Jon Dycaico

👤 🦊 🌐

jdycaico@protonmail.com | +15302204139

SUMMARY

Experienced Security Engineer with experience in detection and threat mitigation. Proven in creating detections, automating security, and managing SOAR platforms. Focusing on cybersecurity for crypto-focused companies.

EXPERIENCE

GAUNTLET TECHNICAL FELLOW   *JAN 2025 – FEB 2025*

GAUNTLET AI

- AI-coding and AI Engineering bootcamp, including RAG and multi-agent architectures

SENIOR SECURITY ENGINEER   *FEB 2024 – NOV 2024*

OKTA

- Built the Privacy Deletion Service in Go with Privacy team on k8s multi-cloud architecture

SENIOR CYBERSECURITY ENGINEER   *AUG 2023 – FEB 2024*

DOCUSIGN

- Tines Migration: migrated all of our SOAR logic from Houston to Tines
- Worked cross-functionally, performed Threat Modeling, extended Tines functionality
- Integrated SOC stack with AWS and Azure services, began an AI ticket auto-closure system

CYBERSECURITY ENGINEER   *APR 2020 – AUG 2023*

DOCUSIGN

- Maintained and extended Houston, our in-house SOAR, a proprietary fork of Huginn
- Built, tested, and maintained detections in Splunk and Azure Sentinel
- Assisted with security incidents such as Log4j using new detections and automation

ASSOCIATE, TECH-X PROFESSIONAL   *JUL 2019 – APR 2020*

T-MOBILE

- Trained models, rewrote Python code, managed CI for Product Analytics Jupyter notebooks

WEB MARKETING INTERN *JUN 2018 – AUG 2018*

MEDINTELLIBASE

- Administered WordPress site including SSL, HTML/CSS code, extensions and backups

EDUCATION

BA IN BUSINESS ADMINISTRATION *JUN 2019*

UNIVERSITY OF WASHINGTON

- Concentration: Management Information Systems
- Gray Hats Cybersecurity Club Treasurer

CERTIFICATIONS

CERTIFIED JENKINS ENGINEER *APR 2023*

CLOUDBEES

GIAC CERTIFIED WINDOWS SECURITY ADMINISTRATOR *MAY 2021*

SANS INSTITUTE

CYBERSECURITY RISK MANAGEMENT

UNIVERSITY OF WASHINGTON CONTINUUM COLLEGE *JUN 2019*

SKILLS

SOFT SKILLS

Quick Learner, Strong Communicator, Empathetic, Values-Driven, Cross-domain Translator

DATA

Jupyter notebooks, Pandas, Model training, Extract-Transform-Load, Risk Scoring, Tuning

SECURITY

Detection Engineering, Security Automation, SIEM, SOAR, MITRE ATT&CK, NIST CSF

ENGINEERING

Python, Ruby, Go, PowerShell, CI, Linux, Docker, Kubernetes, Terraform, AWS, Azure

INTERESTS

Crypto, Digital Privacy, Electronic Music, Health & Fitness, Technology & Society, History & Futurism, Internet Culture, The Great Outdoors, Other countries