SATHEESHKUMAR P

SECURITY ANALYST

☎ 6383160084 ✉ satheeshpvm09@gmail.com Coimbatore, Tamilnadu

Dedicated SOC Analyst with a proven track record in monitoring, analyzing, and responding to security incidents. Seeking to apply strong analytical skills and hands-on experience with advanced security tools to enhance threat detection and incident response, and to strengthen the organization's proactive security posture.

WORK EXPERIENCE

Security Analyst

Mar-2022 - Present

Nakoa Technologies Pvt Ltd, Coimbatore, Tamilnadu

- Working on various tools such as Sumo logic and Crowdstrike
- Continuously monitor dashboard panels of SecureWorks XDR for security alerts and analyze event logs ingested from a variety of different technologies across multiple platforms.
- Detect and investigate potential threats, triage the alerts, and appropriately escalate incidents to L2/L3 analysts for additional assistance.
- Proactively manage incidents to minimize customer impact and meet SLA's. Utilize Jira tool for management of incidents and ticket tracking.
- Search firewall, email, web or DNS logs to identify and mitigate intrusion attempts.
- Interact with customers to address their security issues through slack channel communication.
- Prepare briefings and reports about results of investigations on repeated low and medium alerts utilizing analysis methodologies.
- Organize and conduct training sessions for new hires on SOC processes, procedures, workflows and utilized technologies such as Sumo logic, CrowdStrike, Mimecast.
- Take active role in creation of Document Repositories. Used MITRE ATT&CK, an open framework and knowledge base of adversary tactics and techniques based on real-world observations, provides a structured method.
- Used Open-Source Reputation Channel's such as VirusTotal, AbuseIPDB, AnyRun, Hybrid Analysis, Cisco Talos, Alienvault OTX, Recorded Future and Shodan collecting key findings for incident report.
- Referenced Cyber Kill Chain to determine if malicious actor was able to perform all techniques and tactics. Out of Hours “On Call” work to ensure 24/7 service delivery.

EDUCATIONAL HISTORY

BACHELOR OF ENGINEERING

Jun-2014 - Mar-2018

Anna University, Chennai

CERTIFICATION

CCNA CERTIFIED

2019-Apr

Prompt Infotech Pvt Ltd

CERTIFIED ETHICAL HACKER (CEH)

2020-Aug

Prompt Infotech Pvt Ltd

ETHICAL HACKIING ESSENTIALS

Coursera

INTRODUCTION TO MICROSOFT AZURE CLOUD SERVICES

Coursera

MICROSOFT AZURE MANAGEMENT TOOLS AND SECURITY SOLUTIONS

Coursera

SUMO LOGIC FUNDAMENTAL

Netskope

NETSKOPE CLOUD SECURITY SALES ASSOCIATES

Netskope

TECHNICAL SKILLS

- Language : Python Basic
- SIEM : wazuh, Splunk ESM, Sumologic
- EDR : CrowdStrike
- Email Gateway : Mimecast
- Ticketing tool : Jira
- Tools : Wireshark, Open-Vas, Burpsuite
- Key Skills : DLP, UBA, Malware analysis, Phishing Email analysis, Netskope CASB Policies.

SKILLS

Solid understanding of common network services and protocols.

Good knowledge on cyber-attacks and attack vectors

Good Understanding of various SOC processes like monitoring, analysis, playbooks, escalation, incident documentation, report walkthroughs, bridge calls etc.

Continuous learning and staying up-to-date with the latest security trends and technologies.

Strong communication and documentation skills Ability to think critically and analytically, and to develop and implement effective security strategies.