

ASHAR S. AHMED

Security Engineer, Detection & Cloud Security | CISSP | Canadian & U.S. Citizen
(647) 328-3346 | ashar@aaahmed.ca | github.com/asharahmed | linkedin.com/in/asharsahmed

Skills

Automation: Docker, Kubernetes, Terraform, Terragrunt; Bash, CI/CD, C#, JavaScript, .NET, Policy-as-Code, PowerShell, Python, TypeScript
Cloud: AWS, Azure, Entra ID, Microsoft 365; Administration, Compliance, Conditional Access, IAM, Logging, MFA, Monitoring, Networking, Security
Security: Checkov, Defender for Cloud, Defender for Endpoint, Defender XDR, Dependabot, Sentinel, Snyk, Trivy, Wazuh; Alert Tuning, Detection Engineering, EDR, Incident Response, KQL, MITRE ATT&CK, SIEM, Threat Modeling, Vulnerability Management, XDR
Systems: Intune, Linux, macOS, Windows; Backup, BitLocker, DHCP, DNS Filtering, FileVault, Firewall, Hardening, Patching, VPN
Compliance: ISO 27001, NIST CSF, PHIPA

Experience

Information Security Officer

Jan. 2023 - Present

Dr. Shariq Mumtaz Medicine Professional Corporation

- Built the practice's security and privacy program from scratch where no formal controls existed, producing audit-ready evidence: risk register, PHIPA-aligned policies, breach-response plan, restore-tested 3-2-1 backups, and vendor security reviews
- Administered the site's IT infrastructure end to end: Windows and macOS servers and endpoints, firewall and router configuration, and DNS, DHCP, and VPN services
- Deployed Microsoft Sentinel as the practice's SIEM, ingesting identity, endpoint, and email signal through Microsoft Defender XDR connectors where logs were previously uncollected, reducing mean-time-to-detect from days to under an hour
- Engineered custom detection content mapped to MITRE ATT&CK (T1110 brute force, T1595 scanning, T1078 valid accounts) as Sentinel analytics rules in KQL and Wazuh decoders, correlating repeated authentication failures into credential-stuffing alerts that fired on real attempts
- Standardized endpoints and identities on Microsoft Defender for Endpoint, Microsoft Intune, and Microsoft Entra ID with Conditional Access and MFA, plus full-disk encryption, DNS filtering, and enforced patching; automated configuration and compliance checks in Python, PowerShell, and Bash

Software Developer

Feb. 2021 - Jan. 2022

Government of Canada (ISED & Canadian Digital Service), Ottawa, ON

- Designed passive request validation that eliminated bot-driven abuse on public form endpoints without adding user friction, and rolled it out across all public-facing forms
- Engineered secure AWS infrastructure (IAM, S3, DynamoDB, CloudWatch) via Terraform/Terragrunt; enforced policy-as-code scanning with Checkov across all modules
- Added security and quality checks to CI/CD (automated testing, policy-as-code scanning), cutting client-reported data incidents from 4-5 to 1-2 per cycle and raising test coverage from ~20% to 85%
- Developed and maintained public-facing departmental web applications; recognized with the Directors' General Award of Merit

Software Developer Intern

Sep. 2020 - Dec. 2020

National Research Council Canada

- Wrote Oracle SQL and PL/SQL and built applications on Oracle Application Express (APEX) and Oracle Platform Apps
- Built an Oracle APEX tool to sanitize and pipeline data from a legacy system into a modern platform as part of a data-migration project

Certifications

Certified Information Systems Security Professional (CISSP) (ISC) ²	2026
CompTIA Cybersecurity Analyst (CySA+) CompTIA	2024
Systems Security Certified Practitioner (SSCP) (ISC) ²	2023
AWS Certified Solutions Architect – Associate Amazon Web Services	2022
AWS Certified Developer – Associate Amazon Web Services	2022

Education

M.S., Cybersecurity & Information Assurance Western Governors University	2024
B.Sc., Computer Science Dalhousie University	2018 – 2024