

PHILIP ZANGARA, M.S.

Cybersecurity Analyst | Detection Engineering | Vulnerability Management
[linkedin.com/in/philip-zangara](https://www.linkedin.com/in/philip-zangara) | github.com/philipzangara | philipzangara.com
philipzangara996@gmail.com

Summary

Cybersecurity analyst with experience in vulnerability management, threat hunting, detection engineering, and security monitoring. Hands-on experience with Tenable, Microsoft Defender for Endpoint, Splunk, Microsoft Sentinel, Sigma, and MITRE ATT&CK. Developed Python-based phishing triage and IOC enrichment tools while driving measurable security improvements through automation, vulnerability remediation, and threat detection.

Certifications

CompTIA: SecurityX (formerly CASP+), CySA+, PenTest+, Security+, A+

Splunk: Core Certified Power User, Core Certified User

Microsoft: AZ-900

Centri: Blue Team Level 1

Technical Skills

SIEM & Detection: Splunk, Microsoft Sentinel, Microsoft Defender for Endpoint, AlienVault OTX, Sysmon, Sigma

Network Security: Suricata, Wireshark, pfSense, NSG/Firewall Rules, IDS/IPS

Vulnerability Management: Tenable, DISA STIG, OpenSCAP, Risk Prioritization

Threat Intelligence: MITRE ATT&CK, VirusTotal, MalwareBazaar, AbuseIPDB, OSINT

Cloud: AWS, Azure

Scripting: Python, PowerShell, Bash, KQL

OS & Virtualization: Windows, Linux, Proxmox, Docker

Work Experience

Cybersecurity Analyst Intern | Log(N) Pacific

Jul 2026 – Sep 2026

- Conducted vulnerability scans and risk-prioritized assessments using Tenable across Windows and Linux environments; implemented PowerShell-based remediations contributing to a 50% reduction in critical, 100% in high, and 83% in medium vulnerabilities for the server team.
- Executed secure configurations and DISA STIG compliance audits using Tenable, automating remediation and STIG implementation with PowerShell to meet industry standards.
- Performed threat hunting with EDR (Microsoft Defender for Endpoint), identifying IOCs from brute force attacks, data exfiltration, and ransomware; developed custom detection rules to automate isolation and investigation.
- Reduced brute force incidents by 100% by implementing inbound NSG and firewall rules to limit internet exposure; built Microsoft Sentinel dashboards to monitor logon failures and malicious traffic, querying logs with KQL.

Customer Service Staff / Deli Associate | Publix Supermarkets

2004 – Present

- Recognized for reliability and communication in a high-volume customer environment.
- Mentored new associates and delivered process training.

Detection Engineering & Security Automation Projects

Simple IOC Lookup (Python)

- Built an IOC enrichment platform supporting four IOC types and aggregating intelligence from VirusTotal, AbuseIPDB, WHOIS, and AlienVault OTX.
- Automated verdict generation and ATT&CK-based enrichment for accelerated threat triage.

NIST CSF 2.0 Control Gap Analyzer (Python)

- Developed a Python-based assessment platform that evaluates cybersecurity maturity against all 106 NIST CSF 2.0 subcategories and generates automated gap analysis reports
- Implemented coverage calculations across 6 Functions and 22 Categories with interactive heatmap visualization.

Simple Phishing Analyzer (Python)

- Developed a Python-based phishing triage tool that automates analysis of .eml files, including SPF, DKIM, and DMARC validation, URL reputation enrichment through VirusTotal, attachment hashing via MalwareBazaar, and weighted risk scoring.
- Mapped detections to MITRE ATT&CK techniques T1566, T1566.001, and T1566.002 to support analyst investigations and phishing response workflows.

Detection Engineering & SIEM Development

- Published Sigma detection rules covering five ATT&CK techniques across Execution, Credential Access, Initial Access, and Defense Evasion; converted detections to Splunk SPL and validated against sanitized sample logs.

Network Detection & Monitoring Lab

- Deployed Suricata on Raspberry Pi with port-mirrored traffic and Splunk integration; tuned Emerging Threats rules to improve detection fidelity and reduce alert noise.

Leadership & Community

- Competed in the Raymond James CTF, BSides, SECCDC, and NCL Capture the Flag events since 2023, placing in cryptography, forensics, and password-cracking challenges.
- Delivered a SECCDC training briefing on the NIST CSF Identify-Protect-Detect-Respond-Recover workflow at St. Petersburg College, covering system hardening, SIEM alerting, and live incident response.
- Vice President of Public Relations, Bay Pines Toastmasters (Jul 2026–Present): Manages the club's Facebook page, website, LinkedIn, and Meetup presence while building public speaking and audience engagement skills.

Education

M.S. Cybersecurity and Information Assurance Western Governors University	April 2025
B.A.S. Cybersecurity St. Petersburg College	May 2024