Ashar S. Ahmed

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

SUMMARY

IT Security Engineer with a strong Windows engineering background, securing Windows platforms and endpoints in fast-moving environments. Hands-on with integrated Windows security technologies — application control (AppLocker/WDAC), host-based firewalls, audit policy and event monitoring, and BitLocker disk encryption — plus endpoint security and vulnerability management (CrowdStrike EDR, AV/anti-malware, vulnerability scanning, patch management). Well-versed in Windows core infrastructure (Active Directory, Entra ID, PKI), OS hardening, privileged access management, and threat TTPs. Strong PowerShell automation. CISSP, AWS-certified.

TECHNICAL SKILLS

Windows Security: OS hardening (CIS benchmarks), AppLocker/WDAC application control, Windows Defender Firewall, audit policy & event monitoring, BitLocker disk encryption
Endpoint & Vulnerability Mgmt: CrowdStrike Falcon EDR/XDR, antivirus/anti-malware, vulnerability scanning & prioritized remediation, patch management
Windows Infrastructure: Active Directory (GPO, OU, hardening), Entra ID (conditional access, identity), PKI / certificate management
Identity & Access: Privileged access management (PAM), least-privilege, MFA, Zero Trust (SP 800-207)
Detection & Threats: SIEM (Wazuh), MITRE ATT&CK TTPs, threat hunting, incident response
Scripting / **Automation:** PowerShell (primary), Python, Bash; security-as-code, intelligent workflow automation
Cloud / **Frameworks:** AWS (IAM, GuardDuty, CloudTrail, Config), Azure; NIST CSF, ISO 27001, CIS Controls v8

PROFESSIONAL EXPERIENCE

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

- Secure and harden a distributed Windows (and macOS) fleet: enforced CIS-aligned baselines, AppLocker/WDAC application control, Windows Defender Firewall policy, audit logging, and BitLocker disk encryption via MDM
- Administer CrowdStrike Falcon EDR/XDR and AV/anti-malware; drive vulnerability scanning, prioritized remediation, and patch-management cadence across the estate
- Manage Windows core infrastructure and identity — Active Directory / Entra ID access, PKI certificate issuance and renewal, and privileged access management with least-privilege
- Automate security workflows in **PowerShell** (and Python/Bash) for endpoint configuration, telemetry collection, and compliance reporting; standardized baselines cut unsolicited traffic by **80%**
- Built SIEM detection (Wazuh) mapped to MITRE ATT&CK TTPs across identity, endpoint, and network telemetry; cut Mean Time to Detect from days to under **1 hour** and led incident response
- Designed, tested, and documented strategic security controls; provided technical advice and remediation prioritization to leadership

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

- Automated infrastructure security as code (PowerShell, Terraform/Terragrunt) with policy-as-code scanning (Checkov) across AWS; enforced auditable IAM and logging controls
- 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**

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

- Investigate large language model failure modes and adversarial/misuse scenarios for a frontier AI lab — informs threat research and detection of emerging attack techniques

PROJECTS

Windows Security Homelab & Detection Lab | GitHub

- Operate a self-built, Windows-hosted security lab: PowerShell automation for endpoint hardening, firewall configuration, and certificate renewal; Wazuh detection engineering mapped to MITRE ATT&CK
- Zero Trust (SP 800-207) segmentation, PKI/SSO with context-aware MFA, and full observability (Prometheus, Grafana, Loki) with self-healing automation; controls mapped to CIS Controls v8 / NIST CSF

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