BRIAN JAMES OWALA

SOC Analyst | Cybersecurity Analyst

Nairobi, Kenya | brianowala231@gmail.com | LinkedIn | GitHub

SUMMARY

SOC Analyst with hands-on experience gained through self-directed security labs, successfully preventing, detecting, investigating, and responding to 100% of simulated threats. Skilled in threat detection, analysis, and incident response using Microsoft Sentinel, Splunk, and Microsoft XDR, with a proven track record built through hands-on labs.

CORE SKILLS

- KQL Queries
- Microsoft Sentinel
- Microsoft Defender XDR
- Threat Investigation & Incident Response
- Detection Engineering (Sigma Rules)
- Vulnerability Management
- Threat Emulation (Atomic Red Team)
- Malware Analysis (Static & Dynamic)
- SIEM & Log Analysis (Splunk, Elastic Stack)
- Phishing & Network Analysis (Wireshark, SPF/DKIM/DMARC)
- MITRE ATT&CK & Cyber Kill Chain
- Risk Assessment
- Risk Management
- Security Analysis
- Information Security
- Open Source Intelligence
- Analytical Skills
- Research
- Communication
- Team Work

PROJECTS

Datacom Cybersecurity Job Simulation — *Forage*

August 19, 2026

- Completed a simulation focussed on how Datacom's cybersecurity team helps protect its clients
- Investigated a cyberattack and produced a comprehensive report documenting findings and outlining key recommendations to improve a client's cybersecurity posture
- Conducted a comprehensive risk assessment

SOC Analyst Simulation — *TryHackMe*

- Investigated real-world security incidents in a simulated SOC environment — analyzing logs, detecting threats, and responding to cyberattacks using SIEM and EDR tools to contain and resolve incidents end to end.

SSH Brute-Force Detection & Threat Hunting — *Splunk*

- Analyzed 1,200+ authentication events in Splunk using custom SPL queries, built two dashboards that surfaced top source/destination IPs and compromised accounts to accelerate brute-force detection.

Threat Simulation & Detection Engineering — *Atomic Red Team, Sigma, Elastic, Sysmon*

- Simulated two WannaCry ransomware techniques in PowerShell using Atomic Red Team, detected the activity via Aurora EDR and Sysmon telemetry, then authored and validated a custom Sigma rule in Elastic Stack to close the detection gap.

Phishing Email Analysis — *EML Analyzer, VirusTotal*

- Triaged a suspected phishing email using EML Analyzer, extracted a malicious domain and IP from embedded links and confirmed both as threats via VirusTotal.

HTTP Traffic Analysis — *Wireshark*

- Reviewed 2,000+ packets in Wireshark, filtered HTTP GET/POST traffic and identified two anomalous POST requests exfiltrating unusually large data volumes.

Vulnerability Assessment — *Nessus*

- Scanned a Windows 10 VM, analyzed findings by severity and exploitability, and prioritized remediation steps for the highest-risk vulnerabilities.

GitHub: github.com/jamese345

CERTIFICATIONS

- Microsoft Security Operations Analyst Associate (SC-200)
- TryHackMe — Security Analyst Level 2 (SAL2)
- TryHackMe — Security Analyst Level 1 (SAL1)
- Qualys Vulnerability Management Certificate

EDUCATION

Bachelor's Degree in Information Technology

Multimedia University of Kenya | Sep 2021 – Jun 2025