Vishva Teja Chikoti

Cybersecurity | Applied AI | SDET / QA Automation

New Haven, CT | Open to opportunities throughout the United States

vishvatejack@gmail.com | https://github.com/ckvishwa

Professional Summary

CompTIA Security+ certified engineer with an M.S. in Cybersecurity & Networks and professional manual and automated testing experience at Cognizant, including Selenium and Java. Background combines enterprise application testing, REST API and database validation, log analysis, and hands-on projects in security detection, machine learning, and automated testing. Built a behavioral malware-analysis platform, a simulated enterprise SOC environment, cloud IAM attack-path analysis, and automated tests for distributed and cross-platform applications.

Technical Skills

- **Cybersecurity:** Splunk, SPL, Sysmon, MITRE ATT&CK, Windows event analysis, incident investigation, IOC extraction, timeline reconstruction, CAPEv2, YARA, Ghidra, Wireshark, Nmap, Burp Suite, Active Directory, AWS IAM concepts.
- **AI and data:** Python, Random Forest classification, SHAP explainability, feature extraction, model evaluation, NetworkX, graph-based risk analysis, AI API integration.
- **Testing:** Selenium, Java test automation, manual testing, Postman, Playwright, pytest, JUnit, Testcontainers, Vitest, React Testing Library, Flutter Test, functional and regression testing, API testing, database testing, concurrency testing, security testing.
- **Programming:** Python, Java, TypeScript, JavaScript, SQL, PowerShell; project experience with Dart and Rust.
- **Platforms and delivery:** Linux, Windows Server, VMware, Spring Boot, Flask, Next.js, React, Flutter, PostgreSQL, SQLite, SQLCipher, Supabase, Docker, Docker Compose, Git, GitHub Actions, Maven, Jira.

Professional Experience

Cognizant Technology Solutions

Quality Assurance and Test Automation *(functional description; official title to confirm)*

January 2022 - July 2023

- Performed manual testing and automated testing using Selenium and Java.
- Performed functional, regression, smoke, and post-change testing across more than 15 enterprise applications to support release readiness.
- Validated REST APIs using Postman and performed SQL-based database and data validation.
- Investigated application failures through Splunk and application/system logs, supporting defect reproduction and root-cause troubleshooting.
- Reported, tracked, and triaged defects in Jira; collaborated with engineering teams to retest fixes and validate releases.

Selected Projects

MalTrace - Behavioral Malware Analysis and Machine Learning

Python, CAPEv2, Random Forest, SHAP, VMware, Flask, MITRE ATT&CK

- Built a behavioral malware-analysis pipeline combining sandbox execution, feature extraction, machine learning classification, and prediction explanations.
- Extracted 54 behavioral and static PE features and evaluated classification across 64 malware families using a family-held-out evaluation design.
- Used SHAP to explain individual predictions and mapped detected behavior to MITRE ATT&CK techniques.
- Integrated CAPEv2 with VMware through a Flask control bridge to automate VM lifecycle operations and clean-snapshot restoration.
- Tested injected failure conditions and corrected malformed behavior and network-data handling.

Enterprise SOC Detection and Incident Response Lab

Splunk, SPL, Sysmon, Windows Server, Active Directory, Kali Linux, PowerShell

- Built a three-VM lab with a domain controller, Windows endpoint, and Kali Linux system for controlled security simulations.
- Configured Active Directory, DNS, Sysmon telemetry, and Splunk log collection.

- Completed 14 lab simulations, committed 8 SPL detection files, and analyzed more than 8,000 Windows and Sysmon events from controlled simulations.
- Investigated suspicious PowerShell, authentication attacks, persistence, SMB/RDP activity, and beacon-like network behavior.
- Produced eight investigation reports covering evidence, timelines, indicators, severity, false positives, and ATT&CK mappings.

Access Risk Analyzer - Cloud IAM Attack-Path Analysis

Python, NetworkX, AWS IAM concepts, Dijkstra, pytest

- Modeled identities, roles, permissions, and resources as a weighted graph using synthetic cloud IAM data.
- Applied shortest-path analysis to identify administrative escalation paths, including a scenario involving iam:PassRole and ec2:RunInstances.
- Generated least-privilege recommendations, risk reports, and machine-readable JSON/CSV outputs.
- Created automated tests enforcing security invariants.

REVA - Local-First Personal Assistant (Phase 1A)

Python, FastAPI, SQLite, Pydantic, pytest, GitHub Actions

- Implemented a local authenticated API for typed messages, explicit memory creation, retrieval, and audit events.
- Persisted user-approved memory in SQLite and tested restart recovery and source-aware retrieval.
- Added security tests for loopback-only binding, bearer-token authentication, and secret redaction.
- Configured Windows GitHub Actions checks for formatting, linting, types, and Python test suites.

FulfillX - Distributed Services and Test Automation

Java 21, Spring Boot, JUnit, Testcontainers, PostgreSQL, Flyway, Docker Compose, JWT

- Built authentication, product, and inventory services with automated service and integration tests against PostgreSQL; scaffolded the order service.
- Tested password hashing, JWT issuance and validation, role-based authorization, and database constraints.
- Validated atomic, idempotent inventory reservations and deterministic concurrency behavior.
- Used Docker Compose for service infrastructure and configured a GitHub Actions Java/Maven workflow; the workflow has not been validated on GitHub.

Education

M.S. in Cybersecurity & Networks

University of New Haven | 2025

B.Tech in Computer Science

Certifications

CompTIA Security+