ALI CHISOM

Cybersecurity Analyst | CySA+ Certified

Contact

Phone: +234 902 4676 339
Email: contact@alichisom.com
LinkedIn: https://linkedin.com/in/ali-chisom-7266021aa
Portfolio: https://alichisom.com/
GitHub: https://github.com/PwnPoint
Badge: https://www.credly.com/badges/e13e56ad-9778-42be-8ffe-ac8b41db3d61/public_url

PROFILE

Security analyst with hands-on experience in monitoring, threat hunting, incident triage, and hardening internet-facing systems. Comfortable moving between logs, endpoints, and network traffics—then writing clear findings that engineers can act on. Strong foundation from systems/network administration, which helps me spot misconfigurations and operational gaps early.

Certification

- GREM Certification (in progress) Expected Q4 2026
- CompTIA CySA+ (Certified) | 2026
- CompTIA Security+ | 2021
- Cisco CCNA | 2020

Skills

- **Managements:** Vulnerability Management, Threat Management, Risk Management
- **Detection & Analysis:** Vulnerability Analysis, Threat Intelligence, Threat hunting, log analysis, malware analysis (static + behavioral), SIEM, EDR
- **Incident Response:** End-to-end triage, digital forensics, attack chain reconstruction
- **Infrastructure & Hardening:** Vulnerability assessment (Nessus), web server hardening, network security
- **Scripting:** Python, PowerShell, Bash (automation, config management)
- Reporting And Communication

Experience

Cybersecurity Analyst

BcKash Cooperative / Microfinance Bank (Promoted)
Full-time | June 2025 – Present

- Executed vulnerability assessments and provided security control recommendations.
- Monitored web and system logs to identify repeated probes, abnormal requests, and signs of automated scanning and Fuzzing.
- Detected and investigated suspicious activity end-to-end — from initial request patterns down to what the attacker is trying to execute.
- Wrote detailed incident reports that explained what happened, why it mattered, and how to fix it without complicating things.
- Worked on hardening systems after investigations (closing exposed endpoints, improving configurations, **reducing attack surface by 60%**).
- Tracked attack patterns and reused them to improve detection and response over time.
- Detected and analyzed a coordinated attack campaign against a web server with over **20000 automated requests** and confirmed no compromise after validating controls and configurations
- Investigated exposed infrastructure caused by misconfiguration and documented how sensitive files like environment configs and database dumps could be accessed without authentication.
- Reviewed compromised server artifacts showing active malware execution, web shell presence, and command injection behavior in a real incident.

Junior Cybersecurity Analyst

BcKash Cooperative / Microfinance Bank *(Nigerian fintech cooperative)*
Full-time | Sept 2023 – May 2025

- Performed vulnerability assessments using Nessus, identifying and categorizing over 10 critical and high-severity vulnerabilities and supporting risk-based remediation prioritization.
- Reviewed alerts, checked logs, and separated real issues from false positives.
- Supported phishing investigations by tracing attachments, payloads, and user activity.
- Conducted vulnerability checks and followed up on remediation until issues were resolved.
- Documented findings clearly so others could follow the same process during similar incidents.
- Developed malware analysis capability through hands-on investigation of suspicious files, identifying behavioral indicators and execution patterns

System and Network Administrator

Phamatex Industries Limited *(Pharmaceutical company)*
Full-time | Oct 2021 – Aug 2023

- Managed systems, user accounts, permissions, and routine maintenance (patching, backups, access reviews).
- Handled network setup and troubleshooting — including switching, VPN issues, and connectivity problems.
- Identified and fixed risky configurations (open services, weak permissions, exposed directories).
- Supported daily operations while taking on security-related responsibilities.

Selected Projects (Real Work)

Network Automation Script

- Developed a Python-based automation script used to log into network devices and push configuration updates automatically, reducing the time needed to manage multiple switches.

  Project_Link

Malware Analysis – Phishing Dropper Campaign

- Investigated a phishing attack delivering a disguised invoice that led to a staged malware infection.
- Traced the infection chain from archive → disk image → executable → persistence script.
- Identified how the malware created persistence through startup scripts and maintained communication with a remote server.
- Documented indicators of compromise including dropped files, network traffic, and persistence mechanisms.

  Project_Link

Ransomware Analysis – A.E.S.R.T

- Analyzed encryption behavior, persistence methods, and system impact of a ransomware sample.
- Observed how it encrypted files, appended extensions, and removed recovery options like shadow copies.
- Mapped its behavior to attack techniques and documented how it spreads and executes.

  Project_Link

Ransomware Analysis – 7ev3n-HONE$T

- Studied how ransomware spreads through phishing, executes, and modifies files across systems.
- Identified persistence through registry keys and file renaming activity across drives.
- Documented file artifacts, network indicators, and recovery considerations.

  Project_Link

PowerShell Infostealer Analysis (Credential & Wallet Theft)

- Analyzed an obfuscated PowerShell-based malware performing system profiling and data exfiltration.
- Observed anti-analysis behavior such as process checks and environment validation before execution.
- Identified how it searches for browser and desktop cryptocurrency wallets and sends data to remote servers.
- Documented command-and-control communication patterns and payload execution behavior.

Project_Link

Security Incident Investigation – Compromised Server

- Reviewed artifacts from a real server compromise involving malware, botnet activity, and remote command execution.
- Identified web shells, payload downloads, and attacker-controlled infrastructure.
- Reconstructed the attack chain from initial access to persistence and post-exploitation use.

Project_Link

Education

Federal Polytechnic Oko, Anambra State

National Diploma (OND) – Computer Science

Tools

Nessus, Wireshark, Nmap, Burp Suite, PE analysis tools, debuggers, IDA, SIEM, EDR, WAF, IDS/IPS