Konstantin Red-Team-Holzweissig

Senior Red Team Operator

konstantin.holzweissig@example.de
+49 30 9988 7766
Frankfurt am Main, Deutschland
holzweissig-redteam.dev
linkedin.com/in/konstantin-holzweissig-redteam
github.com/holzweissig-redteam

PROFIL

Red Team Operator mit M.Sc. IT-Sicherheit (RUB HGI Bochum, Note 1,2) und 7 Jahren Offensive-Security-Erfahrung bei NVISO DACH und HiSolutions AG. OffSec OSEP + OSED + OSCE3 + CRTO II zertifiziert, Lead-Operator von 24 Red-Team-Engagements pro Jahr fuer DAX-Konzerne und BaFin-regulierte Banken. 4 BaFin-TIBER-DE-Engagements und 2 ECB-TIBER-EU-Engagements als Lead-Operator durchgefuehrt. Speaker auf x33fcon Gdynia 2024 + Hackfest Quebec 2024.

BERUFSERFAHRUNG

Senior Red Team Operator / Lead Operator

10/2022 - heute

NVISO DACH GmbH — Frankfurt am Main, Deutschland

Lead-Operator im 18-koepfigen Red-Team fuer TIBER-DE-, TIBER-EU- und DORA-TLPT-Engagements

- Lead-Operator fuer 24 Red-Team-Engagements pro Jahr inkl. 4 BaFin-TIBER-DE + 2 ECB-TIBER-EU + 6 DORA-TLPT
- Adversary-Emulation von APT29, FIN7, BlackCat und LockBit nach MITRE-ATT+CK mit dokumentierter TTP-Coverage
- Entwicklung von 18 Custom-BOFs und Loadern in C/C++/Rust mit EDR-Evasion gegen CrowdStrike + Defender + SentinelOne
- Phishing-Simulationen mit GoPhish und Evilginx2 fuer 48.000 Mitarbeitende, Initial-Access-Rate 12-28%
- Active-Directory-Compromise in 4 BaFin-Bank-Engagements binnen durchschnittlich 38 h ab Initial Access
- Mentor von 4 Junior-Operatoren mit OSEP-Bestehensquote 4/4 (100%) und 2 CRTO-II-Erfolgen
- Speaker auf x33fcon Gdynia 2024 und Hackfest Quebec 2024

Red Team Operator

10/2019 - 09/2022

HiSolutions AG — Berlin, Deutschland

Red-Team-Operator im 14-koepfigen Offensive-Team fuer Banken, Versicherungen und KRITIS

- Durchfuehrung von 28 Red-Team-Engagements pro Jahr nach BSI-IS-Pentest und TIBER-DE Methodologie
- Aufbau einer internen C2-Infrastruktur mit Cobalt Strike + Sliver auf AWS + Azure Redirector-Chains
- Entwicklung von 12 Aggressor-Scripts fuer Cobalt Strike und 6 Mythic-Agent-Profile fuer EDR-Evasion
- Lead-Operator fuer 4 BaFin-TIBER-DE-Engagements mit dokumentierter Threat-Intel-Phase und Red-Phase

Junior Penetration Tester

10/2017 - 09/2019

secunet Security Networks AG — Essen, Deutschland

Junior-Pentester im 24-koepfigen Offensive-Team fuer Bundesbehoerden

- Durchfuehrung von 38 Penetration-Tests pro Jahr fuer BSI-, BfV- und Bundeswehr-Kunden
- Aufbau einer internen Active-Directory-Lab-Range mit 14 Domain Controllern fuer interne Schulungen

AUSBILDUNG

M.Sc. IT-Sicherheit

10/2015 - 09/2017

Ruhr-Universitaet Bochum (RUB) - Horst-Goertz-Institut — Bochum, Deutschland

IT-Sicherheit — 1,2

B.Sc. Informatik

10/2012 - 09/2015

Ruhr-Universitaet Bochum — Bochum, Deutschland

Informatik — GPA: 1,4

FÄHIGKEITEN

- Cobalt Strike + Sliver C2 + Mythic + Havoc
- BloodHound + Rubeus + Mimikatz + impacket
- Active Directory + Azure AD + Entra ID Attacks
- Initial Access + Phishing + GoPhish
- Malware-Loader-Entwicklung (C/C++/Rust)
- EDR-Evasion + AMSI/ETW-Bypass
- MITRE ATT+CK Adversary Emulation + Caldera
- OffSec OSEP + OSED + OSCE3 Methodologie

PROJEKTE

havoc-tradecraft-de (Open Source)

06/2023 - heute

Open-Source-Repo mit 48 BOFs (Beacon Object Files) und Aggressor-Scripts fuer Cobalt Strike, 1.840 GitHub-Stars, in 28 Red-Team-Firmen produktiv.

x33fcon Gdynia 2024 - Speaker

09/2024

Vortrag 'TIBER-DE Lessons Learned: 4 DAX-Bank-Engagements im Vergleich', 280 Teilnehmer:innen, 4,9/5 Bewertung.

ZERTIFIKATE

Zero-Point Security CRTO II

11/2024

OffSec OSCE3 (OSEP + OSED + OSWE)

06/2024

OffSec OSEP (PEN-300)

11/2022

OffSec OSED (EXP-301)

06/2022

OffSec OSCP (PEN-200)

03/2020

Zero-Point Security CRTO

09/2019

SPRACHEN

Deutsch	Muttersprache
Englisch	C2

PUBLIKATIONEN

09/2024

Konferenz-Vortrag bei x33fcon mit 280 Teilnehmer:innen, Bewertung 4,9/5.

11/2024

Konferenz-Vortrag bei Hackfest Quebec mit 320 Teilnehmer:innen, Bewertung 4,8/5.

STÄRKEN

Adversary-Mimikry

Emuliere konkrete Threat-Aktoren (APT29, FIN7, BlackCat) nach MITRE-ATT+CK-Profilen mit dokumentierter TTP-Coverage.

OPSEC-Disziplin

Plane jede Operation mit klarem OPSEC-Plan (Infra, Domains, Beacons, EDR-Profil), keine Detection ohne Absicht.

Klare Berichte

Schreibe TIBER-DE-konforme Berichte mit Attack-Path-Grafik, MITRE-Mapping und Blue-Team-Empfehlungen pro Phase.