ESRA ABUARQOB

Austin, TX | (843) 421-7145 | e.arqub@gmail.com
LinkedIn: linkedin.com/in/esra-arq-57259b88

PROFESSIONAL SUMMARY

Cybersecurity and cloud professional with six years of engineering experience across security operations, threat analysis, and enterprise network infrastructure. Holds a Master of Information Technology in Cybersecurity with a 4.0 GPA and certifications in CompTIA Security+ and Cisco CCNA. Experience investigating phishing, authentication anomalies, endpoint activity, and network behavior using structured security assessment and incident-response workflows. Academic research includes AI/ML security, adversarial attacks, prompt injection, phishing detection, and the secure AI lifecycle. Proficient in Python, AWS, Azure, SIEM platforms, MITRE ATT&CK, and technical reporting for technical and non-technical stakeholders.

CORE COMPETENCIES

AI/LLM Security: AI security, LLM threat analysis, prompt injection, adversarial attacks, phishing evasion, MLSecOps, secure AI lifecycle, machine-learning model evaluation

Security Assessment: Threat detection, vulnerability assessment, phishing investigation, alert triage, incident response, log analysis, endpoint security, authentication analysis, risk assessment, remediation guidance

Frameworks and Methodologies: MITRE ATT&CK, NIST Cybersecurity Framework, OWASP security concepts, security operations workflows, risk management, governance and compliance

Cloud and Infrastructure: AWS, Microsoft Azure, enterprise networks, routing and switching, network optimization, VMware, VirtualBox, CI/CD security, DevOps, Cisco Packet Tracer

Tools and Technologies: Python, Jupyter Notebook, SQL, Microsoft Sentinel, Splunk, Windows, security monitoring tools, predictive analytics

Communication and Leadership: Technical reporting, findings documentation, stakeholder presentations, cross-functional collaboration, security awareness training, workflow coordination, junior engineer training

PROFESSIONAL EXPERIENCE

Cybersecurity Awareness Specialist

Coastal PC Support | Myrtle Beach, SC
August 2024–December 2025

- Investigated phishing indicators, suspicious authentication activity, credential threats, and malicious behavior patterns through structured triage and escalation workflows.
- Documented investigation findings, escalation decisions, identified risks, and recommended mitigation steps in clear language for technical and non-technical stakeholders.
- Supported account-security and threat-analysis activities involving multifactor authentication, credential protection, endpoint visibility, alert triage, and incident response.
- Delivered cybersecurity programs covering phishing defense, ransomware prevention, social engineering, endpoint security, credential protection, and AI-driven cyber threats.
- Presented security risks and remediation guidance during customer-facing discussions, translating technical findings into practical actions.
- Monitored emerging phishing, social-engineering, account-compromise, and AI-assisted threat techniques to keep training and response guidance current.

Revenue and Reservation Manager

SeaMist Resort | Myrtle Beach, SC
March 2022–May 2023

- Increased revenue and customer engagement performance by 23% through data analysis, workflow optimization, and operational process improvements.
- Managed customer-facing CRM, reservation, and business systems in a high-volume environment, troubleshooting platform issues and coordinating timely resolutions.
- Protected confidential customer and business information while managing competing priorities and maintaining service quality.
- Produced analytical reports and communicated operational findings and recommendations to business stakeholders.
- Coordinated cross-functional workflows requiring strong organization, issue tracking, and stakeholder communication.

3G & LTE Optimization and Planning Engineer

Umniah Mobile Provider | Jordan
May 2017–March 2021

- Assessed enterprise telecommunications networks through traffic analysis, performance monitoring, troubleshooting, and infrastructure optimization.
- Investigated connectivity issues, anomalous traffic behavior, coverage limitations, and infrastructure reliability concerns across large-scale network environments.
- Identified technical weaknesses and recommended configuration and optimization changes to improve network performance, visibility, and reliability.
- Supported engineering teams with escalated troubleshooting, root-cause analysis, technical reporting, and validation of corrective actions.

- Communicated project status and technical findings across teams in a high-volume, SLA-driven environment.
- Trained junior engineers on network assessment methodologies, infrastructure analysis, troubleshooting processes, and technical documentation.

AI/LLM AND CYBERSECURITY PROJECTS

AI and Machine-Learning Security Research

- Evaluated Random Forest Classifier and Support Vector Machine models for phishing detection and threat classification using Python and Jupyter Notebook.
- Performed data preprocessing, feature extraction, class labeling, predictive analysis, and model-output evaluation against known phishing and safe-email labels.
- Examined security risks affecting AI and machine-learning systems, including adversarial attacks, prompt injection, phishing evasion, and manipulation of model inputs.
- Studied MLSecOps practices and secure AI lifecycle controls for identifying and reducing weaknesses before production deployment.
- Analyzed model behavior, false positives, false negatives, and classification results to identify weaknesses and document potential security implications.
- Produced clear technical documentation describing testing methodology, findings, model performance, risks, and recommended improvements.

SOC, SIEM, and Threat-Monitoring Assessments

- Investigated simulated security alerts involving authentication anomalies, phishing incidents, suspicious endpoint activity, and potential account compromise.
- Used Microsoft Sentinel and Splunk to perform log analysis, correlate security events, validate alerts, and distinguish actionable threats from false positives.
- Documented testing activities, findings, response actions, escalation decisions, and remediation recommendations.
- Applied MITRE ATT&CK concepts to organize observed behaviors and connect technical evidence with relevant threat tactics and techniques.
- Practiced communicating security findings and recommended actions through concise, stakeholder-focused reporting.

Cloud and Infrastructure Security

- Assessed AWS and Microsoft Azure security concepts involving identity, access controls, cloud configuration, monitoring, and risk management.
- Applied vulnerability-assessment and security-monitoring principles to virtualized and cloud-based lab environments.
- Examined CI/CD security, DevOps practices, and secure deployment concepts within the software and cloud-service lifecycle.
- Used VMware and VirtualBox to build controlled environments for cybersecurity exercises, testing, and technical analysis.

EDUCATION

Master of Information Technology, Cybersecurity

Coastal Carolina University | Conway, SC
2023–2025 | GPA: 4.00

Relevant focus: AI/ML security, threat detection, SIEM, cloud security, vulnerability assessment, incident response, governance, and risk management

Bachelor of Telecommunication Engineering

Al-Balqa Applied University | Jordan
2012–2016

CERTIFICATIONS

- CompTIA Security+
- Cisco CCNA Routing and Switching
- LTE Optimization and Planning

TECHNICAL SKILLS

Programming and Data: Python, SQL, Jupyter Notebook, data preprocessing, feature extraction, predictive analytics, model evaluation
Security Operations: Microsoft Sentinel, Splunk, SIEM, SOC workflows, threat detection, alert triage, incident response, log analysis
AI Security: Prompt injection, adversarial attacks, AI/ML threat analysis, phishing evasion, MLSecOps, secure AI lifecycle
Cloud and Systems: AWS, Microsoft Azure, VMware, VirtualBox, Windows, enterprise network infrastructure
Network Security: Routing and switching, traffic analysis, network monitoring, performance optimization, technical troubleshooting
Standards and Frameworks: MITRE ATT&CK, NIST Cybersecurity Framework, OWASP security concepts, HIPAA, PCI-DSS