Aisha Rahman

Security Engineer
Washington, DC · aisha.rahman@example.com · (202) 555-0145 · LinkedIn · GitHub

SUMMARY

Security engineer with 7 years in detection, incident response and cloud security on AWS. Cut mean time to detect from hours to under an hour with new detections, ran the vulnerability program for 25 cloud accounts, and led the technical work for a clean SOC 2 Type II audit. CISSP.

EXPERIENCE

Security Engineer — Ironbark Software

Washington, DC · May 2022 – Present

- Built 60 Splunk detection rules for cloud attack techniques mapped to MITRE ATT&CK, cutting mean time to detect from 9 hours to 40 minutes.
- Ran vulnerability management for 25 AWS accounts, bringing the median time to fix critical findings from 34 to 7 days.
- Led the technical work for SOC 2 Type II, building 45 controls and passing the audit with no exceptions.
- Rolled out phishing-resistant MFA with hardware keys to 700 employees, with no successful account takeovers in the 18 months since.

Security Analyst — Fairmont Systems Group

Arlington, VA · Jun 2019 – Apr 2022

- Triaged about 120 alerts a week in the SOC and led response on 15 confirmed incidents, including a ransomware attempt stopped before encryption.
- Wrote Python scripts that enriched alerts with asset and user data, cutting average triage time by 35%.
- Ran quarterly phishing simulations for 1,200 staff, lowering the click rate from 14% to 4%.

SKILLS

Security: Detection engineering, incident response, threat modeling, vulnerability management, AWS security

Tools: Splunk, CrowdStrike Falcon, Wiz, Burp Suite, Okta

Frameworks: SOC 2, NIST CSF, ISO 27001, MITRE ATT&CK

Scripting: Python, Bash, SQL, Terraform

CERTIFICATIONS

Certified Information Systems Security Professional (CISSP), 2024

AWS Certified Security – Specialty, 2023

CompTIA Security+, 2019

EDUCATION

B.S. Cybersecurity, George Mason University, 2019

Fictional example by FindAJobAI: the person, employers and numbers are invented.