**Remala Balasairam**

E Mail**: remalabalasai@gmail.com**

M Mobile: 9490852603



##### Career objective:

Seeking a responsible and challenging position, in an energetic, self-motivating environment were

My professional attitude and constant drive towards success enables me to help the growth and development of the organization and myself.

##### Summary:

* Having **3years** of experience in **Information Technology** and currently working as **Security Analyst.**
* Experience in Incident management, Incident detection, Security event analysis using SIEM Tools. Good network knowledge, OSI layer, TCP/IP, Ports, DNS, DHCP etc.
* Knowledge in **Firewalls** and **Intrusion detection systems**/ **Intrusion prevention systems**.
* Knowledge in common network services (web, mail, FTP, SSL), network vulnerabilities etc.
* Good understanding security assessment tools like Anti-virus, DLP, Proxy, Firewall, IPS, Email security etc.
* The ability to analyze logs from various security devices and web servers.
* Good knowledge on networking concepts.
* An open mind, willingness to be challenged and strong desire to learn.

##### Technical Proficiency:

* SIEM Tools: **Arc Sight** **ESM**, **IBM** **Qradar**, **LogRhythm.**
* Email gateway: **Mimecast**

**Company: Micro Spark Software Solutions Pvt Ltd.**

**Designation: Cyber Security Analyst**

**Duration**: **June 2018 – Present**

##### Roles and Responsibilities:

* Detect incidents by monitoring the SIEM console, rules, reports and dashboards.
* Monitor the log from Firewall, IPS/IDS, Proxy server, AD Server, DNS, DHCP or other Servers.
* Investigate incident, remediation, and follow-up for incidents.
* Create and track investigation to resolution.
* Basic trouble shooting of log source issues.
* Phishing mail analysis in a mail gateway (Mimecast).
* Handling a various alert related to SQL attack, XSS attack, Possible phishing attack, Phishing mail attack, Brute force attack, Logon failure, Router configuration change, Disabled account login attempt alert, Dos attacks, Malware attack like file infected by virus or worm, alert related to Port Scan, Network scan etc.
* Distinguishing alerts into false positive and true positive in order to raise the tickets on true positive alerts and to escalate the same for responsible team as per the given escalation matrix.
* Remediating the incidents if possible otherwise, will gathering information then raise a ticket and write the description then escalate to next level.
* Performing the follow up activities in order to send the reminders to the respective persons or team to take action on raised tickets within a stipulated time.
* Performing ticket closure activities once the action taken on raised tickets.
* Generate daily incident reports, Anti-virus reports and monthly reports on time.
* Maintaining the data of daily Black listed IP sheet.
* Maintain the timely delivery of reports.
* Knowledge of security best practices and concepts.
* Ensure software is patched and able to protect from threats.
* Review, analyze, and respond to security events triggered through the security monitoring systems according to internal security procedures for cyber events.
* Provide proactive feedback to senior personnel and management as required.
* Assisting L2 team for fine-tuning of reports.
* Communicate with external team to resolve the queries relating to the raised incidents
* Provide real-time guidance to customers on attack mitigation procedures
* Responsible for shift handover.

##### Additional skills:

* Excellent communication skills both oral and written.
* Demonstrated capacity to work effectively in teams and independently as evidenced through work history.
* Displayed excellent abilities like positive outlook, Integrity, communication and commitment skills.
* Hard working, self-motivated to excel professional development.
* Ability to complete tasks within the specified span of time.
* Good leadership qualities and ability to optimize resources.

##### ACADEMIC PROFILE:

* Completed my B. TECH from JNTU college of engineering Kakinada, (2017 passed out).
* Completed my Intermediate from SVL KRANTHI Jr College with aggregate 67%.
* Completed my 10th from Vidya Vikas English Medium School with 86%.

##### DECLARATION:

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

**Place: Nagayalanka Name: Remala Balasairam**