Name: Bhaskar Sai Teja Samana

Email: Bhaskarsaiteja80@gmail.com

Phone: +91 9182882182

***Objective****:*

*To be an integral part of a professional Information Security team for applying my knowledge and Professional skills to add value to the organization’s business and also achieve the corporate objectives whilst getting valued exposure and professional satisfaction along with personal growth.*

***Professional Summary:***

* 3.8 Years of hands on Experience in securing the network environment using SIEM tools like HP Arc Sight, IBM Qradar and working experience on other Tools like Websense DLP, HP logger.
* Experience in Monitoring & Investigating the incoming Events in the Arc-sight, Qradar.
* Work closely with business units to ensure that they know what and how to feed data into Qradar and to create network hierarchy.
* Experience in Information Security with on security operations, incident management, intrusion detection, and security event analysis through Micro Focus ArcSight, Qradar SIEM’s
* Experience of working in 24x7 operations of SOC team, offering log monitoring, security information management, global threat monitoring.
* Good understanding of log formats of various devices such as Websense, Vulnerability Management Products, IDS/IPS, Firewalls, Routers, Switches, OS, DB Servers, and Antivirus
* Expertise in defining resources like Rules, Filters, Dash Boards, Data Monitors, Active Channels
* Experience in generating Daily, Weekly & Monthly Reports from ArcSight, Qradar and Sourcefire IPS.
* Having good knowledge in Log Management by administering Arc-Sight Logger.
* Strong knowledge on Incident management life cycle.
* Familiar with Networking Concepts.
* Responsible for triage of a variety of alerts stemming from Malware.
* Responsible for monitoring the Phishing attempts.
* Exposure to Ticketing tool like Service Now.
* Strong in team coordination and managing tasks.
* Well in both team and individual environment.
* Ability to build successful rapport with co-workers, employees, Clients.
* Good communication, problem solving skills and the ability to acquire new skills in a timely manner.

***TECHNICAL SKILLS:***

|  |  |
| --- | --- |
| * IBM Qradar * Fire eye HX * TrendMicro * Vulnerability scanners * Web gateway * Endpoint Security | * Email Gateway * Spam Filters * Firepower Management Centre * IDS/IPS * Incident Response and Forensic Analysis * Splunk |

***Professional Skills:***

* Security Information and Event Management (SIEM) – IBM Qradar, Fire eye Helix
* Security monitoring and Incident response
* Vulnerability Assessment – Rapid7 VM, Qualys
* Security Coordination and Incident Handling – ServiceNow
* Endpoint Security and Antivirus (AV) – Fire eye HX
* Email security – CES
* Network Traffic Analysis – Wireshark
* Cloud Platforms - Azure
* Defense Centre – Cisco FMC
* Intrusion Detection Systems (IDS/IPS)– Cisco
* Microsoft Teams, SharePoint, MS- Excel, MS-Word, MS- PowerPoint
* Excellent analytical, problem-solving skills, critical thinking, interpersonal, customer service and organizational skills
* Ability to learn rapidly and adapt quickly to new processes and technology.

***Current Experience Details:***

*Company:* TCS – Hyderabad (NOV – 2017 to Till Date)

*Designation:* SOC Analyst

***Roles and Responsibilities:***

* Working in Security Operation Center (24x7), monitoring of SOC events, detecting and preventing the Intrusion attempts.
* Monitoring security event from all the log sources in ArcSight SIEM.
* Analyzing the threat, anomaly behavior and other activates leading to an incident.
* Understanding the incident based on to determine whether it’s false or true positive.
* Reporting the content of false positive to L2 in order to make the rule fine Tuned.
* Reporting to L2 about the devices which are not sending logs to SIEM in every shift.
* Assigning incidents to right team that has been created and following up on the same to make sure the alert is mitigated.
* Taken care of providing reports on daily basis with false Positive and True positive trends.
* To make sure the ticket we raise for the alert is not violating SLA.
* To make sure the action taken in the shift has been informed to the next shift Engineer through shift handover.

***Tools Used:*** SIEM – ArcSight & Qradar, Ticketing tool.

***Declaration:***

I hereby declare that the above-mentioned information is correct up to my knowledge.

Yours’s faithfully,

Bhaskar Sai Teja.