HUSSEIN OMAR

(206) 915-4736 | Omarsecure30@gmail.com | Austin, TX | linkedin.com/in/fullstackomar

Cybersecurity Engineer with 3+ years securing enterprise data and cloud environments, specializing in data protection, exposure remediation, and identity security at scale. Recently promoted for leading a Data Protection team responsible for monitoring 163+ TB of files and remediating over 2.1 million exposed sensitive records. Skilled across Varonis, Microsoft Purview, Defender for Cloud Apps, and Azure security tooling.

RELEVANT SKILLS

Security Platforms: Varonis DatAdvantage & SaaS, Microsoft Defender for Cloud Apps (MDCA), Microsoft Purview DLP, Microsoft Sentinel, Exabeam

Cloud & Container Security: Kubernetes, Docker, Terraform, CI/CD Pipeline Security, Cloud Security Posture Management (CSPM), Zero Trust Architecture

Security Operations: Threat Hunting, Vulnerability Management, Incident Response, SIEM, Data Classification & DLP, Exposure Remediation

Identity & Cloud: Azure AD, Azure Security, RBAC, PIM, Conditional Access, Active Directory, Azure Policy

Networking & Infrastructure: TCP/IP, Firewalls, Nasuni File Servers, ServiceNow, Linux/Bash, SCCM

Scripting & Development: PowerShell, Python, Git/GitHub, GitLab, HTML/CSS/JavaScript

Productivity & Collaboration: Microsoft Office Suite, Microsoft Teams, OneDrive, UXD

EXPERIENCE

Boeing Employee Credit Union, Seattle, WA

Cybersecurity Engineer *March 2026 – Present*

- Lead the Data Protection team's monitoring of 163+ TB of files and folders across the organization's file server environment.
- Run data classification scans against 25+ critical servers to identify, categorize, and track sensitive data at scale.
- Expanded monitoring and scanning coverage to 3.3 million sensitive files using Varonis SaaS.
- Identified 2.1 million sensitive files exposed organization-wide through global group permissions.
- Remediated 2.1 million+ exposed sensitive files using Varonis automation, reducing overall exposure by 85.5%.
- Deployed Microsoft Defender for Cloud Apps (MDCA) sanctioning policies to block newly identified, unauthorized generative AI applications.
- Rolled out multiple Microsoft Purview DLP policies to prevent data exfiltration and reduce the organization's attack surface.

Cybersecurity Administrator (FTE) *September 2024 – March 2026*

- Strengthened security posture by implementing Microsoft Defender for Cloud, Sentinel, and automated response workflows.
- Managed and secured 500+ Azure resources, including VMs, storage accounts, networking, and security configurations.
- Closed 95% of security-related tickets within SLA by optimizing incident response processes and automating remediation tasks.
- Improved compliance posture by 30% by implementing Microsoft Purview, Azure Policy, and security baselines.
- Administered Azure AD for 5,000+ users, managing RBAC, PIM, conditional access, and identity protection policies.
- Reduced VM vulnerabilities by 50% by enforcing Defender for Servers, patch management, and security hardening best practices.
- Increased log analysis efficiency by 60% using KQL queries, Azure Monitor, and Log Analytics for threat hunting.

Digital Asset Protection Admin (Contractor) *April 2024 – September 2024*

- Ran automated exposure remediation policies on the Nasuni file server, cutting global security group permissions on folders by over 40%.
- Performed weekly maintenance and upgrades on Data Protection-owned servers and applications to maintain performance and security.

- Authored knowledge base articles for new processes and applications, supporting efficient troubleshooting and onboarding.
- Resolved 400+ ServiceNow Data Asset Protection (DAP) tickets, providing timely support to employees and members.
- Contributed to data protection policy development within Microsoft Purview, strengthening the organization's data security framework.

Digital Asset Protection Intern *September 2023 – April 2024*

- Helped onboard Varonis SaaS and troubleshot file server connectivity and event collection issues.
- Assisted in building and enabling inconsistent-permission remediation policies, remediating 50,000+ folders on the Nasuni file server.
- Created knowledge base articles for Varonis SaaS to support future troubleshooting and remediation work.
- Assisted in onboarding Varonis DatAlert into the SOC team's Exabeam alert monitoring tool, improving the team's ability to monitor and respond to Varonis SaaS security alerts.

Allied Universal, Seattle, WA

IT Technical Support, Tier 2 *January 2022 – September 2023*

- Managed Active Directory for 200+ users, including user and group creation, OU structure design, and permission assignments.
- Resolved ServiceNow tickets with an average resolution time of 45 minutes and a 95% first-call resolution rate.
- Automated routine Active Directory tasks with PowerShell scripts, reducing ticket resolution time by 35%.
- Deployed and maintained software across 150+ endpoints via SCCM, and managed Windows servers for updates, backups, and security hardening.
- Installed Microsoft Defender Antivirus on 15+ on-premises servers.

EDUCATION

Western Governors University
B.S., Cybersecurity and Information Assurance | GPA: 3.95

Seattle Central College, Seattle, WA
A.S., Programming and IT Support | March 2021 – March 2023 | GPA: 3.92

Year Up / Seattle Central College, Seattle, WA
Certificate in Computer Network Support | April 2023 – September 2023 | GPA: 4.0

- Completed coursework in IT Helpdesk, Project Management, Microsoft Applications, and Business Communications, with specialized training in Computer Network Support.

CERTIFICATIONS & TRAINING

Certifications: CompTIA Security+, CompTIA Network+, CompTIA A+, CCNA, AZ-500 Azure Security Engineer, AZ-900 Azure Fundamentals, SC-900 Security Compliance and Identity, Oracle Cloud Foundations Associate

Additional Training: Rapid Ascent Cybersecurity Certificate, Google's Automate Cybersecurity Tasks with Python