus, FIN7, BlackCat, LockBit, Akira)
- Erstellung von 84 Threat-Intel-Briefings pro Jahr fuer 38 DAX-Konzerne und 4 Bundesbehoerden inkl. CTAS Mandiant
- Pflege eines internen MISP-Streams mit 18.000 IOCs pro Monat aus Mandiant Threat Intel Grid
- Co-Author von 4 Mandiant-M-Trends-Reports 2023-2025, davon 2 mit DACH-Kapitel-Lead
- OSINT- und Dark-Web-Monitoring auf 28 Telegram-Channels und 14 Tox-Foren mit dokumentierter Methodologie
- Mentor fuer 4 Junior-CTI-Analysten:innen mit Karriere-Roadmap und GCTI-Bestehensquote 4/4 (100%)

Cyber Threat Intelligence Analyst

10/2019 - 09/2022

IBM X-Force DACH / IBM Security — Boeblingen, Deutschland

CTI-Analyst im IBM X-Force Threat Intelligence Team fuer DACH-Banken und Versicherungen

- Erstellung von 48 X-Force-Threat-Briefings pro Jahr fuer DACH-Banken, Versicherungen und Industrie
- Pflege eines internen X-Force-Exchange-Streams mit 12.000 IOCs pro Monat und 84 YARA-Regeln pro Quartal
- Lead-Analyst fuer 6 IBM-X-Force-Threat-Reports zu Banking-Trojanern (TrickBot, Emotet, IcedID)
- Co-Lead von 4 internen Threat-Hunting-Operationen mit IBM QRadar bei 8 DAX-Banken

Junior Threat Intelligence Analyst

10/2018 - 09/2019

T-Systems International GmbH — Bonn, Deutschland

Junior-CTI-Analyst im Telekom Cyber Defense Center fuer Bundesbehoerden

- Pflege eines MISP-Streams mit 4.800 IOCs pro Monat aus OSINT und kommerziellen Feeds
- OSINT-Recherche zu APT-Aktoren mit Maltego, theHarvester, SpiderFoot und Shodan

Education

M.Sc. IT-Sicherheit

10/2016 - 09/2018

Universitaet des Saarlandes - CISPA Helmholtz-Zentrum

Saarbruecken, Deutschland

IT-Sicherheit — 1,3

B.Sc. Informatik

10/2013 - 09/2016

Universitaet des Saarlandes

Saarbruecken, Deutschland

Informatik — GPA: 1,5

Projects

apt-tracker-dach (Open Source) 01/2023 - heute

Open-Source-Repo mit MITRE-ATT+CK-Profilen, IOCs und YARA-Regeln fuer 18 APT- und Ransomware-Aktoren mit DACH-Fokus, 1.480 GitHub-Stars, in 38 SOCs produktiv.

Mandiant M-Trends 2024 - Co-Author DACH-Kapitel 06/2024

Co-Author des DACH-Kapitels im Mandiant-M-Trends-2024-Report mit Schwerpunkt LockBit + Akira + BlackCat in deutschen Krankenhaeusern.

Publications

06/2024

Co-Author des DACH-Kapitels im Mandiant-M-Trends-2024-Report mit Schwerpunkt LockBit, Akira und BlackCat in deutschen Krankenhaeusern.

09/2023

Contributor zur DACH-Sektion mit Schwerpunkt APT29-Aktivitaeten gegen deutsche politische Stiftungen.

Skills

- MISP + OpenCTI + Mandiant Advantage
- Recorded Future + Anomali + IBM X-Force
- Maltego + theHarvester + SpiderFoot OSINT
- Shodan + Censys + GreyNoise + ZoomEye
- MITRE ATT+CK + Diamond Model + Kill Chain
- STIX + TAXII + YARA + Sigma
- Python + Go + Rust CTI-Automation
- Dark-Web-OSINT + Forum-Monitoring (Tox, Telegram, DDW)

Certificates

GIAC Cyber Threat Intelligence (GCTI)
06/2024

EC-Council CTIA (Certified Threat Intelligence Analyst)
11/2022

SANS FOR578 Cyber Threat Intelligence
03/2022

(ISC)2 CISSP 09/2021

Maltego Master Certified Analyst

06/2020

CompTIA CySA+ (CS0-001)

02/2019

Languages

Deutsch	Muttersprache
Englisch	C2
Russisch	B2

Strengths

Strukturierte Analyse

Folge dem Diamond Model + Kill Chain + MITRE ATT+CK fuer jeden Aktor, dokumentiere Confidence-Level transparent.

Sprach-Tiefe

Russisch B2 ermoeglicht Original-Forum-Analyse (XSS, Exploit.in), keine Uebersetzungs-Verzerrung in CTI-Reports.

Klare Briefings

Bereite Threat-Briefings fuer Vorstand, BaFin und BSI auf, mit klarer Geschaeftsfolge und ohne FUD.