|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | |  |  | **NAME HERE**  SOC Analyst |  |  |  |  |  | | --- | --- | --- | --- | |  | **Professional Summary**   |  |  | | --- | --- | |  | Dynamic and motivated cybersecurity enthusiast with a year of intensive training and hands-on experience in vulnerability assessment (Nessus, OpenVAS), network monitoring (Suricata & Snort), and SIEM (Elastic-ELK). Demonstrated ability to identify, analyze, and mitigate security threats, leveraging deep knowledge of threat intelligence and incident response. Proficient in log analysis and excellent at communicating complex security information to diverse audiences. Adept at enhancing security measures and strategies in fast-paced environments. | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | |  | **Work History**   |  |  | | --- | --- | | 2024-02 - Current | **Cybersecurity Intern**  AIT, Remote   * Alert monitoring and incident response using Elastic SIEM * Analyze threats by taking the events from Firewalls, Endpoints, Servers, and IDS/IPS and identify false positives and true positives * Generation & formatting of reports for Nessus Vulnerability scans performed * Analyze Network Traffic Using Wireshark and Tcpdump * Analyze Phishing Email using OSINT tools and PhishTool * Vulnerability scanning and assessment using Nessus and OpenVAS to identify, classify and prioritize vulnerabilities in computers systems, apps and networks * Assist in investigating incidents, remediation, tracking and follow-up for incident closure with teams and stakeholders * Contributed to vulnerability assessments and penetration testing exercises |  |  |  | | --- | --- | |  | **Your Other Job Experience**  Company Name, Location  Add anything that's cyber or IT related you did on this job. If NON then add soft skills (Ex: Communication, Critical Thinking, Verbal and Written, and more) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | |  | **Education**   |  |  | | --- | --- | |  | **Bachelor of Science: Add Field of Study Here**  Add School Name Here - School Location |  |  |  | | --- | --- | |  | **Master of Science: Add Field of Study Here**  Another School Name Here - School Location Here | |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **Certifications**   |  |  | | --- | --- | |  | CompTIA Sec + |  |  |  | | --- | --- | |  | CompTIA CySA+ |  |  |  | | --- | --- | |  | Add Cert Here |  |  |  | | --- | --- | |  | Another Cert Here | |  |  |  |  |  | | --- | --- | --- | --- | |  | **Tools & Technology**   |  |  | | --- | --- | |  | * Security Information and Event Management (SIEM): Splunk and Elastic-SIEM * Intrusion Detection and Prevention Systems (IDPS): Suricata and Snort * Sandbox: Any.Run * Endpoint Detection and Response (EDR/XDR): Wazuh * Ticketing: ServiceNow * Network Traffic Analysis: Wireshark and Tcpdump * Vulnerability Scanning and Assessment: Tenable Nessus and OpenVAS * Incident Response and Threat Intelligence: MISP and Security Onion-Cases and TheHive * Malware Analysis: PhishTool * Forensic Analysis: Volatility, Autopsy, and velociraptor * OSINT: VirusTotal, IPVoid, URLScan, etc | | |  | |  |  | | --- | --- | |  | **Contact**  **Address**  City, State Zipcode  **Phone**  555-555-5555  **E-mail**  Youremailhere@gmail.com |  |  |  | | --- | --- | |  | **Skills**  1. Familiarity with networking concepts (TCP/IP, DNS, HTTP/HTTPS) and tools (Wireshark, TCPDump)  2. Experience working with Elastic-ELK and Splunk to collect and aggregates log data from various sources to provide real-time analysis of security alerts  3. Ability to gather, analyze, and apply threat intelligence to enhance security measures and response strategies  4. Proficiency in analyzing log files from various sources to detect suspicious activities or confirm the occurrence of a security incident  5. Excellent written and verbal communication skills to report findings, explain complex technical issues to non-technical stakeholders, and collaborate with team members  6. Advanced analytical skills to solve complex problems and identify root causes  7. Proficiency in scripting languages (Python or PowerShell) to automate tasks and analyze data  8. Helps in identifying and mitigating phishing attempts and educating users through simulated phishing campaigns  9. Vulnerability scanning and assessment using Nessus and OpenVAS to identify, classify and prioritize vulnerabilities in computers systems, apps and networks  10. Ability to think critically and solve problems under pressure, often with limited information | |

.