Zachary Woo

SECURITY-AWARE IT TECHNICIAN

San Ramon, California | zachary.chinn.woo@gmail.com | linkedin.com/in/zachary-woo

PROFESSIONAL SUMMARY

Security-aware IT Technician with hands-on experience supporting users, endpoints, accounts, and operational processes in a multi-site environment. Primary direction: Endpoint Support and IAM. Additional direction: GRC, IT Compliance, and Security Operations.

PROFESSIONAL EXPERIENCE

IT Technician | Futures Explored, Inc.

April 2026 - Present | Multi-site nonprofit IT

- Provisioned or redeployed 35+ Windows, macOS, ChromeOS, and mobile devices, including Entra joins, software configuration, MDM verification, inventory updates, and user handoff.
- Reduced a Jira helpdesk backlog from approximately 160-180 tickets to 57 after 80+ follow-ups, closing stale or resolved items and prioritizing active work by operational impact.
- Supported enterprise password manager adoption through evaluation, rollout materials, role-based access organization, onboarding 16 employees, and migration and recovery follow-up.
- Used Datto to audit approximately 20 endpoints, remediate authorized update issues, and escalate monitoring, activation, storage, and configuration risks.
- Detected and quarantined malware on a shared endpoint using Microsoft Defender, initiated deeper scanning, expanded endpoint review, and documented concerns for escalation.
- Supported Google Workspace, Microsoft 365, Microsoft Admin, and Entra account workflows while creating provisioning, phishing-awareness, secure-deletion, and authentication guidance.

Tech Support | Bay Alarm Company

March 2026 - April 2026

- Troubleshot alarm, access-control, CCTV, and IP-connected security system issues using remote programming tools, service logs, documentation, and defined escalation paths.

Volunteer IT Support | St. Raymond Catholic Church

January 2026 - March 2026

- Troubleshot public-facing AV and livestream systems, restricted unauthorized wireless access, validated changes, and documented baseline configurations and operational risk.

EDUCATION AND CERTIFICATIONS

B.S. Software Engineering Minor in Justice Studies	San José State University 2025
CompTIA Security+	SY0-701 | February 2026
Google Cybersecurity Certificate	December 2025

SELECTED TECHNICAL PROJECTS

Active Directory Domain Deployment & RBAC

Built an isolated Windows domain, configured AD DS and DNS, created an OU and security-group structure, joined a Windows client, and validated role-based access with representative accounts. Scope was a single-domain home lab without enterprise-scale automation.

Wazuh SIEM Incident Response

Correlated Linux SSH, PAM, and sudo alerts; reconstructed an authentication timeline; mapped observed behavior to MITRE ATT&CK; and verified that no successful unauthorized login or privilege escalation was observed. This was controlled home-lab activity, not production SOC ownership.

SSH Brute-Force Detection & Mitigation

Analyzed native Linux authentication logs, separated remote SSH activity from local PAM events, configured fail2ban, and validated that the source was blocked after the configured threshold. The environment was small and simulated.

Secure Router Provisioning & Hardening

Factory-reset and reprovisioned a previously used router for a WAN-isolated workload, applied WPA3 and protected management frames, disabled unnecessary remote services, and documented residual risk and manual maintenance needs.

TECHNICAL SKILLS

Endpoint & systems	Windows 10/11, macOS, ChromeOS, iOS/iPadOS, Ubuntu Linux, device provisioning, Entra joins, MDM verification, software configuration
IAM & administration	Google Workspace, Google Admin, Microsoft 365, Microsoft Admin Center, Microsoft Entra ID, user provisioning, account termination, security groups, MFA, passkeys, Dashlane
IT operations	Jira Helpdesk, Datto, AssetTiger, Addigy, Splashtop, OneDrive, Microsoft Teams, Google Drive, asset tracking, multi-site support
Security & documentation	Microsoft Defender, Wazuh SIEM, BitLocker, secure deletion, endpoint audits, least privilege, incident documentation, SOP development, phishing training