Ashar S. Ahmed

Security Engineer | U.S. Citizen | ashar@aahmed.org | GitHub

SUMMARY

Security engineer with 3+ years securing cloud infrastructure, containers, and CI/CD pipelines across fast-moving environments. Hands-on with cloud security (AWS, GCP), container/Kubernetes hardening, infrastructure-as-code security (Terraform/Checkov), SIEM and detection engineering (Wazuh), and DevSecOps "security as code." Comfortable building security programs from the ground up — IAM, vulnerability management, incident response, and compliance aligned to ISO 27001 / NIST CSF. AI/ML-aware, with experience assessing LLM risk and authoring AI governance. CISSP, AWS-certified.

TECHNICAL SKILLS

Cloud Security: AWS (IAM, GuardDuty, Security Hub, CloudTrail, Config, VPC, S3), GCP (IAM, org policy), Azure
Containers / **IaC:** Docker & Kubernetes hardening, image scanning (Trivy), Terraform, Checkov (policy-as-code), runtime/baseline controls
DevSecOps / **CI-CD:** GitHub Actions security gates, dependency & secret scanning, security-as-code automation (Python, PowerShell, Bash)
Detection / **SIEM:** Wazuh (custom decoders/rules), detection engineering, IDS/network telemetry, MITRE ATT&CK, Prometheus/Grafana/Loki
IAM / **Zero Trust:** SSO, context-aware MFA, least-privilege access, Zero Trust (SP 800-207)
Incident Response: detection, triage, containment, remediation, post-incident review
Compliance / **GRC:** ISO 27001, NIST CSF, CIS Controls v8; SOC 2 & GDPR control mapping; vendor/third-party risk, security awareness training
AI / **ML Security:** LLM risk assessment, AI acceptable-use & governance, prompt injection & data-exfiltration mitigation

PROFESSIONAL EXPERIENCE

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

- Sole security owner for a regulated practice: run day-to-day security operations, monitoring, and incident response across AWS cloud and a mixed macOS/Windows fleet
- Built and tuned SIEM detection pipelines (Wazuh, custom decoders/rules) correlating identity, endpoint, and network telemetry; cut Mean Time to Detect (MTTD) from days to under **1 hour**
- Automated security tasks in Python/PowerShell/Bash — endpoint hardening, patch cadence, and compliance reporting across a distributed fleet; standardized baselines cut unsolicited traffic by **80%**
- Led incident response end to end (detection → containment → remediation) with post-incident reviews; managed IAM least-privilege access and remediation SLAs
- Established an **AI acceptable-use policy and governance framework**; assessed generative-AI and copilot tools for data-handling, privacy, and shadow-AI risk
- Authored security policies and KPI dashboards aligned to ISO 27001 / NIST CSF; translated technical risk into business reporting for leadership

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

- Embedded security into CI/CD: enforced policy-as-code scanning (Checkov) across all Terraform/Terragrunt modules provisioning AWS infrastructure (IAM, S3, DynamoDB, CloudWatch)
- Built automated 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
- Designed passive request validation that eliminated bot-driven abuse across all form endpoints without adding user friction; awarded the **Directors' General Award of Merit**

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/ML threat modeling (prompt injection, model abuse, data exfiltration)

PROJECTS

Security Homelab & Containerized SOC | GitHub

- Operate a self-built SIEM/SOC on a Dockerized, IaC-managed stack: Wazuh detection engineering with custom decoders/rules and automated response, hardened container baselines, and image scanning
- Zero Trust (SP 800-207) segmentation, SSO with context-aware MFA, and full observability (Prometheus, Grafana, Loki, Alertmanager) with self-healing automation; controls mapped 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