DANIEL OKAFOR

CYBERSECURITY ANALYST

daniel.okafor@example.com • +1 555 0142 • Austin, TX, USA • LinkedIn • GitHub

PROFESSIONAL SUMMARY

Cybersecurity analyst with 5 years of experience in security operations and vulnerability management. Triaged 1,000+ alerts a month in Splunk, cut mean time to respond by 35% and closed 92% of critical vulnerabilities within 14 days. Holds Security+ and CySA+, and communicates risk clearly to engineers and executives.

EXPERIENCE

Cybersecurity Analyst, Meridian Financial Services — Mar 2022 – Present
Austin, TX

- Triaged 1,000+ monthly alerts in Splunk and escalated true incidents with clear timelines.
- Reduced mean time to respond by 35% by writing playbooks for phishing and malware cases.
- Ran weekly Nessus scans on 900 assets and drove 92% of critical findings to closure within 14 days.
- Led a phishing awareness programme for 1,200 staff, cutting click rates from 14% to 5%.
- Documented incidents and presented monthly risk reports to the CISO.

SOC Analyst I, Bluewater Managed Security — Jun 2020 – Feb 2022
Dallas, TX

- Monitored SIEM dashboards across 12 client networks in a 24x7 rotation.
- Investigated endpoint alerts with CrowdStrike and contained 40 infected machines.
- Tuned detection rules and reduced false positives by 28%.

SKILLS

SIEM (Splunk) | Incident response | Vulnerability management | Nessus | CrowdStrike | Wireshark | MITRE ATT&CK | NIST CSF | Python scripting | Firewalls | IAM | Threat hunting

EDUCATION

B.S., Information Systems Security, University of Texas at Dallas — 2016 – 2020
Dallas, TX | GPA 3.6

CERTIFICATIONS

CompTIA Security+, CompTIA — Sep 2020

CompTIA CySA+, CompTIA — Nov 2022

GIAC Certified Incident Handler (GCIH), GIAC — May 2024