Conner Jordan

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

Security/DevSecOps Engineer who ships production security services and automation (cloud + endpoints), translating requirements into deployable controls and measurable risk reduction

TECHNICAL SKILLS

Languages: Python, C, C++, TypeScript, Java, SQL, PowerShell, Bash, Swift, Rust, Go

Security Tooling: Security Tooling: Vulnerability management, SIEM, EDR, XDR, SOAR, endpoint management, patch orchestration.

AI/ML and Research: RAG pipelines, vector databases, NLP, retrieval evaluation and tuning, LLM developer tooling

Frameworks and Infrastructure: Flask, FastAPI, Django, React.js, Node.js, Docker, Spring Boot, MCP/FastMCP, Next.js

DevOps and CI/CD: CI/CD pipelines, infrastructure as code, configuration management, container orchestration, serverless compute, managed databases, secrets management, AWS/GCP/Azure

Databases: Databases: PostgreSQL, MySQL, MongoDB, DynamoDB, SQLite, Redis, Snowflake, ClickHouse, Databricks, vector databases.

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 & 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/ML-powered RAG security chatbot using LangChain, vector databases, and NLP techniques, establishing the technical standard for internal AI deployments and enabling instant retrieval of SecOps knowledge across the organization.
- Built API-driven vulnerability response automation for a heterogeneous fleet of macOS and Windows devices, analyzing vulnerability classes and accelerating patch deployment to ensure compliance with 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 both engineers and leadership to drive informed decision-making.
- Pioneered audit-ready governance for AI security tooling across UC's developer ecosystem, including org-wide runbooks that operationalized standardized asset remediation.

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 endpoint agent updates, patching, and BitLocker enforcement across 10,000+ devices.
- Developed security certificate deployment tooling using CrowdStrike RTR and PowerShell scripting, preventing service disruptions and saving an estimated 200 hours annually through automated remediation.
- Engineered a PowerShell CLI tool integrated with Microsoft Graph API to manage distribution lists of 10,000+ users, eliminating manual error and reducing annual workload by over 500 hours.
- 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.
- Developed custom Python tools to analyze phishing simulation data from KnowBe4, transforming raw metrics into actionable security insights that improved organizational compliance rates by 25 percent.

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.
- Implemented automated security and accessibility testing using Selenium, integrating WCAG/ADA compliance checks into development workflows to surface issues early and reduce defects.
- Conducted systematic cross-browser and cross-device compatibility testing with scripted automation, root-causing rendering discrepancies and achieving a 30 percent reduction in 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*