Joshua Hynes

Nairobi, Kenya| Phone number: +25479302249 |email: hynesjoshua3@gmail.com
LinkedIn: www.linkedin.com/in/joshua-hynes-8b7833314

Aspiring Information Security Analyst

Electrical & Electronic Engineer turned information security analyst with a robust foundation in critical systems and a recent, intensive specialization in cybersecurity. Passionate about applying a methodical, analytical, and security-first mindset, honed in high-stakes engineering environments, to protect digital assets and ensure compliance. Eager to contribute to Monzo's mission by securing financial systems and customer data.

Technical Skills

- **Security Domains:** Governance, Risk & Compliance (GRC), Vulnerability Management, Incident Response, Cloud Security, Identity & Access Management (IAM), Web Application Security, Cyber Threat Intelligence (CTI), PCI DSS, Penetration Testing, Digital Forensics.
- **Cloud & Tools:** AWS (WAF, IAM, CloudTrail), Splunk, Wazuh (SIEM), Burp Suite, Metasploit, VirtualBox/VMware, Packet Tracer, OpenBAS.
- **Programming & Scripting:** Python (for Cybersecurity & Engineering), C/C++.
- **Operating Systems & Networking:** Linux & Windows System Administration, TCP/IP, DNS, DHCP, HTTP/S, Subnetting, Firewall Configuration.
- **Frameworks & Standards:** PCI DSS, NIST, Shared Responsibility Model, Cloud Auditing.

Hands-On Cybersecurity Projects

Web Application Penetration Test: Uber.com | Moringa School | 2025

- Conducted an authorized, ethical penetration test on a replica of the Uber.com web application to identify security vulnerabilities.
- Utilized **Burp Suite** to intercept and analyze HTTP/S traffic, discovering and exploiting injection flaws and cross-site scripting (XSS) vulnerabilities.

- Documented the attack methodology, evidence of exploitation, and provided a detailed report with actionable remediation strategies, demonstrating a thorough understanding of the OWASP Top 10.

Vulnerability Assessment & Exploitation: Metasploitable3 | Moringa School | 2025

- Deployed and configured the intentionally vulnerable **Metasploitable3** virtual machine in a isolated lab environment.
- Used **Nmap** for comprehensive network enumeration and service discovery to identify open ports and running services.
- Leveraged the **Metasploit Framework** to research, select, and execute exploits against identified vulnerabilities, successfully gaining unauthorized access to highlight critical security misconfigurations.

Incident Response Tabletop Exercise: Akira Ransomware | Moringa School | 2025

- Participated in a simulated ransomware crisis using the **OpenBAS** platform, mimicking a real-world attack by the Akira ransomware group.
- Executed the NIST Incident Response lifecycle: acted swiftly to **contain** the threat by isolating affected systems, **eradicated** the ransomware, and began recovery procedures.
- Collaborated with a team to analyze IoCs (Indicators of Compromise), document the incident timeline, and present lessons learned to improve the security posture against future attacks.

Education & Certifications

Moringa School | Nairobi, Kenya
Cybersecurity Bootcamp | Feb 2025 - Oct 2025

- Comprehensive training aligned with CompTIA Security+ objectives. Gained hands-on experience in security tools, threat analysis, and defensive techniques.
- **Key Skills:** SIEM (Splunk, Wazuh), Python for Security Scripting, Linux Administration, Vulnerability Management, Firewall Configuration, Cryptography, Network Security.

CompTIA Security+ (Scheduled) | Expected Nov 2025

Jomo Kenyatta University of Agriculture and Technology (JKUAT)
Bachelor of Science, Electrical and Electronic Engineering | Sep 2019 - Jan 2025

- **Relevant Coursework:** Critical Systems Design, Problem-Solving, Complex System Analysis, C/C++ & Python for Engineering Applications, Embedded Systems, IoT.

Cybersecurity Simulations & Certifications

Deloitte Australia - Cyber Job Simulation (Forage) | Aug 2025

- Analyzed a modern IT environment to identify security gaps and vulnerabilities.
- Developed a prioritised risk assessment and proposed mitigation strategies to enhance the security posture.

Mastercard - Cybersecurity Job Simulation (Forage) | Aug 2025

- Conducted a forensic analysis of a security incident to identify the attack vector and scope of impact.
- Formulated and documented an incident response plan to contain and eradicate the threat.

Tata - Cybersecurity Analyst Job Simulation (Forage) | Aug 2025

- Performed log analysis and triaged security alerts to distinguish false positives from genuine threats.

Other Certifications: Cloud Audit Academy – Cloud Agnostic (AWS) | Introduction to AWS WAF (AWS) | Foundation Level Threat Intelligence Analyst (arcX) | Trusted AI Safety Expert (TAISE)

Professional Experience

Intern | KenGen Kenya | Naivasha, Kenya | Jan 2023 - Apr 2023

- **Applied Rigorous Processes:** Executed strict testing and preventive maintenance protocols on high-voltage transformers and grid systems, understanding the criticality of reliability and safety in essential infrastructure—principles directly transferable to maintaining system integrity in a financial context.
- **System Monitoring:** Monitored a complex, live grid system, developing a keen eye for anomalies and deviations from baseline operations, a skill analogous to monitoring SIEM alerts and network traffic.

Intern | Prowatt Enterprises | Nairobi, Kenya | Jan 2022 - Apr 2022

- **Precision & Documentation:** Designed electrical panels and created detailed installation documentation, emphasizing accuracy, adherence to standards, and clear audit trails—directly relevant to creating and maintaining clear security policies and compliance evidence.

- **Risk Assessment:** Conducted load calculations and energy audits to identify and mitigate risks of system failure, demonstrating a proactive approach to risk management.