Adaora Nwosu Senior Security Engineer

Kirkland, WA · adaora.nwosu@gmail.com · +1 425-555-0169 · linkedin.com/in/adaoranwosu

PROFILE SUMMARY

- **Senior Security Engineer** with **7 years** of experience securing **corporate identity, laptops and networks** at an **endpoint management software company** and a **healthcare provider**, specializing in **zero trust access and detection engineering**.
- Hands-on with **Okta** and **CyberArk** for identity, **Tanium** for endpoints, **Cloudflare Zero Trust** for access, **Splunk** for logs, **HashiCorp Vault** for secrets, and **Go**, **Python** and **Tines** for automation.
- Deep expertise in **device-trust sign-in**, **VPN replacement**, **detection as code** and **one-click response**, working to **NIST CSF 2.0** and **MITRE ATT&CK** so every new control has an owner and a test.
- Works with **IT**, **Infrastructure**, the **SOC** and **Legal**, leads security reviews for new internal systems, and sits on the **change advisory board** for anything that touches sign-in or the network.
- Mentors **2 security engineers**, owns the team's **detection catalog** and **zero trust runbook**, and holds the **CISSP**.

TECHNICAL SKILLS

Identity & SSO:	Okta (FastPass, Workflows), Microsoft Entra ID, CyberArk, YubiKey, SAML 2.0, OpenID Connect, SCIM
Vulnerability Scanning:	Qualys, Tanium Comply, CISA KEV, EPSS, CVSS 4.0
Endpoint & MDM:	Tanium, Microsoft Defender for Endpoint, Jamf Pro, Microsoft Intune, CIS Benchmarks
Firewalls & ZTNA:	Cloudflare Zero Trust, Palo Alto Networks, Tailscale, DNS filtering, DMARC
SIEM & Detection:	Splunk Enterprise Security, Cribl Stream, Sigma, MITRE ATT&CK, SPL
Cloud & Secrets:	AWS, Google Cloud, HashiCorp Vault, AWS KMS, AWS Secrets Manager
Languages, Automation & Frameworks:	Go, Python, Terraform, Tines, NIST CSF 2.0, HIPAA Security Rule

EDUCATION

NYU Tandon School of Engineering — **M.S. in Cybersecurity** — Brooklyn, NY · Sep 2017 to May 2019

ISC2 — **CISSP** — Seattle, WA · Apr 2023

WORK EXPERIENCE

Tanium — Senior Security Engineer — Kirkland, WA · Mar 2022 to Present

- Moved **2,400 employees** to passwordless sign-in with **Okta FastPass** and device trust checks, so only managed laptops can open company apps, and removed SMS and push MFA from every admin account.
- Enforced CIS Level 1 baselines through **Tanium** on 3,100 Windows, Mac and Linux machines, and got critical patches onto **96% of the fleet** within 7 days of release.
- Designed company access on **Cloudflare Zero Trust** for **180 internal apps**, retired the always-on VPN for all staff, and closed 9 admin panels that were reachable from the internet.
- Rebuilt the log pipeline with the SOC, routing Okta, CloudTrail, GitHub and endpoint data into **Splunk** through Cribl, and added 11 log sources while cutting ingest volume by **34%**.
- Wrote **Tines** stories and small Go tools that revoke Okta sessions and isolate a laptop in one click when a detection fires, cutting response time on account takeover from **45 minutes to 6**.

One Medical — Security Engineer — San Francisco, CA · Aug 2019 to Feb 2022

- Ran **Qualys** scanning for 1,200 servers and clinic workstations with fix deadlines by severity, and took open critical vulnerabilities from **240 to 38** before the yearly HIPAA risk assessment.
- Reviewed about **45 designs a year** for new patient-facing features and vendor integrations, writing the SSO, encryption and audit logging requirements engineering signed off before the build.
- Moved secrets for **60 services** from environment files into **HashiCorp Vault** with AWS KMS, and set 30-day rotation for every database credential with access to patient data.