WILLIAM A. MEDINA

Fort Lauderdale, FL • 954.651.0375 • hello@willmedina.dev • willmedina.dev • linkedin.com/in/williammedina-cybersecurity

PROFESSIONAL SUMMARY

Security operations professional with 4+ years of hands-on IT security experience and 9 years of mission-critical technical operations (U.S. Marine Corps). Holds CompTIA Security+, Network+, and Project+ with a B.S. in Computer Engineering. Directly operates Darktrace AI behavioral analytics (IDS/IPS) and AT&T AlienVault SIEM in a production financial services environment, manages 427 endpoints via Microsoft Intune, and actively contributed to incident response during a live enterprise cybersecurity breach in May 2025. Skilled in SIEM operations, threat detection and log analysis, MITRE ATT&CK framework application, endpoint security, identity lifecycle management, and regulatory compliance (FFIEC/NCUA/PCI-adjacent) in a federally-regulated institution. Targeting remote security analyst and security operations roles where operational depth, regulatory experience, and technical discipline translate immediately into measurable team impact.

CORE COMPETENCIES

SIEM Operations (AT&T AlienVault) • IDS/IPS Monitoring & AI Threat Detection (Darktrace) • Endpoint Security & MDM (Intune)

Incident Response & Breach Recovery • Microsoft Defender & Defender for Endpoint • Active Directory & Identity Lifecycle Management

Backup & DR Architecture (Acronis / Veeam) • PowerShell & Microsoft Graph API Automation • Microsoft 365 & Azure Ecosystem

MITRE ATT&CK · Threat Investigation & Hunting • NIST CSF / Security Frameworks • FFIEC / NCUA Regulatory Compliance

Vulnerability Management & Log Analysis • Role-Based Access Control (RBAC) • Containerized Infrastructure (Docker)

PROFESSIONAL EXPERIENCE

Systems Support Specialist — Security & Infrastructure | *BrightStar Credit Union* June 2024 – Present

- Served as primary technical responder during a May 2025 enterprise cybersecurity breach — executing containment measures, coordinating with AT&T AlienVault SOC, orchestrating shutdown of compromised core banking systems, and restoring operations via Acronis backup — achieving partial operational recovery within 2 weeks and full restoration within 30 days with zero permanent data loss.
- Eliminated endpoint provisioning gaps and enforced uniform security policy across the organization by architecting and managing an MDM framework covering 427 devices (Windows, macOS, iOS) via Microsoft Intune and Apple Business Manager — standardizing enrollment workflows, app deployment, and security policy enforcement at scale.
- Strengthened threat detection and reduced mean time to respond (MTTR) by operationalizing Darktrace AI behavioral analytics (IDS/IPS) alongside AT&T AlienVault SIEM and Microsoft Defender — conducting daily threat investigation and anomaly-driven threat hunting across endpoint and network telemetry, triaging AI-generated alerts, mapping observed attacker behaviors to MITRE ATT&CK TTPs, and maintaining 24/7 incident coverage through Opsgenie on-call rotation.
- Hardened network security posture and eliminated LAN connectivity failures by engineering a Group Policy Object (GPO) enforcing Ethernet-over-WiFi prioritization across all docked endpoints — reducing wireless attack surface, enforcing a network segmentation control across 427 devices, and resolving a recurring banking application performance issue with zero reoccurrence post-deployment.
- Reduced data loss risk and formalized disaster recovery by architecting BrightStar's entire Acronis backup environment from scratch — establishing department- and branch-level backup policies, documented recovery runbooks, and regular DR testing cadence, ensuring validated recoverability across all production systems.
- Maintained zero unauthorized access incidents by managing the full identity lifecycle for all Active Directory accounts — enforcing RBAC, administering security group memberships, and executing timely deprovisioning — supporting least-privilege access compliance requirements.
- Supported continuous FFIEC and NCUA regulatory compliance posture at a federally-regulated financial institution by enforcing least-privilege access controls, maintaining audit-ready security event documentation,

and ensuring information security procedures aligned with FFIEC IT examination guidelines — contributing to zero examination findings related to information security controls.
- Reduced manual backup validation effort by engineering PowerShell automation for Intune backup operations — integrating SHA-256 integrity verification, automated logging, and Microsoft Graph API calls — establishing a fully scripted, auditable DR workflow eliminating human error from the verification process.

Help Desk Technician | *Nova Southeastern University* Sept 2022 – June 2024

- Maintained high-resolution service quality for a large academic user base by resolving Tier 1/2 hardware, software, and network support requests across phone, in-person, and remote channels — consistently meeting ticket SLAs for faculty, staff, and students.
- Supported consistent network uptime for academic operations by monitoring LAN/WAN infrastructure performance, identifying issues proactively, and executing preventive maintenance — minimizing disruptions during peak semester periods.
- Reduced repeat security-related support incidents by delivering end-user security awareness guidance covering phishing recognition, password hygiene, and acceptable use practices — contributing to a stronger security culture across departments.

Communication Specialist | *United States Marine Corps* Jan 2009 – Nov 2015

- Ensured zero communication blackouts for 20,000+ personnel across multiple installations by installing, configuring, and maintaining classified and unclassified network communications infrastructure — sustaining mission-critical connectivity across active operational environments.
- Achieved 100% mission-critical system continuity by completing 200+ telecom service requests for DSN, VoIP, and VoSIP systems with no missed SLAs — supporting uninterrupted command communications through deployment cycles.
- Recognized for operational excellence and technical performance with NATO Meritorious Service Medal, Navy Meritorious Unit Medal, and Global War on Terrorism Medal — demonstrating consistent above-standard delivery in high-stakes environments.

HOME LAB & TECHNICAL PROJECTS

- Identity & Access Management Lab: Deployed a Windows Server environment with functional Domain Controller, Active Directory, Group Policy, and RBAC configuration — building hands-on proficiency in enterprise identity management directly applicable to IAM-focused security analyst roles.
- Container Infrastructure: Self-host and maintain a Docker environment running multiple containerized applications — gaining operational experience in container lifecycle management, application deployment, and infrastructure operations relevant to AI tooling and MLOps support environments.
- Security Automation: Author PowerShell scripts for log analysis, API-driven administrative workflows, and system task automation — building scripting capability applicable to AI tool governance, Copilot administration, and security orchestration pipelines.
- AI Tooling & LLM Infrastructure: Home lab (Unraid + Twingate remote access) actively expanding into local LLM hosting and AI security testing — developing practical familiarity with AI model deployment in self-managed infrastructure environments.

EDUCATION & CERTIFICATIONS

B.S., Computer Engineering — Florida Atlantic University 2021
A.A., Computer Science — Broward College 2016
Certifications: CompTIA Security+ | CompTIA Network+ | CompTIA Project+
Military Training: IT Essentials, Communication Antenna Systems (USMC)
Security Clearance: Former U.S. Secret (USMC) — eligible for reinstatement

TECHNICAL SKILLS

Security & Detection Tools: Darktrace (AI Behavioral Analytics / IDS/IPS), AT&T AlienVault SIEM (USM Anywhere), Microsoft Defender / Defender for Endpoint, Opsgenie (on-call/incident management)
Endpoint & Identity Management: Microsoft Intune, Apple Business Manager, Apple Configurator, Active Directory, Group Policy, RBAC, full MDM lifecycle (iOS/macOS/Windows)
Scripting & Automation: PowerShell (automation, log analysis, Microsoft Graph API), Docker (container orchestration)

Infrastructure & Cloud: Windows Server, Active Directory, Microsoft 365, Azure, VMware (former), Physical Infrastructure, Jack Henry Symitar

Backup & Recovery: Acronis (full org deployment architect), Veeam, DR planning and testing

Frameworks & Compliance: MITRE ATT&CK, NIST CSF, FFIEC IT Examination Handbook, NCUA Security Controls, PCI-DSS (adjacent), RBAC / Least Privilege

Networking: LAN/WAN, DNS, VoIP/VoSIP, DSN, Firewalls, Switches/Routers, Network Troubleshooting