DURGAPRASAD KOPPIREDDY

SOC Analyst

koppireddydurgaprasad018@gmail.com

8008136684

Career Objective:

Having **3 Years** of Experience in INFORMATION SECURITY. Well- Versed with analysis in SIEM tools like Azure Sentinel, Qradar and Splunk and with exposure towards wide range of vulnerabilities and threats. Able to execute with a high degree of success in integrating and/or solving problems.

Professional Summary:

- Overall **3 Year's** of experience in IT and as SOC Analyst.
- Experience on working in the area of security operations including Incident management, and log analysis through SIEM.
- Experience in Information Security on security operations, incident management, intrusion detection.
- Experience in Monitoring & Investigating the incoming Events.
- Experience on working in 24x7 operations of SOC team, offering log monitoring, and security information management and security event analysis using SIEM tool Azure Sentinel, Arc-Sight and IBM Q-radar.
- Experience on performing log analysis and analyzing the crucial alerts at immediate basis through SIEM.
- Handling critical alerts from Symantec Endpoint Protection and working for resolution.
- Handling alerts from Crowd strike EDR and investigation.
- 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 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
- Experience in generating Daily, Weekly & Monthly Reports.

Work Experience:

SOC Analyst at DXC Technology(Bengaluru)

May 2022 - Till Date

Roles and Responsibilities:

- Monitoring alerts triggered from sentinel and by analyzing logs and by taking necessary actions with respect to alerts and remediate the alerts by meeting SLA.

- Worked on SNOW incidents creation to closing and Updating IOC's In Threat Intelligence in Sentinel.
- Performed Use Cases query development in Azure Sentinel for Internal and Client Engagements.
- Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating the attacks
- 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..
- Determine the scope of security incident and its potential impact to Client network.
- Filling the Daily health checklist.
- Installation of Application Software and Antivirus software.
- Installing the Operating Software such as Windows.
- 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.
- Experience on performing log analysis and analyzing the critical alerts at immediate basis through Antivirus.
- Handling and Analyzing suspicious executions through EDR Crowd strike.
- Preparing daily, weekly, and monthly report as per client requirement.
- Recommend steps to handle the security incident with all information and supporting evidence of security events.
- Creation of reports and dashboards and rules fine tuning.
- Using components with known vulnerabilities, Insufficient logging and monitoring.
- Creation of reports and dashboards and rules.
- Maintain & Document the application support strategy

Technical skills:

- **SIEM**: Q-radar, Arcsight, & Azure Sentinel
- Phishing & Email Analysis
- **EDR**: Falcon Crowd strike
- **Vulnerability**: Nessus, Qualys
- Carbon Black Power shell
- IDS,IPS,DLP and O365 Defender
- **Ticketing Tool**: Service Now
- Proxy: Web Proxy, Zscaler

Education:

B.Tech graduated form Aditya College Of Engineering in **2022**.

Declaration

I hereby declare that the above-mentioned information is correct up to my knowledge and I bear that responsibility for the correctness of the above-mentioned.

DURGAPRASAD KOPPIREDDY