John Kasonga – SOC Analyst Portfolio (Detailed, 2025)

Fort Worth, TX | 617-849-1247 | johnkasonga0572@outlook.com
LinkedIn: https://www.linkedin.com/in/john-kasonga-4ab914148/ | GitHub: https://github.com/JKASONGA1

Summary

SOC Analyst with hands-on experience building a SOC lab environment, implementing SIEM solutions, and responding to simulated incidents. Adept at using Splunk, Security Onion, and Wireshark for monitoring, correlation, and threat detection. Skilled in creating dashboards, detection rules, and runbooks to streamline SOC operations.

Core Skills

- SIEM: Splunk (SPL queries, dashboards, correlation searches), Security Onion (Zeek/Suricata)
- Threat Detection & Monitoring: Log normalization, event correlation, alert triage, anomaly detection
- Networking: TCP/IP, DNS/HTTP, TLS, ports/protocols, packet capture and analysis with Wireshark
- SOC Processes: Incident escalation, ticketing workflows, KPI reporting, playbook development
- Tools: Kali Linux, OpenVAS, Metasploit, Nmap, Git/GitHub

Detailed Projects

TDIR-SBN (Threat Detection & Incident Response – Small Business Network): Designed a simulated enterprise network with Windows servers, Linux machines, and Security Onion. Built Splunk dashboards (radial gauges, geo-maps, anomaly detections) and detection rules for brute-force attacks, suspicious DNS, and HTTP POST floods. Authored IR runbooks and an executive summary report.

Windows & Apache Log Monitoring – VSI vs JobeCorp: Collected and analyzed Windows Security logs and Apache web logs. Correlated multi-source data in Splunk, created alerts for brute-force patterns and unusual HTTP verbs, and demonstrated SOC visibility improvements.

MegaCorpOne – C2 Detection: Simulated C2 beaconing with periodic callbacks. Detected JA3/SNI anomalies in Splunk, built detections for beaconing traffic patterns, and developed a hunt notebook for SOC use.

Threat Hunting with Zeek + Sigma: Imported malicious PCAPs (beacons, exfil), formed 3 hypotheses (DNS tunneling, JA3 anomalies), converted into Sigma rules and scheduled detections, and produced a findings report.