Ashar S. Ahmed

Information Security Analyst | U.S. Citizen | ashar@aahmed.org | GitHub

SUMMARY

Information security analyst with 3+ years owning day-to-day security operations, monitoring, and incident response across cloud and endpoint environments. Hands-on with CrowdStrike Falcon EDR/XDR (configuration, threat hunting, alert triage, response), AWS security services (IAM, GuardDuty, CloudTrail, Security Hub, Config), and the Microsoft 365 security suite (Defender, Purview, Intune, Secure Score). Builds AI security governance programs covering LLM risk, acceptable-use policy, and shadow-AI. Frameworks-driven (NIST CSF, ISO 27001); strong at translating technical risk into business language. CISSP, AWS-certified.

TECHNICAL SKILLS

Endpoint / EDR-XDR: CrowdStrike Falcon (administration, threat hunting, IR), Wazuh, MDM, endpoint hardening
Cloud Security: AWS (IAM, GuardDuty, Security Hub, CloudTrail, Config, VPC, S3, CloudWatch), Azure, Terraform, Checkov (policy-as-code)
Microsoft 365: Defender for Endpoint, Purview, Intune, Secure Score, Exchange Online, Conditional Access
Detection / SIEM: Log correlation pipelines, detection engineering, MITRE ATT&CK, Prometheus/Grafana/Loki, structured logging
AI Security: LLM risk assessment, AI acceptable-use & governance frameworks, shadow-AI, prompt injection & data-exfiltration mitigation
GRC / Risk: NIST CSF, ISO 27001, CIS Controls v8, Zero Trust (SP 800-207), vendor & third-party risk, vulnerability management & remediation tracking, security awareness training
Scripting: Python, PowerShell, Bash, SQL

PROFESSIONAL EXPERIENCE

Cyber Security Advisor, Dr. Shariq Mumtaz Medicine Professional Corporation **Jan. 2023 – Present**

- Sole security owner for a regulated healthcare practice: run day-to-day security operations, monitoring, and incident response across AWS cloud and a mixed macOS/Windows endpoint fleet
- Administer and optimize **CrowdStrike Falcon** EDR/XDR — configuration, alert triage, threat hunting, and response workflows; tuned detections to cut noise and accelerate containment
- Secure and administer **Microsoft 365** (Defender for Endpoint, Purview, Intune, Secure Score); enforced MDM baselines and DNS/email controls that reduced spam and unsolicited traffic by **80%**
- Built correlation-driven detection pipelines across identity, endpoint, and network telemetry; cut Mean Time to Detect (MTTD) from days to under **1 hour**
- Established an **AI acceptable-use policy and governance framework**; assessed generative-AI and copilot tools for data-handling, privacy, and shadow-AI risk
- Developed security policies and remediation SLAs aligned to NIST CSF / ISO 27001; ran vulnerability assessment and remediation tracking; produced KPI dashboards and metrics for leadership

Technical Contractor (AI Safety & Evaluation), Mercor Intelligence, San Francisco, CA **May 2026 – Present**

- Evaluate large language model outputs and failure modes for a frontier AI lab, including adversarial and misuse scenarios — directly informs AI threat modeling (prompt injection, model abuse, data exfiltration)
- Assess model behavior for accuracy, reasoning quality, and specification adherence across technical domains

Software Developer, Department of Industry, Canadian Digital Service **Feb. 2021 – Jan. 2022**

- Hardened AWS infrastructure (IAM, S3, DynamoDB, CloudWatch) via Terraform/Terragrunt; enforced policy-as-code scanning with Checkov across all modules
- Designed passive request validation that eliminated bot-driven abuse across all form endpoints without adding user friction
- Implemented CI/CD security and quality gates, raising code coverage from ~20% to **85%** and cutting client-reported data incidents from 4–5 to 1–2 per cycle; awarded the **Directors' General Award of Merit**

PROJECTS

Security Homelab & Detection Lab | GitHub

- Operate a self-built SIEM/SOC lab: Wazuh detection engineering with custom decoders/rules, automated response, Authelia SSO with context-aware MFA, and Zero Trust (SP 800-207) segmentation
- Instrumented full observability (Prometheus, Grafana, Loki, Alertmanager) with self-healing automation; mapped controls to NIST CSF and CIS Controls v8

EDUCATION

Master of Science (M.S.) Cybersecurity & Information Assurance | Western Governors University Awarded 2024
Bachelor of Computer Science (BCompSci) | Dalhousie University Awarded 2024

CERTIFICATIONS

Certified Information Systems Security Professional (CISSP) Awarded 2026
Systems Security Certified Professional (SSCP) Awarded 2023
AWS Certified Solutions Architect & Developer - Associate Awarded 2022