Maria Okafor

maria.okafor@example.com | (555) 010-0162 | Arlington, VA
U.S. citizen | Security clearance: Secret (current)

SUMMARY

Information security specialist with two years at the GS-9 level and three years in a health-care contractor’s security team. Monitors logs, runs vulnerability scans and tracks findings to closure, and writes security plan documentation under the NIST Risk Management Framework.

WORK EXPERIENCE

IT Specialist (INFOSEC), GS-2210-09
Department of Veterans Affairs, Office of Information and Technology, Washington, DC
07/2023 – Present | 40 hours per week

- Reviewed firewall and Windows event logs in Splunk every working day and reported suspected incidents to the security operations center within the one-hour reporting window.
- Ran monthly Tenable Nessus scans across 420 servers and tracked each finding to closure with system owners in a plan of action and milestones (POA&M).
- Reduced open high-severity findings from 61 to 18 in nine months by sending owners a weekly list sorted by age and agreeing fix dates with each one.
- Drafted and updated control descriptions in the system security plans for three systems under the NIST Risk Management Framework.
- Prepared test results, diagrams and evidence for two Assessment and Authorization (A&A) packages that received an authorization to operate.
- Wrote two standard operating procedures for patch verification and trained two new analysts to follow them.
- Checked weekly that patches were applied on 420 servers and raised a ticket with the owner of each server that missed the patch window.
- Reviewed new user access requests against the access policy and returned incomplete requests to supervisors with the missing approval named.
- Took part in two incident response exercises, recording each step in the incident log and drafting the after-action notes.

Information Security Analyst
Cardinal Health Partners, Washington, DC
06/2020 – 06/2023 | 40 hours per week

- Monitored security alerts for 1,800 user accounts and closed or escalated each alert under the company’s incident procedure.
- Updated access control lists after staff transfers and documented each change for the quarterly access review.
- Answered questions from users and system owners about account access rules and closed 95% of tickets within the two-day service target.
- Ran quarterly phishing-awareness reports for 1,800 users and sent each department head a list of staff who had not completed training.
- Configured endpoint protection policies for 600 laptops and documented each policy change for the change board.

Help Desk Technician (part-time)
George Mason University, Information Technology Services, Fairfax, VA
09/2017 – 05/2020 | 20 hours per week

- Reset passwords, unlocked accounts and set up laptops for students and staff, logging each request in the ticket system.
- Wrote short how-to guides for the three most common requests, which the help desk added to its self-service page.

EDUCATION

George Mason University, Fairfax, VA
Bachelor of Science, Information Technology, 05/2020, GPA 3.4

CERTIFICATIONS

CompTIA Security+, 10/2021

TRAINING

Splunk Fundamentals 1, 04/2022 | Federal Information Security Awareness, annual, latest 10/2025

TOOLS

Splunk, Tenable Nessus, Microsoft Defender, ServiceNow, PowerShell