Joseph McMahon [redacted] **// joemac.io**

[redacted]

Experienced cybersecurity architect focused on supporting the efficient and effective operation of enterprise information security programs. Interested in identifying and pursuing measurable risk reductions via holistic deployment of security controls and evidence-based risk management. Critical thinker. Asks a lot of questions.

Education & Credentials

M.S., Information Technology, Virginia Polytechnic Institute & State University (2024)
- Concentrations: Cybersecurity & Cybersecurity Leadership, VT Graduate Honor Society.
- Targeted coursework on NIST SP 800-53 risk assessments, effective metrics and measures for enterprise risk modeling, reducing bias in AI systems, and developing agentic AI systems for identity and access management.

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

Certified Information Systems Security Professional (CISSP) *(ISC2 Member:* [redacted]
SANS GIAC Certified Enterprise Defender (2019-2023)

Highlighted Skills

Technical: Python | Bash | Powershell | Network Security | AWS | Identity and Access Management | Cloud Security | Endpoint Detection and Response | Email Security | Secure Remote Access | SASE | CASB | Cryptography | macOS/ Windows MDM | Zero Trust Network Access (ZTNA) | SQL | Artificial Intelligence | Vulnerability Management

Non-Technical: Project Management | Public Speaking | Professional Research | Report Writing | Enterprise Communication | Agile | Incident Response | People Mentoring | Vendor Management | Risk Assessments | Risk Analysis | Quantitative Analysis | People Leadership | Cost Analysis | Compliance | Threat Modeling | Enterprise Communication | Compliance Frameworks

Career Experience

ScienceLogic, Jul 2025 – Present (Reston, VA, Hybrid)

Security Architect

- Broad-scoped, most senior security individual contributor in a 650 FTE org using an “internal agency/advisory” model.
- Provides enterprise-wide security guidance to teams and departments across the organization, including product engineering, legal, HR, SRE, and corporate IT.
- Leads efforts to ensure the thoughtful, practical, and secure use of AI and agentic services in the enterprise.
- Proactively identifies opportunities to ensure cost effectiveness in the information security program, including driving over $50,000 in reduced AWS spend year-over-year and $30,000 in annual savings from tool consolidation.
- Architected and executed an initiative to reduce SaaS spend by over $100,000 a year by bringing cryptographic code signing services in-house.
- Coordinates effective day-to-day operations of security tooling (EDR, DLP, CSPM, AppSec) with security team.
- Facilitated incident response and recovery from a severe security incident attributed to a nation-state threat actor.
- Works alongside compliance team, ISSO, and external auditors and assessors to ensure and maintain technical compliance with audit standards, including SOC2, ISO 27001, and FedRAMP.
- Develops and maintains key enterprise and infrastructure risk and performance metrics and indicators.
- Performs light FinOps duties to monitor and control for cloud cost overruns, correlating to potential security events.
- Creates board-level artifacts (reports, presentations, diagrams) to communicate value-generating activities and project status updates from the information security team.
- Provides indirect people leadership, mentoring, and task delegation to a team of four.

The MITRE Corporation, Feb 2025 - Jun 2025 (McLean, VA, Hybrid)

Lead (Staff) Engineer, Cyber Architecture & Resiliency

- Performed professional research on the novel uses of AI capabilities in security operations centers. Contributed to efforts to modernize and update the MITRE ATT&CK framework.
- Position eliminated due to involuntary reduction in force/layoff due to sweeping contract changes in the federal government.

Arcadia, May 2022 - Jan 2025 (Denver, CO, Remote)

Security Engineer III May 2022 - July 2024 > Senior Enterprise Security Engineer, Tech Lead Aug 2024 - Jan 2025

- 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.
- Designed and implemented the organization's first ever evidence and impact-based vulnerability management program for over 1200 endpoints.
- Led and executed strategy to consolidate multiple IdP tenants through M&A activities ahead of schedule, saving the company over $120,000 on renewal charges.
- Improved scalability, repeatability, and operational excellence of security tooling by migrating and maintaining configurations and security infrastructure as code, where possible.
- Led and executed project to migrate over 1200 users and contractors off legacy VPN to a zero-trust network access (ZTNA) solution fully integrated with IdP and EDR with zero operational disruption.
- Onboarded and managed Crowdstrike endpoint detection and response (EDR) solution for over 1200 macOS and Windows endpoints. Reduced year over year pricing by over 10% by optimizing licensing costs.
- Designed and implemented passwordless authentication for 1200 employees and contractors, implemented phishing resistant authentication with FIDO2 and Okta FastPass, reducing password reset requests to IT by over 70%.
- 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.
- Facilitated technical governance/risk/compliance (GRC) activities including SOC2 evidence collection, verification, and client questionnaires, ensuring zero-finding audits.

Arlington Public Schools, Jun 2017 - May 2022 (Arlington, VA, Hybrid)

Network Security Analyst II June 2017 - May 2019 > Senior Network Security Analyst June 2019 - June 2022

- Facilitated migration of entirely on-premises environment to Azure hybrid cloud model required by operational challenges presented by the COVID-19 pandemic.
- Migrated management of over 30 Juniper EX routers to centralized and scalable configuration using Ansible.
- Protected over 30,000 hosts by architecting and maintaining resilient Palo Alto Networks next-gen firewall solution, maintaining 99.9% operational SLA.
- Created over 30 custom detections for benign and suspicious events using deep packet inspection and advanced packet disassembly techniques.
- Migrated APS from a legacy to fully access-segmented, zero trust security model using 802.1x and User-ID for over 35,000 users, improving security and efficiency.
- 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.

Carbonite (OpenText), Nov 2015-May 2017 (Boston, MA, Remote)

Network Security Engineer

- Maintained and updated software-defined network and application policies on Juniper SRX-series and Check Point firewalls with a particular focus on enterprise security policies and resilient site-to-site VPNs.

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

IT Manager

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

Previous (2008-2014) Carbonite, Inc (Network Engineer). Apogee Telecom (Network Technician).

About Me: Home chef, gamer, Japan fan, runner, and cruise enthusiast. Big reader.