Ashar S. Ahmed

LinkedIn | GitHub | ashar@aahmed.ca | +1 (647) 328-3346
Canadian and U.S. Citizen

SUMMARY

Security operations professional with hands-on detection engineering, alert triage, and vulnerability remediation experience across hybrid on-prem and cloud environments. Led endpoint monitoring, incident response playbook development, and compliance evidence collection in a boutique healthcare practice and federal settings. Writes detection logic with SQL, regex, and query-based systems; automates security operations with Python, PowerShell, and Bash.

PROFESSIONAL EXPERIENCE

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

- Built endpoint and identity monitoring workflows with structured alert triage, correlating activity across identity, endpoint, and network contexts — reducing MTTD from days to under 1 hour
- Designed and tuned detection logic for anomalous access patterns using log analysis, regex-based pattern matching, and event correlation across multiple data sources
- Implemented MFA, FileVault, patching cadences, and MDM controls across the full endpoint fleet; maintained security baselines and audit-ready documentation for compliance reviews
- Authored incident response playbooks, investigation templates, and remediation tracking workflows aligned with PHIPA/PIPEDA requirements
- Coordinated vulnerability validation, prioritization, and closure with leadership and external IT vendors, supporting evidence collection and remediation timelines

Software Developer — Oct. 2021 – Jan. 2022
Canadian Digital Service (Treasury Board of Canada Secretariat, 1-year term appointment)

- Engineered secure AWS infrastructure (IAM, S3, DynamoDB, CloudWatch) for Terraform/Terragrunt deployments with Checkov policy-as-code scanning
- Built Python/Flask bot-abuse detection controls, analyzing request patterns and tuning thresholds to reduce false positives while maintaining detection accuracy
- Produced security runbooks and incident-support documentation adopted org-wide, standardizing response procedures

Software Developer — Feb. 2021 – Oct. 2021
Department of Industry (ISED, 1-year term appointment)

- Decomposed a monolithic application into service-based components, reducing incident blast radius and improving production reliability
- Implemented CI quality gates and automated testing, increasing code coverage from ~20% to 85% and reducing production defect rates
- Awarded the **Directors' General Award of Merit** for critical delivery impact on national spectrum operations

Software Developer Intern (Co-op) — 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

QR-CLI | Open-Source Developer Tool | qr-cli.dev

- Built and published a cross-platform CLI tool (Node.js) generating QR codes as ASCII art with PNG export; fully offline, released under MIT license on npm/GitHub

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 (Cyber Centre), synthesizing open-source sources on threat intelligence operations, detection capabilities, and critical infrastructure protection

EDUCATION

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

CERTIFICATIONS

Systems Security Certified Professional (SSCP)	Awarded 2023
AWS Certified Solutions Architect - Associate	Awarded 2022
AWS Certified Developer - Associate	Awarded 2022
Associate of ISC2 (CISSP Exam Passed)	Awarded 2025

TECHNICAL SKILLS

SecOps / Detection: SIEM alert triage, EDR investigation, log correlation, alert tuning, detection logic (SQL, regex), incident response playbooks, threat modeling
Vulnerability Mgmt: CVE triage, vulnerability validation/prioritization, remediation coordination, evidence collection, compliance closure tracking
IAM / Endpoint: MFA, macOS/Windows hardening, FileVault, patch compliance, MDM policy enforcement, endpoint baselines, DNS filtering
Cloud / IaC: AWS (IAM, S3, DynamoDB, CloudWatch, CloudWatch Logs, CloudTrail), Azure (Defender for Cloud), Terraform, Terragrunt, Checkov, Docker, Kubernetes
Scripting / Automation: Python, PowerShell, Bash, JavaScript/TypeScript
Compliance: ISO 27001, SOC 2, PHIPA, PIPEDA, audit documentation, control evidence workflows