Ashar S. Ahmed

Security Engineer, Detection & Cloud Security | CISSP | Canadian & U.S. Citizen
ashar@aahmed.ca | github.com/asharahmed | linkedin.com/in/asharsahmed

Profile

Security engineer (CISSP) in detection engineering, cloud security, and vulnerability management, with a software-development background spanning Terraform-managed AWS, SIEM/EDR detection logic, and full-stack and iOS applications. Built and run the security and privacy program for a PHIPA-regulated medical practice, and delivered secure, policy-as-code AWS infrastructure for the Government of Canada.

Technical Skills

Security Operations / Detection: SIEM alert triage (Wazuh), EDR/DFIR investigation, log correlation, alert tuning, detection logic (SQL, regex), MITRE ATT&CK mapping, IR playbooks, threat modeling
Vulnerability Management: CVE triage, validation/prioritization, scanner integration (Snyk, Trivy, Dependabot), remediation coordination, evidence collection, compliance tracking
IAM / Endpoint Security: MFA, macOS/Windows hardening, FileVault, patch compliance, MDM policy enforcement, DNS filtering
Cloud / IaC: AWS (IAM, S3, DynamoDB, CloudWatch, CloudTrail), Azure (Defender for Cloud), Terraform, Terragrunt, Checkov, Docker, Kubernetes
Scripting / Automation: Python, PowerShell, Bash, JavaScript/TypeScript
Languages / Frameworks: C#, .NET, Blazor, Node.js, Swift/SwiftUI, SQL, PL/SQL
AI / LLM: LLM application development (Claude/OpenAI APIs), prompt engineering, agentic automation, LLM/prompt-injection security
Compliance: NIST CSF, ISO 27001-aligned controls, PHIPA-oriented controls, audit documentation, control evidence workflows

Professional Experience

Cyber Security Advisor Jan. 2023 - Present
Dr. Shariq Mumtaz Medicine Professional Corporation (PHIPA-regulated medical practice)

- **Built and run the full security & privacy program** for a PHIPA-regulated medical practice (risk register, remediation SLAs, prioritized roadmap, and KPI reporting)
- Centralized identity, endpoint, and network logging where none existed and built alerting on anomalous access and sign-ins, cutting **mean-time-to-detect from days to under an hour**
- Authored custom **Wazuh** decoders and **MITRE ATT&CK**-mapped rules (T1110 brute force, T1595 scanning, T1078 valid accounts) for log sources Wazuh can't parse natively, correlating repeated auth failures into credential-stuffing alerts that fired on real attempts against internet-exposed services
- Standardized all **9 managed endpoints** on **MFA, full-disk encryption (FileVault/BitLocker), EDR, DNS filtering, and enforced patching**, reaching **100% policy compliance** with zero unmanaged devices
- Scripted automation in Python, PowerShell, and Bash for endpoint configuration, telemetry collection, and compliance reporting across the macOS/Windows fleet; cut unsolicited inbound traffic (firewall-blocked connections, malicious DNS queries, and spam) by **80%**
- Implemented and **restore-tested 3-2-1 backups** to cut ransomware recovery risk; authored PHIPA-aligned policies, a breach-response plan, and audit evidence, and ran security reviews of EMR/IT vendors handling PHI

Technical Contractor (AI / LLM Security Evaluation) May 2026 - Present
Mercor Intelligence, San Francisco, CA (Remote)

- Evaluate large language model outputs for technical correctness and for security/safety failures such as prompt injection and unsafe tool use; deliver structured feedback used in model training

Software Developer, Government of Canada Feb. 2021 - Jan. 2022

Innovation, Science & Economic Development Canada (ISED) *Feb. - Oct. 2021*

- Designed passive request validation that eliminated bot-driven abuse on public form endpoints without adding user friction, while increasing detection coverage
- Produced security runbooks adopted org-wide across delivery teams
- Awarded the **Directors' General Award of Merit** for delivery impact on national spectrum operations

Canadian Digital Service (CDS) *Oct. 2021 - Jan. 2022*

- Engineered secure AWS infrastructure (IAM, S3, DynamoDB, CloudWatch) via Terraform/Terragrunt; enforced policy-as-code scanning with Checkov across all modules
- Extended the passive anti-abuse validation across the platform's form endpoints, sustaining low-friction protection and detection coverage
- Added automated testing and CI/CD checks, raising code coverage from ~20% to **85%**; reduced client-reported data incidents from 4-5 to 1-2 per cycle

Software Developer Intern Sept. 2020 - Dec. 2020
National Research Council of Canada (NRC)

- Developed full-stack Oracle Database applications powering research data pipelines across multiple NRC divisions
- Engineered PL/SQL stored procedures and SQL-based automation to replace manual workflows, eliminating ~10 hrs/week of manual processing

Projects & Publications

Ravelin: Vulnerability SLA & Compliance Tracker getravelin.xyz

- Built a vendor-neutral platform that ingests findings from Dependabot, Snyk, and Trivy, assigns severity-based remediation SLAs, and tracks breaches with full history and compliance reporting
- *Stack:* C#, .NET 10, Blazor, Azure, Azure DevOps, Docker, Terraform, SQL Server

QR-CLI | *TypeScript, Node.js, Commander, qrcode* qr-cli.dev

- Built and published a cross-platform CLI that generates QR codes as ASCII art with PNG export, works fully offline, released under MIT on npm and GitHub

Tally Habit Tracker | *Swift/SwiftUI, SwiftData, WidgetKit, CloudKit* tally.aahmed.ca

- Built and published a privacy-first iOS habit tracker with three habit types, flexible scheduling, streak heatmaps, Live Activities, inline notification actions, and Google Reminders import; zero telemetry, no third-party SDKs

The Cyber Centre and Technologies: A Meta-Analysis | *Accepted, Canadian Military Journal (forthcoming)*

- Authored an accepted meta-analysis on the Canadian Centre for Cyber Security, reviewing open-source literature on how it runs threat intelligence and protects critical infrastructure

Education

Western Governors University Awarded 2024
Master of Science (M.S.), Cybersecurity & Information Assurance

Dalhousie University 2018 - 2024
Bachelor of Computer Science (BCompSci)

Certifications

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