Zachary Mariskanish

(412) 217-8220 | ZMWorkCyber@proton.me | Pittsburgh, PA | zmariskanish-cyber.github.io/Portfolio

Summary

CompTIA Security+ certified cybersecurity professional focused on vulnerability management, external security testing, infrastructure security, and Python automation. Hands-on experience with CVE analysis, dark web monitoring, API integrations, and security reporting for mid-market and enterprise organizations ($250M–$1B revenue). Investigates attack surfaces, builds security workflows, and turns findings into practical remediation.

Professional Experience

Cybersecurity Analyst — Cowbell | *February 2024 – Present*

- Research and assess CVEs using threat intelligence to identify actively exploited or high-risk vulnerabilities, delivering concise reporting to customers to support timely risk-based alerting and decision-making
- Conducted authorized micro penetration tests (external, limited scope) with remediation reporting
- Performed dark web monitoring and aggregation, delivering reports within 1–2 business days
- Consulted with $250M–$1B revenue organizations on cybersecurity best practices
- Configured API integrations across Microsoft 365, AWS, Google Workspace, Cloudflare, and Sophos
- Led development of a team metrics database and executive reporting dashboards (Tableau and Salesforce)
- Automated real-time cyber risk ratings for internet-facing assets using dark web data

Risk Administrator — Cowbell | *April 2022 – February 2024*

- Produced weekly vulnerability and Spotlight reports on emerging threats; authored vulnerability summaries and determined alerting vs. direct notification strategy
- Supported policyholders with platform onboarding, API connector setup, and security awareness training
- Built API adoption reports and maintained policyholder technology stack data
- Aggregated risk engineering metrics (call volume, engagement type) for leadership reporting
- Researched and summarized industry threat intelligence (Verizon DBIR, IBM Threat Report)

Security Projects *Case studies: zmariskanish-cyber.github.io/Portfolio*

Micro Penetration Testing Methodology — *Nmap, Nikto, Nuclei*

- Developed a repeatable methodology for external attack-surface assessment — reconnaissance, scanning, controlled validation, and risk-prioritized remediation guidance

Endpoint Monitoring & Detection Lab — *Wazuh, VirtualBox, Windows, Ubuntu, Wireshark*

- Deployed a Wazuh SIEM across virtualized Windows and Ubuntu endpoints on an isolated host-only network; implemented file integrity monitoring, custom detection rules, and real-time event correlation and alerting

Security Reporting & Automation — *Python*

- Built tooling that parses structured security data and automates report generation with input validation and error handling, standardizing output and reducing repetitive analyst work

Infrastructure Security Lab *(in development) — Proxmox, pfSense/OPNsense, Terraform, Ansible*

- Building a home-lab environment for infrastructure-as-code, network segmentation, and hardened Linux and Windows Server systems

Education & Certifications

- **CompTIA Security+** — March 2024
- **Robert Morris University** — B.S. in Cyber Forensics and Information Security, December 2020

Technical Skills

- **Security:** Vulnerability management, CVE analysis, external security testing, risk assessment, incident response, malware analysis, network traffic analysis & detection
- **Tools:** Nmap, Nikto, Nuclei, Wazuh, Wireshark, Sleuth Kit, Autopsy, FTK Imager, EaseUS
- **Automation & Cloud:** Python, AWS configuration and cloud management, API integrations (Microsoft 365, Google Workspace, Cloudflare, Sophos), automated report generation, Tableau, Salesforce
- **Infrastructure:** VirtualBox, Proxmox, pfSense/OPNsense, Terraform, Ansible, Linux and Windows hardening, network segmentation
- **Compliance:** GDPR, HIPAA