ZACHARY MILLA

South Jordan, UT • hello@zacmilla.com • linkedin.com/in/zac-milla • zacmilla.com

SUMMARY

Security-focused IT professional with 10+ years of experience spanning endpoint security, identity & access management, and compliance. Deep hands-on background with Microsoft Entra ID, Intune, SentinelOne, Jamf Pro, and Automox, with a strong interest in threat intelligence and OSINT-driven security practices. Proven ability to build and enforce Zero Trust controls, automate user lifecycle workflows, and drive SOC 2, ISO 27001, and TISAX compliance — translating technical security work into measurable risk reduction.

PROFESSIONAL EXPERIENCE

Degreed — Salt Lake City, UT

Sr. IT System Administrator — May 2026 – Present

- Serve as subject matter expert for Automox, SentinelOne, Microsoft Intune, and Jamf Pro, leading endpoint security and compliance initiatives across a 300+ device fleet.
- Conduct endpoint incident response 3–4 times per week via SentinelOne, triaging alerts and enriching indicators in VirusTotal — including leading the full investigation of a macOS infostealer incident (InstallFix malvertising campaign) involving credential exfiltration, cloud token theft (AWS/Azure/GCP), and root-level persistence installation, completed within 96 seconds of initial execution.
- Designed and enforced Conditional Access Policies and SSO integrations (SAML/OIDC) via Microsoft Entra ID, reducing unauthorized access incidents and strengthening identity governance posture.
- Implemented Zero Trust authentication methods — including Windows Hello for Business, passkeys, and PSSO — eliminating password-based attack surface across the organization.
- Automated user lifecycle management across BetterCloud, Google Workspace, Microsoft Entra ID, and Intune, cutting provisioning time by 40% and reducing audit findings related to access control.
- Collaborated cross-functionally with security and compliance teams to achieve and maintain SOC 2 Type II, ISO 27001, and TISAX certifications.
- Built and maintained IT policy documentation, runbooks, and a self-service knowledge base, enabling helpdesk representatives to resolve Tier 1/2 issues without escalation.
- Managed MDM deployments via Microsoft Intune for Windows and macOS, implementing configuration and compliance profiles that improved device security posture and streamlined new-hire onboarding.

IT System Administrator — April 2021 – May 2026

- Spearheaded endpoint security tooling evaluation and rollout, establishing Automox and SentinelOne as the organization's primary patch management and EDR platforms.
- Drove initial implementation of Zero Trust Conditional Access policies and SSO integrations, laying the foundation for the organization's identity governance program.
- Led automation of onboarding and offboarding workflows across Google Workspace, Entra ID, and Intune, reducing manual provisioning steps by 40%.
- Supported SOC 2, ISO 27001, and TISAX audit preparation by maintaining accurate access logs, policy documentation, and control evidence.

IT Service Desk Representative — November 2018 – April 2021

- Delivered Tier 1/2 end-user support, handling hardware/software troubleshooting and asset management across a growing remote workforce.
- Maintained accurate access logs and documentation to support internal audits and compliance reviews.

- Promoted to IT System Administrator within 2.5 years for technical excellence and proactive contributions to IT operations.

Morgan Stanley
South Jordan, UT

Client Service Professional
November 2017 – November 2018

- Provided technical and account support for client-facing financial web portals, ensuring secure access and data integrity through client education and troubleshooting.

Independent IT Consultant & Web Developer
Salt Lake City, UT

Freelance
January 2015 – November 2017

- Designed and secured office networks and infrastructure for small business clients, including firewall/router configuration and network troubleshooting.
- Delivered WordPress web development with a focus on data protection and SEO; managed hardware procurement for 10+ client engagements.

Earlier Career

Box Support – Computer Technician (2014–2015) • *eFixnow – Computer Technician (2013–2014)* • *Wells Fargo – Collector (2012–2013)* • *Musician's Friend – Technical Support (2011–2012)*

VOLUNTEER & SECURITY RESEARCH

Guardian Group — Project 1591®
Remote

Volunteer OSINT Analyst
January 2025 – Present

- Conduct passive OSINT investigations in support of U.S. law enforcement efforts to identify underage victims of sex trafficking, working exclusively with publicly available information sourced from the surface web.
- Execute end-to-end investigations averaging 8–14 hours each, pivoting from escort platform indicators (phone numbers, usernames, emails) through Maltego, SpiderFoot, Shodan, and Google Dorks to establish true identity and corroborate age.
- Completed approximately 10 full investigations to date, producing structured lead submissions with documented sources, analysis steps, and visual corroboration — forwarded to law enforcement agencies upon Guardian Group validation.

Personal Security Research Lab (Proxmox VE Homelab)
2024 – Present

- Built and maintain a VLAN-segmented Proxmox homelab with a dedicated OSINT research environment (CSI Linux) isolated on its own VLAN with all egress routed through ProtonVPN/WireGuard to prevent home IP exposure during live investigations.
- Designed an air-gapped malware sandbox (separate VLAN, full egress block at the firewall) for safe detonation and analysis of threat samples without internet exposure.

Publications & Research

“What Happens When a Developer Runs a Fake Claude Code Installer” — April 2026

Full IR walkthrough of a real macOS infostealer incident (InstallFix malvertising campaign): 6-phase attack chain reconstruction from SentinelOne EDR telemetry, forensic imaging of an M-series MacBook with FileVault, control gap analysis (SentinelOne + BeyondTrust), and published IOCs for defensive use.

CERTIFICATIONS

CompTIA Security+ • **ISC2 Certified in Cybersecurity (CC)** • CWCT Cloud Systems Administration – Ivy Tech • Mastercard Cybersecurity Virtual Experience – Forage

TECHNICAL SKILLS

Security & Compliance	SentinelOne, Microsoft Defender, Conditional Access, Zero Trust, SOC 2, ISO 27001, TISAX
Identity & Access Management	Microsoft Entra ID (Azure AD), SSO (SAML/OIDC), Windows Hello for Business, Passkeys, PSSO, MFA
Endpoint Management	Microsoft Intune, Jamf Pro, Automox, Configuration & Compliance Profiles, MDM/MAM
Automation & Lifecycle Mgmt	BetterCloud, Google Workspace, PowerShell, Bash, Python (scripting/automation)
Platforms & OS	macOS, Windows, Linux
Threat Intelligence & OSINT	Maltego, SpiderFoot, Shodan, VirusTotal, CSI Linux, Google Dorks, passive OSINT, PAI collection, indicator pivoting
Documentation & GRC	Policy authoring, runbook creation, audit preparation, risk & compliance frameworks

EDUCATION

Valley High School 2011
High School Diploma • South Jordan, UT