ACTIVE SECRET CLEARANCE | PUBLIC TRUST

OMANI REED

Alexandria, VA | 240-807-2221 | Reed.omani22@gmail.com
linkedin.com/in/omaireed | github.com/Oshun2

PROFESSIONAL SUMMARY

Cloud Security Engineer with 5+ years of experience securing Azure and hybrid environments, specializing in identity and access management, threat detection, and compliance-driven infrastructure. Proven track record of supporting secure environments for 500+ users by identifying misconfigurations, reducing risk, and enforcing security controls aligned with NIST, Zero Trust, and CMMC frameworks. Hands-on experience with Microsoft Defender, Sentinel, Log Analytics, and Conditional Access to enhance visibility, strengthen detection capabilities, and enforce least-privilege access across cloud environments.

EDUCATION

Master of Science, Cybersecurity & Information Assurance — Western Governors University
Bachelor of Science, Criminal Justice — Virginia State University

CERTIFICATIONS

Microsoft Azure Administrator (AZ-104) — Expected July 2026

- CompTIA Cybersecurity Analyst (CySA+) — March 2025
- CompTIA PenTest+ — April 2025
- Microsoft Security, Compliance & Identity Fundamentals (SC-900) — June 2024
- Microsoft Azure AI Fundamentals (AI-900) — June 2024
- Microsoft Azure Fundamentals (AZ-900) — February 2024

TECHNICAL SKILLS

Security, Policy & Governance: Cybersecurity Governance, Compliance Requirements, Risk Management Framework (RMF), Authorization to Operate (ATO), Information System Continuous Monitoring (ISCM), Computer Network Defense (CND), Cybersecurity Vulnerability Assessment (CVA)
Tools & Platforms: Splunk, Prisma Cloud, Nessus, Tenable.SC, ACAS, Qualys, OpenVAS, Microsoft Intune, Azure, Entra ID, M365, Microsoft Defender, Sentinel, Log Analytics, Wireshark, SolarWinds, PowerShell, APIs, ServiceNow, Salesforce, Zoho

PROFESSIONAL EXPERIENCE

Trace Systems — Cloud Engineer *October 2025 – Present*

- Investigated a user-reported phishing email impersonating a known vendor that Microsoft Defender had auto-classified as “passed,” escalating from an Outlook phishing report and helpdesk ticket; analyzed the evidence artifacts Defender flagged (sender IP and message indicators) to overturn the automated verdict and confirm a targeted social-engineering attempt against an executive.
- Executed the documented incident-response SOP end-to-end as the sole responder: reset credentials, enforced MFA remediation, coordinated with internal IT to validate scope, and monitored the user’s device and mailbox for two weeks — containing the incident to a single account with no spread across the organization.
- Engineered and enforced hybrid cloud security controls across Azure and on-premises Active Directory environments supporting CMMC-aligned compliance requirements.

- Implemented identity security solutions, including Conditional Access policies, privileged access controls, and Azure AD Connect synchronization.
- Assessed security vulnerabilities and configuration risks across cloud and on-prem systems, recommending and implementing mitigation strategies.
- Hardened endpoint and server configurations using Group Policy Objects (GPOs) aligned with security baselines.
- Collaborated with security, infrastructure, and compliance teams to remediate vulnerabilities and strengthen overall security posture.
- Contributed to asset management and lifecycle tracking to support compliance reporting and operational visibility.
- Documented security standards, procedures, and system configurations for audit and operational use.

Cloudforce — System Administrator *May 2024 – October 2025*

- Administered and secured Azure and Microsoft 365 environments, implementing identity and access controls using Entra ID, RBAC, MFA, and Conditional Access.
- Monitored and analyzed cloud security telemetry using Azure Monitor and Log Analytics to detect misconfigurations, anomalies, and potential threats.
- Investigated security incidents and alerts, performing root cause analysis and supporting remediation efforts across cloud environments.
- Supported cloud security posture management by identifying configuration gaps and enforcing security baselines across Azure resources.
- Managed patching and security updates for Azure VMs and AVD environments to maintain compliance and system integrity.
- Supported ISO and CMMC compliance initiatives through access reviews, audit preparation, and control validation.
- Built dashboards and reporting solutions to provide visibility into security risks, system performance, and remediation progress.

Synergy Interactive — Identity & Access Management Administrator *October 2022 – April 2024*

- Managed identity lifecycle operations, including RBAC, SSO, and MFA enforcement across enterprise platforms.
- Conducted access reviews and supported compliance and audit readiness initiatives.
- Built Power BI dashboards to track access governance and operational performance metrics.
- Supported secure system integrations and identity federation across cloud-based applications.
- Documented IAM processes, system configurations, and access control procedures.

U.S. Secret Service — LMS Helpdesk Analyst *August 2020 – June 2022*

- Provided Tier 1–2 technical support in a regulated and security-sensitive environment.
- Resolved authentication, access, and connectivity issues across enterprise systems.
- Maintained secure account records and access documentation aligned with compliance requirements.
- Developed user training materials and troubleshooting documentation.