Jonathan Roeseler
https://www.linkedin.com/in/jonathanroeseler/

EDUCATION / CERTIFICATIONS

CompTIA Security+, Network+, AZ-900 Microsoft Azure Fundamentals

Bachelor of Cybersecurity, Old Dominion University. 3.95 GPA. [2023-2026]

TRAINING / SKILLS

- Windows, Powershell & Python Scripting, Wireshark, Linux/Bash, M365/Azure, Splunk
- Virtualization - VMWare, Hyper-V, VirtualBox
- Understand and able to implement various networking concepts, tools and devices securely
- RMF, NIST CSF, FedRAMP
- Complex architecture review
- Vulnerability management (Nessus, Defender)
- Remediation, Incident Response, Change and Configuration Management
- DNS, DHCP, HTTP, SMTP, IAM, VPN, Firewall expertise
- MS-203: M365 Messaging, AZ500, AZ800, SC300

PROFESSIONAL EXPERIENCE

Network/Systems Administrator, Directory Services (CURRENT)

- **Administer mission-critical Air Force networks** by resolving complex server and network issues within a high-security environment with several thousand users. Includes VSphere.
- **Manage hybrid Active Directory infrastructure**, ensuring seamless identity and access management across on-premises and cloud environments.Utilized scripting.
- **Harden and remediate AD environment** across Domain Controllers, DHCP Servers, and endpoint devices.
- **Strengthen system security posture** by implementing STIGS and troubleshooting Group Policy Objects (GPOs) to maintain strict compliance standards.
- **Analyze logs,** such as Event Viewer, to resolve issues, like service account lockout issues
- **Create GMSA's** to support Kerberos best practices and ensure compliance
- **Maintain active Secret Clearance**, demonstrating a high level of trust and reliability in handling sensitive government data.
- **Utilize ServiceNow** to track, manage, and document technical resolutions for complex enterprise systems

Help Desk Administrator, Xylem Tree Experts (Oct 2024 - Oct 2025)

- **Spearheaded DMARC implementation project**, successfully configuring SPF, DKIM, and DMARC protocols to prevent domain spoofing and enhance email security.
- **Optimized endpoint security** by configuring Intune and Microsoft Defender for Endpoint, increasing visibility and protection for all domain-joined devices. Used CIS Benchmarks.
- **Led incident response and remediation efforts** for email security, investigating quarantined messages and neutralizing sophisticated phishing attempts using Exchange, Purview, and Mimecast.
- **Orchestrated company-wide security initiatives**, leading meetings for 100+ participants to train staff on cybersecurity best practices and MFA, RBAC adoption. Created numerous SOPs.
- **Evaluated and deployed enterprise security tools**, including SIEM, AV, and Data Loss Prevention (DLP) solutions such as Crowdstrike, SentinelOne, and Varonis.
- **Automated device lifecycle management** using MDM solutions for proactive monitoring, troubleshooting, and inventory auditing.
- **Achieved the highest ticket closure rate** in the department, consistently resolving hardware, software, and Microsoft 365 issues
- **Modernized employee onboarding** by developing training programs centered on secure identity management within Entra and Intune