Curt Fornolles

|  |
| --- |
| **Tampa, FL Tampa, FL | (813) 326‑6447 | curtfornolles@gmail.com | WWW: linkedin.com/in/curt‑fornolles |** |

**Websites, Portfolios, Profiles**

* https://cfornolles.github.io

**Skills**

Knowledge of MITRE ATT&CK Framework, Sandbox/Virtual Environment, Malware/Log Analysis, Vulnerability Management, and Network Security. Proficient in PowerShell, JavaScript, SQL, KQL, HTML, CSS, and PHP.

**Certifications**

**CompTIA Secure Infrastructure Specialist: Security+, Network+, and A+.**

**TestOut Network Pro**

**HDI Support Center Analyst (HDI)**

**Work History**

Tier 2 Technical Support Specialist 09/2021 - Current

National Veterinarians Associates – Tampa, FL

* Manage and secure Active Directory & Azure AD M365 user accounts.
* Resolved a high volume of tickets, consistently ranking **Top 3** Performer in the department.
* Lead special projects for software deployment, training, & presentation for over **40 users.**
* Collaborated with Cybersecurity to troubleshoot EDR software & perform Malware Analysis.
* Troubleshot network, application, & server issues, identifying & resolving problems to minimize downtime & ensure business continuity.

Manager 09/2019 – 09/2020

Sekushi Restaurant – Tampa, FL

* Maintained payroll integrity, ensuring adherence to financial rules and confidentiality standards.
* Effectively handled unexpected staffing challenges, preserving smooth restaurant operations.
* Swiftly adjusted to changing menus, marketing strategies, and staff training to meet customer needs.
* Managed payroll with precision, minimizing errors for accurate employee compensation.
* Applied creative solutions for improved staff scheduling and overall operational efficiency.

Manager 01/2015 – 08/2019

Koizi Endless Hibachi and Sushi Eatery – Brandon, FL

* Used data insights to understand customer preferences and optimize marketing efforts.
* Clearly conveyed policies, promotions, and training to foster a cohesive team.
* Collaborated with diverse teams for common goals, enhancing customer experiences.
* Maintained composure in high-pressure situations, addressing challenges with resilience.
* Analyzed performance metrics to identify and implement improvements for better efficiency.

**Projects/Open-Source**

**System Information and Event Management (SIEM)**

* Utilized custom PowerShell script to extract Windows Event Viewer metadata and integrate with a third-party API for geolocation data.
* Configured Azure Log Analytics Workspace, utilized Kusto Query Language (KQL), and created visual representations in Azure Sentinel Workbook to display global RDP Brute Force attack data on a Virtual Machine (Honeypot).

**Vulnerability Management and Risk Mitigation**

* Configured Nessus Essentials for credential vulnerability scans on Windows 10 hosts, leading end-to-end vulnerability management on sandbox networks, including discovery, assessment, reporting, and remediation.

**Intrusion Detection and Prevention (IDS/IPS)**

* Set up a virtualized environment with VirtualBox, running Ubuntu and Kali Linux Virtual Machines, and implemented a custom SNORT Alert Rule for detecting and analyzing TCP/IP traffic. Successfully triggered the rule during an NMAP scan on the Honeypot.

**Education**

Associate of Science: Cybersecurity 08/2023

Hillsborough Community College - Tampa, FL

**Relevant Coursework:**

* EC-COUNCIL: CEH v11, CND v2, & CPENT.
* Zero To Mastery Academy: Web Security & Bug Bounty.