CURT FORNOLLES

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+.

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 SentinelOne performing Malware Analysis.
- Troubleshot network, application, & server issues, identifying & resolving problems to minimize downtime & ensure business continuity.

Projects/Open-Source

System Information and Event Management (SIEM)

- Developed 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: CEH v11, CND v2, & CPENT.