Arnold P. Mavhezha

New York, NY 10282 | amavhezh@mail.yu.edu | (917) 449-0928 | LinkedIn | Portfolio

EDUCATION

Yeshiva University, Katz School of Science and Health — New York, NY
Master of Science in Cybersecurity, GPA: 4.0 — *May 2027*
Relevant Coursework: Network Security, Secure System Design, Risk Management, Secure SDLC Concepts

Parul University, Parul Institute of Engineering and Technology — Gujarat, India
Bachelor of Technology in Computer Science and Engineering, GPA: 3.8 — *July 2020*

CERTIFICATIONS

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | ISO/IEC 27001:2022 Lead Auditor

PROFESSIONAL EXPERIENCE

Security Engineer — *April 2022 – July 2025*
Exceedingly Great Technologies, Harare, ZW

- Engineered threat detection logic across 1,000+ endpoints using Splunk SIEM, cutting mean time to detect (MTTD) by 35% through custom correlation rules and behavioral analytics mapped to MITRE ATT&CK TTPs
- Led vulnerability assessment and penetration testing exercises using Nessus and Nmap, mapping findings to CVSS attack vectors and eliminating 45% of critical CVEs within 30-day remediation cycles
- Conducted adversarial simulation and firewall rule-set analysis, stress-testing network perimeter defenses and identifying blind spots - reducing threat-blocking failures and cutting false positives by 30%
- Deployed and operated Microsoft Defender EDR/XDR, containing advanced threats including malware, ransomware precursors, and lateral movement activity, achieving 98% incident resolution within SLA
- Hardened AWS cloud environment by enforcing IAM least-privilege access, MFA, Security Groups, and CloudTrail logging, identifying and closing 40% of unauthorized access vectors before adversarial exploitation
- Spearheaded end-to-end incident response operations, triage, containment, and forensic root-cause analysis successfully neutralizing 50+ security incidents with zero business disruption
- Drove ISO 27001 and NIST CSF compliance by implementing technical controls and closing audit gaps, achieving 100% successful external audit outcomes across consecutive assessment cycles

Junior Security Analyst — *February 2021 – March 2022*
Exceedingly Great Technologies, Harare, ZW

- Triaged and investigated 1,200+ daily SIEM alerts in Splunk, reducing false positives by 25% through improved detection tuning and behavioral pattern recognition
- Investigated and escalated an average of 15 potential incidents per week, ensuring timely containment of malware, phishing, and unauthorized access attempts
- Performed vulnerability assessments across 250+ endpoints and 10 servers identifying and helping remediate 95% of critical vulnerabilities within SLA, with findings mapped to real-world attack vectors
- Executed targeted phishing simulation campaigns against 80+ staff members, analyzing click rates and credential harvesting susceptibility, achieving a 60% improvement in phishing awareness scores
- Collaborated with network teams to enforce security controls including MFA rollout and password policy hardening, reducing account lockout incidents by 40%
- Documented forensic incident reports and root-cause analyses, improving team knowledge base and cutting average response time by 20%
- Produced weekly security metrics dashboards for management, visualizing incident trends and control performance, driving data-informed security decisions across business units

Junior Developer *August 2020 – January 2021*
Exceedingly Great Technologies, Harare, ZW

- Designed and developed REST and SOAP APIs integrated with payment processors, Google Maps, and social login services, gaining deep insight into API attack surfaces including authentication flaws and injection points
- Improved API execution performance 2× by migrating to Node.js, while analyzing and resolving performance bottlenecks across 10+ existing backend systems
- Implemented security controls and data protection settings within full-stack applications, experience that directly informs understanding of application-layer vulnerabilities and secure-by-design principles
- Delivered in an Agile environment, contributing to sprint planning, code reviews, and cross-functional collaboration with design, QA, and product teams
- Assisted in deploying 10+ automated intelligent business systems, acquiring hands-on experience in how automation pipelines can be exploited or hardened

SKILLS

- **AppSec & Security Testing:** Burp Suite, Nessus, OWASP Top 10, MITRE ATT&CK, Threat Modeling
- **SAST/DAST Familiarity:** Exposure to static and dynamic analysis methodologies; understanding of Snyk
- **Scripting & Programming:** Python, Bash, PowerShell, JavaScript, SQL, PHP, HTML/CSS
- **DevOps & Version Control:** Git/GitHub, CI/CD pipeline security concepts, Jenkins
- **SIEM & Monitoring:** Splunk, MITRE ATT&CK
- **Frameworks & Standards:** NIST CSF, ISO/IEC 27001, CIS Benchmarks, CSA, COBIT, Secure SDLC
- **Operating Systems:** Linux, Windows

PROJECTS

Web Application Penetration Test – OWASP Juice Shop *February 2026*
Tools: Burp Suite CE, curl, Python 3, Firefox/FoxyProxy | Methodology: OWASP Testing Guide v4

- Conducted a gray-box web application penetration test against OWASP Juice Shop, identifying 9 vulnerabilities across 7 OWASP Top 10 (2021) categories — 4 Critical, 3 High, and 2 Medium severity
- Achieved full authentication bypass via SQL injection (CVSS 9.8) on the login endpoint, gaining admin JWT, password hash, and complete application control
- Discovered and exploited DOM-based XSS in the search bar, demonstrating session token theft risk due to JWT storage in localStorage rather than HttpOnly cookies
- Identified IDOR vulnerability allowing sequential enumeration of all users' basket data via unauthenticated API requests; enumerated 35+ API endpoints through client-side JavaScript analysis
- Exposed critical sensitive data leakage: plaintext crypto wallet seed phrase in public feedback API, admin OAuth credentials in unauthenticated config endpoint, and MD5 password hashes in JWT payloads
- Bypassed client-side file upload restrictions using Burp Suite request interception; documented missing security headers (CSP, HSTS) and exposed Prometheus metrics endpoint
- Delivered a 33-page professional pentest report with executive summary, CVSS-scored findings, screenshots, PoC steps, and a prioritized remediation roadmap

MEMBERSHIPS

International Information System Security Certification Consortium (ISC2) *January 2026 – Present*
Junior Chamber International (JCI) *January 2025 – Present*