VARRE SATYA PREM SANDEEP

SOC Analyst L1

vspsandeep28@gmail.com | 9148127738

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.

Summary

- Experience in Information Security with emphasis on security operations, incident management, intrusion detection.
- Experience on working in 24x7 operations of SOC team, offering log monitoring, and security information management and security event analysis using SIEM tool Qradar.
- Experience in Monitoring & Investigating the incoming Events.
- Working on deploying and managing security policies based on Zero Trust principles, helping organizations segment their network to reduce risk and ensure strict access controls.
- Experience in generating Daily, Weekly & Monthly Reports.
- Experience in SSL Scanning for checking certificates are correctly implemented, and remain secure.
- Exposure to Ticketing tool like Service Now.
- Strong knowledge on Event Life Cycle and its Phases.
- Strong knowledge on Incident management life cycle.
- Good communication, problem solving skills and the ability to acquire new skills in a timely manner.
- Strong in team coordination and managing tasks.

Work Experience

OUT WORKS SOLUTIONS (CLIENT : ON-SITE KYNDRYL)
SOC Analyst - APRIL 2024 to Till Date

Roles & Responsibilities:

- Monitoring alerts triggered from Qradar and by analyzing logs and by taking necessary actions with respect to alerts and remediate the alerts by meeting SLA.
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
- Maintain keen understanding of evolving internet threats to ensure the security of client networks. 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 the attacks.
- Working on deploying and managing security policies based on Zero Trust principles, helping organizations segment their network to reduce risk and ensure strict access controls.
- Gaining experience in monitoring network traffic, identifying anomalies, and responding to incidents, ensuring that security policies are correctly implemented and enforced.
- Monthly SSL Scanning for checking certificates are correctly implemented, and that communication channels remain secure.
- Determine the scope of security incident and its potential impact to Client network.
- Installing the ColorToken agent on the Linux servers.
- Filling the Daily health checklist and providing daily KPI report to the Client.

- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS,DHCP etc.
- Good understanding of security solutions like Firewalls, DLP, Anti-virus, IPS, Email Security etc.
- Preparing daily, weekly, and monthly report as per client requirement.
- Maintain & document the application support strategy.

Skills

Technical Skills: ColorTokens Zero Trust, Qradar SIEM, SSL, Crowdstrike Falcon, F5 DNS
Soft Skills: Team-Player, Communication, Time Management

Certifications

- ColorToken Zero Trust Micro Segmentation Certification.

Education

B. Tech from Bharath Institute of Higher Education And Research, Bharath University in **2022.**

Declaration

I Here declare that the above given information is correct to the best of my knowledge and belief.

(VARRE SATYA PREM SANDEEP)