**SOUNDHARYA JANAKALYAN**+(966) 57 089 0166|sound.janak@gmail.com

Currently have 5+ years of Global Cyber Security operations/Incident response experience for providing cross functional services in Network Security, Information security and related fields. Strong Knowledge in the SIEM tools like Qradar, Vulnerabilities, Pen testing and Malware EPS Technologies.

* Interacting with Clients, Security Experts and concerned teams to mitigate threats.
* Experience in network traffic analysis of packet capture data, net flow, IPS/IDS and custom sensor output.
* Spam/phishing Mails processing and actions with respective service till the containment.
* Malware Hunting: Process and track down the infected Workstation/server to remediate.
* Handling Spam Attacks, Spam Mail Analysis, IOC, and Attachment Analysis.
* Security Devices: Antivirus, Proxy, Firewall, IPS, IDS etc.
* Good understanding on different types of attacks such as DOS, DDOS, SQL, ARP Poisoning, DNS Poisoning.
* Knowledge in firewalls and Intrusion detection systems/ Intrusion prevention systems.
* Knowledge in common network services (web, mail, FTP, SSL/TLS), network vulnerabilities etc.
* The ability to analyze logs from various securitydevices and web servers.
* Malware Analysis, Sandboxing (Threat Grid, Hybrid Analysis).
* Handling Spam Attacks, Spam Mail Analysis, IOC, and Attachment Analysis.
* Analyzing malware on virtual platforms by both static and dynamic techniques.
* Good knowledge on networking concepts.

**TECHNICAL EXPERTISE:**

* **SIEM Tool:** IBM QRadar 7.3.2
* **Ticketing Tool:** Service now
* **Endpoint Protection:** Symantec V14
* **IPS/IDS:** SourceFire
* **Firewall:** CISCO ASA
* **Vulnerability tool:** Nexpose

**WORK EXPERIENCE:**

**(Nokia Solutions and Networks, Chennai)**   **DEC 2014– JAN 2018**

**Cyber Security Analyst**

* Managed Cyber Security operations/Incident response including event monitoring which includes incident detection/response/mitigation for in house security projects. Operations include threat hunting, Host analysis, malware analysis.
* Perform Advanced Threat Investigation source from SOC monitoring. Take action to block all security devices and track down the infected system to remediate.
* Using analysis tools to continuously monitor and analyze real time logs for any suspicious event.
* Monitoring organization’s network for security breaches and investigating violations when one occurs.
* Experience in network traffic analysis of packet capture data, net flow, IPS/IDS and custom sensor output.
* Malware Hunting: Process and track down the infected Workstation/server to remediate.
* Handling Cyber and Data Security Incidents.
* Detecting Malware infected issues, analysis and removal from Network.
* **Sandbox (Threat Grid, Hybrid analysis and VirusTotal**) – we use these tools during investigation for better analysis.
* **CISCO IPS -** Analysis of traffic, detections and remediation of infections with help of PCAP Files, HTTP status codes and HTTP return methods.
* **QualysGuard, Nexpose** – Scheduling the scan on network device when needed, investigation of vulnerabilities proactively and reporting

**(SPIRO SOLUTIONS) DEC 2023- Present**

**SOC Analyst 1**

* Monitoring organization’s network for security breaches and investigating violations when one occurs.
* Managed Cyber Security operations/Incident response including event monitoring which includes incident detection/response/mitigation for in house security projects.
* Handling Spam Attacks, Spam Mail Analysis, IOC, and Attachment Analysis.
* Detecting Malware infected issues, analysis and removal from Network.
* Malware Analysis, Sandboxing (Threat Grid, Hybrid Analysis).
* **IBM Qradar:** event monitoring which includes incident detection, investigation and remediation. Tracking and analyzing real time use cases and creating basic rules for SIEM, report generation.
* **Bluecoat Proxy** – Able to handle the request of blocking and whitelisting the URL.
* **ServiceNow (Ticketing tool) –** Tool used for Managing all the security department tickets and trace back with investigation notes.

**EDUCATION QUALIFICATION:**

**Specialization**: B.E (ECE)

**College**: Srinivasan Engineering College

**DECLARATION:**

I hereby declare that all the details furnished above are correct and true to the best of my knowledge. And also, I assure that if given an opportunity to join in your esteemed organization, I will discharge my duties with sincerity and honesty to the satisfaction of my superiors.

**Place:**   **Date:**