PRAVEEN

SECURITYANALYST(Security Operation Center (SOC)

praveendanda09@gmail.com +91 6281994017

Profile Summary

- I have 3.6 years of experience as a SECURITY ANALYST in the field of Cyber security Operations for 24*7 SOC environment.
- Expertise in SOC (Security Operations Centre) Operations methodology such as Incident Handling, Threat detection, Network traffic monitoring, real time event handling, log analysis, identifying and classifying attempted compromises to networks through heuristics identification of suspect traffic.
- Experience in device configuration for various devices and applications including Firewalls, IDS, IPS, Windows servers, Linux servers, Database servers and other applications as per the custom requirements

Certifications

- Certified in SC -900, ITIL V4

Skills

SIEM Tools

IBM Q Radar

EDR

MS Defender,

System Security

Windows & Linux

servers**Phishing Email**

Mx Tool, Proof point

XDR

Sentinel ONE

Ticketing tools

Summit AI, Service now.

Software

Ms Office Suite (Word, Excel, PowerPoint)

Professional Experience

Organization : Persistent Systems PVT. LTD.
Designation : Security Analyst.
Duration : Sep 2022 to till date.

Organization : TECHMATRICS SOLUTIONS PVT. LTD.
Designation : Security Analyst.
Duration : Feb 2021 to till Sep 2022.

Roles & Responsibility's

- Monitoring and analysis of events generated by various security and network tools like Firewalls, Proxy servers, AV,IPS/IDS, System Application, Windows and Linux servers e.t.c
- Working as Security Analyst for SOC 24*7 environment.
- Security Incident Response: Responsible for monitoring of security alerts. Analysis of logs generated by appliances,investigation, and assessment on whether the incident is false positive or False Negative.
- Microsoft Defender - Handling end point protection like monitoring and analysis of events generated security threats,alerts and taking mitigation actions, scans.
- Email security - analyzing the customer reported mails and taking actions accordingly. Blocking the suspicious linksand id's. And as per customer request whitelist and blocking the mail id's and domains.
- Sentinel one XDR tool handling servers. Monitoring the threats and taking actions accordingly like server scans,blocking and exclusions.
- Use SIEM tools (IBM Q radar) to detect possible signs of security breaches and perform detailed investigation to confirm successful breach. Perform root cause analysis (RCA) and appropriately handle the incident as per definedIncident Management Framework.
- Following end to end Incident Investigation and Incident Response process, ensuring to close the investigationwithin defined SLA.
- Escalation of security incidents to concerned teams and their management and follow-up for closure.
- Creating tickets in Service now and tracking the status of the incidents.
- Finding the Critical servers and application inventory from respective business owners and scheduling the scanweekly, monthly and Quarterly basis.
- Knowledge sharing session with the team members whenever complex incident issues are raised and also lessonslearned from other team members.
- Attending calls with business owners, Windows and Linux team for scheduling the Vulnerability Managementpatching and remediation part without business disruptions.

Education

2016 **Post-Graduation – Master of Technology,** *JNTUH*