Zane Merlo

Phone: 443-846-3587 **Email:** zanemerlo0308@gmail.com

Relevant work experience

Client Support Engineer | CMIT Solutions | Baltimore County West & Upper Chesapeake
Columbia, MD
08/2024 - Present
Hours per week: 40

● Infrastructure Management: Orchestrated IT operations for 50+ businesses and 6 regional branches, supporting 100s of users across hybrid Cloud (M365/Azure/GCP) and on-prem environments.

● Threat Mitigation: Slashed phishing click rates by 35% (initial) and an additional 18% (Second Round) by initiating a Webroot/Datto Security Awareness program.

● Critical Problem Solving: Managed a high-volume queue of 100 monthly tickets

● Managed Detection and Response Architecture: Implemented a multi-layered defense strategy utilizing SonicWALL firewalls, Barracuda networks, Datto, Webroot, and ConnectWise services to protect client data and device security.

● Email Spoofing Attacks: Utilizing clients DNS in order to check for SPF, DKIM, and DMARC entries to resolve email spam and email spoofing attack strategies from external threat actors.

● System Optimization: Eliminating SharePoint sync errors and "path-too-long" failures by re-engineering file architectures from 10+ nested levels into a flattened, high-efficiency structure.

● Access Control: Managed Active Directory's GPOs to enforce "Least Privilege" security, including hardware-level port blocking and automated MFA rollouts, as well as resource management including a print server.

● Rapid Threat Containment: Executed emergency offboarding and remote-wipe scripts for unreturned corporate devices; investigated account compromises by tracking intruder IPs via Azure/Exchange and revoking unauthorized sessions. As well as backing up and transferring user data.

● SonicWall Breach Response (September 2025): Responded to a global firmware breach within 5 hours. Neutralized brute-force risks for 30 clients by resetting all MFA, user credentials, and VPN Secret Keys within a 14-hour window. Standardized administrative security policies and verified all environment hardening via the SonicWall Config Analysis Tool to ensure zero follow-on impact.

● Network Infrastructure Project: Worked on a hardware migration project for a local school by decommissioning legacy Ruckus switches and deploying modernized Datto switches on all the schools network racks (4). Optimized campus-wide connectivity by installing and configuring 30 high-density access points, ensuring seamless high-speed wireless coverage for students and faculty.

● Azure Integration & Platform Support: Facilitated third-party application integrations within Microsoft Azure by managing API keys, configuring service permissions, and handling the administrative backend. Acted as the technical point of contact to ensure external apps could securely connect to the internal environment.

IT Systems Administrator | Harford County Toys for Tots | Jarrettsville, MD
08/2025 - Present
Hours per week: 10

● Digital Transformation: transitioned current file system from physical filing systems to a cloud-based environment; digitized years of paper records into a structured SharePoint to eliminate the need for physical storage.

● Infrastructure Build-out: Architected the organization’s first Microsoft 365 tenant, including the configuration of Teams, Outlook, and Shared Calendars to coordinate logistics for volunteer workforce.

● Cloud Logistics (AWS): Deployed and managed a self-hosted Traccar instance on AWS EC2 (Linux/Debian) to provide real-time GPS tracking for delivery and pickup routes via volunteer smartphones.

● Automated Workflow: Configured geofencing triggers to automate data collection; programmed mobile pop-ups that prompted volunteers for total amount of boxes picked up or dropped off immediately upon arrival at donation sites.

● Identity & Access Management: Enforced a "Zero Trust" model by implementing Microsoft Authenticator MFA for all volunteers and utilizing Access Control Lists (ACLs) to secure sensitive organizational data.

● Technical Writing: Authored comprehensive Standard Operating Procedures (SOPs) for onboarding, resulting in a seamless self-service setup process for volunteers on personal mobile and desktop devices.

Networking & IT Systems Intern | Federal Pegasus Radio | Aberdeen, MD
06/2023 - 08/2023
Hours per week: 30

• Infrastructure Assembly: Assembled and wired professional grade system racks for high profile clients, including the Smithsonian; integrated Cisco routers, switches, transmitters, and UPS units into ready-to-deploy kits.

• Network Reliability: Hand crimped and tested RJ45 cabling to ensure 100% connectivity standards; performed firmware updates and hardware troubleshooting to maintain equipment readiness.

• Asset Tracking & Documentation: Managed a detailed physical inventory by logging serial numbers and MAC addresses for all components of the system racks, ensuring accurate tracking for deployments.

• Systems Configuration: Collaborated with senior engineers to program radio communication systems and customize firmware protocols for secure federal and commercial use.

• Technical Documentation: Created the primary documentation for network rack assemblies, providing a blueprint for future maintenance and quality control.

Education, certification or licensures

Beacon College | Leesburg, FL **Completion date:** 05/2024
Bachelor's degree | **GPA:** 3.96 of a maximum of 4.0
Major: Computer Information Systems - Information Track | **Minor:** Cybersecurity and Digital Forensics | **Honors:** Summa Cum Laude

Certificates: CompTIA Security+ 701, Test Out Routing & Switching Pro, Test Out Ethical Hacker Pro

Fallston High School | Fallston, MD **Completion date:** 06/2020
High school diploma or equivalent | **GPA:** 3.6 of a maximum of 4.0
Honors: Cum Laude

Job-related training

Eligible for a U.S. Security Clearance.
Willing to relocate.

Language skills

English **Spoken:** Advanced | **Written:** Advanced | **Read:** Advanced

Additional information

● Cybersecurity Internship | Mastercard (Remote)

Social Engineering Defense: Conducted simulated phishing assessments across various business units to identify high-risk departments and tailored security training procedures to mitigate human-element vulnerabilities.

● Incident Response & Malware Analysis: Successfully bypassed and neutralized a $4,000 ransomware lockout by identifying software backdoors; performed forensic cleanup including OS re-imaging, DNS-level blocking of remote access tools, and disabling vulnerable RDP services within Windows Firewall.

● Used FTK Imager to create copies of my hard drive and USB stick to preserve data. Analyzed the images in Autopsy to successfully recover deleted files.