# Mohd Kashif — SOC Analyst

Erding, Bavaria, Germany 85435
☎ (+49) 176 7318 7128 • ✉ md.kashif8858@gmail.com
mkashif.me • in penkashif

## Summary

*Master's graduate in Cybersecurity with over four years of experience in security operations, specializing in 24/7 incident response, vulnerability assessment and proactive threat detection. Skilled in SIEM, EDR and Microsoft XDR tools with proven ability to triage incidents, collaborate with cross-functional teams, and develop detection rules to further hardening the systems.*

## Technical Proficiencies

- **Tools**: Crowdstrike, Splunk, TheHive, Palo Alto Cortex XDR, Microsoft Sentinel, Microsoft Defender, Nessus, Python, SPL, Bash, SIGMA, YARA
- **Frameworks**: MITRE ATT&CK, Cyber Kill Chain, ISO 27001
- **Areas of Expertise**: SOC Analysis, Incident Response, Vulnerability Assessment, Threat Intelligence
- **Leadership**: Team Mentorship, Cross-functional Collaboration, Project Planning

## Home Lab Setup

Set up a home lab with 4 VMs to simulate attacks on a victim machine using Atomic Red Team and creating detection rules on a logging server using Elastic and Splunk.

## Professional Experience

**Amadeus Data Processing Gmbh** — **Erding, Germany**
*Associate Information Security Analyst* — *May 2025 - Oct 2025*

- **Cyber Security Incident Response:**
  - Investigating endpoint threats using EDR tools to resolve security incidents.
  - Analyzing phishing attempts using Microsoft Email Security and PhishER tools, leading to improved user awareness and reduced compromise rates.
  - Managing SIEM tool for threat hunting and log correlation.
  - Case handling through TheHive platform, enabling collaborative response and efficient resolution tracking.
- **Splunk Dashboards:**
  - Building and maintaining Splunk dashboards to monitor SLA metrics, driving accountability and performance improvements.

**SCHWARZ IT** **Neckarsulm, Germany**
*SOC Analyst (Working Student)* *May 2023 - Dec 2024*

- **Gap Analysis:**
  - Performed MITRE ATT&CK based gap analysis, and developed 30+ new Splunk detection rules.
  - Led the optimising and fine tuning of 20+ existing Splunk use cases, reducing false positives by 40%.
  - Mapped Cyber Kill Chain and MITRE ATT&CK Framework to categorise use-cases for better identification of attack scenarios
- **Automation**
  - Leveraged MISP to correlate IoCs, reducing manual analysis time by 25% and enhancing ISMS.
  - Collaborated with cross-functional teams (EDR, Email, AD, IDS/IPS, Firewall, Antivirus) to implement CIM-compliant data models, enhancing log correlation and resolving 60% of log inconsistencies.
- **Cross-Functional Leadership:**
  - Designed client-facing Splunk dashboards tailored for customer requirements, enhancing real-time visibility into critical security metrics.
  - Mentored 10+ junior analysts and colleagues via developing and maintaining Splunk training modules and runbooks, improving SOC workflow efficiency by 25%.

**CISPA Helmholtz Center for Information Security** **Saarbrücken, Germany**
*Research Assistant (Working Student)* *July 2022 - Dec 2022*

- Collaborated with researchers to develop a performance analysis tool in the research group of Nico Döttling for homomorphic encryption operations, quantifying computational time requirements for various cryptographic functions.

**TATA Consultancy Services** **New Delhi, India**
*SOC Analyst* *Nov 2018 - Oct 2020*

- Supported 24/7 SIEM-based monitoring and incident response achieving a significant uptime in threat detection and log analysis capabilities.
- Conducted monthly vulnerability assessment to identfy potential vulnerabilities using Nessus scanner.
- Coordinated weekly customer sync ups to align security strategies with business requirements, ensuring timely project delivery.
- Improved Threat Detection by utilising Search Processing Language in Splunk to create 15+ new alerts identifying and mitigating previously undetected security risks.
- Mentored 5+ new team members by providing knowledge transfer sessions and creating IR playbooks, standardizing cybersecurity best practices and reducing resolution time by 20%.

## Education

**Universität des Saarlandes** **Saarbrücken, Germany**
*Masters (Cybersecurity)* *Oct 2021 - Dec 2024*

- Grade: 2.1
- Thesis: A Haskel to Fully Homomorphic Encryption Transpiler with Circuit Parallelisation
  (Published in CCS '25: ACM SIGSAC Conference on Computer and Communications Security)

**Jamia Hamdard University** **New Delhi, India**
*Bachelors (Electronics & Communication)* *Oct 2014 - Aug 2018*

- CGPA: 8.76

## Certifications

Junior Penetration Tester by TryHackMe
SOC Analyst Learning Path by LetsDefend
CompTIA Security+ Certified Security Professional by LinkedIn Learning
Splunk 7.x Fundamentals
13.5 hours live training on "Using Splunk Enterprise Security"

## Languages

**English**: Professional Proficiency
**Hindi**: Native Proficiency
**German**: Beginner (In Progress)