****

**NAVEEN TUPPA**

**Address:** Hyderabad

**Email:** naveentuppa30@gmail.com

**Phone: +**91-9441083059

**LinkedIn Profile:** **https://www.linkedin.com/in/naveen-tuppa-76a476344/**

**Career Objective:**

A position in organization providing the opportunity to make a strong contribution to organizational goals through continued development of my skills.

**Professional Summary:**

* A competent professional with 4 Years of experience in Cyber Security – Incident Response Analyst.
* Supervised and performed installation of new IT network equipment and system software.
* Strong knowledge in Security Monitoring and Operation.
* Skilled in quickly detecting and handling security threats through incident response.
* Good experience in SIEM tools.
* Good experience in McAfee tools, IBMQ-Radar.
* Worked on IBM QRADAR & Ticketing Service now
* Monitor and manage SIEM setup which includes ESM, logger and connectors.
* Preparing daily, weekly and monthly report as per client requirement.
* Investigating and creating case for the security threats and forwarding it to Onsite SOC team for further investigation and action.
* Performing Log analysis &analyzing the crucial alerts at immediate basis.
* Responsible for monitoring, analyzing and reporting multiple security events from devices like IDS/IPS, firewall etc, using the QRadar and other Security Information & Event Management (SIEM) tools to detect IT security incidents.
* Aware on writing rules based on use cases.
* Preparing reports as per client request.
* Reporting weekly / monthly dashboards to customer.
* Recognizing attacks based on their signatures
* Monitoring and carrying out second level analysis incidents.

**Organizational Experience:**

Security Analyst –Sep 2020- Dec 2024 in Ust Global Pvt Ltd, Thiruvananthapuram, Kerala from Alfred analytics Pvt Ltd

**Education:**

* MBA in Finance from Osmania university Hyderabad in 2018
* B. Com Computers from Kakatiya University, Warangal in 2015
* CEC (Intermediate) from Board of Intermediate, Nirmal in 2012
* Secondary School Certificate from Board Of SSC, Nirmal in 2010

**Certification:**

* Certified IBM QRadar SIEM Foundation

**Professional Project Details:**

|  |  |
| --- | --- |
| **Organization:** Alfred Analytics Pvt Ltd  **Project:** Ust Global Pvt Ltd | **Technologies:** SIEM, IDS, Phishing-analysis, firewall,  IBMQ-Radar,Servicenow,SOCRADAR,ProofPoint, Sentinelone, EDR, Incidence Response |
| **Role:** Security Analyst |  |

**Description:**

The main goal of this project is to deliver SOC-Monitoring, Alerting, Incident Response, Reporting, and IOC

and incident handling. plans to deploy SOC environments in client location using IBM Q-Radar.

**Project Roles and Responsibilities:**

* Monitoring of SOC events, detecting and preventing the Intrusion attempts.
* Ad hoc report for various event sources customized reports and scheduled reports as per requirements.
* An Incident Response Analyst quickly identifies and isolates threats to minimize damage and protect systems.
* Collecting the logs of all the network devices and analyze the logs to find the suspicious activities.
* Monitor and manage SIEM setup which includes ESM, logger and connectors.
* Well Versed with MITRE Att&Ck and Cyberkill Chain Process
* Responsible for monitoring, analyzing, and reporting multiple security events from devices like IDS/IPS, firewall etc. using the IBM Q-Radar and other Security Information & Event Management (SIEM) tools to detect IT security incidents.
* Experience with Networks and web proxy solutions
* Investigate the security logs, mitigation strategies and Responsible for preparing Generic Security incident report.
* Responsible to preparing the Root cause analysis reports based on the analysis.
* Analyzing daily, weekly and monthly reports.
* Creating case for the suspicious issue and forwarding it to Onsite SOC team for further investigation.
* Monitoring the events on SIEM tool.
* Creating the tickets in ticketing tool.

**Declaration:**

I Naveen Tuppa declare that the above given information is correct to the best of my knowledge and belief.

**(Naveen T****uppa)**