Single Threaded Leader (STL) – Security & Compliance, Amazon Web Services (AWS)

(Owned end-to-end security delivery for customer-facing AWS Professional Services programs across Europe, Middle East & Africa (EMEA))

AHSAN ZIAULLAH

MASTER INFORMATIK - IT SECURITY

- CISSP-certified security leader with 14+ years of experience across cloud security, software delivery, and enterprise risk management

- Specialized in aligning secure architecture, privacy by design, and threat modeling with global compliance frameworks including NIST, ISO 27001, DORA, GDPR, and CIS Benchmarks

- Led delivery of security programs for 35+ enterprise clients in regulated sectors, including telecom, banking, pharma, and digital finance

- Recognized as a strong collaborator and program lead, skilled at bridging engineering, compliance, and legal functions to deliver secure, scalable, and audit-ready solutions.

Erdinger Str 47A, 85459 Berglern, Germany

ahsanzia17@gmail.com

+49 - 17682540420

Ahsan Ziaullah Erdinger Str 47A 85459 Berglern Germany +4917682540420 ahsanzia17@gmail.com

Résumé

Professional Experience

05/2022 – Present

Single Threaded Leader - Security & Compliance at AWS – Munich

- Accountable for security execution, operational governance, and stakeholder alignment across strategic AWS cloud transformation engagements in EMEA
- Led multi-stakeholder security programs for 35+ enterprise clients across regulated sectors including telecommunications, banking, pharmaceuticals, and digital finance, aligning engineering, legal, and compliance teams to deliver secure-by-design cloud transformation.
- Directed large-scale security initiatives including GenAI governance, SAP cloud migrations, digital asset compliance, and on-prem-to-cloud transitions — embedding privacy by design, threat modeling, and audit-aligned controls across architecture, delivery, and operations.
- Delivered "Responsible AI & Security" workshops as part of AWS GenAI readiness efforts (~80 participants), achieving CSAT 4.63. Recognized with the **"Most Impactful GenAI Hackathon Project Award"** for secure GenAI delivery tooling.
- Led the implementation of a **Sovereign Cloud** environment for a highly regulated customer, embedding data residency enforcement, jurisdictional controls, and policy guardrails in collaboration with compliance stakeholders.
- Defined and implemented security strategies aligned to global frameworks: **GDPR, ISO 27001, NIST 800-30, DORA, ISAE 3402, and CIS Benchmarks**, ensuring proactive compliance and audit readiness.
- Architected secure AWS Landing Zones with integrated IAM, encryption, network segmentation, and automated policy enforcement for compliance-sensitive environments.
- Built executive-facing risk dashboards using AWS native solution (Security Hub, GuardDuty, Config) to surface threat exposure, mitigation progress, and regulatory posture.
- Strengthened customer assurance by embedding security controls into project delivery workflows, reducing security gaps prior to go-live and enabling secure, auditable operations across multiple client engagements.
- **Conducted 90+ risk-focused security reviews** across customer architecture, technical deliverables, and production readiness as an AWS Guardian — enabling secure deployments, identifying critical risks, and aligning solutions with regulatory expectations.
- Acted as the designated Security Lead in early project scoping and risk assessments, conducting 50+ architecture and delivery risk reviews to advise on secure design, compliance alignment, and remediation of high-risk decisions.
- Led security planning for complex production migrations across large-scale infrastructure and sensitive workloads, ensuring risks were addressed through secure Statements of Work (SOWs) and pre-deployment controls.
- Built an internal platform to automate security assessments and remediation workflows; led a team of developers and consultants, improving review turnaround time by 5–6% across diverse customer engagements.
- Enabled secure cloud adoption across high-value customer workloads in telecom, pharma, and financial services by leading strategic risk mitigation and compliance-aligned security delivery.
- Recognized with multiple awards including **"Telco ProServe Deliver Results"**, **"Awesome Builder"**, and **"Learn and Be Curious"** for leadership in security innovation and cross-functional enablement.
- Actively supports diversity in tech as a **mentor in the AWS Cloud Women Mentorship program**, helping guide and develop women pursuing careers in cloud and cybersecurity.

02/2021 – 04/2022

Security Architect Senior Specialist at SAP SE – Walldorf

- Subject Matter Expert (SME) for NIST Cybersecurity Framework (CSF) assessments of SAP products, mapping controls across Identify, Protect, Detect, Respond, and Recover domains to evaluate SAP's risk posture.
- Organized and facilitated Threat Modeling Workshops, driving the identification of potential threats, misconfigurations, and architectural weaknesses; provided structured risk mitigation strategies aligned with NIST and secure architecture best practices.

Ahsan Ziaullah Erdinger Str 47A 85459 Berglern Germany +4917682540420 ahsanzia17@gmail.com

- Led Red Team engagements to simulate real-world cyberattacks against SAP systems, providing detailed risk assessments and presenting findings with actionable recommendations to the executive and security leadership boards.
- Directed a cross-functional team in the implementation of encryption across SAP products to meet compliance requirements (e.g., GDPR, ISO 27001), ensuring secure data-at-rest and data-in-transit across multiple modules.
- Evaluated open-source components within SAP's centralized architecture for known vulnerabilities (e.g., via NVD, OSS Index), integrating remediation strategies and maintaining software supply chain integrity.
- Designed and integrated security building blocks such as malware scanners, internal PKI infrastructure, user authentication stores, and TLS-secured connections to harden SAP product environments.
- Oversaw penetration testing initiatives (internal and external) for new and legacy SAP features; collaborated with engineering teams to implement fixes, reduce residual risk, and validate remediation through retesting.
- Led static code analysis efforts by establishing secure code review pipelines, conducting security evaluations, and providing ongoing guidance to developers on secure coding standards (e.g., OWASP, SAST tools).
- Recognized with the SAP Spot Award for outstanding contributions in strengthening product security and risk posture within a compressed delivery timeline.

04/2016 – 01/2021 **Information Security Engineer at EQS GROUP AG - Munich**

- Played a key role in implementing and aligning security practices with the ISO/IEC 27001 framework, including the design, review, and formalization of ISMS controls to support the company's certification readiness and audit success.
- Reviewed and validated information security policies, risk treatment plans, and control effectiveness in preparation for ISO/IEC 27001 certification, ensuring alignment with international standards and best practices.
- Led the Red Team responsible for conducting IT security assessments, providing comprehensive risk reports and threat modeling insights to the management board to guide strategic decisions.
- Conducted internal penetration testing and managed external penetration test engagements for EQS products, prioritizing identified risks and tracking remediation progress.
- Designed the integration roadmap for IDS/IPS systems and formalized the technical approach for enhancing intrusion detection and prevention capabilities across the organization.
- Developed and initiated the SIEM integration strategy, improving visibility and enabling centralized security event collection, correlation, and automated response mechanisms.
- Delivered Secure Software Development Lifecycle (SSDL) training to internal development teams, raising awareness of secure coding practices and reducing application-level vulnerabilities.
- Led the deployment of application-layer security controls to mitigate external threats and reduce the risk of exploitation of web-facing applications.
- Led incident response and forensic investigations, analyzing and responding to advanced persistent threats and suspicious activities.
- Designed and developed the security architecture for a major Investor Relations web application, embedding compliance and secure-by-design principles.
- Managed client security questionnaires and third-party risk assessments, ensuring transparency and alignment with industry compliance expectations.

02/2015 – 03/2016 **Software Developer at INTEL - Munich**

- Incorporating data aggregation and visualization techniques in the development of Intel XMM 7360 to enhance the debugging capabilities.
- Identifying Security risk in the architecture of Intel XMM 7360.
- **Awarded**: - Intel Heros of tomorrow for identifying architectural improvements in the trace tools to improve the call drop prediction scenario for Intel XMM 7360 modem used by iphone.

03/2014 – 02/2015 **Software Developer at MIVITEC GMBH - Munich**

- Architectural design and development of cloud monitoring system which improved the response time after an incident assessment improved the incident management system.
- Data center risk Assessment.

09/2013 – 03/2014 **Student Assistant at CAMP, Technical University Munich**

Ahsan Ziaullah Erdinger Str 47A 85459 Berglern Germany +4917682540420 ahsanzia17@gmail.com

- Development of infrastructure in aws in order to deploy internal project management system

09/2011 – 09/2013 **Junior Software Developer at AUI SOL - Lahore**

- Provided user requirements analysis and design for several customer applications
- Contributed software engineering expertise in development throughout software life cycle
- Carried out several presentations introducing new software tools & languages to adopt emerging standards

Educational Background

09/2013 – 03/2016 **Masters Informatics, Technical University Munich**

- Thesis: Automotive Lane Keeping Assistant Software for Embedded Systems on FPGA
- Major: - Artificial Intelligence and Robotics
- 2nd Major: - IT Security.

Additional Qualifications

Certification

Certified Information System Security Professional (CISSP) – ISC2
AWS Certified DevOps Engineer Professional - AWS
AWS Security Specialty - AWS
AWS Certified Solution Architect Associate - AWS
AWS Certified Cloud Practitioner - AWS
Offensive Security Certified Professional (OSCP) – Offensive Security
Certified Network Security Specialist (CNSS) - ICSI
AWS Advanced Security – Udemy
ISO/IEC 27001. Information Security Management System – Udemy
Information Security Management - Udemy
Data Science Orientation – IBM
Data Science Methodology – IBM
Open-Source Tools for Data Science - IBM
AWS CloudFormation – Udemy

Technical Skills

Programming Java | C++ | C | Vb/C#.net | Perl | Php | Matlab | Html/Css | Javascript | Python | Nodejs
Infrastructure Git | Jenkins | Docker | AWS
Organizational Jira | Confluence | Crucible
Security Tools Kali Linux | Metasploit | Netcat | Nmap| Wireshark | John the Ripper | Nikto | Nessus | OpenVAS Burpsuite | Zed Attack Proxy | w3af | THC Hydra | Cain & Abel | Sqlmap | BeEF