Chandrashekhar Reddy. D

+91 7095297048

chandrashekharreddy935@gmail.com

OBJECTIVE:

Motivated Information Security Associate with strong analytical, technical, and problem-solving skills, aiming to safeguard organizations from security breaches, mitigate risks, and contribute to their overall security posture and growth.

Professional Summary:

I'm a Consultant with Risk Advisory, Cyber Operate in **SANTROTECH SOFTWARE TECHNOLOGIES PVT LTD** As a cyber operate practitioner, Monitoring and investigating suspicious activities using Cloudsek & Threat Intel & SIEM tools, used to check daily health checks of servers and console.

Performs real-time monitoring, security incident handling, investigation, analysis, reporting and escalations of security events from multiple log sources.

Information Security Associate who can apply his analytical, technical and innovative skills to support and guard organizations against security breaches and help them to mitigate risks and grow in the organization.

I had a experience of 3.7 Months and has worked with multi-geography and diverse teams during my career.

I'm an empathetic, innovative and Immediate learner. I am also a fitness enthusiast and enjoys reading, cooking, gardening and watching movies.

Key Skills: SIEM, Cloudsek, Threat Advisory, TCP/IP, Malware Analysis, Vulnerability assessment, Email Security, Threat hunting, Incident Management/Response,

Tools: Qradar, Cloudsek, Qualys, Cortex Xsoar, Zscaler Deception, MS Defender, NAC, IBM CP4, McAfee ESM, IDS/IPS, EDR, Threat grid, HPSM, Bluecoat, Proofpoint, Tenable, Radware.

EXPERIENCE:

Santrotech Software Technologies Pvt Ltd,

Role: SOC Analyst, SEP 2021 to

April 2025.

RESPONSIBILITIES:

- In Threat Intel, we used to track cyber activities that threaten information systems, such as computer hacking or malware attacks. We analyze data about attackers, their capabilities, and motives to help organization to prevent those cyber-attacks.
- In the Cloudsek, the major responsibilities that we are Performing Deep & Dark Web Monitoring, Brand Risk Monitoring Data Leak Monitoring & Infrastructure Threats
- In the SIEM, we are Analyzing potential infrastructure security incidents to determine if incident qualifies as a legitimate security breach.
- Handling the phishing mails through MS defender.
- Analyzing URL Inbound & Outbound related alerts from XSOAR and Recon related from Deception.
- After analysis will rise a ticket to particular team which includes all information about the offense.
- Conclusion & closing of each incident with the help of MITRE mapping tactics.
- Creating & fine-tuning the rules according to the Security configurations as per client requirement.
- Produce security incident reports and briefings to be distributed to the team lead and manager.
- Analyze various reports from security devices such as firewall, IPS/IDS, Proxy etc.
- Performing Weekly, Monthly and NCIIPC reports as per the client requirement, also used prepare a complete incident report when a suspicious or malicious attack happens in a network.

Tools Used:

SIEM: QRadar

- Log & event analysis, incident investigation, and reporting.
- Integrating new devices with QRadar for real-time log collection.
- Troubleshooting log source devices for log collection issues.
- Basic correlation rule implementation and case studies.
- Report, dashboard creation, and rule fine-tuning.
- Assessing incidents, analyzing impact, risk assessment, and mitigation guidance
-

Cloudsek:

- Deep & Dark Web, Brand Risk, Data Leak & Infra Threat Monitoring.
- Alert escalation, rule creation, report downloads.
- Purchase tracking, takedown initiation/tracking, asset config & tracking.
- CloudSEK support, IOC sharing, audit reviews, weekly & daily alert reports.

Vulnerability Assessment: Security Center / Nessus:

- Quarterly scanning of Servers and Preparing remediation report.
- Validating mitigated VA points using NMAP and Kali Linux.

Threat Intel:

- Analyzing advisories from NCIIPC & CERT-In using CVSS.
- Tracking cyber activities like hacking, malware, etc.
- Maintaining daily IOC/vulnerability trackers, weekly client sharing.
- Coordination with security teams for risk mitigation.

SIEM: Splunk Phantom:

- Log/event analysis, incident handling within SLA.
- Raw log analysis from critical systems for anomalies.

EDR:

- Monitoring security safeguards & system performance.
- Vulnerability assessments and endpoint threat analysis.
- Reporting incidents to SOC responders.

Anti-DDOS: Radware DefensePro:

- Monitoring, threat analysis, IP blacklisting/whitelisting.
- Weekly/Monthly report analysis.

MS Defender: • Phishing email analysis based on client/user reports.

Cortex XSOAR:

- URL & playbook incident analysis.
- Monitoring integrated QRadar dashboard data.
- Playbook rerun for process completion on errors.
- URL & playbook incident analysis.

Zscaler Deception:

Recon incident analysis, attacker TTP (Tactics, Techniques, Procedures) understanding.

NAC: Access to detailed user/system info including servers, routers, switches, printers, etc..

CP4s: Deep investigation of threats, IOCs, DDoS, and vulnerabilities.

Courses:

- Qradar SIEM Foundation
- EHE

- CORP Security Risk Framework
- OWASP top 10
- Cybersecurity Essentials (LFC108)

Certifications:

- Microsoft Excel
- CEH,
- CCNA
- Comptia CYSA+.

ACADEMIC CREDENTIALS:

Completed Btech from Swami Vivekananda Institute Of Technology (JNTUH University) in -2023

PERSONAL INFORMATION:

Date of Birth: 18/04/2000
Present Resident Address: Guggilla(V), Bejjanki(M), Siddipet Dist-505528

Languages known: English, Telugu & Hindi.

I hereby declare that all the information stated above is true to the best of my knowledge.

Date: March 2025 **Chandrashekharreddy.D**