Chandrashekar S

Senior security engineer

Email: chandrucsa02@gmail.com
Mob: 9113504819

Objective

Working as a SOC analyst, seeking a challenging and rewarding opportunity where I can recognize & utilize my true potential while nurturing my analytical and technical skills.

Professional Summary:

- Senior security engineer, having an overall **6** years of IT experience and **5** years of experience in Cyber Security services, Security operations center **(SOC)**, incident management.
- Good experience in communicating with different IT infrastructure teams like **Network, Operating system, Database, Endpoint** and **Infosec** to build and manage effective SOC.
- Good experience in information security technologies and methods.
- Good working experience on **SIEM technologies** such as **LOGRHYTHM, RSA NETWITNESS**.
- Good hands-on experience about **EDR (CARBON BLACK RESPONSE).**
- Hands on experience about **IDS/IPS, DELL SECURE WORKS**.
- Brief understanding and hands-on experience about **PALO ALTO XDR, Microsoft Defender.**
- Experience working on **SERVICE NOW** ticketing tool.
- Brief understanding and working knowledge on **DLP (SYMANTEC)** and **WSA (CISCO IRON PORT)**.
- Good self-learning skills, learning new technology by available resources.

Certification:

CERTIFIED ETHICAL HACKER (CEH V.10)

Professional Experience:

Happiest Minds Technologies — Senior security Engineer — **SEP 2021 - Present**

- Integration of new Log Sources (Windows, LINUX) and regular inspection of health check of the integrated devices for better monitoring coverage through SIEM tool.
- Integration of Network work devices to SIEM such as Firewalls, Switches & Routers.
- Creation of GLPR (global log processing rules) to suppress the unwanted/false events.
- Performing Real-time Monitoring, Investigation, Analysis, Reporting and Escalation of Security Events from Multiple Log Sources to determine intrusion and malicious events.
- Dashboard creation, reports generation, correlation rules, Fine tuning of alerts/alarms in LogRhythm.
- Responsible to prepare weekly and Monthly security posture for the clients' infrastructure and submit to the client.
- Proactively handling Dell secure works (IDS/IPS) Incidents.
- Checking health status of the sensors of Dell secure works (IDS/IPS).
- Blocking of the malicious IP'S at respective sensors on SECURE WORKS
- Complete handling of the EDR, Carbon black response for the clients.
- Sensor Installation/uninstallation for the client end systems/Servers.
- Adding users to CBR and granting roles/permissions for the users.
- Creation of Sensor groups with respect to client.

- Upgradation of Sensor version for both Windows/LINUX.
- Coordinating with tool partner for any issues related to the CBR and for the CBR version upgradation.
- Banning of IOC'S in CBR shared by internal teams.
- Trained and mentored associates on the security technologies and on boarding them to SOC team.

MFX Services Infotech pvt Ltd SOC Analyst SEP 2018 - SEP 2021

- Hands on experience on working with LR alerts and raising Incidents in SNOW.
- Good experience in working/communicating with cross-functional IT infrastructure team like Network, Infosec, Desktop and Messaging team etc.
- Analysis of Phishing mails for Indicators of Compromise (IOC) by verifying SPF, DKIM and DMART using open source tools.
- Exposure to Incident Response process and Kill chain stages involved in Cyber Security.
- Analyze threats by taking all the security events from Firewalls, Endpoints, Servers, and IDS/IPS etc. and identify a false positive and a true positive.
- Responsible to check ticket queue for any new request for ID creation, deletion, new scan or any launch Remediation Scan, to add new asset or delete assets.
- Responsible to prepare security advisories in daily basis regards to various Vulnerabilities, Threats & Malwares that we come across daily and send it to Internal concerned teams & client to have them updated.
- Exposure to Incident Response process and Kill chain stages involved in Cyber Security.
- Analyze threats by taking all the security events from Firewalls, Endpoints, Servers, IDS/IPS etc. and identify a false positive and a true positive.
- Proactively handling Dell secure works (IDS/IPS) Incidents.
- Checking health status of the sensors of Dell secure works (IDS/IPS).
- Blocking of the malicious IP'S at respective sensors.

Triad infosec Pvt Ltd Technical Consultant **Dec 2016 – Aug 2017**

- Performing Real-time Monitoring, Investigation, Analysis, Reporting and Escalation of Security Events from Multiple Log Sources in LogRhythm.
- Exposure to Incident Response process and Kill chain stages involved in Cyber Security.
- Analyze threats by taking all the security events from Firewalls, Endpoints, Servers, and IDS/IPS etc. and identify a false positive and a true positive.

Kayeen integrated solutions pvt ltd System Engineer **Aug 2012 – Dec 2013**

- Complete Handling of perimeter security project.
- Integration of Gallagher controller with the system for intrusion alarm monitoring.
- Installation of AV and other software's for the systems at office infrastructure.
- Involved in the configuration and integration of Access control by using Gallagher command center software.
- Communication with clients and visiting sites to resolve the issues related to the project.

Education Qualification

➢ **M. Tech (CNE, Computer Network Engineering)** from **BNM Institute of Technology** 2014-2016, Bangalore VTU.

Place: Bangalore

Date: