MICHAEL CHANDLER

Senior Cybersecurity Engineer | Infrastructure Security | Technical Leadership

Fountain, CO

michaelchandler.us | linkedin.com/in/mikechandler82 | TS/SCI

Professional Summary

Cybersecurity engineer and technical leader with 23 years across IT infrastructure, security operations, and enterprise modernization. Built and secured virtualized Microsoft environments, integrated security monitoring in constrained environments, and led IT teams supporting 4,000 users. Experience spans hands-on automation, resilient systems, technology evaluation, and security authorization. Retired Army Chief Warrant Officer 3 with CISSP and six GIAC certifications.

Technical Expertise

Security: Elastic Security, Palo Alto firewalls, Windows hardening, security architecture, ACAS/Nessus

Infrastructure: VMware ESXi, Active Directory, DNS, SQL Server, SharePoint, SCCM, WDS

Automation and security controls: PowerShell, Linux scripting, Group Policy, PKI-based MFA, DISA STIGs

IT governance and compliance: RMF, Authority to Operate (ATO), Interim Authorization to Test (IATT), eMASS

Professional Experience

GuidePoint Security | Feb 2026 - May 2026

Cybersecurity Engineer | SkillBridge Fellowship | Remote

- Designed and optimized security data pipelines using Cribl and Google SecOps, translating client requirements into log ingestion and routing workflows to improve threat visibility and security operations.

U.S. Army | May 2005 - Jul 2026

Cybersecurity Engineering Lead | Hawaii | Aug 2023 - Jul 2026

- Integrated Elastic Security into a secure operating environment, adapting Linux scripts and certificate configurations to resolve deployment and data pipeline failures.
- Designed monitoring architecture for deployable cyber defense kits operating over limited-bandwidth connections across the Asia-Pacific region; adapted configurations as networks changed.
- Hardened a Palo Alto firewall for a cyber exercise using least-privilege access rules; no successful red-team penetration through the firewall occurred during the exercise.
- Validated security documentation, coordinated with vendors, approving authorities, organizational leadership, and stakeholders, and pursued policy exceptions to resolve authorization gaps. Supported addition of products to testing authorizations and kept leadership informed of approval status.
- Led two cyber defense analysts and mentored approximately 12 junior personnel; oversaw inspection readiness, trained a successor, and helped another organization install its Elastic Security stack.

Services Branch Lead | Germany | Jul 2020 - Jun 2023

- Directed three project managers and three to six engineers across three teams delivering enterprise infrastructure projects in an environment supporting more than 40,000 users.
- Guided data center modernization and evaluated lifecycle replacements against security, compatibility, and capability requirements, including Cisco ACI networking. Developed funding justifications and priority recommendations to advance projects under budget constraints.
- Tested a proposed Commercial Solutions for Classified (CSfC) remote-access solution and identified identity integration and scalability gaps. Advised against adoption, avoiding duplicate account provisioning and implementation work.
- Conducted two digital forensic examinations at leadership’s request, providing findings to support legal proceedings and an ongoing investigation.

IT Infrastructure and Security Lead | Colorado | Jul 2016 - Dec 2019

- Led approximately 12 IT personnel across service desk, server administration, and cyber defense teams supporting 4,000 users across seven organizational units.
- Resolved imaging compatibility problems and standardized deployment procedures, cutting imaging time from six hours to under one hour per computer and supporting compliance across more than 1,000 systems.
- Established redundant services and automated client failover, maintaining access during distributed operations with no unplanned service interruptions during those operations.
- Adapted an established VMware ESXi design and built the virtual environment, deploying Active Directory, DNS, SQL Server, SharePoint, WDS, SCCM, and collaboration services including DDS/BCCS and Openfire.
- Automated account provisioning and routine administration with PowerShell and SCCM; applied Group Policy and DISA benchmarks to hardened Windows 10 images, supporting a 100% cybersecurity inspection result for the assessed network.
- Enabled PKI-based multifactor authentication by coordinating account and credential provisioning before deployment, increasing secure-network access readiness from 15% to 95%.

Executive Communications Support | Asia-Pacific | Apr 2013 - Jun 2015

- Provided round-the-clock IT and communications support to a four-star general during travel, establishing secure remote access and resolving technical problems to keep executive services available.
- Adapted legacy router and switch configurations for a backpack-sized travel system, reducing equipment bulk; travel-kit configuration upgrades improved availability from 95% to 99%.
- Collaborated with contractors on a secure executive audiovisual communications upgrade completed one month ahead of schedule; identified and eliminated more than $10,000 in unnecessary upgrade costs.

Earlier Army experience included network, voice, and collaboration systems support as a Signal Support Systems Specialist.

Nexus Information Systems | Sep 2003 - May 2005

Computer Service Technician

- Provided on-site support for Wells Fargo and BlueCross BlueShield, supporting more than 5,000 users across four locations; resolved service tickets, diagnosed server and desktop hardware faults, and performed warranty replacements.
- Resolved endpoint connectivity issues, built and deployed Windows images with Symantec Ghost, and supported network and operating-system migrations.

Education and Professional Development

B.S. Cybersecurity and Information Assurance | Western Governors University | 2023

A.A.S. Information and Network Technology | Brown College | 2003

U.S. Army Technical Training

Cyberspace Defense Warrant Officer (255S) | Warrant Officer Advanced Course (WOAC) | Jan 2020 - Jun 2020

Information Services Technician (255A) | Warrant Officer Basic Course (WOBC) | Oct 2015 - Jun 2016

Signal Support Systems Specialist (25U) | Advanced Individual Training (AIT) | Feb 2006 - Jun 2006

Certifications

ISC2: CISSP, SSCP | GIAC: GCWN, GCIH, GSNA, GCIA, GSEC, GPEN

CompTIA: SecurityX, Security+, Project+, Network+, A+ | ITIL