Conner Jordan

Application Security Engineer

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

PROFESSIONAL SUMMARY

Application Security Engineer who builds production-grade automation and data-driven ASPM systems, bridging development, security, and compliance in cloud-native environments

TECHNICAL SKILLS

Security Engineering & Automation: Vulnerability remediation automation, endpoint hardening workflows, patch orchestration, deployable security controls, Python and PowerShell scripting for CI/CD gates

Cloud & Platform: AWS ECS, Docker containers, IAM roles and secrets management, CI/CD pipelines with Jenkins/GitHub Actions, infrastructure as code using Terraform and Ansible

Security Data & AI: Multi-source asset correlation, Pandas and NumPy log analytics pipelines, RAG pipelines using LangChain with ChromaDB and FAISS vector databases, retrieval evaluation via MRR and Recall@K metrics

WORK EXPERIENCE

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

Security Engineer
March 2025 - Present

- Designed and built Coraline, an open-source-ready Dockerized Flask and React security tool deployed on AWS ECS; integrated five disparate data sources including Qualys, Jamf, Active Directory, ServiceNow, and SentinelOne to build unified asset views using hierarchical confidence scoring and entity resolution heuristics across 7,000+ endpoints.
- Engineered an AI/ML-powered RAG security chatbot using LangChain, ChromaDB vector store, and sentence-transformers embeddings to index internal SecOps runbooks and vulnerability databases; enabled engineers to retrieve context-aware remediation guidance in under three seconds per query.
- Built API-driven vulnerability response automation using Python and the Jamf Pro API to classify vulnerabilities by severity and asset criticality, triggering automated patch workflows for macOS and Windows endpoints while maintaining audit trails compliant with University-wide cybersecurity mandates.
- Architected secure server infrastructure for a 2,900-user identity portal using Docker containers on AWS ECS; led cross-departmental integration of Okta and Duo MFA providers, enforced network segmentation through code review checklists and Terraform security modules.
- Translated complex FFIEC and SOC 2 compliance requirements into deployable controls by partnering across IAM, Networking, and Endpoint teams; documented control mappings in Confluence and presented technical trade-offs to engineering leadership using threat modeling diagrams.
- Pioneered audit-ready governance for AI security tooling across UC's developer ecosystem by creating org-wide runbooks that codified standardized asset remediation workflows, including rollback procedures and validation checks for AI-assisted triage decisions.

Great Wolf Resorts
Chicago Corporate Office (Remote)

Security Support Engineer
May 2023 - March 2025

- Built and maintained Python and PowerShell security automation tools for hybrid Azure tenant management, deploying CrowdStrike Falcon endpoint agents, applying monthly patch cycles, and enforcing BitLocker encryption across 10,000+ Windows and macOS devices using Azure Automanaged Compute.
- Developed security certificate deployment tooling using CrowdStrike RTR and PowerShell scripting to validate certificate validity across internal services, preventing service disruptions during renewal windows and eliminating manual certificate inventory tasks that saved approximately 200 hours annually.
- Engineered a PowerShell CLI tool integrated with Microsoft Graph API to manage distribution lists of 10,000+ users, implementing batch processing and error recovery logic to eliminate manual errors in onboarding and offboarding workflows across HR systems.
- Built Python-based log analysis frameworks in Rapid7 InsightVM using Pandas and NumPy to process vulnerability scan results, developing dynamic visualizations in Matplotlib that highlighted recurring vulnerability patterns across business units and asset categories.
- Developed custom Python tools to analyze phishing simulation data from KnowBe4, extracting behavioral signals such as click timing and device metadata; transformed raw metrics into actionable security insights that improved organizational compliance rates significantly.

Simple.biz
Durham, NC (Remote)

Freelance Web Developer
August 2022 - May 2023

- Delivered production-grade web applications to paying clients using React and Node.js, building CI/CD pipelines with GitHub Actions that enforced automated build validation, security scanning via ESLint and SonarQube, and deployment gates for production releases.
- Implemented automated security and accessibility testing using Selenium WebDriver with WCAG 2.1 compliance checks, integrating axe-core into CI pipelines to surface semantic HTML issues and ARIA labeling gaps before code merged to main branch.
- Conducted systematic cross-browser and cross-device compatibility testing using scripted automation in Puppeteer and Playwright, root-causing rendering discrepancies across Chrome, Firefox, Safari, and Edge to achieve measurable improvements in user-reported UI 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 feature extraction and LLM-based classification to detect phishing attacks; awarded Most Innovative Project at the 2024 Capstone Festival.

CERTIFICATIONS

AWS Certified Cloud Practitioner *January 2025*