**Name: Bana Shakti**

**Mobile no: 8143230516**

**E-mail**: banashakti090@gmail.com

**CAREER OBJECTIVE**

To work in a challenging and creative environment that enhances my technical skills.

**PROFESSIONAL SUMMARY:**

Total 3.8 years of experience in Security Operation Centre (SOC). Good analytical, communication, leadership skills, ability to deal with people diplomatically, willingness to learn and a good team member.

**TECHNICAL SKILLS**

|  |  |
| --- | --- |
| **SIEM Tool** | Microsoft Azure Sentinel |
| **SOAR** | Splunk |
| **Cloud Email Security** | Abnormal Security, Barracuda email Protection |
| **EDR** | CrowdStrike, SentinelOne |
| **DLP** | Varonis |
| **Ticketing Tool** | ServiceNow, Jira |

**EXPERIENCE SUMMARY**

|  |  |
| --- | --- |
| **Company** | Wipro |
| **Role** | Security Analyst |
| **Client** | Security Operation center |

**Primary Roles and Responsibilities**

* Technically sophisticated professional with about 3.8 years of experience in Information Technology.
* Experience on performing log analysis and analyzing the crucial alerts at immediate basis through SIEM
* Having experience on SIEM, SOAR, EDR, Sandbox…etc.
* Act as first level support for all Security Issues.
* Fine tuning the Use case based on the false positive detection.
* Monitoring the alerts triggered from Sentinel and by analyzing logs and by taking necessary action with respect to alerts and remediate the alert by meeting the Service Level Agreement (SLA).
* Create documentation for support and operations tasks regarding the above tools.
* Handling the different issues like Phishing, Spam, Scam and Malicious email.
* Participating in the incident response and investigation process.
* Working on incidents and reviewing the alerts and do detailed analysis on alerts.
* Good understanding on key customer infrastructure components Proxy, Firewall, Antivirus
* Identifying False-Positive offences and perform fine tuning over them with the help of TEAM.
* Monitoring 24x7 for Security Alerts and targeted phishing sites by using SIEM tool with the help of technologies such as Abuse mailbox and similar sounding domains.
* After analyzing alert raising incident in ticketing tool for true positive incidents and follow up the team up to incident closure.
* Having Knowledge of the Cyber Kill Chain, the MITRE attack framework, various TTPs described within and commonly used by attackers as well as how to write detection rules for them in SIEM and EDR solution.
* Report alerts and investigate issue identified during monitoring the live traffic.
* Preparing Daily/weekly/Monthly Reports for clients.
* Responsible to investigate the health checkup,
* Providing 24\*7 support and coordinating with required team to resolve the issues.
* Preparing RCA documents and daily/weekly/monthly Reports.
* Collaborate and share knowledge with other Engineers and Analysts.
* Mentor and train lower-level team members.
* Handling mostly US, UK region calls.
* Coordinates with all the teams to Mitigate/Remediate the issue
* Able to work in shifts on a rotating basis for 24X7.

**DECLARATION**

I hereby declare that the information furnished above is true to the best of my knowledge.

Place: Name: Bana Shakti

Date: