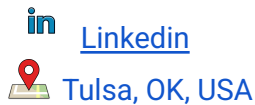


Jonathan Angeles

CYBERSECURITY & DATA SCIENCE PROFESSIONAL



9177022992

jonathan@nimda.sh

Summary

Driven Cybersecurity and Data Science professional with a decade of experience spearheading secure software development, risk management, and governance initiatives. Expert in applying cutting-edge data science and AI/ML methodologies to enhance cybersecurity posture, from vulnerability management to threat modeling. Committed to continuous learning, as evidenced by a Master's in Cybersecurity, post-graduate studies in AI/ML and Generative AI, and a comprehensive suite of industry certifications, including OSCP and AWS Cloud Practitioner.

Skills & Training

DS/AI/ML

- Supervised Machine Learning: Linear regression, logistic regression, and Decision Tree
- Ensemble Techniques
- Unsupervised Machine Learning
- EDA, Data Preprocessing & Customer Profiling, and Feature Engineering
- ML Model Selection & Hyperparameter Tuning
- AI - Neural Networks ANN, CNN, RNN, Computer Vision, and NLP
- Gen AI LAMA, Mistral, GPT4, W2V, RoBERT, BERT and RAG

Tools

- Scikit-learn, Pandas, Matplotlib,
- TensorFlow, Jupyter Notebook, NumPy, Scipy, Google Colab, Hadoop and RAG Pipelines

Core Security

- Security Information Systems
- Network Security Architecture
- Computer Forensics
- Linux Security
- Vulnerability Management Process
- Software Security Program

Programing Language

- Shell Bash Scripting
- Python
- JAVA

Soft Skills

- Curiosity, Teamwork, Adaptability, Creativity, Communication, and Self-motivated

Languages

- English Fluent
- Spanish Fluent

SecDevOps / Appsec

- CI/CD Security Checks SCA, SAST, SC, and DAST
- Threat Modeling STRIDE
- Software Security
- OWASP SAMM framework, MAESTRO framework
- OWASP TOP 10, OWASP TOP 10 API, CVSS V3
- OWASP TOP 10 for LLM
- Security Requirements
- Security Code Review

Tools

- Ansible, GIT, Snyk Code, Open Source, Snyk Security Container, and InsightAppsec Rapid7, Jenkins, BitBucket, Github, JIRA, Kubernetes, Docker, DefectDojo, Kali Linux, Burp Suite Proxy, ZAP proxy, JD-GUI, and Android Studio

Professional Experience

Seegrid Robotics Automation
Product Security Engineer

June 2024 - October 2025

- Strengthened the security of AI-driven applications by embedding security best practices across the ML and software development lifecycle.
- Conducted secure code reviews and application security testing for AI models, APIs, and supporting microservices.
- Collaborated with data scientists and developers to identify and remediate vulnerabilities in ML pipelines and data handling processes.
- Performed AI-specific threat modeling and risk assessments addressing issues such as model poisoning, data leakage, and adversarial manipulation.
- Ensured AI systems were designed and deployed with robust security, privacy, and integrity controls.

Jonathan Angeles

City National Bank

October 2022 - January 2024

Application Security Engineer

- Perform Pentesting, manual security code review, and deliver reports, collaborating with the development team to mitigate existing or potential security flaws and bugs.
- Review architectural designs for adherence to security principles.
- Reduced vulnerability backlog by 40% through CI/CD SAST,DAST,and SCA automation.
- I helped developers understand vulnerabilities findings and propose remediation solutions or mitigation controls.
- Designed and led City National's application security program, implementing the OWASP SAMM framework
- Defining and embedding technical security policies, principles, and standards within the application.
- Developed a Generative AI-powered ChatBot to address queries regarding Cyber Security Policies and Procedures.

Spoton, Los Angeles, CA

OCT 2019- OCT 2022

Machine Learning Engineer - Entry Level

- Teaming up with the Data Science team to explore and analyze data sources to build Data Sets
- Apply machine learning techniques to gain insights from the datasets previously built
- Building and Maintaining machine learning models to predict Churn Customer Scores using (Bagging and Random Forest, Boosting Classifier - AdaBoost, Gradient Boosting, XGBoost & Stacking Classifier using Hyperparameters Tuning)

DevSecOps Engineer

- Partner with product teams to help improve the security posture, ensuring the adoption of Software Security Practices
- Led implementation of 3 new security tools across 5 teams.
- Collaborate competently with other teams within the organization, performing regular security assessments through penetration testing, SAST, DAST, and SCA analysis, finding vulnerabilities, and providing mitigation recommendations to development teams
- Implement and automate Security Tools within the SDLC CI/CD. If appropriate, present threat models to validate and support the risk to the organization.
- Collaborating with the development team to mitigate existing or potential security flaws and bugs.

BBVA USA, Birmingham AL

November 2014 - September 2019

Application Security Engineer

- Plan, design and conduct penetration tests.
- Report vulnerabilities.
- Advice about security best practices.
- Stay up-to-date on security trends.
- Managing and performing application security vulnerability management.
- Assisting in the development of automated security testing to ensure the organization is following best practices.

Information Security Risk Analyst

- Assist with information security and privacy risk management
- Review architectural designs for adherence to security principles.
- Guide system and mission owners in making risk-informed decisions.

Jonathan Angeles

Education

Academia

[The University of Texas at Austin - Post-Graduate Program in Generative AI for Business Applications](#)
[MIT Applied Data Science Program- Leveraging AI](#)

[The University of Texas at Austin - Post-Graduate Program in AI/ML](#)

IPN - MSe in CyberSecurity

IPN - Post-Graduate Program in Computer Forensics & Technology

UNITEC - Bachelor's in Computer Science



[Github Portfolio](#)



[AI/ML Academic Portfolio](#)

[GenAI Academic Portfolio](#)



[AI/ML Academic Portfolio](#)

Certifications

Current	EC-Council: Ethical Hacking & Network Security Analyst Offensive Security: Offensive Security Certified Professional (OSCP)
2025	Michigan University: Python Specialization License JJNPP3EELKA3 CTZGH2JSFZ49 TWLRMTLM7EP2 B7E5PWZE80SZ
2022	University of Maryland: Security Specialization License VVBRASV96PWN
2012	Learn Quest: JAVA Programming License GK3B9OZPNXL2 GRM9HU28ZHF4
2009	Duke University: Programming with JavaScript, HTML, and CSS License TWLRMTLM7EP2
2008	University of Maryland, College Park: Software Security License VVBRASV96PWN Red Hat RHCSA License 170-171-573 Amazon Web Services: AWS Cloud Practitioner
2025	ML Model Deployment AI Agents program