Marcus Whitfield-Osei

Lead Cybersecurity Analyst | Cybersecurity Analyst | Network Security Technician

marcus.whitfieldosei@email.example • (703) 555-0136

PROFESSIONAL SUMMARY

Senior cybersecurity analyst and detection engineering lead with 12 years protecting federal and defense networks. Leads analysts through threat hunting, incident response and detection development, and builds programs aligned with NIST and agency requirements. CISSP certified with an active TS/SCI clearance.

PROFESSIONAL EXPERIENCE

Lead Cybersecurity Analyst

Mar 2020 — Present

Potomac Mission Systems · Arlington, VA

- Lead a team of eight analysts in a 24/7 security operations center supporting a federal agency, setting triage standards, escalation paths and training plans.
- Built a detection engineering process with version-controlled Splunk rules, peer review and test cases, raising true positive rates across major alert types.
- Led response to a targeted intrusion attempt on a public-facing application, containing access within hours and supporting the agency's required reporting.
- Automated common enrichment and containment steps in SOAR, letting tier 1 analysts close routine alerts faster and focus on investigations.

Cybersecurity Analyst

Jul 2016 — Feb 2020

Chesapeake Defense Solutions · Columbia, MD

- Hunted for threats in network and endpoint data using Zeek and Elastic, documenting findings mapped to MITRE ATT&CK for defense customers.
- Supported assessments against NIST 800-53 and 800-171 controls, writing evidence and remediation plans for contract requirements.
- Mentored four junior analysts through their first incident investigations and certification exams.

Network Security Technician

Jun 2012 — Jun 2016

Shenandoah Federal IT Services · Herndon, VA

- Monitored intrusion detection systems and firewall logs for a government customer network, escalating events according to defined procedures.
- Maintained network security documentation and supported annual security inspections and audits for the customer agency.

EDUCATION

BS, Cybersecurity and Information Assurance — Commonwealth Online University *2016*

SKILLS

Technical: Detection engineering, Threat hunting, Incident response leadership, Splunk Enterprise Security, Elastic, Network forensics, Zeek, MITRE ATT&CK, NIST 800-53, SOAR, Python, Analyst mentoring

Certifications: CISSP · GIAC Certified Intrusion Analyst (GCIA) · CompTIA Security+