SAMSON IDOWU

Cybersecurity Engineer

+2347032844735 • mailtosamsoni@gmail.com • Abuja, Nigeria • linkedin.com/in/samson-idowu • samsonidowu.netlify.app

I help organizations see what is happening inside their environments before attackers do. My specialty is in building the detection and monitoring systems that give security teams real confidence in their coverage, not just checkbox compliance. I have designed and deployed SIEM solutions used by enterprises across cloud and on-premises platforms, written detection logic that has been adopted by over 100,000 security professionals worldwide, and consistently turned complex security requirements into infrastructure that works at scale. I thrive at the intersection of engineering and security strategy, and I bring the communication skills to translate both to any audience.

WORK EXPERIENCE

Security Engineer

Wazuh Inc., San Jose, USA (Remote) May 2023 – Present

- Engineered 200+ custom detection rules and decoders targeting MITRE ATT&CK tactics, including: lateral movement, credential access, and defense evasion, using PCRE/PCRE2 regex, improving high-fidelity alert coverage by 45% and reducing false positive rates by 30%.
- Architected multi-node Wazuh SIEM clusters across AWS and Azure environments, onboarding 50+ log sources including VPC Flow Logs, CloudTrail, Azure Activity Logs, and Sysmon for unified visibility across hybrid multi-cloud estates.
- Designed cloud security monitoring pipelines integrating AWS Security Hub, GuardDuty, and CloudTrail with Wazuh SIEM, enabling real-time detection of IAM privilege escalation, S3 bucket exposure, and unauthorized API calls.
- Developed CIS Benchmark Level 1 and 2 Security Configuration Assessment (SCA) policies for Linux, Windows, and macOS, automating compliance measurement across 1,000+ endpoints, reducing audit preparation time by 40%.
- Automated SIEM infrastructure provisioning using Terraform and Ansible, reducing deployment time from days to under two hours and cutting manual effort by 60%.
- Performed static and dynamic malware analysis, extracting IOCs (file hashes, C2 IPs, registry keys) and behavioral TTPs operationalized into detection rules and contributed to Wazuh's Cyber Threat Intelligence knowledge base.
- Contributed technical blogpost content and threat intelligence research adopted by over 100,000 security professionals worldwide.

Security Researcher

Innopolis University, Innopolis, Russia Aug 2022 – May 2024

- Conducted memory forensics investigations using Volatility3, extracting process injection, rootkit, and credential dumping artifacts from Windows and Linux memory dumps to reconstruct attacker timelines and support incident response at the Innopolis SOC project.
- Hardened AWS infrastructure by enforcing least-privilege IAM policies, enabling GuardDuty and Security Hub, and implementing VPC security group rules across EC2, EKS, and S3 workloads.
- Performed threat modeling on startup applications using STRIDE, identifying 25+ threat scenarios delivering remediation recommendations that improved application security architecture.
- Integrated SAST/DAST testing (Snyk, SonarQube, StackHawk) into CI/CD pipelines on GitHub Actions and Jenkins, reducing critical and high-severity vulnerabilities in deployed applications by 35%.
- Built botnets and offensive security test tools for penetration testing operations and research purposes.
- Performed malware analysis and threat intelligence operations, contributing to knowledge base within the Innopolis security and network engineering lab.

Infrastructure Security Engineer

Hardcore Biometric Systems, Abuja, Nigeria Nov 2021 – Jul 2022

- Deployed a centralized SIEM across 200+ servers and endpoints, ingesting Windows Event Logs, Syslog, firewall syslogs, and application logs — improving threat detection coverage and incident detection speed by 55%.
- Built and tuned SIEM correlation rules for high-priority use cases including brute-force, privilege escalation, and suspicious outbound traffic, reducing alert fatigue through iterative false positive tuning.
- Configured Suricata-based IDS/IPS with custom detection rule sets, integrating network alerts into the SIEM for centralized triage and automated incident ticketing.
- Automated server provisioning, security hardening, and application deployments using Terraform, Vagrant, Ansible, Jenkins, Kubernetes, and Docker, reducing deployment cycle time by 50% and enforcing consistent security baselines at scale.

- Investigated and responded to SIEM and IDS-surfaced incidents, performing root cause analysis, containment, and post-incident reporting, achieving a 98% SLA compliance rate.

Technical Support Engineer
Zeta-Web, Abuja, Nigeria Aug 2019 – Oct 2021

- Administered and hardened Linux and Windows systems aligned to CIS security baselines.
- Monitored enterprise infrastructure using PRTG Network Monitor and WhatsUp Gold, reducing network downtime by 35%.
- Maintained regular patch compliance across 400+ endpoints through structured vulnerability remediation cycles, measurably reducing the organization's exploitable attack surface.
- Enforced approved security baseline configurations on firewalls, load balancers, and proxies, reviewing change requests against security policy before approving production upgrades.

IT Technician
Multichoice, Port Harcourt, Nigeria Dec 2018 – Aug 2019

- Supported 300+ end users across LAN, WAN, and VSAT-connected environments.
- Resolved hardware, operating system, and enterprise application issues, reducing business downtime by 60%.
- Produced comprehensive IT procedure documentation covering incident workflows, network topology, and escalation paths, improving team response consistency.

SKILLS

- **Security Operations:** SIEM Engineering, Detection Engineering, Log Source Onboarding, Alert Tuning & Correlation, Identity & Access Management, Malware Analysis, Threat Intelligence, Incident Response, Digital Forensics
- **Security Frameworks:** STRIDE, MITRE ATT&CK, NIST 800-53, ISO 27001, PCI-DSS, CIS Benchmarks
- **SIEM, XDR & Monitoring:** Wazuh SIEM & XDR, Splunk, Microsoft Sentinel, FortiSIEM, NewRelic, ELK Stack, Shuffle SOAR, PRTG Network Monitor, WhatsUp Gold
- **Security Tools:** Caine Linux, Volatility3, Burp Suite, Nmap, Wireshark, Metasploit, Hashcat, OWASP ZAP, HashiCorp Vault
- **Automation & DevOps:** Terraform, Ansible, Docker, Kubernetes, GitHub Actions, Jenkins, Snyk, SonarQube, SAST/DAST, Dependency Scanning, Git
- **Networking:** Firewall configuration, OSPF, BGP, VPN, DHCP, DNS, VLAN, WLAN configuration, Cisco, Fortinet, Mikrotik, Ubiquiti, Checkpoint, Sophos
- **Cloud and Infrastructure:** AWS - GuardDuty, Security Hub, S3, Route53, Lambda, IAM, KMS, Secrets Manager, Config, CloudTrail, Shield/WAF, DynamoDB, VPC, EC2, RDS, EKS, VMware ESXi, HyperV, OpenStack
- **Programming & Scripting:** Python, PowerShell, Bash, Regex (PCRE/PCRE2), YAML, JSON
- **OS & Platforms:** Linux, Windows, macOS, AWS, Azure, GCP
- **Soft Skills:** Leadership, Communication, Cross-Functional Collaboration, Project Management, Research, Technical Writing

TRAINING & CERTIFICATIONS

- CISSP — In Progress
- AWS Certified Solutions Architect – Associate (Dec 2024)
- Certified Network Security Practitioner, SecOps Group (Nov 2024)
- Network Security Associate NSE 1, 2 & 3, Fortinet (Mar 2022)
- Microsoft Azure Fundamentals AZ-900 (Jul 2021) | Security, Compliance and Identity Fundamentals, Microsoft (Jul 2021)
- CompTIA Security+ (May 2021)

EDUCATION

M.Sc., Computer Science — Computer Security and Networks Aug 2022 – Jul 2024
Innopolis University, Innopolis, Russia

B.Eng., Computer Engineering Jan 2012 – Jun 2017
University of Uyo, Uyo, Nigeria

PROJECTS & PUBLICATIONS

GitHub: github.com/SamsonIdowu/projects-publications/blob/main/publications.md