KOUSRI PRAVEEN
kosuri2912@gmail.com
Mobile: +91 86889 12477

Career Objectives:

To utilize my technical skills with a self-motivated and positive approach with an organization that will help to improve my professional and personal growth.

Professional Summary:

- **Having Key Experience: 2 years working in SOC, across one or more of the following: Security Analysis, Security Monitoring, Security Incident Management, and Incident Response.**
- Have hands-on experiences with SIEM tools **Exabeam.**
- Knowledge of email security threats and security controls, including experience in analysing email headers, attachments, and URLs.
- Create formal incidents and support the investigation of such incidents to not only mitigate the current threat but also prevent future occurrences.
- Using various security tools to perform monitoring and analysis of security events to detect security risks and threats within established customer Service Level Agreements.
- Recognize successful attempts of cyber intrusions and compromises through log review and analysis of relevant event detail information.
- Differentiate the false positives from true intrusion attempts and help remediate/prevent them.
- Support escalation and work closely with stakeholders as required.
- Quick response to interpret security incidents and to provide root cause analysis.
- Respond to common alerts in a consistent and repeatable manner from multiple alerting sources.
- Actively investigates the latest security vulnerabilities, advisories, incidents, and notifies clients when appropriate.
- Working on Windows/Linux Security Logs as well as logs from IDS/IPS, DLP, Cisco ASA, Next-Generation Firewalls, Anti-Virus/Malware, Active Directory Integration.
- Worked closely with other teams to support the incident management process.
- Responsible for triage of a variety of alerts stemming from malware, or phishing attempts.

- Monitor the networks of clients using our SIEM, ensure the availability of SIEM infrastructure, and recommend solutions that would improve the security posture of the client.

Work Experience:

Current Company: Inspira

April 2023 to Till Date

Role: Security Analyst

Responsibilities:

- Working in Security Operation Centre (24*7), monitoring SOC events, Detecting and Preventing Intrusion attempts.
- If it's a false positive alert close from my end with proper closure notes and it's a true positive collect the all evidence and submit to L2 for the next level investigation.
- Responsible for analysing the SOC Mail box where any end user reports the phish alarm.
- Recognize successful attempts of cyber intrusions and compromises through log review and analysis of relevant event detail information.
- Recognizing attacks based on their signatures.
- Using AV and other analysis tools to perform Malware Analysis and complete removal of malware from the client's environment.
- Differentiate the false positives from true intrusion attempts and help remediate/prevent them.
- Document all actions were taken during incident investigations.
- Work closely with other teams to support the incident management process.
- Expertise in preparing the biweekly and threat intelligence reports.
- Research, analysis, and response for alerts; including log retrieval and documentation
- Analyse and investigate the alerts in the **SOC monitoring** tools to report any abnormal behaviours, suspicious activities, traffic anomalies, etc.
- Conduct analysis of network traffic and host activity across a wide array of technologies and platforms.
- Recognize cyber-attacks based on their signatures. Differentiate the false positives from true intrusion attempts and help remediate/prevent cyber-attacks.

- Direct prior experience with core security technologies (SIEM, EDR, firewalls, IDS/IPS, proxies, DLP, AV, etc.)

Skill Highlights:

- SIEM _ Exabeam
- Email Gateway _ Proofpoint
- EDR _ Crowd Strike
- DLP_Netskope
- Open-Source Intelligence_ Virus Total, Cisco Talos intelligence, Mx Tool box, AbuseIPdb, IP void, URL Scan.io, Any. Run.

Education Qualification:

- B.Sc.from Samata Degree College.
- Intermediate from P.S.M Vasavi Junior College.
- SSC from K.P.M High School.

Declaration:

I hereby declare that all information furnished above is correct to the best of my knowledge.

(K PRAVEEN)