Kundan Vidhate

SOC Analyst & Detection Engineer

Voßstraße 12, 10117 Berlin, Germany | +49 15565518087 | kundanvidhate8@gmail.com
linkedin.com/in/kundan-vidhate-3479833b1 | github.com/Strixhack

PROFESSIONAL SUMMARY

Cybersecurity graduate student specializing in SOC operations, detection engineering, and incident response. Experienced in building detection content mapped to MITRE ATT&CK and aligned with EU compliance frameworks (NIS2, GDPR). Completed a six-month cybersecurity internship at ITKART, Pune. Currently pursuing an M.Sc. in Cybersecurity in Berlin and seeking a SOC Analyst or Detection Engineering internship starting October 2026 across Germany, the Netherlands, Belgium, and Ireland.

EDUCATION

M.Sc. Cybersecurity
SRH Berlin University of Applied Sciences — 2025 – Present (expected Sep 2027) — Berlin, Germany
GPA: 1.8 | Deutschlandstipendium Scholar | Rated top 10% of cohort by faculty

B.Sc. Computer Science
Savitribai Phule Pune University — Pune, India
CGPA: 7.95 / 10

PROFESSIONAL EXPERIENCE

Cybersecurity Intern
ITKART — Pune, India — February 2024 – August 2024

- Supported security monitoring and log analysis tasks as part of the security team.
- Gained hands-on exposure to enterprise security tooling and incident documentation practices.
- Assisted with vulnerability assessment and reporting activities.

CERTIFICATIONS

- TryHackMe – SOC Level 1 (Top 5% globally)
- TryHackMe – AI Security
- Cisco Networking Academy – Network Support and Security Learning Path
- CompTIA Security+ – In Progress

TECHNICAL SKILLS

SIEM / SOC Platforms: Wazuh, Microsoft Sentinel, Defender XDR, OpenSearch

Detection & Threat Frameworks: MITRE ATT&CK, Cyber Kill Chain, NIS2, GDPR, PCI-DSS

Case Management / Threat Intel: TheHive, Cortex, Jira, VirusTotal, AbuseIPDB, MISP

Network & Endpoint Analysis: Wireshark, Zeek, Nmap, Sysmon, YARA

Languages & Query: Python, Bash, KQL

Identity & Zero Trust: SPIFFE/SPIRE, X.509, mTLS

Dev / Infra: Git, GitHub, Docker, Linux

PROJECTS

SOAR Platform

- Built a security orchestration platform on Wazuh 4.14.4, OpenSearch, and Streamlit — 9 modules with a 14-rule custom detection engine.
- Integrated automated enrichment via VirusTotal and AbuseIPDB on alert generation.
- Tagged every alert against NIS2, GDPR, and PCI-DSS compliance requirements (TLP:AMBER classification).

Threat Detection Lab

- Built a Wazuh + Sysmon detection lab and validated rules against 10 simulated attacks, including Mimikatz, EternalBlue, and Hydra brute-force.
- Achieved a 100% detection rate with mean time to detect under 30 seconds.
- Documented each simulated incident formally through TheHive.

Sentinel SIEM

- Deployed Microsoft Sentinel paired with Defender XDR and authored 8+ custom KQL detection rules.
- Covered lateral movement, brute-force, LOLBins, and PowerShell obfuscation, mapped to MITRE ATT&CK.
- Aligned detection logic with NIS2 monitoring requirements.

Phishing Investigation Platform

- Built a full-stack incident response tool (FastAPI, React, Docker) integrating YARA rules for indicator detection.
- Reduced phishing triage time from approximately 30 minutes to 60 seconds per case.
- Integrated with TheHive and Cortex for case creation and automated analysis, with full audit logging (TLP:AMBER).

Zero Trust Workload Identity Research

- Researched SPIFFE/SPIRE workload identity and identified trust-domain naming, rather than cryptography, as the dominant unaddressed failure surface in dynamic environments — a gap not covered by NIST SP 800-207A.
- Built a working system (SPIFFE CA, two services, dashboard) via Docker Compose with mTLS (CERT_REQUIRED) and X.509 SVIDs; validated with an 18-test GitHub Actions CI suite.
- Found that 100% of induced trust-domain misconfigurations produced a silent, undetected failure rather than an alert (e.g., sidecar bypass returning HTTP 200 with a null identity); CA rotation gaps caused hard outages rather than graceful degradation.
- Delivered a GitHub repository with three research notes (NIST gap analysis, STRIDE threat model, failure taxonomy), a 25-slide research deck, and a 10-slide demo walkthrough.

LANGUAGES

English — Fluent | German — A2 (actively studying toward B1)