

# Mario Tagaras

## Cyber Security Analyst/Engineer

Motivated Cyber Security Analyst with hands-on experience in SIEM deployment, log analysis, and script automation. Completed a 1 yr internship at DCI. I lead secure homelab projects using Firewalls + Tailscale VPN and VMs running Linux, macOS, & Windows. Skilled in scripting, system administration, and endpoint security. Earned a B.S. in Cyber Criminology, Computer Science at FSU and am CompTIA Security+ certified. Eager to begin a full-time entry-level analyst/engineer role.

mario.cybers@gmail.com

(727) 482-4795

Dunedin Florida, United States

linkedin.com/in/mario-gt

github.com/Mario-CyberS

## WORK EXPERIENCE

### Cyber Security Analyst Diverse Computing, Inc.

05/2024 - 04/2025

Tallahassee, FL

Diverse Computing, Inc. is a government-focused software company providing secure solutions for law enforcement agencies to meet CJIS compliance.

#### Achievements/Tasks

- Configured, deployed, and tuned Wazuh SIEM servers and agents for multi-log monitoring/alerting/analysis
- Automated firewall config backups and alerting using Bash/Rancid/Expect scripts and Zabbix monitoring integration
- Conducted vulnerability assessment research and supported incident response investigations on internal systems

Contact : Adam Corvin - [acorvin@diversecomputing.com](mailto:acorvin@diversecomputing.com)

## PERSONAL PROJECTS

### Wazuh SIEM Deployment & Tuning (09/2024 - Present)

- Deployed a single-node Wazuh SIEM on RHEL with custom log ingestion, ClamAV integration, Suricata integration (NIDS/NIPS), Slack/Email alerts, ISM policies, & indexer tuning. Enhanced indexer performance for long-term log retention. Automated ASA config backups using Bash/Expect.

### Tailscale Pi Firewall Gateway (04/2025 - Present)

- Set up a Raspberry Pi as a secure Firewall/NAT gateway and Wake-on-LAN relay using Tailscale VPN. Configured ACLs, tagging, and MagicDNS to enable private remote access and segmented traffic between internal devices without port forwarding.

### Automated Cyberscan Orchestrator (05/2025 - Present)

- This project automates bug bounty target testing and discovery using a Python/Selenium/undetected-chromedriver web scraper, AI/LLM-driven tool selection, and safe recon scanning. It selects tools and launches scans, enabling automated vulnerability reporting. Future plans include adding a CMP server for task dispatch, tool execution, and job tracking across distributed agents.

## EDUCATION

### Bachelors - Computer Science, Cyber Criminology Florida State University (FSU)

08/2025

## SKILLS

SOAR

SIEM Deployment & Tuning (Wazuh)

Log Analysis & Syslog Ingestion

Bash/Expect/Python Scripting

Endpoint/Network Security & Hardening

Network Monitoring (Cisco ASA, Suricata)

Firewall & NAT Configuration

Vulnerability Assessment

Virtualization (VMware, Linode, Azure)

Containerization (Docker/Kubernetes)

Secure Remote Access (Tailscale VPN, SSH)

Linux/Windows/macOS System Administration

Government Regulation Compliance

CIA-AAA-DAD

Fast Learner

Cautious Implementer

## CERTIFICATES

CompTIA Security+ SY0-701 (06/2025 - 06/2028)

## LANGUAGES

English

Native or Bilingual Proficiency

Spanish

Professional Working Proficiency

## INTERESTS

Cybersecurity Homelabbing & SIEM Engineering

Network Architecture & Firewall Automation

Open-Source Security Tools & Scripting

Digital Forensics & Malware Analysis

Bug Bounty Hunting

Entry Tier Pen-Testing

Physical and Mental Health training through physical exercise