Conner Jordan

Software Engineer II

+1 (805) 975-9793 | connercharlesjordan@gmail.com | San Luis Obispo, CA
linkedin.com/in/conner-jordan-4b268514a | github.com/cjordan223 | connerjordan.com

PROFESSIONAL SUMMARY

Security-aware full-stack engineer who delivers accessible, reliable systems end-to-end, building secure internal tools with React, Python, and CI/CD automation while integrating AI to empower educators and learners globally

TECHNICAL SKILLS

Security Engineering & Automation: Vulnerability remediation automation, endpoint hardening workflows, patch orchestration, deployable security controls

Cloud & DevSecOps: AWS ECS, Docker, CI/CD automation, infrastructure as code, secrets management, Microsoft Graph API, CrowdStrike RTR

Security Data, Analytics & AI: Asset correlation, Pandas/NumPy log analytics, RAG pipelines (LangChain + vector databases), retrieval tuning, AI governance

WORK EXPERIENCE

University of California, Office of the President
Oakland, CA (Remote)

Security Engineer
March 2025 - Present

- Delivered Coraline, an open-source-ready Dockerized Flask and React security tool on AWS ECS that ingests and correlates data from five disparate security and IT inventory sources; implemented hierarchical confidence-matching algorithms to reconcile over 500 drifted assets across 7,000+ endpoints.
- Engineered an AI-augmented security chatbot using LangChain and vector databases, enabling instant retrieval of SecOps knowledge across the organization while ensuring governance and auditability for internal deployments.
- Developed API-driven vulnerability response automation for macOS and Windows endpoints, analyzing vulnerability classes and accelerating patch deployment to meet University-wide cybersecurity mandates.
- Architected secure server infrastructure for a 2,900-user identity portal; led cross-departmental integration of MFA providers and enforced strict network security protocols through code review and secure implementation practices.
- Translated complex security requirements into deployable controls by partnering across IAM, Networking, and Endpoint teams; communicated technical architectures to engineers and leadership to drive informed decision-making.
- Operationalized standardized asset remediation across UC's developer ecosystem through org-wide runbooks, supporting secure adoption of AI tooling and internal security services.

Great Wolf Resorts
Chicago Corporate Office (Remote)

Security Support Engineer
May 2023 - March 2025

- Built Python and PowerShell automation tools for hybrid Azure tenant management, deploying endpoint agent updates, patching, and BitLocker enforcement across 10,000+ devices.
- Developed a PowerShell CLI tool integrated with Microsoft Graph API to manage distribution lists of 10,000+ users, eliminating manual error and reducing annual workload significantly.
- Built Python-based log analysis frameworks in Rapid7 using Pandas and NumPy, developing data pipelines and dynamic visualizations to detect anomalous behavior and common vulnerability patterns.
- Created custom Python tools to analyze phishing simulation data from KnowBe4, transforming raw metrics into actionable insights that improved organizational compliance rates.
- Engineered certificate deployment tooling using CrowdStrike RTR and PowerShell, preventing service disruptions and saving substantial engineering hours through automated remediation.

Simple.biz
Durham, NC (Remote)

Freelance Web Developer
August 2022 - May 2023

- Delivered production-grade web applications to paying clients, building CI/CD pipelines with automated build and deployment scripts that ensured consistent, secure releases.
- Integrated WCAG accessibility compliance checks into development workflows using Selenium, surfacing issues early and reducing user-reported defects.
- Conducted systematic cross-browser and cross-device compatibility testing with scripted automation, root-causing rendering discrepancies and reducing user-reported issues.

EDUCATION

California State University - Monterey Bay

B.S., Computer Science

Capstone Award for Innovation

Developed PhishFinder, a security tool comprising a Chrome extension and Python backend API that performs automated analysis of SPF, DKIM, and DMARC protocols using NLP and LLM-based classification to detect phishing attacks; awarded Most Innovative Project at the 2024 Capstone Festival.

CERTIFICATIONS

AWS Certified Cloud Practitioner *January 2025*