Habib Garba

mustaphahabib2@gmail.com | linkedin.com/in/habibmg | github.com/Cyberbibs

Cybersecurity Analyst *with hand-on experience in SIEM (Microsoft Sentinel, Splunk), EDR (Defender, CrowdStrike), and cloud security (Azure, AWS). Skilled in threat detection, incident response, vulnerability management, data loss prevention and Zero Trust IAM with Microsoft Entra ID. Proven ability to implement DLP policies using Microsoft Purview and align security programs with NIST CSF, SOC2, MITRE ATT&CK, and ISO 27001 standards.*

CORE COMPETENCIES

- **SIEM:** Microsoft Sentinel, Splunk
- **EDR:** Microsoft Defender for Endpoint, CrowdStrike
- **Threat Detection & IR:** KQL, MITRE ATT&CK, IOC/TTP Analysis, Threat Hunting
- **Vulnerability Management:** Nessus, Qualys, Defender Vulnerability Management
- **IAM:** Microsoft Entra ID, MFA, Conditional Access, RBAC, SSO
- **DLP:** Microsoft Purview (Cloud & On-Premises)
- **Cloud Security:** Azure Security Center, Defender for Cloud
- **Compliance:** NIST CSF, ISO 27001, SOC 2, CIS Benchmarks
- **Network Security:** TCP/IP, DNS, DHCP, Firewalls, IDS/IPS, Wireshark, Nmap
- **Automation & Scripting:** PowerShell, Bash, and basic python
- **SOAR:** Azure Logic Apps, Playbooks, ServiceNow, Cortex XSOAR
- **Soft Skills:** Analytical Thinking, Diligence, Communication, Teamwork, Reporting, Adaptive Learner, Willingness to learn.

EXPERIENCE

Cybersecurity Analyst at **Cyblack, Remote** (May 2025 - Present)

- Monitored and triaged security alerts in Microsoft Sentinel, Defender XDR, and EDR tools, detecting and escalating threats that reduced incident response time by 15%.
- Analyzed phishing emails and malware to identify threats, mitigate impact, and educate users on security risks.
- Deployed and tuned ASR rules in Microsoft Defender, reducing endpoint compromise risks.
- Enforced Zero Trust access controls using Conditional Access and RBAC, cutting unauthorized access attempts by 20%.
- Designed and implemented DLP policies in Microsoft Purview, preventing sensitive data exfiltration across email, Teams, and SharePoint.
- Designed and implemented DLP policies in Microsoft Purview, preventing sensitive data exfiltration across email, Teams, and SharePoint.
- Automated detection and response workflows via Logic Apps and playbooks, reducing manual triage efforts by 15%.

IT/Customer Support Specialist(Contract) at **Fusion CX, Montreal, CA** (May 2025 - Present)

- Monitored and triaged security alerts in Microsoft Sentinel, Defender XDR, and EDR tools, detecting and escalating threats that reduced incident response time by 15%.
- Analyzed phishing emails and malware to identify threats, mitigate impact, and educate users on security risks.
- Deployed and tuned ASR rules in Microsoft Defender, reducing endpoint compromise risks.

Information Security Specialist at **Guaranty Trust Bank, Lagos, Nigeria** (May 2025 - Present)

- Investigated and remediate security incidents flagged in Splunk, minimizing downtime and potential monetary impact.
- Analyzed malware and phishing attempts, applying containment and remediation to prevent breaches.
- Configured NGFW rules to block 95% of malicious traffic and unauthorized external access attempts.
- Monitored patch compliance across 500+ endpoints and servers, reducing vulnerabilities by 60%.
- Conducted threat intelligence research, improving detection and prevention configurations by 20%.

Customer Insight Analyst (Transaction Services) at **Guaranty Trust Bank, Lagos, Nigeria** (May 2025 - Present)

- Analyzed service data to identify workflow bottlenecks, improving operational efficiency by 15%.

EDUCATION

- Meng, Information Systems Security, Concordia University Montreal, CA Aug 2024
- Btech, Computer Science, Federal University of Technology, Minna, NG Oct 2011

CERTIFICATIONS

- Microsoft Certified Security Operations Analyst (SC-200)
- CompTIA Security+
- ISC^2 Certified in Cybersecurity
- CCNA Certification of Completion (Cisco NetAcad)