



PROFESSIONAL SUMMARY

Cybersecurity professional with hands-on experience in **SOC operations**, **security monitoring**, **incident investigation**, and **cloud security**, supported by a strong understanding of enterprise IT infrastructure and operational resilience principles. Experienced with **Microsoft Sentinel**, **Microsoft Defender for Endpoint**, **Microsoft Entra ID**, and **Azure Monitor** for threat detection, log analysis, security investigations, and risk mitigation across cloud environments.

Strong foundation in **SIEM**, **IT risk**, **cybersecurity governance**, **vulnerability management**, **MITRE ATT&CK**, **network security**, and **OWASP Top 10**, with a keen interest in **Business Continuity**, **Disaster Recovery**, **Operational Resilience**, and regulatory compliance. **ISC2 Certified in Cybersecurity (CC)**, committed to strengthening organizational resilience through proactive risk management, continuous monitoring, and secure, resilient technology practices.

WORK EXPERIENCE

Software Security Intern

March 2026–Present

BLDAR

Riyadh, KSA

- Strengthened application security across a production e-commerce platform by implementing **Role-Based Access Control (RBAC)**, secure session management, input validation, audit logging, and Secure SDLC practices across **60+ business workflows** and **50+ RESTful APIs**.
- Integrated security controls throughout the application lifecycle by validating authentication and authorization flows, enforcing **least-privilege access**, **reviewing API endpoints**, and **identifying potential security misconfigurations** before production deployments.
- Supported vulnerability management by reviewing **security findings**, **validating risks**, **prioritizing remediation activities**, and collaborating with development teams to implement security hardening measures across cloud-hosted applications.
- Investigated authentication anomalies, suspicious sign-in activities, and application security events using **Microsoft Sentinel**, **Microsoft Entra ID**, **Microsoft Defender for Endpoint**, and **Azure Monitor** to assist with incident investigation and risk mitigation.
- Collaborated with engineering teams to resolve production security issues involving authentication, CORS, SSL/TLS, session handling, and environment-based configurations, improving the overall security and reliability of cloud-hosted applications.

TECHNICAL SKILLS

Cybersecurity	Security MonitoringThreat DetectionSIEMLog AnalysisIncident Response & InvestigationVulnerability ManagementRisk Assessment
Digital Resilience	Business ContinuityDisaster RecoveryOperational ResilienceIT RiskGovernanceRegulatory Compliance
Cloud & Infrastructure	Microsoft AzureAWSMicrosoft Entra IDAzure MonitorCloud SecurityIdentity & Access Management
Security Platforms	Microsoft SentinelMicrosoft Defender XDRMicrosoft Defender for EndpointMicrosoft Defender for Cloud
Networking	TCP/IPDNSHTTP/HTTPSVPNFirewallsWireshark
Security Standards	NIST CSFISO 27001MITRE ATT&CKOWASP Top 10CIS Controls
Operating Systems	WindowsLinuxPowerShell

CERTIFICATIONS

- **Certified in Cybersecurity ISC2:** 2664231
- **Certified in Site Reliability Engineering:** 4def183e1e3d10

PROJECTS

Explainable Intrusion Detection System (XAI-IDS)

- Developed an **Explainable Intrusion Detection System (IDS)** to identify malicious network traffic using machine learning techniques on the **CICIDS2017** dataset, improving the detection of common cyber attacks.
- Built a data preprocessing pipeline to clean network traffic data and improve model performance.
- Built an ensemble detection model using **Random Forest**, **XGBoost**, and **LightGBM** to classify network attacks with higher accuracy and reduced false positives.
- Integrated **SHAP** and **LIME** to provide explainable predictions, enabling analysts to understand attack classifications and support security investigations.

ACHIEVEMENTS

- **Hackathon Winner:** Won **1st Place** in a university-level Hackathon by developing an innovative software solution under competitive time constraints.
- **Volunteer Experience:** Volunteered at university technical events, supporting event coordination, participant engagement, and technical sessions.
- **Community Participation:** Actively participated in hackathons, coding competitions, and cybersecurity learning activities to strengthen practical problem-solving and teamwork skills.
- **Leadership:** Recognized for taking ownership of projects, collaborating across teams, and delivering solutions within challenging deadlines.

EDUCATION

Osmania University

Bachelor of Engineering in Software Engineering

CGPA: 8.13

Hyderabad, India