

MASON FUNDERBURG

Lead Cybersecurity Advisor | SOC Leadership, Risk & Compliance | Zero Trust, AI Governance & Incident Response
Germantown, MD | MasonDFunderburg@outlook.com | linkedin.com/in/mason-funderburg-7aa573108

PROFESSIONAL SUMMARY

My path into cybersecurity started in airport operations, where safety protocols and split-second incident response weren't optional — a mindset that carried into IT and into leading SecOps for a managed security provider. As Lead Cybersecurity Advisor, I oversee security health across multiple client organizations, specializing in Microsoft 365 hardening, threat hunting, vulnerability management, and compliance — a practical, operations-first approach shaped by the full IT lifecycle, from hands-on field support to building and leading security programs.

EDUCATION

Middle Tennessee State University (MTSU) | B.S., Aerospace Administration, 2016

CERTIFICATIONS

Microsoft Certified: Identity and Access Administrator Associate (SC-300) • Azure Administrator Associate (AZ-104)
• CompTIA CySA+ • CompTIA Security+ • CompTIA A+

PROFESSIONAL EXPERIENCE

ImageQuest LLC

Remote / Nashville, TN

Managed Security Service Provider (MSSP) serving community banks and regulated financial institutions.

Oct 2020 – Present | Progressed: IT Support Specialist II > Field Support Specialist > Lead Client Support Specialist > SecOps Engineer > SecOps Team Lead > Lead Cybersecurity Advisor

Lead Cybersecurity Advisor

Jan 2026 – Present

- Serve as a cybersecurity advisor to client organizations, including regulated financial institutions, translating technical risk into business-level guidance for IT and executive leadership.
- Lead IAM reviews and monthly security health checks covering access, device compliance, patch management, and role changes.
- Configure and enforce Microsoft 365 security policies across Entra ID, Defender, Purview, and Intune to harden environments against evolving, AI-accelerated threats.
- Investigate escalated incidents, coordinate remediation, and maintain PCI DSS, GDPR, and HIPAA controls.
- Advise clients on AI governance and risk, including AI DLP implementation, enterprise AI tool structure, and AI program review.

SecOps Team Lead

Jan 2025 – Jan 2026

- Led vulnerability identification and risk assessment across diverse environments, prioritizing remediation.
- Directed monitoring and threat hunting across 5,000+ workstations, leading investigations to remediation.
- Built cloud security tooling, including vendor/app management policies and API integrations.
- Managed email security posture across client environments, including hosted and third-party spam filtering solutions to reduce phishing and email-borne threats.
- Implemented application whitelisting and default-deny (zero trust) architecture as a standard security baseline across client environments.

SecOps Engineer

Aug 2022 – Jan 2025

- Identified vulnerabilities and monitored workstations, investigating network traversal, malware (e.g., Gootloader), and business email compromise, implementing targeted remediation.
- Configured and maintained network security architecture (IDS/IDPS, access control, firewalls, switches, access points) and secured cloud environments through policy development and SIEM API integration.
- Supported SOC 2 compliance through monthly reporting, documentation, and asset management/destruction; contributed to disaster recovery and business continuity planning.
- Wrote PowerShell scripts for remediation at scale for varying environments and vulnerabilities.

IT Support Specialist II > IT Field Support Specialist > Lead Client Support Specialist

Oct 2020 – Aug 2022

- Delivered remote and on-site technical support resolving hardware, software, and network issues (DNS, DHCP, VLAN) for clients and internal teams, using remote access tools (RDP, Automate) and collaboration platforms (Teams, Zoom, GoToMeeting).
- Designed and maintained network infrastructure including firewalls, switches, access points, and local DNS routing across client environments.
- Promoted to lead a team of Field Technicians, Dispatchers, and Onboarding/Offboarding Specialists, aligning service delivery across clients.
- Managed large-scale hardware and software installation projects to SLA, coordinating across clients, vendors, and internal teams.
- Built asset management and documentation processes, including a Hard Drive Destruction Plan supporting SOC 2 compliance.
- Grew the team through active recruiting, candidate evaluation, and structured interviews.

HCTec

Remote

Healthcare IT and telehealth support services company, staffing hospital systems during the COVID-19 pandemic.

Service Desk Analyst | Apr 2020 – Aug 2020

- Supported patients configuring remote telehealth systems across a wide range of devices and environments during the COVID-19 pandemic.
- Provided technical support to medical professionals and patients for telehealth platforms and day-to-day hospital technology, including EMR systems.

Airport Operations

Williston Basin Int'l (ND) > Eugene Airport (OR) > Mobile Airport Authority (AL)

Airfield operations roles across three U.S. airports, focused on regulatory compliance, safety inspections, and emergency management.

Operations Officer > Operations Supervisor > Operations Duty Officer > Airfield Operations Specialist | Jul 2016 – Feb 2020

- Conducted daily airport and facility safety/security inspections ensuring strict compliance with federal regulations (14 CFR Part 139, Part 77, TSR 1542).
- Trained in Incident Command and Aircraft Rescue and Firefighting (ARFF) response operations; led performance and development of Airport Operations Officers.
- Maintained the Airport Emergency Plan (AEP), Airport Certification Manual (ACM), and Wildlife Hazard Management Plan (WHMP) as living compliance documents.
- Planned and facilitated a Triennial Full-Scale Emergency Incident Exercise across 10+ organizations, coordinating multi-agency planning meetings and after-action review, consistent with NIMS emergency management standards.
- Served as Airport Security Coordinator, managing security incidents and coordinating directly with TSA on access control and identification compliance.

CORE COMPETENCIES

- **Detection & Response:** SOC operations, security event monitoring, alert triage, threat hunting, SIEM, XDR, EDR, MDR, incident response and handling (malware, phishing/email compromise, lateral movement), root cause analysis
- **Identity & Cloud Security:** Microsoft Entra ID, Microsoft Defender, Purview, Intune, IAM, access governance, conditional access, M365/SaaS security, Azure, Microsoft Sentinel, cloud policy and vendor/app management
- **Risk & Compliance:** Vulnerability management, PCI DSS, HIPAA, GDPR, SOC 2, audit readiness, disaster recovery, business continuity, security awareness training, ransomware recovery advisory
- **Infrastructure, Automation & Leadership:** Network security architecture (IDS/IPS, firewalls, switches, access points), DNS/DHCP/VLAN, PowerShell automation, API integrations, application whitelisting, default-deny / Zero Trust architecture
- **AI Governance & Security:** AI data loss prevention (DLP), enterprise AI tool management and structure, AI usage policy, AI program review and governance