Carolin Blue-Team-Pries

Cyber Security Analyst L2/L3

carolin.pries@example.de
+49 89 1234 5678
Muenchen, Deutschland
pries-cysec.dev
linkedin.com/in/carolin-pries-cysec
github.com/pries-cysec

Profil

Cyber Security Analyst mit M.Sc. IT-Sicherheit (TU Darmstadt CYSEC, Note 1,4) und 4 Jahren SOC-Erfahrung bei Allianz Cyber Insurance und Commerzbank CyberSec. CISSP, GIAC GCIH und CompTIA CySA+ zertifiziert, Lead-Analyst fuer 18 Detection-Use-Cases nach MITRE ATT+CK. MTTD von 14 auf 4 Minuten reduziert, 2 BAIT-Audits ohne Major Findings begleitet. Co-Maintainer einer Open-Source-SOAR-Playbook-Library mit 1.240 GitHub-Stars.

Berufserfahrung

Cyber Security Analyst L2/L3

Allianz Cyber Insurance / Allianz SE • Muenchen, Deutschland

10/2023 - heute

L2/L3-Analyst im 28-koepfigen Allianz Group SOC fuer 38 Konzerneinheiten in 14 Laendern

- Lead-Analyst fuer 18 Detection-Use-Cases nach MITRE ATT+CK (Initial Access, Lateral Movement, Exfiltration)
- MTTD von 14 auf 4 Minuten und MTTR von 2 h auf 28 Minuten in 18 Monaten reduziert durch SOAR-Automatisierung
- Aufbau von 38 Splunk-SOAR-Playbooks fuer Phishing-, Ransomware- und BEC-Response mit messbarer MTTR-Reduktion
- Incident-Lead fuer 24 Major-Incidents (S1/S2) inkl. BaFin-Meldung nach VAIT 9.1 + 9.2
- Co-Lead von 2 BAIT-/VAIT-Audits ohne Major Findings, 84 Kontrollen nach BSI IT-Grundschutz dokumentiert
- Mentoring von 6 L1-Analysten mit woechentlichen 1:1-Reviews und MITRE-ATT+CK-Schulungen

Ausbildung

M.Sc. IT-Sicherheit

Technische Universitaet Darmstadt - CYSEC

Darmstadt, Deutschland

10/2019 - 09/2021

IT-Sicherheit • 1,4

B.Sc. Informatik

Technische Universitaet Darmstadt

Darmstadt, Deutschland

10/2016 - 09/2019

Informatik • GPA: 1,6

Fähigkeiten

Splunk ES + IBM QRadar SIEM

CrowdStrike Falcon + SentinelOne EDR

Microsoft Sentinel + KQL

MISP + OpenCTI + MITRE ATT+CK

Python + PowerShell SOC-Automation

Splunk SOAR (Phantom) + Cortex XSOAR

Wireshark + Zeek + Suricata

BSI IT-Grundschutz + ISO 27001

Cyber Security Analyst L1/L2

Commerzbank AG CyberSec • Frankfurt am Main, Deutschland

10/2021 - 09/2023

L1/L2-Analyst im 22-koepfigen Commerzbank Cyber Defense Center (BaFin-reguliert)

- Triage von durchschnittlich 124 SIEM-Alerts pro Schicht in IBM QRadar mit dokumentiertem MITRE-Mapping
- Phishing-Mail-Analyse mit URLScan, VirusTotal, Any.Run und MISP, 1.240 verifizierte Faelle in 24 Monaten
- Aufbau von 28 KQL-Hunting-Queries fuer Microsoft 365 Defender, MITRE-ATT+CK-Coverage von 38% auf 72% gesteigert
- BAIT-Audit 2022 + 2023 mit 0 Major Findings im SOC-Bereich, 18 Kontrollen nach BSI 200-2 dokumentiert

Projekte

soar-playbook-library (Open Source)

- 01/2024 - heute

Open-Source-Library mit 84 Splunk-SOAR- und Cortex-XSOAR-Playbooks fuer Phishing, Ransomware und Lateral Movement, 1.240 GitHub-Stars, in 38 SOC-Pipelines produktiv eingesetzt.

Masterarbeit: SOAR-Wirkung auf MTTR

- 09/2023 - 03/2024

Empirische Studie ueber 14.000 Incidents bei 4 DACH-Banken, MTTR-Reduktion von 4 h auf 24 Minuten durch SOAR nachgewiesen, Note 1,1.

Stärken

Detection-Engineering

Schreibe Sigma-, KQL- und SPL-Regeln mit Atomic-Red-Team-Test-Cases und betreue 18 Use-Cases von Idee bis Production.

Incident-Lead

Leite Major-Incident-Bridges mit 8-12 Beteiligten, dokumentiere Timeline und Lessons Learned nach BSI 200-4.

Klare Eskalation

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

Zertifikate

(ISC)2 CISSP

- 09/2024

GIAC Certified Incident Handler (GCIH)

- 03/2024

CompTIA CySA+ (CS0-003)

- 06/2023

Splunk Core Certified Power User + SOAR Certified Admin

- 02/2023

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

- 11/2022

Sprachen

Deutsch • Muttersprache

Englisch • C2