Mohammed Alrashid

Security Engineer

Salt Lake City, UT | mohammed@malrashid.com | (541) 514-3151
malrashid.com | linkedin.com/in/mohammedh-alrashid

PROFILE

Security Engineer with experience securing a building automation platform across GCP, Azure, Entra ID, and on-premises infrastructure. Own vulnerability management, IAM, incident response, and platform risk reviews. Interested in penetration testing and zero trust security.

EXPERIENCE

Security Engineer | PassiveLogic Feb 2024 - Present

- Own authenticated scanning with Rapid7 InsightVM across cloud, server, and endpoint environments; track remediation SLAs and coordinate patch campaigns through Jamf and Intune.
- Use Wiz across GCP and Azure to identify and close attack paths involving public exposure, static credentials, and excessive IAM permissions; consolidate findings into a shared remediation queue.
- Manage SAML and OIDC federation, SCIM provisioning, workforce identity federation, and Conditional Access in Entra ID and GCP, including guest access and MFA.
- Investigate phishing, business email compromise, account compromise, and token or session abuse using Microsoft Defender for Office 365; lead response through root cause analysis and postmortems.
- Review internally developed platforms before release for unsafe remote execution, credential handling, and excessive privilege; authored a tiered framework for cloud, OAuth consent, secrets, and infrastructure as code controls.
- Design and operate firewall failover, VLAN segmentation, site-to-site and remote access VPNs, and availability monitoring; validate failover under live conditions.
- Own security control evidence and audit responses supporting SOC 2 and GDPR requirements.

Security Intern | PassiveLogic Aug 2023 - Dec 2023

- Established the company's first documented cloud security controls across GCP, Azure, and Microsoft Exchange.
- Assessed cloud and network security posture, managed vulnerabilities, and administered IAM in GCP and Azure Active Directory toward least privilege.

TECHNICAL SKILLS

Cloud and identity: GCP, Azure, Entra ID, SAML, OIDC, SCIM, Conditional Access
Security: Rapid7 InsightVM, Wiz, Defender for Office 365, CVSS, CSPM, SAST/SCA, SPF/DKIM/DMARC
Network: VLANs, firewall policy, high availability, WireGuard, site-to-site VPN, DNS, TLS/PKI
Platforms and code: Linux, Windows, macOS, Python, Bash, SQL, C++, Terraform, Git, Docker, Proxmox
Governance and languages: SOC 2, GDPR, policy and audit support | English and Arabic (fluent)

HOME LAB

Self-hosted infrastructure and local AI. Run Proxmox with filtered DNS, a reverse proxy and automated TLS, file and media services, scheduled backups with restore validation, and health monitoring. Isolate lab, IoT, and management networks with VLANs and firewall rules; use a dual-GPU inference server to explore security tooling.

EDUCATION

B.S. Cybersecurity and Network Management | Minor in Computer Science
Weber State University, Ogden, UT | December 2023