Zuber Ali Mohammed

CYBER SECURITY ANALYST - Security Operations, Threat Detection & Incident Response

✉ m.zuberali404@gmail.com ☎ +1 (236) 514-5066 in LinkedIn 🌐 Portfolio

SKILLS

- **Security Frameworks:** GDPR, HIPAA, PIPEDA, PCI DSS, ISO 27001, NIST CSF, Incident Response
- **Security Operations:** SIEM, Threat Hunting, Threat Detection (IDS/IPS, WAF), and Data Breach Manage
- **Vulnerability Management:** Penetration Testing (VAPT), Threat Prevention (IAM, DLP), OWASP ZAP
- **Programming & Scripting:** Strong knowledge of Python and PowerShell for automating security tasks
- **Cloud & Network Security:** Experienced with Azure Security, CASB, SSH Hardening, and Network Firewalls

EDUCATION

Master of Science in Cybersecurity January 2022 – December 2023
New York Institute of Technology, Vancouver

Bachelor of Engineering in Computer Science July 2016 – December 2020
Osmania University, India

WORK EXPERIENCE

Cyber Security Consultant **January 2024 – Present**
SonvixTech *Ontario*

- Conducted comprehensive evaluations of cybersecurity concepts, including encryption standards, secure network design, analyzing SIEM logs & access control models, threat detection, and incident response efficiency by 30%.
- Improved data integrity, confidentiality, and compliance by 25% through covering cryptographic methods, authentication mechanisms, and secure communication protocols, enhancing incident response readiness.
- Performed automated and manual code reviews (SAST/DAST) using OWASP ZAP and Postman to detect 30% vulnerabilities in applications and monitor for Indicators of Compromise (IOC) and strengthen security posture.
- Co-ordinated in the implementation of NIST SP 800-53, ISO 27001, CIS Critical Security Controls, and GDPR policies, ensuring regulatory adherence, risk mitigation, and reducing compliance audit findings by 40%.
- Developed Security Information and Event Management (SIEM) correlation rules, and incident protocols, improving anomaly detection rates by 35% and accelerating mean time to detect (MTTD) threats by 50%.

Teaching Assistant **September 2023 – December 2023**
New York Institute of Technology *Vancouver*

- Mentored and instructed 40+ students in data mining techniques, statistical data analysis, and predictive modeling, improving comprehension by 40% through hands-on projects and real world datasets and entities.
- Facilitated and initiated group support, resolving over 50+ queries related to core concepts, enabling students to perform data processing, clustering, and classification with a 95% success rate in assignments & coursework.
- Evaluated 100+ assignments and exams, maintaining 100% accuracy in grading, delivered 4+ practical assignments demonstrations using Weka, ensuring adherence to key techniques and providing actionable feedback.

VOLUNTEER EXPERIENCE

Cybersecurity Experience **September 2023 – December 2023**
New York Institute of Technology *Vancouver*

- Identified and reported 20+ network vulnerabilities, including SQL injection, Cross-Site Request Forgery (CSRF), and command injection for remediation, improving system web application security by 40%.
- Improved in-depth penetration testing on cPanel based websites, uncovering SQL injection points, weak cipher suites, improper access controls, vulnerabilities, and enhancing the security posture of applications by 30%.

PROJECTS

Enhanced Threat Detection Capabilities

- Spearheaded a 25% improvement in SIEM-based detection efficiency by leveraging advanced log aggregation, event correlation, anomaly detection algorithms, threat intelligence feeds, and machine learning models.

Comprehensive Penetration Testing

- Executed and directed comprehensive penetration testing across 10+ web applications, identifying over 20 high risk vulnerabilities using tools such as Burp Suite, OWASP ZAP, XSS, SQL injection, and privilege escalation.

Incident Response Optimization

- Streamlined and advised incident response protocols, reducing resolution time by 30% through process engineering, playbook automation, security orchestration Automation and Response, and system root cause analysis.

SYN Flood Mitigation

- Led mitigation efforts that reduced SYN flood attack risk by 25% through the implementation of SPI, intrusion prevention systems (IPS), rate limiting, adaptive filtering, traffic analysis, anomaly detection, and load balancing.

Cybersecurity Training

- Trained and taught in cybersecurity workshops, leveraging threat strategies and interactive trainings, resulting in a 45% reduction in human-factor vulnerabilities and a measurable improvement in awareness scores by 30%.

CERTIFICATIONS

- **CompTIA Security plus(COMP001022670645), Preparing for CRISC and CISA certifications**