ALI CHISOM JOSHUA

SOC Analyst | Cybersecurity Engineer | Malware Analyst
+234 902 4676 339 | contact@alichisom.com
LinkedIn | Portfolio | GitHub

PROFESSIONAL PROFILE

Defensive-focused cybersecurity professional with hands-on experience in SOC operations, malware analysis, incident response, and enterprise system administration across real production environments. Proven ability to investigate security incidents, analyze live malware samples, extract actionable IOCs, and implement network and endpoint defenses using Splunk, EDR, FortiGate firewalls, Active Directory, and Linux/Windows systems. Strong background in malware reverse analysis (static & dynamic), detection engineering (YARA, Snort), and security automation using C++, Python, Bash, and PowerShell. Comfortable operating in fast-paced environments, supporting incident response, and improving detection capability through practical tooling and analysis.

CORE TECHNICAL SKILLS

Security Operations & Blue Team
SOC Monitoring & Alert Triage • Incident Response • Digital Forensics • Malware Analysis (Static & Dynamic) • Threat Hunting • IOC Extraction • Detection Engineering

Detection & Monitoring
SIEM (Splunk) • YARA • Snort • Log Correlation • Network Traffic Analysis (Wireshark) • MITRE ATT&CK Mapping

Infrastructure & Network Security
FortiGate Firewalls • IDS/IPS • VPN • NAT • Active Directory • Windows Server • Linux Administration • Backup & Disaster Recovery

Cloud & Virtualization
AWS (EC2, IAM) • Azure VMs • VMware • VirtualBox • Hyper-V

Scripting & Programming
Python • Bash • PowerShell • C++ (Windows API, defensive tooling)

Others
Teamwork • Problem solving and decision making • Communication • Professionalism

PROFESSIONAL EXPERIENCE

Cybersecurity Engineer & Systems Administrator

Quantum Konet Services — Full-time
Aug 2025 – Present

- Delivered cybersecurity and IT infrastructure services for small-to-mid-size organizations (250+ users), covering network security, system administration, and secure deployment of on-premise and cloud environments.
- Improved security posture through vulnerability remediation, firewall hardening, and access control enforcement across client environments.
- Conducted recurring vulnerability assessments and security hardening across client networks, servers, and endpoints, identifying and remediating 10–25 misconfigurations per environment, including exposed services, weak access controls, and insecure firewall rules.
- Designed, implemented, and maintained FortiGate firewall policies, IDS/IPS controls, VPNs, and segmented network architectures using VLAN, significantly reducing unauthorized access paths and attack surface.
- Investigated live malware incidents involving persistence, lateral movement, and suspicious C2 traffic; performed triage, forensic analysis, IOC extraction, containment, and system recovery across Windows endpoints.
- I administered Windows servers, domain controller, backups, and recovery processes to ensure availability and operational resilience.
- Analyzed and classified multiple real-world malware samples across different families, extracting indicators and behaviors to support detection and response.
- Provided security awareness and technical training to clients and junior engineers, improving secure system usage and early incident reporting.

Malware Analyst / SOC Analyst

Freelance
Jan 2025 – Present

- Performed static and dynamic malware analysis using FLARE VM and REMnux to identify execution flow, persistence mechanisms, and C2 behavior.
- Extracted IOCs (hashes, domains, IPs, registry keys) and mapped malware behavior to MITRE ATT&CK techniques.
- Developed and tested Splunk detection queries and YARA/Snort rules mapped to MITRE ATT&CK techniques to detect analyzed malware samples and similar variants in lab environments.
- Produced technical analysis reports for SOC and blue-team use.

Cybersecurity Analyst / System Administrator

Phamatex Industries Limited — Full-time
Oct 2023 – Aug 2025

- Monitored and correlated network and endpoint logs across 50+ endpoints, identifying malware infections, policy violations, and anomalous behavior using SIEM and packet analysis tools.
- Configured and maintained firewalls and endpoint protection, strengthening the organization’s security posture.
- Conducted vulnerability assessments, patch management, and security audits, reducing exposure to known threats and misconfigurations.
- Developed and enforced cybersecurity policies and procedures aligned with internal governance and data protection requirements.
- Led security awareness training for 20+ staff, improving phishing detection and reporting of suspicious activity.
- Maintained and supported Windows and Linux servers, ensuring uptime, performance, and reliability of business-critical services.
- Administered Domain Controller, Group Policy, DNS, and DHCP
- Implemented backup, disaster recovery, and system hardening procedures to improve resilience and reduce recovery time.
- Automated routine administrative and security tasks using PowerShell and Bash, reducing manual effort and configuration errors.
- Proactively ‘hunt’ for potential threat actors on the network and provide recommendations
- Work with other groups to ensure continuity and coverage of the enterprise
- Develop, operationalize and contribute to core Cyber Security and Data Protection functions including but not limited to SOC and Incident Response
- Analyzes and assesses vulnerabilities in the infrastructure (software, networks) and provide recommendations
- Investigates available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices
- Analyzes and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions

Networking & Cybersecurity Instructor

Cyclobold
May 2023 – Oct 2023

- I delivered hands-on training in networking and cybersecurity aligned with industry fundamentals.
- Led practical labs covering firewalls, threat analysis, network security, and ethical hacking concepts.

- Mentored students on cybersecurity career paths, tools, and professional ethics, supporting entry into technical roles.

SELECTED PROJECTS

- *Analyzed a trojan loader sample exhibiting registry persistence and outbound C2 over HTTPS; extracted IOCs and authored a YARA rule to detect similar samples.*
- *Built Splunk detection dashboard to monitor suspicious endpoint and network activity, including abnormal process execution, PowerShell abuse, failed authentication spikes, and outbound C2-like traffic patterns.*
- *Developed YARA rules based on extracted strings and behavioral indicators from analyzed malware samples; tested rules against benign and malicious datasets to reduce false positives.*
- *Investigated phishing emails that resulted in malware execution; analyzed the attachment, traced execution behavior, extracted IOCs, and documented mitigation recommendations.*
- *Investigated a malware outbreak affecting multiple endpoints; performed alert triage, isolated infected systems, extracted IOCs, and supported system recovery and post-incident review.*
- *Investigated a malware dropper that downloaded and executed a secondary payload; traced execution flow, persistence mechanisms, and network callbacks, and documented the full infection chain.*
- *Analyzed a credential-stealing malware targeting browser-stored credentials; identified process injection behavior, registry persistence, and outbound C2 traffic; extracted hashes, domains, and mutex indicators.*

Labs & Implementations

- Active Directory deployment and Group Policy management
- FortiGate firewall configuration (VPN, NAT, rule hardening)
- Linux server automation and containerized services
- Cloud infrastructure deployment (AWS EC2/IAM, Azure VMs)
- Network monitoring and security hardening using Wireshark
- Virtualized security labs (VMware, VirtualBox, Hyper-V)

EDUCATION

National Diploma (OND) – Computer Science
Federal Polytechnic Oko, Anambra State
2018 – 2021

LANGUAGES

English (Professional) • Igbo (Native)

ADDITIONAL

- Active contributor to open-source security research and tooling
- Continuous self-directed learning in malware analysis, SOC operations, and defensive security engineering