KATTEBASAPPA KATTEPPAGARI

SOC Analyst

kattebasappa1996@gmail.com

+91 9676962982

Bangalore, Karnataka

LinkedIn: https://www.linkedin.com/i/katteppagari-kattebasappa-2885911a2.

Skills

SIEM
Splunk, Q Radar, MS Sentinel.

EDR
Trend micro-Apex central
Trend micro-Apex one
Trend micro Deep security

VA
Tenable Nesuss

Forcepoint
Web proxy and Email gateway

Ticketing Tools
Service Now and Sapphire

Threat inteligence
IBM X - Force, Virus total, URL Void, IP Void, Cisco Talos and OSINT Frame work

Certificates

- SQL Injection
- Trend micro apex central, Apex one and Deep security

Education

Bachelor's of Engineering
Jawaharlal Nehru technological University
2019 | Anantapur, India

Profile

Over 2.6 years of experience with focus on working in a large -scale SOC (Security operation centre). Able to use various security tools and good understanding of different types of attacks and working in 24/7 operational support.

Professional Experience

SOC Analyst
IBM
Mar 2024 | Bangalore, India

- Effectively monitoring security alerts and logs through SIEM platforms to identify potential threats and anomalies.
- Exposure to use SIEM tools like Splunk, IBM Q Radar and MS Sentinel.
- Alert Prioritization: Assess and prioritize incoming security alerts based on their severity, potential impact, and urgency to ensure timely and effective response.
- Suggesting the finetuning to admin and particularly modifying the points like Contextual Rules, Threshold Adjustments and log source Etc.
- Basic Knowledge on KQL query.
- Maintaining the tracker like alerts, blocked Rouge IP, security advisory, Whitelisting tracker.
- Managing the SLA as per client requirement based on the severity of alerts.

- Taking the follow ups based on the escalation matrix.
- Closing the tickets based on the business justification and artifacts.
- Preparing the daily, weekly, monthly dashboard reports.
- Preparing the SOPs for analysis of alerts.

Security Analyst
DXC TECHNOLOGY
(July,2022-Feb 2024) | Banglore,India

- Monitoring and analysis of Threats by using EDR.
- Health check of the servers and maintaining its AV.
- Creating the AV compliance report for daily record.
- Vulnerability assessment by using the tenable Nessus and preparing the reports for remediating process.
- Preparing the vulnerability assessment graph reports on monthly basis.
- Proficiency in the preparation of various reports, dashboards, and documentation.
- Troubleshooting security and network problems including log analysis.
- Providing the exceptions and creating the policy in the web proxy level and daily basis health check on proxy content gateways.
- Analysis of the mails by using the Email gateway.
- Keeping security servers up to date for implement to the security policy.
- Preparing the sops as per BAU.

Declaration

I here declare that all the information mentioned above is true to the best of my knowledge.

KATTEPPAGARI KATTEBASAPPA
BANGALORE