

# Jessica Anderson

---

Houston, TX | (404) 797-9293 | jesmanderson@gmail.com | [LinkedIn](#) | [GitHub](#)

## Professional Summary

Cloud Security Engineer with 6+ years of IT infrastructure experience and hands-on expertise in AWS, Azure, and Microsoft 365 security. Proven success delivering projects in DORA compliance, IAM hardening, and Zero Trust architecture. Skilled at implementing identity controls, encryption, monitoring, and compliance frameworks (NIST, SOC 2, ISO 27001).

## Core Skills

- **Cloud Security:** IAM, Zero Trust, Encryption (KMS, Key Vault), MFA, Conditional Access
- **Cloud Platforms:** AWS (IAM, GuardDuty, CloudTrail, Security Hub), Azure (AD, Sentinel, Defender for Cloud, Site Recovery), Microsoft 365
- **Governance & Compliance:** DORA, SOC 2, ISO 27001, NIST CSF, CIS Controls, Risk Registers, Gap Analysis
- **Networking & Infrastructure:** CUCM, Ribbon SBC, SIP, VPNs, VLANs, Firewalls
- **Automation & Scripting:** PowerShell, Python, Terraform basics, CloudFormation basics
- **Monitoring Tools:** PRTG, ServiceNow, Azure Monitor, Security Hub, Sentinel

## Highlighted Projects

### DORA Compliance Audit – Financial Services Company (Upwork)

- Conducted gap analysis of AWS IAM and Azure AD environments against DORA requirements.
- Built a risk register mapping resilience, monitoring, and IAM gaps to compliance standards.
- Designed resilience testing plan using AWS Backup, Azure Site Recovery, GuardDuty, and Defender for Cloud.
- Delivered roadmap that improved audit readiness by 40%.

### IAM Hardening Implementation – Teknikally Speaking

- Audited AWS IAM roles, Azure AD accounts, and Microsoft 365 access policies.
- Identified excessive permissions and implemented least privilege, MFA, and conditional access.
- Automated IAM drift detection and reporting with PowerShell.

### Zero Trust Security Assessment – Teknikally Speaking

- Designed and deployed Zero Trust model across AWS and Azure test environments.

- Configured identity-based access control, micro-segmentation, and conditional access policies.
- Implemented unified monitoring with AWS Security Hub and Azure Sentinel.
- Aligned lab implementation with NIST Zero Trust framework.

## Professional Experience

### **Unified Communications Collaboration Engineer – TechnipFMC | Remote | Mar 2023 – Present**

- Managed global CUCM clusters and hybrid Teams Voice infrastructure with Ribbon SBCs.
- Built CUCM disaster recovery and SBC failover documentation.
- Implemented centralized CUCM backup rotation with automated cleanup logs.
- Deployed and supported MTR (Microsoft Teams Rooms) across enterprise offices.
- Piloted AI-driven troubleshooting tools to improve UC operations efficiency.

### **System Engineer II – Unified Communications – NexGen Technologies | Remote | Aug 2021 – Mar 2023**

- Provided Tier 3 support for Teams, CUCM, CUBE, Zoom, and Webex environments.
- Integrated SBCs, enforced secure SIP trunking, and monitored call quality.
- Partnered with vendors for SIP routing, call flow, and security troubleshooting.

### **Cisco Voice Engineer III – Aston Technologies | Minneapolis, MN | Jul 2019 – Aug 2021**

- Designed and supported multi-cluster CUCM SIP networks across enterprise sites.
- Managed voicemail, paging, E911, and UCCX scripting.
- Delivered end-to-end VoIP support and technical training for enterprise staff.

## Certifications

- AWS Solutions Architect – Associate (SAA-C03)
- CompTIA Security+ (SY0-701)
- Microsoft Certified: Azure Fundamentals (AZ-900)
- Microsoft Teams Voice Engineer (MS-721)
- Cisco CCNA (200-301)
- In Progress: Microsoft Azure Security Engineer (AZ-500)

## Education

Chaney High School – Youngstown, OH