Shade Ajibola

Email: Sadenuga1@gmail.com

 Address : Dartford, London

**Summary**

SOC Analyst with great experience working network, endpoint, and phishing investigations. Ability to perform Intrusion Detection, Vulnerability Assessment, Security Incident Response, and strategies needed to safeguard highly sensitive systems, data, and communications resources. Self-motivated and goal-oriented cybersecurity professional, with a demonstrated ability to handle complex responsibilities in a demanding environment.

**Skills**

|  |  |
| --- | --- |
| * Endpoint Investigations
* Phishing Email Investigations
* Network Security Protocols/
* TCP/IP
* Splunk
* Firepower
* ServiceNow/SharePoint
* Windows
* Active Directory/Microsoft Office
* VirusTotal, IP/URLvoid
* Malware Analysis/Endpoint
* Security
* Incident Response/Cyber Threat
* Intelligence
 | * Data Loss Prevention/Anti-
* Phishing
* Palo alto/Cisco
* Microsoft Azure
* 0365 Defender
* Microsoft Defender
* Azure Sentinel
* Protecting Networks
* Risk Mitigation
* Linux Server
* Tenable Nessus
* Kali Linux
* Splunk SIEM
 |

**Experience**, 01/2021 to Present

**SOC Analyst, Zonal**

* Performing security monitoring, incident response and treat management
* Monitoring security tools related to Intrusion Prevention and Endpoint detection and response
* Identifying potential threats, intrusions, and indicators of compromise
* Performing initial analysis and investigation into potentially malicious activity before escalating to additional engineers
* Supporting incident response process activities, including detection, response, and reporting
* Conducted routine certification testing and maintained the security and integrity of cyber systems and networks
* Monitored IT security systems into corporate and stored computing environments including systems used for logging, monitoring, intrusion detection, centralized cyber security knowledge base, and behavioral analysis
* Participated in after incident lessons learned meetings to give input on recommendations for additional tools or other mitigations for future incidents
* Remediated issues occurring with any IT security systems including but not limited to unexplained system outages, cyber security incidents, issues with data collection feeds or interfaces with external MSSP providers
* Collaborated with IT teams to remediate any potential hardware or network issues that prevented detection capability
* Collaborated with senior staff in planning, designing, developing, deploying, integrating, and maintaining cyber security tools
* Provided support in more complex cyber investigations
* Monitored new developments in the cyber security software/hardware marketplace, emerging technology trends and the security risks associated with those technologies
* Supported demonstrating the applicability of tools in real-world applications using a risk- based methodology based on business impact and the threat landscape
* Created, revised, and maintained documentation of processes and procedures in the central knowledge base
* Participated in after incident lessons learned meetings to give input on recommendations for additional tools or other mitigations for future incidents
* Tracked service availability and performance metrics and provided timely updates to management

**SOC Analyst**, 02/2022 to 02/2023

**NHS**

* Supporting Incident Response till resolution following Standard
* Operation Procedures (SOP)
* Prioritizing and differentiating between potential intrusion attempt and false alarms
* Analyzing email logs to confirm malicious emails were not delivered or are quarantined and malicious attachments dropped
* Monitoring and analyzing network traffic, Intrusion Detection Systems (IDS), security events and logs to identify abnormal and suspicious activity
* Staying up to date with current vulnerabilities, attacks, and countermeasures
* Analyzed Threat Patterns on various security devices and validation of false/true positive security incidents
* Performed investigations relating to potential compromise and worked with the IR team to determine impact and eradication
* Evaluated existing technical capabilities and systems to identify opportunities for improvement
* Interpreted information provided by tools to form a sound hypothesis regarding the root cause of an event
* Investigated VPN alerts and reached out to users to confirm legitimacy of such activity
* 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

**Computer Technician**, 03/2018 to 04/2019

**NCR**

* Upgraded laptops & desktops to improve speed and performance
* Configured new employee workstations, including all hardware, software, and peripheral devices
* Configured computers to network drivers and connected printers/other peripheral equipment
* 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

**Computer Technician**, 06/2017 to 01/2018

**ECS**

* Installed motherboards, processors, and graphics cards
* Backed up data each evening, helping alleviate lost information following malware incidents
* Configured computers to network drivers and connected printers and peripheral equipment
* Identified hardware issues caused by component failures using approved diagnostic tools
* Configured new employee workstations, including all hardware, software, and peripheral devices
* Built and repaired computers according to schedule
* Supported employees with advanced troubleshooting on help desk tickets
* Explained technology-related details in easy-to-understand terms to individuals in various roles
* Installed, configured, and setup PCs in all stores for optimal operation and reporting
* Responded to requests from users and directed individuals through basic troubleshooting tasks
* Removed malware and viruses from laptops and desktop systems using specialized software
* Disassembled computer systems to troubleshoot and resolve hardware issues
* Installed software updates and vulnerability patches on servers to prevent possible threats from penetrating networks.

**Education and Training**

**Canterbury Christ Church University**: Social Studies, 09/2013

|  |  |  |
| --- | --- | --- |
|  |  |  |