**Rama Krishna**
**SOC Analyst**
**bramkrishna659@gmail.com**
**+91 9063647213 India**

## CAREER OBJECTIVE

Highly analytical and detail-oriented Software Engineer with 6 years of Experience in achieving tangible results in identifying, diagnosing, and resolving complex security issues. Committed to enhancing system security and efficiency while minimizing the risk of cyber threats.

## PROFEESIONAL SUMMARY

- I have around 4 years of relevant experience in Information security and am currently working as a Security Analyst.
- Experience with SIEM (Security Information and Event Management) tools like monitoring real-time events using ArcSight for performing daily monitoring of security alerts.
- Experienced in analyzing and researching Windows / Unix Security Logs as well as logs from DLP (Netskope) tools, Anti-Virus/Malware, EDR (Falcon crowd strike), web application firewall (Akamai), Firewall(Palo Alto), Ticketing tool (Service Now), Zscaler.
- Troubleshoot and resolve security incidents.
- Documentation of operating procedures and troubleshooting guidelines
- Utilizing my skills in achieving the goals of an organization by working in a team or as an individual and growing professionally, while being innovative and flexible.

## PROFESSIONAL SKILL

| | | | |
|---|---|---|---|
| **SIEM** (ArcSight, Rapid7Insight IDR) | **EDR** Crowd strike, Symantec EDR | **Web Application Firewall** (Akamai) | **IDS/IPS** Tipping Point |
| **Proxy** (Force Point) | **Firewall** Palo Alto | **Email Gateway** Microsoft Defender | **Microsoft Azure** Risky user, MFA |

## PROFESSIONAL EXPERIENCE

### USM BUSINESS SYSTEMS (Nov 2022 - PRESENT)

- Performing Real- Time Monitoring, Analysis, Reporting and Escalation of Security Events from multiple log sources.
- Maintain keen understanding of evolving internet threats to ensure the security of client Networks.
- Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure.
- Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating attacks.
- Troubleshooting SIEM dashboard issues when there are no reports getting to generate or no data available.
- Creation of reports and dashboard and rules fine turning.
- Mostly worked on broken authentication, sensitive data exposure, broken access control, xss, using components with known vulnerabilities insufficient logging and monitoring.
- Having experience on Phishing mail investigation and notifying the users
- Having Experience on monitoring Firewall, IDS/IPS devices events
- Maintain & document the application support strategy.
- Analyzing daily, weekly and monthly reports
- Having Experience on Azure risky user's and MFA Alerts.
- Reporting malware, web application vulnerabilities incidents and maintaining tracker.

### Sagarsoft India Ltd (May 2021 - Nov 2022)

- Monitoring the customer network using ArcSight.
- Working in security operation center (24x7), monitoring of SOC events, detecting and preventing intrusion attempts.
- Monitoring the real-time events, Analyses and escalating true positive events.
- Monitoring real-time events using SIEM tools like HP ArcSight and THE HIVE.
- AD-hoc report for various event sources customized reports and scheduled reports as per requirements.
- Collecting the logs of all the network devices and analyzing the logs.
- Monitoring the Events in Falcon Crowd strike console.
- Creating the logs of all the network devices and forwarding it to Onsite SOC team for further

investigation.

- Responsible for preparing the root cause analysis reports based on the analysis. Analyzing daily, weekly and monthly reports.
- Creating a case for the suspicious issue and forwarding it to the onsite SOC team for further investigation.
- Creating the tickets in the ticketing tool BMC Hilux.
- User management using Windows Domain Controller.
- Assisted in maintaining and improving the system/network environment and proactively monitoring the network to avoid potential issues.
- Operating master consoles to monitor the performance of networks and computer systems. Coordinating computer network access and use
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting, and Escalations of Security Events
- Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing an in-depth analysis of event payload and providing recommendations regarding security.
- Maintain a keen understanding of evolving internet threats to ensure the security of client Networks.
- Monitoring the Indicator of Compromise (IOC'S).
- Provided valuable assistance to the IT security department in various day-to-day tasks and activities.
- Health status of ESM and devices.
- I have experience and understanding of Arc Sight SIEM.

## EDUCATIONAL QUALIFICATION

Completed Graduation from JNTUK, India.