P.RNikhilKrishna

Hyderabad,India | +91-7382277596 nikhilkrishna2590@gmail.com

Summary:

- Having 04 years of experience in SOC Monitoring, with security operations including Incident response through SIEM tools like Microsoft Sentinel & Sumo Logic.
- Cyber security professional with experience in monitoring, detecting, and responding to security incidents. Proficient in using SIEM tools to analyse logs and identify threats while implementing measures to mitigate risks. Strong focus on maintaining network security, conducting vulnerability assessments, and ensuring compliance with industry
- standards. Having great exposure on the Incident response and triaging the security Alarms and taking immediate mitigations on the true positive instances.
- Experience on working in 24x7 operations of SOC team, offering log monitoring, security information management.
- Experience in Security Monitoring and Operations and played as a vital role in the security operations. Experience on SIEM (Security Information and Event Management) tools like Microsoft Sentinel and Splunk.
- Creating the tickets in ticketing tools like Service Desk Plus and Jira.
- Working on Email security tools like Phisher & Microsoft Defender. Worked with core teams to investigate the false and true positive alerts.
- Responsible for following all the steps in incident response process.
- Filling the Daily health checklist.
- Basic Knowledge on the KQL and pulling the logs according to the client requirement. Created SOP RUNBOOKS for various alerts.
- Preparing daily, weekly and monthly reports as per client requirements. Played a vital role in SOC team and worked with core teams to investigate the false and true positives.

Experience

Senior Consultant | 04/01/2024 - 05/04/2024

Birla soft - Hyderabad

- Worked as a Senior Consultant at Birla soft, Hyderabad from Jan 2024 to April 2024.

SECURITY ANALYST | 0 6 / 0 4 /2020 - 1 2 / 1 2 /2023

TCS

- Previously worked as a Security Analyst at **TCS,** from April 2020 to Dec 2023.

Skills

- Incident Response Microsoft Sentinel
- Threat Hunting
- SIEM: Azure Sentinel & Splunk.
- Microsoft Defender
- Email Security: O365, Phisher, Mimecast
- Microsoft Cloud App Security

Languages

Telugu: **English:**

Hindi:

Project Summary

Project:

Nature of Work: Security operations

Role: SOC Analyst

Environment: Microsoft Sentinel

Roles & Responsibilities:

- Worked on Microsoft Azure sentinel which helps to analyse the User Behaviour (UBA) and determining whether any user credentials or accounts had been compromised or any suspicious malware activity occurred in the environment.
- Played a Vital role in SOC team as Security Analyst. Worked with core teams to investigate the false and true positive alerts.
- Monitoring and identify positive security events from Microsoft Azure sentinel dashboard, Orion during the shift hours and take necessary action for the critical events that is seen during each shift's hours with deviations for all the environments that we support.
- Preparing daily and weekly dashboard on the security threats.
- Use the escalation process for multiple users impacting incidents all the time and keep update the management about the progress of incident.
- Will document the tickets fully with all the action taken for the incident and update it on frequent basis and maintain ticket quality by documenting it with all the required
- comments Understanding the incident based on to determine whether it's false or true
- positive. 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.
- Handling a various alert related to Phishing mail attack, Ransomware related attack, Brute force attack, Dos attack related, Malware attack etc.
- Monitoring and analysis of events generated by various security and network tools like Firewalls, Proxy servers, AV, IPS/IDS, System Application, Cloud (Amazon, Azure and Google) Windows and Linux servers etc.

- Creating tickets in SDP tool and tracking the status of the incidents.
- Analysis of daily and monthly report for incident management and compliance.
- Coordinating with Network team, Server team regarding activities and technical issues.
- Creating vulnerability and remedy reports and reporting them to users.
- Finding the Critical servers and application inventory from respective business owners and scheduling the scan weekly, monthly, and Quarterly basis.
- Knowledge sharing session with the team members whenever complex incident issue raised and lessons learned from other team members.

Personal Information

- Name P.R Nikhil Krishna
- Date of birth: 25/06/1990
- Marital status: Unmarried

Mobile: +91-7382277596

Education

B.COM from MAHATMA GANDHI KASHI VIDYAPITH VARANASI
MBA from MAHATMA GANDHI KASHI VIDYAPITH VARANASI

Certifications

- SC200
- NSE1& NSE2

Declaration

I hereby declare that statements made are true and correct to the best of my knowledge and belief.

Place: P. R Nikhil Krishna