Silas Binitie

Email: silasbinitie54@gmail.com | Mobile: +2348145562682 | https://linkedin.com/in/silas-cybersec | Address: Delta, Nigeria

SUMMARY OF QUALIFICATIONS

- Hands-on experience simulating real-world SOC environments through advanced home labs
- Built and managed a complete blue team lab setup with Windows Server (AD DC), Kali Linux, Ubuntu SIEM, and Splunk
- Performed attack simulations (brute force, malware, lateral movement) and analyzed telemetry using Sysmon, Splunk, and Sigma rules
- Proficient in SIEM operations, log analysis, incident response, and endpoint security
- Used MITRE ATT&CK, threat intelligence, and custom detection rules to identify suspicious behavior
- Strong knowledge of Windows Event Logs, Linux logs, and Active Directory structure
- Confident with scripting in PowerShell and Python for automation and analysis
- Solid grasp of NIST CSF, CIS Controls, and SOC playbooks
- Multiple cybersecurity certifications proving industry readiness

AREAS OF EXPERTISE

- **SIEM & SOAR:**
  Splunk Enterprise, Splunk SOAR, IBM QRadar, Sigma Rules, MITRE ATT&CK
- **Endpoint Security & EDR:**
  Velociraptor, Elastic EDR, Sysmon, Windows Event Forwarding, PowerShell Logging
- **Network Security & Monitoring:**
  Wireshark, Zeek, Suricata, pfSense (Firewall & VLAN), Nmap, Nessus
- **Threat Hunting & Incident Response:**
  KQL, YARA, OSQuery, IOC Analysis, Log Parsing (SPL, Python)
- **Malware Analysis:**
  Remnux, CyberChef, PEStudio, Cuckoo Sandbox
- **Infrastructure & Scripting:**
  Windows Server (AD, DNS, GPO), Kali Linux, Python, Bash, PowerShell
- **SIEM** – LogRhythm, Splunk/Splunk SOAR, IBM QRadar

EDUCATION

High School Graduate (2022) 2017-2022
Currently Self-Studying for Cybersecurity Degree

RELATED WORK EXPERIENCE

SOC Analyst / Blue Team Engineer (Home Lab) **Dec 2022 – Present**
Designed, deployed, and operated a full-scale cybersecurity operations center (SOC) home lab replicating real-world enterprise environments. Projects included:

- Built a full SOC lab with pfSense firewall, Windows Server (AD), Kali Linux, Ubuntu (SIEM), and Windows 10 endpoints
- Deployed and configured Splunk Enterprise, Sysmon, Winlogbeat, and MITRE ATT&CK-based detection rules
- Integrated Splunk SOAR for automated alert triage, threat intel enrichment, and endpoint

- Installed Velociraptor and Elastic EDR for endpoint visibility and response; created custom detection playbooks
- Analyzed malicious samples using Remnux**,** PEStudio, CyberChef, and Cuckoo Sandbox
- Captured and inspected traffic using Wireshark**,** Zeek, and Suricata; monitored network anomalies and IDS alerts
- Conducted threat hunting and built incident response reports with triage, root cause, and containment steps

CERTIFICATIONS

Certificate	**Month Obtained Year**
CompTIA CySA+ **(**In-Progress**)**	
CompTIA Security+ – (Studied)	
ISC2 Certified in Cybersecurity (CC) – (Certified)	*Apr 2025*
Google Cybersecurity Certificate – (Certified)	*Dec 2024*
Lets Defend SOC Analyst Path – (Certified)	*Jan 2025*
Try Hack Me SOC Analyst Path – (Certified)	*May 2024*
Active Directory Certificate – (Certified)	*June 2023*

WEBSITE

GitHub - Labs

https://github.com/slybdev

- SOC lab documentation, detection rules, incident reports, Splunk dashboards, and threat hunting guides about

TRAININGS

Title of training **Month Year Completion**

SOC Analyst Level 1 & 2 – Let's Defend

- Hands-on labs in SIEM monitoring, incident triage, malware analysis, and IR documentation

TryHackMe Blue Team Path

- Completed 20+ labs: Splunk, Packet Analysis, Windows Event Logs, Threat Hunting, Real-Time Defense