MICHAEL ERDELY mike@erdelynet.com | 301-905-2224 | codeberg.org/merdely | linkedin.com/in/merdely

Information Technology Professional

IT Leadership | Cybersecurity | System Administration | DevOps

IT and Cybersecurity Professional with 20+ years of experience designing, securing, and automating complex Linux-based infrastructure. Currently managing a 130-server Splunk platform for the FDA, with deep expertise spanning DevOps, network security, and SOAR automation. Known for bridging the gap between hands-on technical execution and strategic IT leadership; and for turning lab-built ideas into production-grade solutions. Committed to continuous learning, thorough documentation, and developing the technical skills of those around me.

CORE COMPETENCIES/AREAS OF EXPERTISE

- **Systems**: OpenBSD, Red Hat (RHEL), Amazon, Oracle (OEL), Kali, Alpine, Debian, Ubuntu Linux, MacOS, Windows
- **Cybersecurity Tools**: Splunk, Cribl, Tenable SecurityCenter, Crowdstrike, Zscaler, VPN, Wireshark/tcpdump
- **DevOps** Tools: VMware, KVM, Docker, AWS, Oracle Cloud, Google Cloud, GitHub, Ansible, Python, PHP, Bash
- **AI Tools**: Ollama, LocalAI, Open-WebUI, Promptfoo, n8n
- **Security**: OpnSense, pfSense, pf, firewalld, ufw, nftables, iptables, Wireguard, OpenVPN, IPsec, SSH

SIGNATURE CONTRIBUTIONS

- **Designed and deployed an AI Platform** providing an agentic interface to Splunk data, bringing modern AI-assisted analysis capabilities to the FDA's Cybersecurity program.
- **Maintained 100% uptime across a 130-server FDA Splunk platform,** with multiple index and search head clusters, through monthly patch and upgrade cycles -- zero unplanned downtime over six+ years.
- **Designed and deployed FDA Splunk VPN Automation** to instantly disconnect and disable users connecting from prohibited locations, saving SOC analysts critical response time on every triggered event. Recognized with the FDA CISO Challenge Coin.
- **Implemented IT automation using Ansible**, reducing week-long administrative tasks to under an hour while ensuring consistency and repeatability across 130 FDA Cybersecurity Platform systems.
- **Migrated an on-premises data center entirely to AWS**, eliminating monthly power/HVAC-related outages and converting dozens of SparkPost's physical and virtual systems to EC2 instances.
- **Launched Okta SSO with an open-source LDAP backend**, cutting onboarding and offboarding time from 2 hours to 30 minutes and reducing the number of passwords SparkPost employees managed by 80%.
- **Led IT and Security evidence collection for SOC2 and Capital One audits**, contributing directly to successful outcomes for both assessments for SparkPost.

CAREER EXPERIENCE

FDA Contractor/Copper River Cyber Solutions - North Bethesda, MD December 2019 - Present

Principal Engineer

Principal Engineer for the FDA's enterprise Cybersecurity Platform, a 130-server Splunk environment running on Linux, providing full-stack DevOps support, security automation, and platform engineering.

- Redesigned Tenable infrastructure from a single server to a multi-tier architecture, improving redundancy, task separation, and overall platform resilience.
- Protected platform systems from several Linux Local Privilege Escalations (LPE) and other vulnerabilities by

testing exploit code in test environment to ensure safety of the platform.

- Employed Gitea DevOps workflows to automatically build custom Docker containers for the platform.
- Deployed firewalld across all 130 platform hosts, enforcing least-privilege port access between systems.
- Migrated 130 systems from Red Hat Enterprise Linux 7 through Oracle Enterprise Linux 7, 8, and 9, keeping the platform current across multiple major OS generations.
- Wrote a Bash script to automate Suricata ruleset management; downloading, testing, and distributing updates to sensors across the FDA; saving the Suricata team several hours per week.
- Implemented low-cost SOAR capabilities using Splunk's Python Add-on framework, automating SOC response tasks triggered instantly by platform events.
- Developed a multi-tab Splunk Dashboard consolidating SOC operational data into a single pane of glass, reducing the time analysts spend context-switching between tools.

Message Systems d.b.a SparkPost - Columbia, MD March 2012 - October 2019
Director of IT/Infrastructure

Managed all aspects of the IT Infrastructure and IT Security including hardware, software, budget, networking, and physical infrastructure (cooling, power). Managed the IT team, mentoring junior administrators and developing the IT Lead into a promoted IT Manager. Coordinated with managers of other departments to ensure IT was providing excellent customer service for the needs of the company. Partnered with Site Reliability Engineering team to ensure Corporate IT was aligned with production systems.

- Directed IT staff supporting 200 office and remote users in the US, Canada, UK, Singapore, and China.
- Implemented and managed infrastructure services: Okta SSO, LDAP, DNS, DHCP, OSPF, SSH, NTP, Palo Alto and OpenBSD Firewalls, OpenVPN, Google G Suite.
- Instituted DUO Multi-Factor Authentication for Okta, 1password, OpenVPN, Slack, Google G Suite, and AWS.
- Wrote Python-based Google Management script that allowed administrators to manage G Suite accounts and groups from the command line, reducing time to make changes from tens of minutes to seconds.
- Wrote scripts using Perl and PHP providing interfaces for administrators and users to manage their LDAP account information.

CyberPoint - Baltimore, MD June 2010 - March 2012
Principal Systems Integration Specialist/IT Team Lead

Collaborated with Director of Technology to support both Corporate and customer IT systems and network infrastructure. Managed the IT staff, providing guidance on how to grow their careers by learning higher level technologies and supporting 100 users across three offices on two continents. The environment’s foundation was built on a robust VMware virtual environment with fiber-connected SAN storage running Windows/Exchange, Linux, OpenBSD systems on a heavily Cisco-based network with VLANs, secure WAN links with local and remote access.

SPARTA/Cobham - Columbia, MD May 2009 - May 2010
Principal Systems Engineer

Responsible for integrating SPARTA software and products with customer systems. Managed relationships between customers and SPARTA contracting. Expanded contracts by increasing number of development projects for customers.

RABA/SRA - Columbia, MD April 2007 - May 2009

MICHAEL ERDELY

mike@erdelynet.com | 301-905-2224

Manager, IT Services

Initially hired as RABA Corporate IT Manager, first duties were to integrate RABA services into SRA ITS services following acquisition of RABA by SRA. After receiving Security Clearance, managed secure spaces where customer work was done in RABA's offices. Managed RABA's IT staff, providing mentorship to junior team members. Responsible for passing customer accreditation of secure spaces. Directed several customer audits of secure spaces in RABA offices.

Epok, Inc - Bethesda, MD September 2003 - April 2007

IT Manager

Responsible for managing IT systems for growing software company. Provided training for IT staff to grow careers. Implemented IT best practices to environment to ensure secure, reliable IT services at low cost by leveraging Open Source technologies including Linux and OpenBSD.

EDUCATION

University of Maryland, University College

Computer Information Technology

- Completed B.S. degree using UMUC Prior Learning Program

AWARDS

FDA CISO Challenge Coin March 2023

Received a CISO Challenge Coin for implementing Splunk VPN Automation

SparkPost: Momentum Award Q4 2012

Received a quarterly Momentum Award for managing two office moves within six months of being hired at SparkPost. Managed all aspects of IT, Security, and connectivity for the moves while assisting with other logistics like furniture, moving companies, and physical security.

SparkPost: Efforts Recognized Q2 2015

Received recognition from executive team for managing the IT aspects of merging Port 25's office and personnel into SparkPost's office following the acquisition of Port 25.