John Kasonga – Incident Response (IR) 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

Incident Response analyst with practical lab experience simulating phishing, malware, and AD attacks. Strong knowledge in evidence collection, containment strategies, and MITRE ATT&CK; mapping. Experienced in creating IR playbooks and after-action reports that bridge technical and executive audiences.

Core Skills

- Incident Handling: Threat hunting, forensic evidence collection, incident documentation
- Forensics: Basic malware analysis, log correlation, packet capture review
- Playbook Development: Containment, eradication, recovery, lessons learned
- Tools: Splunk, GoPhish, Responder, Metasploit, Kali Linux, Wireshark, Wazuh/Sysmon
- Frameworks: MITRE ATT&CK;, NIST IR guidelines

Detailed Projects

Phishing Email Simulation & Analysis: Developed GoPhish campaigns with realistic email templates and landing pages. Captured user interactions, performed payload analysis, and monitored Splunk for unusual HTTP referrers and user-agent anomalies. Produced an IR report including click/open rates, evidence handling, and user awareness recommendations.

Active Directory Pentest (Internal Lab): Conducted Kerberoasting, Responder LLMNR spoofing, and SMB enumeration attacks. Collected artifacts, cracked service tickets with Hashcat, and mapped anomalies to Splunk detections. Wrote a purple-team style IR report with containment and mitigation recommendations.

Linux Hardening & Auditing (BSC): Strengthened PAM policies, enforced password complexity, and restricted sudoers to least privilege. Conducted audits of users/groups, validated secure baselines, and documented changes with logs and screenshots.

Ransomware Simulation & Containment: Simulated early-stage ransomware with Atomic Red Team/Caldera; detected shadow copy deletion attempts via Sigma+Sysmon; auto-contained with Wazuh active response; verified backups and restore RPO/RTO, with timeline and metrics.