Brian Wang

Austin, TX | brian.bwang@proton.me | 210-425-2556

SUMMARY

Senior Security Engineer specializing in enterprise-scale threat detection, AI security automation, and security platform engineering. Over 5 years of experience at Amazon developing detection systems across an environment spanning 3,000+ facilities and 200+ telemetry sources. Experienced in architecting agentic AI workflows with security guardrails, building automated detection validation infrastructure, and providing cross-functional technical leadership for AI-driven security initiatives.

EXPERIENCE

Amazon | Austin, TX
Senior Security Engineer | June 2021 – Present

- Engineered and deployed high-fidelity threat detections across a security environment spanning **3,000+ Amazon facilities and 200+ distinct telemetry sources**, enabling threat visibility across heterogeneous endpoint, network, and industrial control system (ICS) environments.
- Reduced detection development time by **50%** and documentation effort by **80%** by architecting an agentic AI platform using **LangGraph** and a custom **Model Context Protocol (MCP)** server to automate complex detection engineering workflows.
- Designed security guardrails for AI agent access to enterprise security telemetry, implementing a custom MCP integration with **Splunk** that validates generated Search Processing Language (SPL) queries before execution and provides environment-aware tools for detection development.
- Provide cross-functional architectural guidance and design reviews for AI-driven security initiatives, advising engineering teams on the technical design of **agentic incident response and threat hunting systems**.
- Architected an automated detection validation platform across **693 logistics facilities**, applying software engineering testing principles to continuously validate detection functionality and identify coverage gaps at scale.
- Expanded automated **MITRE ATT&CK validation coverage to 43%** by engineering benign network traffic canaries that simulate attacker behaviors and continuously test detection logic.
- Reduced validation runtime by **80%** and false positives by **85%+** through optimization of AWS Lambda services and statistically driven refinement of detection testing.
- Developed and reviewed production detections using **Splunk SPL, Linux auditd, risk-based alerting (RBA), and detection-as-code practices**, contributing to Git-based CI/CD workflows, peer code reviews, and detection quality standards.

- Led architectural design decisions for **Amazon Pharmacy's network traffic inspection infrastructure**, defining a security telemetry architecture supporting threat detection and visibility across sensitive healthcare environments.
- Authored detection engineering runbooks and standardized deployment workflows, enabling new security engineers to independently deploy detections to production RBA pipelines within **two weeks**.
- Remediated risks associated with legacy security infrastructure through system cleanup and decommissioning, reducing recurring maintenance costs by **$10,000 per month**.

FirstEnergy | Akron, OH
Security Analyst | May 2020 – August 2020

- Developed Python and JavaScript SOAR playbooks to automate security investigation and response workflows, reducing manual analyst effort and accelerating incident handling.
- Implemented MITRE ATT&CK-aligned threat intelligence workflows to automate indicator sharing and sightings reporting.
- Developed an automated threat intelligence aggregation tool using the Twitter API to collect indicators of compromise (IOCs).

Copart | Dallas, TX
Security Engineer | May 2019 – August 2019

- Doubled vulnerability scan processing efficiency by developing Python automation for vulnerability management workflows.
- Built a GitHub source code exposure detection tool using natural language processing and similarity analysis to identify potential proprietary code leaks.
- Conducted a security assessment of business applications and browser extensions across an enterprise environment of **10,000 endpoints**.

EDUCATION

Georgia Institute of Technology | Atlanta, GA
Master of Science, Cybersecurity | 2025

Texas A&M University | College Station, TX
Bachelor of Science, Computer Science | 2022

TECHNICAL SKILLS

Programming: Python, TypeScript, JavaScript, C++, Bash, SQL, Splunk SPL
Detection & Response: Detection Engineering, Detection-as-Code, MITRE ATT&CK, Adversary Emulation, Risk-Based Alerting, SIEM, SOAR, Threat Intelligence
AI & Security Automation: LangGraph, Model Context Protocol (MCP), AI Workflow Guardrails
Infrastructure & Tooling: AWS, Splunk, Linux, Docker, Git, CI/CD
Certifications: GPEN, GWAPT