Abdullah Siddiqi

InfoSecAbdullah@gmail.com ❖(813) 895-9461 ❖Tampa, FL ❖LinkedIn ❖Website

Security Analyst with 3+ years of hands-on experience in threat detection, incident response, and security operations. Demonstrated expertise in SIEM technologies, security compliance, and security awareness training. Proven track record of managing enterprise security controls and conducting comprehensive threat assessments using industry frameworks like MITRE ATT&CK.

WORK EXPERIENCE

GRC Analyst **Jan 2025 – Present**
Jün Cyber Tampa, FL

- Developed 15+ security policies and procedures aligned with NIST 800-53 and NIST 800-171 frameworks, addressing regulatory compliance requirements across enterprise infrastructure
- Conducted 30+ vendor security assessments and third-party risk evaluations, implementing risk mitigation controls for critical business partnerships
- Performed quarterly compliance audits covering 100+ security controls, maintaining audit documentation and evidence collection for regulatory examinations
- Delivered security awareness training to 100+ employees monthly, creating 25+ training modules covering phishing detection and incident reporting procedures

Security Analyst **April 2023 – Dec 2025**
UST Global Tampa, FL

- Monitored and analyzed 500+ security alerts daily using advanced SIEM platforms including QRadar, Sentinel, and Splunk
- Conducted 25+ incident response investigations, utilizing digital forensics and malware analysis techniques
- Performed threat hunting activities using EDR solutions like CrowdStrike and Carbon Black to detect lateral movement and behavioral anomalies
- Created 20+ security playbooks and SOAR runbooks to streamline automated detection, alert enrichment, and incident containment workflows

SOC Analyst **June 2022 – March 2023**
Cyber Florida Tampa, FL

- Triaged over 200 security incidents using enterprise SIEM technologies like Splunk and Velociraptor
- Led 15+ in-depth security reviews, using OSINT and threat attribution techniques to identify IOC/IOA patterns
- Developed 10+ detailed threat advisories using the MITRE ATT&CK framework, TTPs, and behavioral analytics
- Managed security controls including 50+ firewalls, endpoint protection tools, and access systems across the cloud

EDUCATION

University of South Florida **Dec. 2024**
Bachelor of Science in Cybersecurity Tampa, FL

- **GPA: 3.7/4.0**
  - **Honors**: Cum Laude

CERTIFICATIONS, SKILLS & INTERESTS

- **Certifications: CompTIA Security+; Blue Team Level 1 (BTL1)**
- **Tools:** Splunk, Arkime, CrowdStrike, Nessus, AWS Inspector, Snort, Splunk, Velociraptor, Wireshark
- **Skills:** Firewall & IDS/IPS Management, OSINT, Python, Threat Analysis
- **Frameworks:** NIST 800-53, NIST 800-171, CMMC, ISO 27001, SOC 2
- **Languages:** Arabic, English, Urdu
- **Interests**: Weightlifting; Rock Climbing; Chess; Fishing