Tobias DFIR-Pfaffenroth

Senior DFIR Specialist / Lead Incident Responder

tobias.pfaffenroth@example.de
+49 69 7788 9900
Frankfurt am Main, Deutschland
pfaffenroth-dfir.dev
linkedin.com/in/tobias-pfaffenroth-dfir
github.com/pfaffenroth-dfir

Profil

Senior DFIR Specialist mit M.Sc. IT-Sicherheit (TU Darmstadt CYSEC, Note 1,2) und 7 Jahren Incident-Response- und Forensik-Erfahrung bei KPMG Forensic DACH und CrowdStrike Services DACH. SANS GIAC GCFA + GCFE + GREM + GCIH + GNFA zertifiziert, Lead-IR-Specialist fuer 38 Major-Incidents pro Jahr inkl. 12 Ransomware-Faelle bei DAX-Konzernen. BSI-Meldung nach BSI 200-4 fuer 8 KRITIS-Faelle koordiniert. Co-Author von 3 BSI-Lagebericht-Beitraegen 2023-2025.

Berufserfahrung

Senior DFIR Specialist / Lead Incident Responder

CrowdStrike Services DACH, Frankfurt am Main, Deutschland

10/2022 - heute

Lead-IR-Specialist im 24-koepfigen CrowdStrike Services Team fuer DAX-Konzerne, Banken und KRITIS

- Lead-IR-Specialist fuer 38 Major-Incidents pro Jahr inkl. 12 Ransomware-Faelle (LockBit, BlackCat, Akira, Royal)
- BSI-Meldung nach BSI 200-4 fuer 8 KRITIS-Faelle 2024 koordiniert (Krankenhaeuser, Wasserwerke, Stadtwerke)
- Forensik mit Velociraptor, KAPE, Plaso und Volatility auf durchschnittlich 24 Hosts pro Engagement
- Malware-Reverse-Engineering mit Ghidra + IDA Pro fuer 14 Custom-Loader und 8 Ransomware-Familien 2024
- Co-Author von 4 CrowdStrike-Threat-Reports 2023-2025 inkl. DACH-Krankenhaus-Ransomware-Bericht 2024
- Mentor von 4 Junior-IR-Specialists mit SANS-GCFA-Bestehensquote 4/4 (100%)
- Speaker auf Heise IT-Security Frankfurt 2024 und FIRST Conference Fukuoka 2024

Fähigkeiten

- Autopsy + Sleuth Kit + FTK + EnCase
- Volatility + Magnet AXIOM + Belkasoft X
- Velociraptor + KAPE + Plaso + Log2Timeline
- Ghidra + IDA Pro + x64dbg Malware-RE
- MITRE ATT+CK + D3FEND + STIX/TAXII
- MISP + OpenCTI + YARA + Sigma
- Python + PowerShell + Bash DFIR-Automation
- BSI 200-4 + ISO 27035 + NIST SP 800-61

Zertifikate

SANS GIAC Network Forensic Analyst (GNFA)

, 11/2024

SANS GIAC Reverse Engineering Malware (GREM)

, 06/2024

DFIR Manager / Forensic Investigator

KPMG AG Forensic Technology, Berlin, Deutschland

10/2018 - 09/2022

DFIR-Manager im 18-koepfigen KPMG Forensic Technology Team fuer DAX- und Mittelstand-Mandanten

- Lead-Investigator fuer 28 Forensik-Engagements pro Jahr inkl. 8 BAIT-/VAIT-Pruefungsergaenzungen
- Forensik mit EnCase, FTK AccessData, Magnet AXIOM und Belkasoft X fuer 14 BaFin-Sonderpruefungen
- Co-Lead von 2 DSGVO-Datenschutzvorfall-Untersuchungen mit Aufsichtsbehoerden-Meldung nach Art. 33
- Mitarbeit an gerichtsverwertbaren Gutachten fuer 4 Landgerichts-Verfahren in 2021 und 2022

Junior Forensic Analyst

secunet Security Networks AG, Essen, Deutschland

10/2016 - 09/2018

Junior-Forensiker im Bundesbehoerden- und KRITIS-Team

- Forensik-Triage mit Autopsy + Sleuth Kit + Volatility fuer 38 Faelle in 2 Jahren
- Aufbau eines internen Lab-Setups mit FLARE-VM, REMnux und Cuckoo Sandbox fuer Junior-Schulungen

Ausbildung

M.Sc. IT-Sicherheit

Technische Universitaet Darmstadt - CYSEC

Darmstadt, Deutschland

10/2014 - 09/2016

IT-Sicherheit, 1,2

B.Sc. Informatik

Technische Universitaet Darmstadt, Darmstadt, Deutschland

10/2011 - 09/2014

Informatik, GPA: 1,4

Projekte

velociraptor-artifacts-dach (Open Source)

, 03/2023 - heute

Open-Source-Repo mit 84 Velociraptor-Artefakten fuer Windows-, Linux- und macOS-Triage in DACH-Konzern-Umgebungen, 1.420 GitHub-Stars, in 28 DFIR-Firmen produktiv.

BSI-Lagebericht 2024 - Co-Author Ransomware-Sektion

, 09/2024

Co-Author der Ransomware-Sektion im BSI-Lagebericht 2024 mit Schwerpunkt Krankenhaus-Ransomware und KRITIS.

SANS GIAC Forensic Examiner (GCFE)

, 11/2022

SANS GIAC Forensic Analyst (GCFA)

, 06/2022

SANS GIAC Certified Incident Handler (GCIH)

, 09/2020

(ISC)2 CISSP

, 03/2019

Sprachen

Deutsch, Muttersprache

Englisch, C2

Publikationen

09/2024,

Co-Author der Ransomware-Sektion im BSI-Lagebericht 2024 mit Schwerpunkt Krankenhaus-Ransomware und KRITIS.

06/2024,

Vortrag 'DACH-Krankenhaus-Ransomware 2023-2024: Lessons Learned aus 12 Engagements', 480 Teilnehmer:innen, 4,8/5.

Stärken

Forensik-Disziplin

Folge ISO 27037 + NIST SP 800-61 strikt: Chain-of-Custody, Write-Blocker, Hash-Verifizierung fuer jedes Artefakt.

Containment unter Druck

Leite Major-Incident-Bridges mit 12-24 Beteiligten, isoliere systematisch ohne Beweismittel zu zerstoeren.

Klare Berichte

Schreibe gerichtsverwertbare Berichte nach ISO 27037 mit MITRE-Mapping und Timeline-Rekonstruktion.