MOHAMMAD SHAHADAT HOSSAIN

Application Consultant | Cybersecurity Practitioner

Authorized Pentesting | SOC/SIEM | Wazuh | Microsoft Sentinel | pfSense | DFIR

Location: Ruhr Region, Germany | **Phone:** +49 1578 1717623
Email: mh8306427@gmail.com
LinkedIn: https://www.linkedin.com/in/mohammad-shahadat-hossain-57abb4142/
GitHub: https://github.com/mshoss
Blog: https://medium.com/@mh8306427
TryHackMe: https://tryhackme.com/p/hossamo2
Hack The Box: https://profile.hackthebox.com/

PROFESSIONAL SUMMARY

Application Consultant with 4+ years of enterprise IT experience, currently transitioning into cybersecurity with hands-on expertise in penetration testing, SIEM operations, and detection engineering. Currently at OpenTAS GmbH, operating across both **Red Team** (offensive security) and **Blue Team** (defensive operations) — bridging application development with proactive security testing.

Conducted **authorized penetration testing in real enterprise environments** beyond CTFs and lab exercises. Built a fully-segmented home SOC lab with **8+ virtual machines, 3 isolated network segments, and 5 threat intelligence APIs**, reducing alert triage time by an estimated **60%** through AI-driven response automation.

Open to roles in: Penetration Testing · SOC Analysis · Security Engineering · DFIR · Cloud Security · Detection Engineering

KEY SKILLS

Penetration Testing | Wazuh SIEM | Microsoft Sentinel | Microsoft Purview DLP | pfSense | Microsoft Defender for Endpoint | Active Directory Security | Detection Engineering | MITRE ATT&CK | Cyber Kill Chain | OWASP Top 10 | Burp Suite | Metasploit | Nmap | BloodHound | Wireshark | Python | PL/SQL | DFIR | GDPR | ITIL 4

CORE COMPETENCIES

Offensive Security: Penetration Testing, Vulnerability Assessment, Active Directory Attacks, Web/API Security Testing, MITRE ATT&CK Mapping, Red Team Operations, OWASP Top 10, Privilege Escalation, Exploitation Validation

Defensive Security / SOC: SIEM Operations, Detection Engineering, Microsoft Purview DLP, Incident Response (DFIR), Malware Analysis, Threat Intelligence, SOAR / Automation, Log Correlation, Endpoint Detection and Response (EDR)

Tools & Platforms: Wazuh, Microsoft Sentinel, pfSense, Snort, Zeek, Burp Suite, Metasploit, Nmap, BloodHound, Mimikatz, Hydra, REMnux, FLARE VM, Wireshark, VirusTotal, AnyRun, AbuseIPDB, Python, PL/SQL, Bash

PROFESSIONAL EXPERIENCE

Inhouse Application Consultant | Cybersecurity Practitioner | OpenTAS GmbH

September 2024 – Present · Hamburg, Germany (Remote)

Hybrid role across enterprise application consulting and cybersecurity — operating as both Red Teamer and Blue Teamer in real production environments.

Application Consulting

- Develop and maintain enterprise applications using **PL/SQL, Python, and SQL** for database management and automation workflows, supporting **multiple business-critical systems**.

- Manage tickets and documentation through **ServiceNow, Jira, and Confluence**; deliver insights via **Power BI** and workflow automation with **n8n**.
- Translate complex technical issues into clear business language for both technical teams and non-technical stakeholders, improving cross-functional communication.

Offensive Security (Red Team)

- Conducted **authorized penetration tests** across **web applications, APIs, and Active Directory environments**, identifying and validating vulnerabilities mapped to MITRE ATT&CK techniques.
- Use **Burp Suite, OWASP ZAP, Nmap, Metasploit, BloodHound, and Hydra** to identify, exploit, and validate vulnerabilities under controlled testing conditions.
- Perform vulnerability scans with **Tenable Nessus, OpenVAS, Nikto, sqlmap, and Acunetix**; score findings using **CVSS v3.1** and align with **OWASP Top 10**.
- Map attack chains to **MITRE ATT&CK** and **Cyber Kill Chain** frameworks; deliver remediation-focused reports prioritized by business risk.

Defensive Security (Blue Team / SOC)

- Hands-on with **Microsoft Purview DLP** — policy configuration, sensitivity labels, and data protection workflows preventing unauthorized data exfiltration.
- Operate **Wazuh SIEM** (Manager, Indexer, Dashboard) and **Microsoft Sentinel** for log correlation, alerting, and threat detection across **Windows, Linux, and firewall sources**.
- Detection engineering with **Snort (IDS/IPS), Zeek (protocol intelligence), Tshark/Wireshark (packet capture), and rsyslog** for centralized log aggregation reducing mean time to detection (MTTD).
- Use **Microsoft Defender for Endpoint (EDR)** for endpoint threat detection and response across managed devices.

DFIR & Malware Analysis

- Malware triage and analysis using **REMnux, FLARE VM, VirusTotal, ANY.RUN, and Hybrid Analysis**, classifying samples by family and behavior.
- Evidence collection and incident investigation aligned with established DFIR workflows and chain-of-custody best practices.

Compliance & Governance

- Apply **GDPR, ITIL 4, and Risk Analysis frameworks** to align security work with regulatory and service management standards.

Inhouse Application Consultant | Implico Group

December 2023 – August 2024 · Hamburg, Germany (Remote)

- Provided application consulting and technical support for **multiple enterprise clients**, focusing on database administration and process optimization.
- Collaborated with cross-functional teams to deliver **SAP-integrated solutions** and resolve technical issues, reducing escalation backlog.
- Documented technical workflows and trained end-users on enterprise applications, improving first-call resolution rates.

IT Consultant | GOD.dev Group

November 2022 – May 2023 · Germany (Remote)

- Delivered **first-level IT support for automotive industry clients**, troubleshooting application and infrastructure issues across distributed environments.
- Coordinated with development teams to escalate, document, and resolve **technical incidents within SLA targets**.
- Supported deployment and maintenance of enterprise software in client environments.

IT Consultant | RWE Supply & Trading GmbH

January 2020 – July 2022 · Essen, Germany

- Managed vendor operations and IT service workflows for **enterprise trading systems**, supporting business-critical infrastructure over **2.5 years**.
- Worked with **SAP ERP, Microsoft Power BI, and Microsoft Azure** for business reporting and infrastructure tasks.
- Supported **vulnerability management** and basic information security operations as part of IT service delivery.

FEATURED PROJECT — HOME SOC LAB

End-to-End Detection, Response & Threat Intelligence Platform

Built a fully-segmented Security Operations Center lab from scratch with **8+ virtual machines**, **3 isolated network segments**, **10+ integrated security tools**, and an **AI-assisted response layer**. Simulates real-world detection-response workflows including credential attacks, ransomware behavior, lateral movement, and data exfiltration. Reduced alert triage time by an estimated **60%** through AI orchestration.

- **Network**: pfSense firewall with WAN/LAN/OPT segmentation, custom firewall rules, IDS/IPS integration.
- **Endpoints**: Windows Server 2022 (Active Directory), Windows 10, Ubuntu Server, Kali, Parrot OS, Metasploitable 2.
- **SIEM Stack**: Wazuh Manager + Indexer + Dashboard with **custom rules and decoders** mapped to MITRE ATT&CK.
- **Detection**: Snort IDS, Zeek protocol intelligence, Tshark packet capture, rsyslog centralized aggregation across **4+ log sources**.
- **Threat Intelligence**: VirusTotal, AbuseIPDB, ANY.RUN, MISP, and Shodan API integrations for IOC enrichment across **5 sources**.
- **AI Response Layer**: OSSEC active response triggers LLM-driven playbook runner — auto blocks IPs, isolates hosts, routes alerts to Slack/email/ticketing within seconds.

TECHNICAL SKILLS

Penetration Testing: Burp Suite, OWASP ZAP, Nmap, Metasploit, sqlmap, Nikto, Hydra, BloodHound, Mimikatz
SIEM & Detection: Wazuh, Microsoft Sentinel, Snort, Zeek, OSSEC, rsyslog, OpenSearch
Vulnerability Management: Tenable Nessus, OpenVAS, Acunetix, CVE/CVSS scoring, OWASP Top 10
Endpoint & DLP: Microsoft Defender for Endpoint, Microsoft Purview DLP, Wazuh Agent
Network Security: pfSense, Firewall Engineering, IDS/IPS, Wireshark, Tshark, Network Segmentation
Threat Intelligence: VirusTotal, AbuseIPDB, ANY.RUN, MISP, Shodan, Hybrid Analysis
DFIR & Malware Analysis: REMnux, FLARE VM, Memory Forensics, Evidence Collection, Incident Response
Frameworks & Compliance: MITRE ATT&CK, Cyber Kill Chain, NIST CSF, OWASP, GDPR, ITIL 4
Programming: Python, PL/SQL, SQL, Bash, PowerShell, C/C++
Cloud & Enterprise: Microsoft Azure, ServiceNow, Jira, Confluence, SAP ERP, Power BI, n8n
Operating Systems: Kali Linux, Parrot OS, Ubuntu, Windows Server 2022, Active Directory
Virtualization: VirtualBox, VMware Workstation

EDUCATION

Master of Science (M.Sc.) — Cybersecurity | Brandenburgische Technische Universität Cottbus-Senftenberg

October 2023 – Present · Germany

- Focus: Penetration Testing, Risk Analysis, OSINT, Vulnerability Assessment, Incident Response.
- Hands-on coursework with: Burp Suite, OWASP ZAP, Nmap, Tenable Nessus, OpenVAS, BloodHound, Metasploit, MITRE ATT&CK.

Bachelor of Science — Computer Engineering, Software Engineering | Universität Duisburg-Essen (UDE)

April 2016 – September 2022 · Germany

- Specialization in software engineering, databases (PostgreSQL, MySQL), and cloud computing.
- Activities: Linux Networking, Cricket, Cooking, Reading.

CERTIFICATIONS

- **Certified SME Cyber Security Officer (CSCSO)** — EU Cyber Academy (Dec 2025)
- **Certified Ransomware Protection Officer (CRPO)** — EU Cyber Academy
- **Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900)** — Microsoft (Oct 2025)
- **Pre Security Certificate** — TryHackMe (Feb 2026)
- **IBM Generative AI for Cybersecurity Professionals** — IBM (Dec 2024)

- **Security Operations Center (SOC)** — Cisco
- **Cyber Threat Management** — Cisco (Sep 2022)
- **Networking Essentials** — Cisco (Oct 2024)
- **ITIL 4 Foundation** — AXELOS (Nov 2023)
- **Foundations of Cybersecurity** — Google (Sep 2023)
- **Operating Systems: Overview, Administration, and Security** — IBM

LANGUAGES

- **German** — Full Professional Proficiency (C1)
- **English** — Full Professional Proficiency (C1)
- **Bengali** — Native