



*Technical information security leader with over 17 years of contributor and management experience across public and private sector employers. Speaks bits, bytes, and business. Excellent oral and written communicator. Fast learner with strong bias to action. Runs toward danger. Minimal supervision required.*

---

## Education

Master of Information Technology @ Virginia Polytechnic Institute & State University (Dec 2024)

- Relevant coursework in artificial intelligence, strategic technical leadership, risk assessments, cybersecurity program management, and critical engineering. 4.0 GPA, VT Graduate Honor Society.

B.S., Business Administration @ University of Mary Washington (May 2008)

SANS GIAC Certified Enterprise Defender (GCED) (exp. 2023)

CompTIA Certified Advanced Security Practitioner (CASP) (exp 2022)

---

## Highlighted Skills

- |                           |                           |                           |                            |
|---------------------------|---------------------------|---------------------------|----------------------------|
| • Python/Bash/Powershell  | • EDR Tools / Crowdstrike | • macOS & Windows MDM     | • Public Speaking          |
| • Network Security        | • Secure Remote Access    | • Artificial Intelligence | • GitOps / DevSecOps       |
| • IAM                     | • IaC (Ansible/Terraform) | • Incident Response       | • API Programming          |
| • Okta / Active Directory | • Cryptography            | • Vendor Management       | • Zero-Trust Networking    |
| • Public Speaking         | • Mentoring               | • Project Management      | • SQL/Relational Databases |
- 

## Career Experience

**Lead for Cyber Architecture and Resiliency - The MITRE Corporation, Feb 2025 - Apr 2025** (McLean, VA, Hybrid)

- Position eliminated due to involuntary reduction in force (layoff). References available.
- Performed in-depth technical research to support and explore novel uses of artificial intelligence and large language models to facilitate offensive and defensive cybersecurity activities for the Internal Revenue Service.
- Drafted new tactic and technique definitions for the MITRE ATT&CK framework to reflect the changing adversarial landscape.

**Senior Enterprise Security Engineer, Tech Lead - Arcadia, Aug 2024 - Jan 2025** (Denver, CO, Remote)

**Security Engineer III, May 2022 - July 2024**

- Led the strategic direction and technical implementation of the enterprise security program. Indirectly led (dotted line) a cross-functional team of two engineers from the IT and information security groups.
- Managed functional areas of endpoint detection and response (EDR), email security, workforce identity and access management (IAM), vulnerability management, and zero trust architecture.
- Executed on strategic initiatives to consolidate and upgrade multiple Okta tenants through M&A activities ahead of schedule, saving the company over \$120,000 on renewal charges.
- Owned security engineering employee lifecycle management from hiring through onboarding plan, career development, 30/60/90 goal development, and follow up for junior staff.
- Wrote and implemented Terraform code to manage and maintain AWS-based security tooling infrastructure with GitOps and Github Actions. Assisted with cloud infrastructure hardening where required.
- Managed and executed project to migrate over 1400 users and contractors off legacy VPN to a zero-trust network access solution fully integrated with IdP and EDR with zero disruption.
- Onboarded and managed Crowdstrike endpoint detection and response (EDR) solution for over 1200 macOS and Windows endpoints. Engaged in vendor selection, proof of concept, and negotiation of pricing.
- Designed and implemented “next-gen authentication” strategy for 1400 users, eliminating use of passwords and moving to phishing resistant authentication with FIDO2 and Okta FastPass.

- Deployed and managed Proofpoint Enterprise to defend against email threats. Managed email authentication protocols and best practices for the company to ensure deliverability. (SPF, DKIM, DMARC).
- Led technical incident response, including responding to and recovering from multiple insider threat events.
- Drove key performance indicators, SLAs, and remediations for vulnerability management across 1200 endpoints.
- Operated security orchestration, automation and response (SOAR) activities using APIs, python, and low/no-code tooling.
- Improved security of mixed-OS endpoint fleet with automated posture checking and integration with EDR and zero-trust tooling.
- Communicated broadly across the company about information security initiatives and updates. Built strong and collaborative relationships with user base. Led trainings and spoke publicly about strategy and initiatives.
- Researched and evaluated security tooling on a technical and cost basis for integration into the environment.
- Participated in technical governance/risk/compliance (GRC) activities including SOC2 evidence collection, verification, and client questionnaires.

**Senior Network Analyst, Arlington Public Schools, Jun 2019-May 2022** (Arlington, VA, Hybrid)

**Network Analyst II, June 2017 - May 2019**

- Facilitated migration of entirely on-premises environment to Azure hybrid cloud model required by operational challenges presented by the COVID-19 pandemic.
- Led project to appropriate a \$100,000 grant from Amazon to design, build, and operate a next-generation STEM lab for networking, cybersecurity, and STEM learning.
- Migrated over 30 Juniper network configurations to infrastructure-as-code (IaC) using Ansible.
- Architected and maintained complex, multi-datacenter hybrid cloud Palo Alto NGFW environment.
- Mitigated distributed denial of service attacks (DDoS) from malicious state-sponsored actors.
- Migrated from a legacy to fully access-segmented security model using 802.1x and User-ID for over 35,000 users.
- Managed, responded to, and remediated security incidents from over 30,000 user endpoints.
- Assisted with management of Endpoint Detection and Response tool (Palo Alto Cortex).
- Managed requests for DNS-based content filtering in line with strict regulatory (FERPA, COPPA, CIPA) and security requirements.
- Maintained a high standard of success and professionalism in a high-stakes, high-scrutiny environment; occasionally required to work with or alongside children and interface with the public.

**Network Security Engineer, Carbonite (OpenText), Nov 2015-May 2017** (Boston, MA, Remote)

- Maintained and updated software-defined network and application policies on Juniper SRX-series and Check Point firewalls.
- Architected and physically installed multiple secure network environments for 4 remote office locations.
- Troubleshoot complex network issues using packet-inspection tools, advanced logging, and real-time monitoring.

**Cloud Systems Engineer, Reclaim Hosting, Aug 2015-Feb 2016** (Remote)

- Scoping and implementation for a solution to automatically manage and monitor cloud web servers for availability, application performance, and heuristic intrusion detection. Part-time, 6-month contract role.

**IT Manager, Apex Clean Energy, Dec 2014 – Nov 2015** (Charlottesville, VA, On-site)

- Managed all corporate IT operations for a 120-person organization, with one direct report.

*Previous (2008-2014) Carbonite, Inc. Apple, Inc (Retail). Apogee Telecom.*

---

**About Me**

- Cruise and travel enthusiast, computer history nerd, avid reader, gamer, half-marathoner, corgi wrangler, proud husband and dad.
- Member of IEEE and Japan-America Society of Washington, DC.