Joel Suarez

☎ 714-217-6428 ✉ Gear8405@gmail.com in Profile 🌐GitHub

PERSONAL PROFILE

Cybersecurity professional with practical SOC experience and a proven ability to detect, investigate, and escalate security threats using tools like Splunk, Wireshark, and Burp Suite. Developed an AI-powered vulnerability detection tool using Python and OpenAI APIs, demonstrating initiative, technical skill, and innovation. Strong communicator with a client-facing background and working knowledge of key frameworks. Well-equipped to contribute to fast-paced security teams from day one.

CERTIFICATIONS

🎖️Foundations of Threat Intelligence | ArcX

🎖️Darkweb Radar Certification | SOC Radar Academy

🎖️Certified Associate in Cybersecurity | Fortinet

🎖️Network Security | Fortinet

EXPERIENCE

CyberNow Labs

SOC Analyst | Jun 2024 - Jan 2025

CyberNow Labs is a U.S.-based cybersecurity training company providing hands-on SOC simulation environments to help professionals gain real-world skills.

In this role, I am responsible for supporting threat detection and incident management, including:

- Monitored approximately 200 security alerts weekly using SIEM tools like Splunk and Elastic, enhancing early threat detection and reducing false alarms.
- Investigated and escalated critical incidents following MITRE ATT&CK guidelines, reducing incident resolution time by 15% during training exercises.
- Developed security policies aligned with NIST standards, improving network security posture in simulated environments.
- Collaborated with teams during red team/blue team exercises, helping decrease successful breach attempts by 20%.

AI-Powered Bug Bounty Tool Developer

Cyber Security Engineer | October 2024 - Present | Independent Project

This self-directed project focused on building an AI-powered tool to automate bug bounty reconnaissance and vulnerability detection, blending machine learning with cybersecurity practices. The project aimed to reduce manual workload and improve threat identification using LLMs and custom scripting.

In this role, I was responsible for designing and deploying the tool's core functionality, including:

- Developed a proof-of-concept bug bounty automation tool using Ollama-hosted LLMs with ChatGPT-assisted scripting, enabling faster vulnerability triage and data parsing across web targets.
- Integrated machine learning techniques like pattern recognition and NLP to improve exploit identification and reduce redundant findings during recon scans.
- Tested the tool across real-world web environments, conducting ethical security assessments that enhanced vulnerability detection speed and reporting clarity.

ADDITIONAL EXPERIENCE

Prior to transitioning into cybersecurity in 2024, I worked in various client-facing and account management roles at companies including Credit Glory and Kaseya. I am happy to provide additional information about these positions upon request.

Credit Glory

Account Manager

Jul 2023 - Jan 2024

Kaseya

Account Manager

Jan 2024 - Jun 2024

SKILLS

Cybersecurity & Technical Skills	Business & Communication Skills
● SIEM Tools – Splunk, Elastic ● Network & Vulnerability Analysis – Wireshark, Burp Suite, Shodan ● Bug Bounty & Ethical Hacking ● Familiar with CIA Triad, Access Control Models, Threat Vectors, and DISA Standards ● Scripting & Development – Python, CSS, JavaScript ● Prompt Engineering ● Terminal & Shell Proficiency – Kali Linux, WSL ● Tools & Platforms – Visual Studio Code, OpenAI API, Ollama LLMs	● Client Relationship Management – Supporting customer success and satisfaction ● Cross-Functional Collaboration – Working with technical, sales, and compliance teams ● Strategic Planning – Aligning client goals with security solutions ● Process Improvement – Streamlining workflows through automation and AI tools ● Conflict Resolution & Customer Retention – Managing sensitive financial or security issues with diplomacy