Joseph McMahon (he/him) [redacted] **// joemac.io**

[redacted]

Technical information security leader with over 16 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

M.S., Information Technology @ Virginia Polytechnic Institute & State University, *2022-2024*

- *Framework for AI-Driven Identity & Access Management Decision Engines*
- *Lean NIST Risk Assessments for Small & Medium Businesses*
- *Open-Source Remediations for Biased Algorithms*

B.S., Business Administration @ University of Mary Washington, *2004-2008*

SANS GIAC Certified Enterprise Defender (GCED), *2019-2023*

Highlighted Skills

- Python/Bash/Powershell
- Network Security
- IAM
- Okta/Active Directory
- Endpoint Detection & Response
- Secure WiFi/802.11i
- IaC (Ansible/Terraform)
- Cryptography
- System Architecture
- macOS/Windows MDM
- Artificial Intelligence
- Incident Response
- Vendor Management
- Email Security
- Risk Assessments
- People Management/ Mentoring
- Public Speaking
- Gitops/DevSecOps
- API Programming
- Zero-Trust Networking
- Project Management
- SQL/Relational Databases

Career Experience

Senior Enterprise Security Engineer, Tech Lead - Arcadia, ***Sep 2024-Present*** ***(Denver, CO, Remote)***

Security Engineer III, June 2023 - August 2024

Security Engineer II, May 2022 - June 2023

- Technical lead for enterprise, corporate, and workforce security at Arcadia, leads a cross-functional team of two.
- Manages functional areas of endpoint detection and response (EDR), email security, workforce identity and access management (IAM), vulnerability management, and zero trust.
- Participates in employee lifecycle management from hiring through onboarding plan, career development, and follow up for junior staff.
- Led and executed project to migrate over 1400 users and contractors off a legacy VPN to a zero-trust network access solution fully integrated with IdP and EDR.
- Onboarded and manages Crowdstrike endpoint detection and response (EDR) solution for over 1200 macOS and Windows endpoints.
- Eliminated use of passwords across the organization as a primary authentication factor in favor of phishing-resistant multifactor authenticators.
- Deployed and manages Proofpoint Enterprise to comprehensively defend against email threats. Manages email authentication protocols and best practices for the company to ensure deliverability. (SPF, DKIM, DMARC).
- Participates regularly in technical incident response, including responding to and recovering from multiple insider threat events.
- Drives key performance indicators and remediations for vulnerability management across 1200 endpoints.
- Operates security orchestration, automation and response (SOAR) activities using APIs, python, and low/no-code tooling.

- Implemented security posture management across endpoint fleet with automated posture checking as part of zero-trust strategy.
- Communicates broadly across the company about information security initiatives and updates. Builds strong and collaborative relationships with user base.
- Researches and evaluates security tooling on a technical and cost basis for integration into Arcadia's environment.
- Participates in technical governance/risk/compliance (GRC) activities when needed including SOC2 evidence auditing and client questionnaires.

Network Analyst III (Senior), 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 a 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.
- Publicly recognized by Arlington County Board for collaboration and contributions to Arlington County fiber network.
- 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).
- Secured IoT devices with unique requirements by creating custom Palo Alto application signatures.
- Appropriately managed requests for content filtering in line with regulatory 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 installed secure network environments for remote office locations.
- Troubleshot 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 Systems Administrator, Apex Clean Energy, Jan 2015-Nov 2015 (Charlottesville, VA, On-Site)

- Responsible for all day-to-day IT operations of the company, including management and training of IT staff.
- Scoped, designed, and installed high-performance virtualization environment for specialized applications.
- Implemented federated identity management system/SSO (Okta) for employee applications.
- People manager for two associate-level employees.

Previous: *Carbonite, Inc. Apple, Inc. Apogee Telecom.*

About Me

- Member, Institute of Electrical and Electronics Engineers (IEEE)
- Travel enthusiast. Avid reader and learner. Gamer. Proud husband and dad of kin and corgi.