# ABOUT

Experienced SOC Analyst with great experience working with SIEM tools, and phishing investigations. Vulnerability Assessment, and strategies needed to safeguard highly sensitive systems, data, and communications resources. Self-motivated and goal-oriented cyber security professional, with a demonstrated ability to handle complex responsibilities in a demanding environment.

# SKILL HIGHLIGHTS

|  |  |
| --- | --- |
| **Securities**   * Ironscales * Logrhythm SIEM * Microsoft Sentinel * Proofpoint(TAP,PPS) * Configuration management * Data Loss Prevention/Anti-Phishing * VirusTotal, IP/URLvoid * Endpoint Investigations * Phishing Email Investigations * Elastic * Exabean * Splunk     **Operating System**   * Linux (Kali & Ubuntu), * Windows * Mac OS     **Security Manage Tools**   * Nessus * NMAP * BurpSuite Pro | **Networking and security**   * TCP/IP * DHCP * Routing   **Language**   * Python * Java * C++       **Software Tools**   * Cisco * Vmware * Wireshark * PuTTY * Citrix workstation **Ticket System** * Service Now * Jira * Unilaunch |

# PROFESSIONALEXPERIENCE

**SECURITY ANALYST** – 01/2021 to PRESENT

**NOVACOAST**, Wichita

**Responsibalities:**

* Investigated phishing alerts up until containment and eradication
* Monitored the health of security devices and syslog instances and responded to anomalies as defined in the SOP
* Performed email-based investigation and successfully contained phishing emails and potential email account takeovers
* Performed threat intelligence including open-source investigations to identify current attacks that may target the client’s industry
* Provided support in identifying malicious network activity, threats impacting network operations and developing appropriate countermeasures, eliminating network threats and vulnerabilities
* Investigated alerts and performed searches on Splunk SIEM
* Performed investigations relating to potential compromise and worked with the IR team to determine impact and eradication
* Supporting Incident Response till resolution following Standard Operation Procedures (SOP)
* Prioritizing and differentiating between potential intrusion attempt and false alarms
* Assisting with the development of processes and procedures to improve incident response times, analysis of incidents, and overall, SOC functions
* Responding to computer security incidents by collecting, analyzing, preserving digital evidence, and ensuring that incidents are recorded and tracked in accordance with organizational SOC requirements.
* Investigated VPN alerts and reached out to users to confirm legitimacy of such activity
* Performed real - time log monitoring in the Security Operations Centre from different devices such as Firewalls, IDS, IPS, Operating
* Interpreted information provided by tools to form a sound hypothesis regarding the root cause of an event
* Investigated endpoints using SEPM and successfully terminated and deleted possible malicious file and processes

**COMPUTER TECHNICIAN**– 10/2018 to 12/2020

**United Parcel Service,** Dallas

* Identified hardware issues caused by component failures using approved diagnostic tools.
* Reviewed hardware/software and recommended modifications to enhance system performance.
* Disassembled computer systems to troubleshoot and resolve hardware issues.
* Responded to requests from users and directed individuals through basic troubleshooting tasks.
* Removed malware and viruses from laptops and desktop systems using specialized software.
* Installed, configured, and setup PCs in all stores for optimal operation and reporting.
* Set up, provided maintenance, and troubleshot printers and scanners.
* Configured computers to network drivers and connected to printers and other peripheral equipment. Using ServiceNow to track and manage ticket, incident management and apply some users request

**SERVICE DESK SUPPORT**– 11/2017 to 06/2018

**Hello fresh**, Arlington

* Take inventory to examine merchandise to identify any discrepancies or items which need to be re-ordered.
* Communicate via E-mail with procurement team on what needs are for current week and future week needs.
* Escalating tickets on undelivered purchase orders via Zoho software.

# Education

**Associated Degree of Applied Science, Computer Programming**

- **Tarrant county college district**

# Certifications

**Cybersecurity Engineer training**

* **Transfotech Academy**

**AWS Solution Architect training**

* **A Cloud Guru**

**COMPTIA CySA + ce**

**COMPTIA SECURITY +**

# Languages

* **English**
* **French**