MARK CIIRA MUNYIRI

Cybersecurity Specialist | IT Risk & Compliance | Security Operations

mmunyiri12@gmail.com | +254 790 489 482 | LinkedIn | Github | Tech_Blog | Nairobi, Kenya

PROFESSIONAL SUMMARY

Results-driven Cybersecurity Specialist with hands-on experience in Security Operations within a regulated banking environment covering 1,500+ endpoints and servers. Core monitoring experience is delivered through the Kaspersky Security Center EDR/EPP console, providing continuous endpoint threat visibility, malware detection, and patch compliance tracking across the bank's infrastructure. Skilled in cyber risk assessment, vulnerability identification, incident response, and security compliance aligned with ISO 27001 and regulatory prudential guidelines. Supplemented by Splunk SIEM study through TryHackMe labs. Experienced in collaborating with SOC, Risk, and IT teams to safeguard information assets, drive vulnerability remediation, and maintain audit-ready documentation. Committed to advancing cybersecurity governance, awareness, and resilience in a regulated financial environment.

CORE COMPETENCIES

Cyber Risk Assessment & Management | Kaspersky Security Center EDR/EPP (Live Production) | Vulnerability Management & Patch Compliance

Incident Response & Containment | Phishing & BEC Investigation | Security Posture Reporting | Splunk SIEM (TryHackMe Labs)

Regulatory Compliance (ISO 27001, Prudential Guidelines) | Log Analysis (Windows Event Logs, Firewall, EDR Telemetry) | Stakeholder Engagement

WORK EXPERIENCE

Cybersecurity Analyst – Security Operations | Ariel Technology Limited | Deployed to Family Bank*May 2025 – Present*

Nairobi, Kenya | Regulated Banking Environment | 1,500+ Endpoints & Servers

- Assess cybersecurity risks and exposures within a regulated banking environment, aligning endpoint security posture with the bank's risk appetite and applicable regulatory frameworks.
- Maintain and update risk and incident records, conducting forward-looking threat identification through daily EDR monitoring and vulnerability tracking via Kaspersky Security Center.
- Conduct continuous real-time endpoint security monitoring via the Kaspersky Security Center EDR/EPP console, detecting threats, malware activity, suspicious processes, and unauthorized software across 1,500+ endpoints and servers.
- Perform incident triage and root cause investigation, correlating Windows Event Logs, firewall logs, and Kaspersky EDR telemetry to reconstruct incident timelines and determine scope.
- Support phishing and Business Email Compromise (BEC) investigations, identifying malicious links, attachments, and social engineering tactics targeting bank employees.
- Monitor endpoint patch compliance and vulnerability exposure through Kaspersky Security Center, flagging unpatched or misconfigured systems and coordinating remediation with IT teams.
- Administer Kaspersky Security Center — maintaining agent connectivity, protection status, and tool health to ensure continuous endpoint visibility across the banking environment.
- Prepare and maintain detailed incident documentation and ticketing records, supporting audit requirements and regulatory compliance reporting in line with prudential guidelines.
- Collaborate with SOC, Risk, and IT teams on remediation of identified vulnerabilities and incidents, escalating high-priority issues within defined SLAs.
- Actively developing Splunk SIEM skills through structured TryHackMe labs covering log ingestion, alert correlation, and dashboard creation.

IT Support Intern | Ariel Technology Limited *January 2025 – May 2025*

Nairobi, Kenya

- Assisted in security monitoring and log analysis, supporting incident investigations and evidence gathering.

- Supported vulnerability assessments and endpoint security checks, identifying misconfigurations and patch gaps.
- Participated in incident response activities including data collection, log review, and compliance documentation.
- Assisted in enforcing secure configurations and IT security policies across endpoints and network devices.
- Led digital invoicing system transition, reducing processing errors by 25% and improving data accuracy by 15%.

PERSONAL PROJECT

Xtracker – Secure Web Application | Personal Project *2024*

- Built Xtracker, a Python (Django) expense tracker implementing relational database models, user-based data access controls, and secure backend design using Django ORM.

EDUCATION

BSc. Telecommunication and Information Technology *Expected: 2026*

Kenyatta University, Nairobi, Kenya

CERTIFICATIONS

- ISC2 Certified in Cybersecurity (CC) – Learner ID: 0d93c011-36d5-461d-a39e-4c4c5fb2b7e4
- Cisco Ethical Hacker – CyberShujaa 2025 Cohort (Cert No. CS2025-RO2508240733101626)
- CompTIA Security+ – In Progress
- ALX Back-End Web Development Certificate
- TryHackMe – SIEM (Splunk), Firewall Fundamentals, Penetration Testing Labs

TECHNICAL SKILLS

- EDR & Endpoint Security: Kaspersky Security Center (live production) — threat monitoring, agent administration, patch compliance, health checks, malware investigation
- SIEM: Splunk — studied via TryHackMe labs; actively developing toward production proficiency
- Security Tools: Nmap, Burp Suite, Metasploit, Wireshark, Sophos, Fortinet
- Risk & Compliance: ISO 27001, OWASP Top 10, PCI-DSS awareness, Prudential Regulatory Guidelines
- Log Analysis: Windows Event Logs, Firewall Logs, EDR Telemetry
- Incident Response: Full lifecycle — Preparation, Detection, Analysis, Containment, Eradication, Recovery
- Networking: TCP/IP, DNS, HTTP/HTTPS, SSL/TLS, subnetting, routing, NAT
- Operating Systems: Linux (Ubuntu, Kali Linux), Windows
- Cloud: AWS, Azure (fundamentals)
- Scripting: Python, Bash

REFEREES

Samwel Wamui – Cybersecurity Engineer, NTT Data
+254 0799 691 925 | Samwel.Wamui@nttdata.com

Emmanuel Simiyu Wamalwa – Software Engineer, Family Bank Limited
+254 711 695 072 | dr.mmash53@gmail.com