RAJA SEKHAR REDDY KARRI

Security Analyst

contact: +91-9849646277
Email: Rajasekhar1632@gmail.com

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 achieve the corporate objectives whilst getting valued exposure and professional satisfaction along with personal growth.

Professional Summary:

- 3.0 Year of hands-on Experience in securing the network environment using SIEM tools like Microsoft Sentinel, Splunk and working experience on other Tools like Force Point DLP, CrowdStrike.
- Experience in Monitoring & Investigating the incoming Events in the Sentinel and Arc Sight.
- 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 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 Force Point, 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
- Good knowledge in CrowdStrike EDR.
- knowledge of PCIDSS, HIPAA, ISO27001
- Familiar with Networking Concepts.
- Responsible for triage of a variety of alerts stemming from Malware.
- Responsible for monitoring the Phishing attempts.
- 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.

WORK EXPERIENCE

COMPANY: Mindtree Duration: Jan2022- Till Now
ROLE: Security Analyst

- Working on the Splunk, Sentinel SIEM (console & web console) providing operations support at the Security Operations Center for different member firms.
- Monitoring alerts (SIEM, IPS, wireless devices, tripwire and other security devices).
- Review/Investigate alerts for new and ongoing tickets from Dark Trace, Crowd Strike.

- Experience working with Darktrace, CrowdStrike for data loss prevention
- Incident response and ticket handling for phishing, internal information being shared, IP logins at unidentified locations, authenticity analysis, etc.
- Experience documenting security threats and the steps taken to re-mediate issues
- Performed threat analysis through research and examining log data.
- Monitoring & analyzing incoming Events in a network.
- Monitoring AV logs in ESM & raising case for malware infections.
- Monitoring Windows logs & raising cases for login failures & lockouts based on defined thresholds.
- Monitoring Tripwire logs for critical file modification on windows servers.
- Monitoring database logs & raise cases for suspicious login failures, DB shut down activities, critical commands execution etc.
- Monitoring IPS logs & Firewall to identify external threats.
- Experience in creating Filters and applying Filters to Active Channels.
- Integrating the Commands, Applying the Inline Filters in an Active Channel to make the investigation process reliable.
- Monitor alerts generated in the security analytics solution includes intrusion detection/prevention systems, firewalls, routers, switches, servers, databases, applications and other devices.
- Working on SIEM tools providing operational support for preventing of Cyber Attacks.
- Identifying potential information security incidents like security attacks and anomalous activities.
- In addition, perform analysis by observing deviations from normal behavior to uncover activities that could undermine security of information assets.
- Validate and confirm potential security incidents through detailed investigation of logs.
- Create incidents for all alerts/findings and regular updates on overall analysis as per the defined SLA's.
- Displaying the event data in different layouts by defining Dash Boards & Data Monitors.
- Checking the overall system health, Connector's health & reporting it to the Admin team on daily basis.
- Providing daily, weekly and monthly reports of incident activity.
- Security Incident Response and closure of Incidents within SLA using Service Now & Service Desk.
- Performing Health check of network security devices.
- Analyzing Phishing and Spam related activities and notifying to the users.
- Preparing daily and weekly dashboard on the security threats and trends on the network.
- Working on Real time network traffic by analyzing the logs from IDS and Firewalls through SIEM Tool.
- Handling the complete incident management framework cycle right from incident identification, incident containment, performing root cause analysis, suggestion and implementation of preventive and corrective controls and perform network analysis as needed on a case-to-case basis.
- Participate in weekly and monthly review calls with client and team meetings to review status of the issues and to provide process updates.

TECHNICAL SKILLS:

- Microsoft Sentinel
- CrowdStrike
- Microsoft Defender ATP
- Cloud Sek
- Endpoint Security
- Darktrace
- Splunk
- Email Gateway
- TrendMicro
- Force Point DLP
- PCIDSS, HIPAA, ISO27001
- Stellar

ACADEMIC QUALIFICATION:

BSc Computer Science from Aditya degree college in the year 2021.

DECLARATION:

I hereby solemnly affirm that all the details provided here are always true to the best of my knowledge and belief and that I shall carry myself in a manner that lends dignity to the organization and worthy enough as a resourceful asset.

Yours Sincerely,
Raja Sekhar Reddy