Chandrashekhar Reddy.D
Mob: +91 7095297048
Email: chandrashekharreddy935@gmail.com

OBJECTIVE:

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.

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 1.8 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 2023 to
March 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

- Responsible for log & event analysis, incident investigation, reporting.
- Integrating new Devices with SIEM (IBM Qradar) to collect real time logs.
- Troubleshooting log source devices for any issues on log collection.
- Case study and Implementation of basic correlation rules.
- Creation of reports, dashboards and rules fine tuning.
- Determine the scope of security incident and its potential impact to Client network, assessment of risk, recommend steps to handle the security incident with all information and help them to mitigate the risks and threats.

Cloudsek:

- Performing Deep & Dark Web Monitoring, Brand Risk Monitoring Data Leak Monitoring & Infrastructure Threats
  - Alert escalations for above module alerts
  - Alert rules creation
  - Report downloading
  - Purchase tracking
  - Takedown initiation and tracking
  - Asset configuration and tracking
  - CloudSEK query and support
  - Threat Intelligence/ IOC sharing with teams
  - Audit overview
  - Weekly reports
  - Daily alert count report

Threat Intel:

- Understanding the daily threat advisories from various NCIIPC & Certin reports and analyzes the vulnerabilities and then uses the Common Vulnerability Scoring System (CVSS) to evaluate the threat level of a vulnerability.
- Tracking cyber activities that threaten information systems, such as computer hacking or malware attacks. They analyze data about attackers, their capabilities, and motives to help organization prevent cyber-attacks.
- Maintain daily trackers for the IOC blocking and Vulnerability patching activities and sharing to the client in Weekly meetings.
- Following up with different security teams for the immediate action of risks & threat activities.

SIEM: Splunk Phantom

- Responsible for log & event analysis, incident investigation, reporting.
- Acting on the incidents within the provided SLA,
- Analyzing the Raw logs from critical servers and Machines to find abnormality in Organization network logs.

EDR:

- Responsible for monitoring and controlling the performance and status of security safeguards.
- Conducts assessments and reports vulnerabilities; monitors their ongoing management with the operations teams.

- Analyze endpoint application data in real time to identify potential throats, rogue systems, vulnerabilities, unauthorized devices and/or system changes, and data loss prevention. Report cyber incidents to SOC incident responders.

Anti-DDOS: Radware DefensePro:

- Monitoring the Radware and analyzing threats.
- Blacklisting and Whitelisting IP's on Radware based on business requirement.
- Analyzing the Weekly/Monthly Reports.

Vulnerability Assessment: Security Center / Nessus:

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

MS Defender: • Analyzing the phishing mails as per user & client requirement.

Cortex XSOAR: • Analyzing URL & playbook related incidents. Checking the completed data analytics of integrated part of Qradar in Dashboard. Also used to reruns the playbook when an error comes for complete process.

Zscaler Deception

- Analyzing recon related incidents. Understanding the attacker tactics and techniques of scanning and other vectors.

NAC: Having the special access for letting know all details of users, systems, servers, routers, switches and printers etc.

CP4s: For the deep dive investigation of threats, we used to check all the IOCs, DDoS and other vulnerability aspects here.

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**