

AUSTIN SILANO

Los Angeles, CA | austin@austinsilano.com | linkedin.com/in/austinsilano | austinsilano.com

EXPERIENCE

Crexi, Los Angeles, CA

May 2026 – Present

System Administrator

- Led migration and security cutover from outsourced MSP to in-house operations across CrowdStrike Complete, Avanan, Dropsuite, and NinjaOne — establishing full internal ownership of endpoint, email, and RMM security tooling.
- Own vulnerability triage and remediation lifecycle for all corporate IT security findings — achieving 100% triage and remediation rate with <5 minute MTTR.
- Audit systems and partner cross-departmentally to close visibility gaps and prevent scope creep, while preparing and evaluating SOC2 controls ahead of upcoming audits.
- Coordinate threat detection across CrowdStrike Complete, Arctic Wolf MDR, and NinjaOne ticketing, and run Falcon Shield SaaS posture management — catching anomalous OAuth grants and unauthorized third-party app access with automated remediation.
- Author security policies, IR playbooks, and SOPs; train helpdesk staff on vulnerability triage and remediation workflows — extending security coverage beyond the security team.

Fuel Cycle, Los Angeles, CA

July 2025 – May 2026

System Administrator – AI & Security

- Monitored and responded to 30+ daily security incidents using Rapid7, CrowdStrike, and ZScaler — risk-based triage, threat detection, and incident response — reducing MTTR by 35%.
- Primary technical liaison for SOC2 Type II audit — coordinating evidence across 100+ controls, interfacing with external auditors, and validating control effectiveness — achieving certification.
- Executed SIEM migration from Rapid7 to NGSIEM with zero SOC downtime — validating alert fidelity and maintaining 100% security visibility throughout.
- Led AI governance program — shadow AI detection via ZScaler, Okta SCIM controls, and ISO 42001-aligned policies — blocking unsanctioned AI tool usage before data exposure.
- Designed and implemented a multi-account AWS environment (Prod, Staging, Security, Monitoring) for an internal IT initiative — federating Identity Center with Okta for SSO/SCIM-based access control, and managing secrets and encryption via Secrets Manager and KMS, with S3/Glacier for data storage and archiving — establishing least-privilege access and centralized identity governance across environments.

Advanced Networks, Los Angeles, CA

July 2024 – July 2025

System Administrator

- Conducted vulnerability management across 20+ networks — remediating 60+ critical and high vulnerabilities across SonicWall, Cisco Meraki, Unifi, and ESXi — reducing client attack surface by 80% and maintaining 98% patch compliance.
- Investigated and remediated Active Directory authentication attacks including password spraying across 15+ clients — Entra ID log analysis, IP geolocation correlation, and conditional access implementation — eliminating unauthorized access attempts within 48 hours.
- Secured email infrastructure for 15+ law firm and enterprise clients using Proofpoint and Zix — tuning detection policies, enforcing SPF/DKIM/DMARC, and coordinating phishing remediation — reducing successful phishing delivery rate by 25%.

Skydance Interactive, Santa Monica, CA

February 2023 – March 2024

IT Technician

- Configured VPN access, whitelisted IP addresses for network/cloud resources, and identified and addressed security vulnerabilities.
- Collaborated in deployment of ESXi, creating 5+ VMs and managing server resources; contributed to server rack installations and upgrades.
- Utilized Active Directory to create/organize 30 new users, unlock accounts, assign privileges and groups, and enforce group policies.

PROJECTS

Argus — Open Source AI Security Posture Assessment Tool 2026

- Identifying shadow AI via OAuth inventory and DNS analysis — classifying tools across seven security risk factors including data retention, compliance certifications, and encryption standards — generating risk scores with Approved/Conditional/Prohibited classification.
- Maps findings to ISO 42001 and OWASP LLM Top 10 with automated PDF report generation — addressing the AI governance gap that enterprise tools solve at six-figure cost with no accessible mid-market alternative. Stack: Python FastAPI, PostgreSQL, React, M365 and Google Workspace OAuth.

Pyzuh — Open Source Python Library for Wazuh SIEM 2024

- 150+ Wazuh SIEM API functions covering user management, agent inventory, and security statistics — reducing SOC automation development time.

SKILLS

Security Operations: Incident Response, Threat Detection, SIEM Analysis, EDR Investigation, Alert Triage, IOC/IOA Analysis, SOAR Automation, Threat Hunting, MITRE ATT&CK

Compliance & Frameworks: SOC2 Type II, ISO 27001, ISO 42001, OWASP LLM Top 10, Third-Party Risk Management

Security Tools: CrowdStrike Falcon, Rapid7, Mimecast, Proofpoint, ZScaler, Okta, BlackKite, KnowBe4, Microsoft Defender, Fusion SOAR, n8n

Networking & Cloud: AWS (Identity Center, IAM, Secrets Manager, KMS, S3/Glacier), Azure/Entra ID, Google Workspace, Terraform, Docker, FortiGate, Cisco Meraki

Query & Automation: KQL (Defender), CQL (CrowdStrike), Python, PowerShell, Bash, Ansible, Terraform IaC

Identity & Access: Okta SAML/SCIM/SSO, AWS Identity Center, Azure AD/Entra ID, Active Directory, Conditional Access, MFA, Zero Trust

CERTIFICATIONS

CompTIA Security+ | CySA+ | Pentest+ | Network+ | A+ | SSCP (ISC2) | LPI Linux | ITIL Foundations

EDUCATION

Western Governors University, Salt Lake City, Utah
B.S. Cybersecurity and Information Assurance