[Name Redacted]

[Email Redacted] | [Phone Redacted] | U.S. and Canadian Citizen

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: SOC 2, ISO 27001, HIPAA-oriented controls, audit documentation, control evidence workflows

PROFESSIONAL EXPERIENCE

Security Operations Analyst, [Employer Redacted] [Dates Redacted]

- Owned security end-to-end as the sole security owner in a boutique medical practice; built the program from scratch (risk register, remediation SLAs, KPI reporting, prioritized roadmap)
- Instrumented identity/endpoint/network telemetry and built correlation-driven triage; reduced MTTD from days to under 1 hour
- Rolled out fleet-wide baseline controls across all endpoints for the business (macOS/Windows): MFA, FileVault, MDM enforcement, and patch cadences; standardized baselines and exceptions
- Operationalized incident response and vulnerability closure with external IT vendors; authored playbooks and audit-ready evidence mapped to HIPAA-oriented controls

Software Engineer (1 Year Term Appointment), [Federal Government] [Dates Redacted]

- Engineered secure AWS infrastructure (IAM, S3, DynamoDB, CloudWatch) via Terraform/Terragrunt; enforced policy-as-code scanning with Checkov
- Built Python/Flask bot-abuse detection controls, analyzing request patterns and tuning thresholds to reduce false positives while maintaining detection accuracy
- Refactored 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
- Produced security runbooks and incident-support documentation adopted org-wide; awarded a director-level merit award for delivery impact

Software Engineer Intern, [Federal Research Agency] [Dates Redacted]

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

PROJECTS & PUBLICATIONS

[Title Redacted] | *Accepted, Peer-Reviewed Defense Journal (forthcoming)*

- Authored an accepted meta-analysis on national cyber defense operations, synthesizing open-source sources on threat intelligence operations, detection capabilities, and critical infrastructure protection

[Project Name Redacted] | Open-Source Developer Tool

- 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

EDUCATION

Master of Science (M.S.) Cybersecurity & Information Assurance | [University Redacted] Awarded [Year]
Bachelor of Computer Science (BCompSci) | [University Redacted] Awarded [Year]

CERTIFICATIONS

Systems Security Certified Professional (SSCP) Awarded [Year]
AWS Certified Solutions Architect & Developer - Associate Awarded [Year]
Associate of ISC2 (CISSP Exam Passed) Awarded [Year]