[First] [Last]

Security Engineer, Detection & Cloud Security | CISSP | Canadian & U.S. Citizen
[email redacted] | [GitHub redacted] | [LinkedIn redacted]

Profile

Security engineer (CISSP) focused on detection engineering, cloud security, and vulnerability management. Built and run the security and privacy program for a regulated (PHIPA) healthcare practice, and delivered secure, policy-as-code AWS infrastructure for a national-government client. Day-to-day work in SIEM detection logic, AWS, and Python/PowerShell automation.

Technical Skills

Security / Detection: SIEM triage (Wazuh), EDR/DFIR investigation, log correlation, alert tuning, detection logic (SQL, regex), MITRE ATT&CK mapping, IR playbooks, threat modeling, CVE triage & remediation (Snyk, Trivy, Dependabot)
IAM / Endpoint: 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
Languages / Automation: Python, PowerShell, Bash, JavaScript/TypeScript, C#, .NET, Blazor, Node.js, Swift/SwiftUI, SQL, PL/SQL
Compliance / GRC: NIST CSF, ISO 27001 & PHIPA-aligned controls, audit evidence workflows

Professional Experience

Security & Privacy Consultant Jan. 2023 - Present
Small PHIPA-Regulated Healthcare Practice

- Built the practice's security & privacy program from scratch to protect PHIPA-regulated patient records and prove compliance under audit: risk register, PHIPA-aligned policies, a breach-response plan, **restore-tested 3-2-1 backups**, and vendor security reviews
- Centralized identity, endpoint, and network logging into a single **SIEM** where none existed, 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) to catch attacks on internet-facing services that off-the-shelf tooling missed, correlating repeated auth failures into credential-stuffing alerts that fired on real attempts
- Standardized every managed endpoint on **MFA, full-disk encryption, EDR, DNS filtering, and enforced patching** to close off the main routes to patient data, with Python/PowerShell/Bash automation cutting **firewall-blocked inbound connection attempts and malicious DNS queries by 80%**

Technical Contractor (AI / LLM Security Evaluation) May 2026 - Present
Contract platform supporting a frontier AI lab (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, National Government (two assignments) Feb. 2021 - Jan. 2022

- 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 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; received a departmental award of merit for delivery impact

Projects & Publications

Vulnerability SLA & Compliance Tracker | *C#, .NET 10, Blazor, Azure, Docker, Terraform, SQL Server*

- Built a vendor-neutral platform ingesting findings from Dependabot, Snyk, and Trivy; assigns severity-based remediation SLAs and tracks breaches with full history and compliance reporting

Meta-Analysis on a National Cyber-Security Centre | *Accepted, peer-reviewed journal (forthcoming)*

- Authored an accepted meta-analysis reviewing open-source literature on a national cyber centre's threat-intelligence and critical-infrastructure work

Education & Certifications

M.S., Cybersecurity & Information Assurance | *Online State University (U.S.)* 2024

B.Sc., Computer Science | *Public Research University (Canada)* 2018 - 2024

Certifications: CISSP (2026), SSCP (2023), AWS Certified Solutions Architect & Developer - Associate (2022)