AUSTIN SILANO

518 Raymond Ave, Santa Monica, CA 90405 | (949) 469-1316 | austin@aquese.com | linkedin.com/in/austinsilano

EXPERIENCE

Fuel Cycle, Los Angeles, CA
System Administrator – AI & Security July 2024 – Present

- 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.
- Built automated containment workflow using Fusion SOAR and n8n — enabling single-input endpoint isolation — reducing manual response time by 40% across concurrent incidents.
- 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.
- Conducted 5+ third-party vendor risk assessments using BlackKite — evaluating vendor security posture and generating risk scores that directly informed procurement and legal decisions.

Advanced Networks, Los Angeles, CA
System Administrator July 2023 – July 2024

- 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
IT Technician February 2023 – March 2023

- Identified 10+ security vulnerabilities through network and cloud assessments — tracking remediation and coordinating fixes with technical teams.
- Administered Active Directory access controls for 30+ users — provisioning, privilege assignment, and GPO enforcement ensuring least privilege.

PROJECTS

Argus — Open Source AI Security Posture Assessment Tool 2026 – Present

- 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, Microsoft Sentinel, Wazuh, Mimecast, Proofpoint, ZScaler, Okta, BlackKite, KnowBe4, Microsoft Defender, Fusion SOAR, n8n
Networking & Cloud: AWS, Azure/Entra ID, Google Workspace, Terraform, Docker, Proxmox, FortiGate, Palo Alto, Cisco Meraki
Query & Automation: KQL (Sentinel/Defender), CQL (CrowdStrike), Python, PowerShell, Bash, Ansible, Terraform IaC
Identity & Access: Okta SAML/SCIM/SSO, 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 June 2024
B.S. Cybersecurity and Information Assurance