M M SAI KUMAR

ASSOCIATE INFORMATION SECURITY

maheshsaikm20@gmail.com
8197053885
HYDERABAD

CAREER SUMMARY

3.0 Years of experience as a Cyber Security in SOC shared delivery Model to support multiple Customers in different security tools with 24/7 work environment. Handling Incident, Threat Detection, Security Alerts, Network security, Security Protocols, Malware Analysis, Cyber Threats, Doc Procedures, Security Investigations, End point security, Security Documentation,run book/Play book Creation, Service Request, and Change request by maintaining the SLA.

- Working in a 24X7 mid-sized team as a Senior Security Analyst handling L1 responsibilities in 2 projects.
- Hands-on experience in SOC tools – SIEM (Splunk, Sentinel), Log Management (**Syslog-NG, Logstash**) EDR (CrowdStrike), XDR (Defender), Email Security (Proofpoint), Threat Intel and Analysis
- Professional strengths in gathering and analyzing client's specific needs and providing InfraSec solutions to enhance operational capabilities and maintain an excellent compliance.
- Analyse spam and phishing emails received by the users, taking necessary action to mitigate the issue.

Professional Experience

2023/11 – 2024/05
Noida, India

ASSOCIATE INFORMATION SECURITY
Company:ESECFORTE TECHNOLOGIES
SPLUNK / SENTINEL,ArcSight

- Security information and event management using Splunk, Sentinel.
- Working on the alerts triggered in Triage by SIEM tools.
- Good knowledge with SPL and KQL Queries.
- Analyzing, monitoring and handling the inbound and outbound traffic log data.
- Monitoring the malicious activities related to any suspicious URL, IP traffic, User.
- User Behavior Analytics using Azure Active Directory to analyze the Sign in logs, Locations,Device, Time.
- Authentication logs to confirm the legitimacy of the activity.
- Event log correlation across multiple data sources and source types.
- Suggesting new Use cases and finetuning scope to reduce the noise of alerts.
- Defender – Blocking IOC's (Ip , url , Hash) and performing scans on the endpoints.

2021/08 – 2023/10
Bangalore, India

SECURITY ANALYST
Company:DXC TECHNOLOGY

- Monitoring of SIEM events, detecting and preventing the Intrusion attempts
- Optimized **Syslog-NG** configurations to streamline log parsing, filtering, and forwarding for improved performance and security.
- Applied **Regex** to create efficient log parsing rules, improving accuracy in data extraction and minimizing false positives in security monitoring.
- Knowledge of Incident response management & Frameworks
- Experience on SIEM (Security Information and Event Management) tools.
- Monitoring real-time events using **ArcSight** SIEM, **IBM QRadar** SIEM, **Splunk**.
- Good understanding of various SOC processes like monitoring, analysis, playbooks, Use cases, incident documentation, SLAs, client meetings, report walk throughs, bridge calls, RFPs, etc.
- Engage with Vendor (MicroFocus) support to troubleshoot issues with SIEM platform.

- Integration of different type of data source (Syslog, windows) into ArcSight smart connector.
- Experience in understanding the logs of various devices (Servers, IDS/IPS, Firewall, Proxy)
- Analyzing Anti-virus, Endpoint protection, Tripwire logs.
- Analyzing email headers for spam and phishing activities.
- Analyzing email attachments for malware.
- Analysis of doc, PDF files for malwares using different tools.
- Knowledge in analysis of malware.
- Developed and deployed automation scripts using **Python/Bash** for log management tasks, including log rotation, filtering, and alerting

Education

2019/06 – 2021/07 **Bachelor of computer science and education**
Raipur, India *ISBM UNIVERSITY*

Key Skills

RSA Netwitness

Crowdstrike falcon EDR/XDR

Networking protocols

Malware (static & Dynamic Analysis)

ESM

Smart Connector & Flex Connector

Knowledge on Linux commands

Deploying & Maintaining Micro Focus ArcSight Environment

Sentinel

Splunk

Forcepoint DLP

IDS/IPS

Threat intelligence

SOAR

Knowledge on Scripting language like power shell

Knowledge on Python

Syslog-NG, Logstash

EMAIL SECURITY

EMAIL SECURITY

- Phishing Email Analysis and responding to the TAP triggered alerts.
- Types of Email threats - Attachment, URL, Imposter, TOAD & Spam mails.
- Performing Email Header Analysis, checking the legitimacy of the mails.
- Taking necessary counter measures like, blocking the sender, embedded URL over proxy,IP over firewall.
- Purging of the mail from End user's inbox and performing AV scan.
- Collection and analysis of Original Email within the Sandbox environment.

ROLES AND RESPONSIBILITIES

24/7 SNOW Queue Monitoring (follow 3 strike rule)- Meeting SLAs (Response SLA).

- In-depth Analysis and documentation of all INC.
- Real time quality check on Incidents and take appropriate action as or when required (PPF).
- 24/7 Bad email monitoring and updating, maintaining Trackers & take appropriate actions.
- Work on fine tune request (false positive) and Suggest admin to fine tune noise Alert's.
- Join all internal & Ad hoc call with admins and lead related to Fine tune, Escalations,Coordinate and Contribute.

- Preparing weekly, Monthly report and Presenting to the customer.
- Shift schedule and handling the conflicts within the Team.
- Handle client requests and questions received via phone, e-mail, or various ticketing tools in a timely and detail-oriented fashion to resolve a multitude of information security related incidents.
- Act as technical first point of contact from L1 side for technical queries and escalate as appropriate.
- Develops and maintains security awareness training programs and materials.
- Trained new analysts to ensure proper completion of access requests and problem resolution with proper Knowledge transfer sessions.

Certifications

CEH

Azure az500

Fortinet NSE1

Fortinet NSE2

Key Achievements

- Splunk 7.x fundamentals.
- Strong written communication skills and presentation skills Cybersecurity Awareness: Phishing Attacks

Declaration

I hereby declare that the above-mentioned information is upto my knowledge and I bear the responsibility for the correctness of the mentioned particulars.

M.M Sai kumar
HYDERABAD