Lorenzo Karuppan

karupplo@mail.uc.edu linkedin.com/in/lorenzokaruppan

Education

University of Cincinnati Cincinnati, OH
Bachelor of Science in Cybersecurity — Minor in Computer Science — GPA: 3.7/4.0 Expected *May 2028*
Affiliations: Cyber@UC, Linux & FOSS, ITSA | **Relevant Coursework:** System Administration, Database Management, Network Monitoring & IPS, System Analysis & Design

Work Experience

Security Engineering Intern | Kroger May 2026 – Present
Cincinnati, Ohio

- Designed and deployed a Retrieval-Augmented Generation (RAG) service using Python, Azure Functions, REST APIs, and Microsoft 365 Copilot, enabling natural-language access to enterprise security policies and standards for **36,000+ associates**
- Built a Python and Playwright automation pipeline with checkpoint-based recovery to migrate 200+ governance records and approximately 119 policy PDFs from a legacy Governance, Risk, and Compliance (GRC) platform into Onspring, reducing a **50-hour manual process to under 2 hours** while improving auditability and data integrity
- Developed an automated **Agentic AI security red-teaming framework** using Microsoft Copilot Studio and Power Automate to generate adversarial prompts targeting prompt injection, data exfiltration, PII/PHI exposure, content moderation bypasses, and financial data handling, validating enterprise generative AI guardrails
- Architected a secure **software supply chain and CI/CD pipeline** using GitHub Actions, JFrog Artifactory, BigFix, cryptographic hashing, and code-signing validation to enable controlled releases, staged quarantine, and rollback for endpoint security software
- Engineered reusable REST API integrations using Python and Azure Functions with enterprise authentication, SSL certificate, and Zscaler proxy support
- Developed PySpark ETL pipelines to load governance and risk data into Azure Synapse Analytics and an enterprise data lake, supporting an **18-metric Cyber Health Score dashboard across five security domains**
- Investigated and triaged enterprise AI security alerts involving shadow AI, unsanctioned application usage, prompt injection, and potential sensitive-data exposure, while supporting migration of the enterprise AI security monitoring platform from Aim Security to Cato Networks

AI Model Trainer | Mercor August 2025 – January 2026

- Evaluated and ranked LLM outputs across multimodal datasets, writing detailed rubric-based feedback on factual accuracy, reasoning quality, and instruction-following to improve model alignment

Information Security Intern | Procter & Gamble June 2024 – October 2024
Cincinnati, Ohio

- Automated enterprise incident reporting workflows using Power Automate & Cortex XSOAR, saving **5,000+ hours annually** and eliminating manual reporting steps across the SOC's incident intake workflow
- Assisted with alert triage, investigation documentation, and escalation within enterprise security operations
- Defined & delivered a Business Continuity Plan potentially saving **$100,000+ in catastrophic incident costs**

Projects

AI-Powered Cybersecurity Chatbot | AWS Lambda, SageMaker, S3, IAM

- Built a serverless chatbot using AWS Lambda and SageMaker-hosted LLM with a controlled RAG architecture to securely retrieve internal policy data from S3
- Implemented role-based IAM policies to protect sensitive documentation

Wi-Fi Hacking Tool | Raspberry Pi, Python, Reinforcement Learning

- Developed and deployed a Wi-Fi penetration testing device using Raspberry Pi, leveraging reinforcement learning to optimize capture of WPA handshakes for wireless security analysis
- Gained hands-on experience with wireless protocols, ethical hacking techniques (deauthentication attacks, packet sniffing), and Linux-based system management

BadUSB | Raspberry Pi Pico, CircuitPython

- Developed a programmable BadUSB device using Raspberry Pi Pico and CircuitPython to execute automated keystroke injection payloads for security testing and automation

Skills and Certifications

Certifications: CompTIA Security+, Google Cybersecurity Certificate, TestOut Ethical Hacker Pro
Languages: Python, Java, C++, JavaScript, SQL, Bash, PowerShell
Frameworks & Tools: PySpark, Playwright, REST API design and integration, Docker, Git, Azure Functions
Cloud & Data: AWS (Lambda, S3, IAM, SageMaker), Azure (Functions, Synapse), ETL pipelines, data lake architecture
AI & Security Engineering: Retrieval-Augmented Generation (RAG), LLM integration, prompt engineering, AI security and governance, Copilot Studio, Power Automate, threat modeling, NIST CSF, ISO 27001, MITRE ATT&CK
Platforms & Tools: Cortex XSOAR, Splunk, Wireshark, Nmap, JFrog Artifactory, BigFix, Onspring, MetricStream, Zscaler, Linux

Recognitions and Community Engagement

- National Cyber Signing Day honoree (2024), NICE K12 Cybersecurity Educator Conference, selected as 1 of 6 students nationally
- Student panel speaker (2022), NICE K12 Cybersecurity Educator Conference, presented cybersecurity student perspectives to an audience of 50+ educators and industry professionals