Bernd Janzen

SOC Analyst

Berlin, Germany +49 179 9117911 bernd.janzen.dev@gmail.com

Summary

SOC Analyst with practical experience in simulated SOC labs (Splunk, Wazuh, Wireshark, Nmap). Currently advancing knowledge with Network+ and Google Cybersecurity Professional Certificate. Combines technical skills with decades of structured operational experience, bringing reliability, attention to detail, and disciplined investigative thinking to security operations.

Education

Masterschool — May 2025 - Jun 2026
Cybersecurity Training Program — Training Program

- Established foundational knowledge in core IT, networking, and security concepts (A+, Security+, Network+ principles) to inform system defense strategy.
- Applied knowledge through practical training: Conducting vulnerability assessments, penetration testing, and incident response while utilizing industry-standard tools like Wireshark, Splunk, Nmap, and SIEM basics.

CareerFoundry — Aug 2023 - Apr 2024
Full-Stack WEB-Development — Bootcamp

Projects

Aurora AI Security GmbH — Mar - Apr 2026
Network & Security Capstone Project

- Deployed Wazuh SIEM (all-in-one: manager, indexer, dashboard), enrolled Win Server 2022 and Win 11 endpoints as agents, and configured alert rules for real-time security monitoring
- Performed SOC triage workflow; monitored incoming alerts, distinguished false positives from real threats, analyzed forensic fields (source IP, user, protocol, MITRE technique), and documented incident classification and escalation recommendation
- Executed red team / blue team simulation - nmap reconnaissance and SMB brute force from Kali Linux; Wazuh rule 60204 fired in real time with full forensic evidence
- Designed firewall rules (pfsense, default-deny), VLAN segmentation, STRIDE threat model, and 5 incident response playbooks aligned to NIST CSF 2.0, GDPR, NIS2 and IT-SiG 2.0.
- Deployed HashiCorp Vault for PAM/Secrets management
- Stack: Wazuh SIEM, Ubuntu Server, Kali Linux, UTM (Apple Silicon)

Movie Database Application — Nov 2023 - Jan 2024
GitHub

Full-stack application with secure RESTful API (Node.js, Express, MongoDB, JWT authentication) and React frontend, demonstrating secure authentication flows and API integration principles.

Experience

Panos.ai — May 2026 - July 2026
Cybersecurity Engineer Intern — remote
https://panos.ai/de

- Regulatory Compliance mapping
- EU AI Act (Low Risk), GDPR requirement
- NIST CF - SP.1300 mapping for small businesses
- Asset inventory automation in AWS, Azure and Google Cloud

Octopus Energy — Oct 2024 - Apr 2025
Customer Service Specialist — Berlin

- Handled 50+ structured cases daily in an audit-logged system environment, executing account-level updates with precision while maintaining procedural compliance and accountability.

ENPAL Sales Enablement GmbH — Sep 2022 - Feb 2023
Backgroundcheck — Berlin

- Managed 80+ daily floor plan creations and 50+ land registry evaluations, ensuring accurate property verification and compliant documentation handling within defined operational procedures.
- Performed high-volume property documentation reviews, including land registry analysis and Power of Attorney verification, ensuring data accuracy and procedural compliance.

Sterntal e.V. — Sep 2018 - Aug 2022
Operations Coordinator — Berlin

- Developed and managed café operations, ensuring efficient high-volume service and HACCP compliance through structured monitoring and documentation.
- Implemented POS system and conducted daily financial reconciliation, identifying discrepancies and coordinating with accounting.
- Trained and supervised a diverse team, including employees with disabilities, while optimizing operational workflows and communication.

Profiles

LinkedIn TryHackMe Portfolio

Technical Skills

SIEM & Monitoring

- Wazuh (alert monitoring, agent management, threat hunting, rule config)
- SIEM (Splunk – log analysis & alert investigation)
- Wireshark (packet inspection)
- Nmap (network scanning & enumeration)
- Snort (IDS fundamentals)

Alert Analysis

- Security event triage
- false positive identification
- MITRE ATT&CK mapping

Networking

- TCP/IP, DHCP, DNS, HTTP/S, Firewalls, VPN fundamentals, Packet Tracer

Compliance & Security Frameworks

- NIST CSF 2.0
- MITRE ATT&CK
- GDPR
- EU AI Act
- ISO 27001
- NIS2
- BSI Grundschutz
- OWASP

Scripting

- Python (basic scripting for parsing)
- Bash

IAM / PAM

- Active Directory
- HashiCorp Vault
- RBAC

OS

- Linux (Ubuntu, Kali, Alpine)
- Windows Server 20222
- Windows 11
- Mac OS

Soft Skills

Attention to Detail

Analytical thinking

Teamwork

Resilience

Certifications

Security+
Jan 2026
CompTIA

Google IT Support
Oct 2025
Google / Coursera

Full-Stack Web-Development
Apr 2024
Career Foundry

Data Processing Merchant, IT
IHK Berlin
Jul 1993

Languages

German
Native

English
Professional working proficiency

Dutch
Basics