Habib Garba

+1 438-282-5910 | Toronto, ON (Open to Relocation)
mustaphahabib2@gmail.com | linkedin.com/in/habibmg | github.com/cyberbibs

Professional Summary

Cybersecurity Analyst experienced in security operations, incident response, and threat detection across cloud, network, and endpoints. Proficient in Microsoft Sentinel, Defender XDR, DLP, and vulnerability management, with a proven track record of reducing risks and strengthening security posture. Skilled in compliance audits, endpoint security, and user awareness training, combining technical expertise with strong problem-solving and communication skills

Education

- MEng, Information Systems Security, Concordia University Montreal, CA Oct 2024

  Key Modules Include: Malware Defense and Application Security, Cryptographic protocols and Network Security, Operating systems security, Security Evaluation Methodologies (Threat Modeling)
- BTech, Computer Science, Federal University of Technology, Minna, NG Oct 2016

Experience

Cybersecurity Analyst at **Cyblack, United Kingdom (Remote)** (May 2025 – August 2025)

- Monitored and triaged security alerts in Microsoft Sentinel, Defender XDR, and EDR tools; detected and escalated threats, reducing incident response time by 15%.
- Investigated phishing emails and malware, mitigating risks and educating users on security awareness.
- Deployed and tuned Attack Surface Reduction (ASR) rules in Microsoft Defender to minimize endpoint compromise.
- Enforced Zero Trust access controls with Conditional Access and RBAC, decreasing unauthorized access attempts by 20%.
- Designed and implemented Data Loss Prevention (DLP) policies in Microsoft Purview, preventing data exfiltration across email, Teams, and SharePoint.
- Developed and delivered cybersecurity awareness training with Vivida to address human factors in security.

IT/Customer Support Specialist (Contract) at **Fusion CX, Montreal, CA** (Nov 2022 – Feb 2023)

- Delivered frontline technical and customer support via phone, handling 30 + inquiries daily with high satisfaction ratings.
- Documented incidents and service requests in the ticketing system (ServiceNow), ensuring accurate tracking and follow up.

Junior Cybersecurity Analyst at **Guaranty Trust Bank, Lagos, Nigeria** (Mar 2021 – Aug 2022)

- Assisted in monitoring and analyzing security alerts across endpoints, networks, and cloud environments, escalating critical incidents to senior analysts.
- Conducted vulnerability assessments using tools like Qualys and Microsoft Defender, identifying and reporting potential security weaknesses.
- Supported patch management and remediation efforts to reduce exposure to vulnerabilities and maintain compliance standards.
- Participated in incident response activities, including malware analysis, phishing investigations, and containment measures.
- Documented incidents, prepared detailed reports, and contributed to internal knowledge base articles to improve security operations efficiency.
- Collaborated with IT teams to implement endpoint protection, DLP policies, and security best practices, reducing organizational risk
- Assisted in performing security audits and compliance checks, ensuring adherence to company policies and industry regulations.

Customer Service Rep (Transaction Services) at **Guaranty Trust Bank, Lagos, Nigeria** (June 2019 – Feb 2021)

- Resolve customers' complaints promptly by using Microsoft Dynamic Software (CRM) which has led to recommendations.
- Advised customers on fraud related issues and assisted customers in setting up and managing mobile/internet

banking.

Help Desk Technician at **New Planet Projects Ltd., Abuja, Nigeria** (June 2017 – Feb 2019)

- Provided technical support for 200+ end users, resolving hardware, software, and network issues (DNS, DHCP, TCP/IP) with a 95% first-call resolution rate.
- Administered Active Directory and Azure Active Directory, including account provisioning, password resets, and access control, ensuring secure and efficient operations.
- Supported Microsoft 365 / Office 365 applications (Outlook, Teams, SharePoint, OneDrive), improving collaboration and reducing recurring support requests by 20%.
- Delivered remote and onsite support using RDP and TeamViewer maintaining a high customer satisfaction rating.
- Monitored endpoint security tools and applied cybersecurity best practices to strengthen device protection and reduce risks.

Key Achievements

- Reduced incident response time by 15% through effective monitoring, triaging, and escalation of security alerts in Microsoft Sentinel, Defender XDR, and EDR tools.
- Prevented sensitive data exfiltration by designing and implementing Data Loss Prevention (DLP) policies across Microsoft Purview (Email, Teams, SharePoint).
- Enhanced endpoint security by deploying and tuning ASR rules in Microsoft Defender, significantly reducing compromise risks.
- Developed and delivered cybersecurity awareness training using Vivida, increasing user understanding of phishing, malware, and human factors in security.
- Achieved high customer satisfaction by providing frontline IT support and troubleshooting for 200+ users, maintaining a 95% first call resolution rate.
- Reduced repeat support tickets by 15% through documentation, knowledge base creation, and end user training.
- Supported compliance and audit readiness by assisting in ISO 27001, SOC 2, and internal security audits.

Core Competencies

- Security Operations and Incident Response (SIEM/XDR – Microsoft Sentinel, Splunk, Defender XDR, EDR)
- Threat Detection, Phishing Analysis, Malware Analysis, and Incident Escalation (MITRE ATT&CK Framework)
- Log Analysis and Security Monitoring across endpoints, networks, and cloud environments
- Vulnerability Management and Patch Remediation (Nessus, Qualys, Microsoft Defender)
- Endpoint Security and Zero Trust Access Controls (ASR, RBAC, Conditional Access)
- Data Loss Prevention (Microsoft Purview – Email, Teams, SharePoint)
- Identity and Access Management (Active Directory, Azure Active Directory, Intune, SCCM)
- Governance, Risk, and Compliance (ISO 27001, SOC 2, Security Audits, Compliance Checks)
- Incident Documentation, Security Reporting, and Knowledge Base Development
- Cybersecurity Awareness and End User Training (Vivida)
- IT Support and Customer Service (ServiceNow, Microsoft 365)
- Soft Skills: Analytical problem solving, collaboration, communication, adaptability, attention to details

Certifications

- CompTIA Cysa+ - In progress
- Microsoft Certified Security Operations Analyst (SC-200) 2025
- CompTIA Security+ 2024
- ISC^2 Certified in Cybersecurity 2024
- CCNA Certification of Completion (Cisco NetAcad) 2016

Memberships

- **Member, (ISC)² –** International Information System Security Certification Consortium 2024- present