SIDDESH S V

Security Analyst

My Contact

siddeshsv97@gmail.com

9945424024

Bengaluru

https://www.linkedin.com/in/siddesh-s-v-298733252/

Skills

- SIEM: Splunk ES , MS SENTINEL
- Firewall - PaloAlto
- IPS - SNORT
- EDR - Cisco AMP , CrowdStrike
- ESA - MS 365 Defender
- DDOS - NETSCOUT Arbor
- Sandbox - Trellix
- Ticking Tool -SNOW
- ELK , Copilot

Area of Intrest

- Alert Analysis
- Threat Intelligence
- SIEM Tool - Splunk
- Malware Analysis
- Email Analysis

Education Background

- Master of Computer Application
  The Oxford College Of Engineering
  Bengaluru in 2022

About Me

Passionated Cyber Security Analyst with 2 years of experience as an incident responder, Certified Splunk ES Power User and good hands-on experience in various security technologies like SIEM,IPS,IDS,AV,Email Security, Firewall, WAF, Proxy.

Professional Experience

Radiare Software Solution PVT LTD | Chennai
Security Analyst

2023 March – Present

- Monitoring of Multiple Security Incidents using SIEM tool- SplunkES
- Real time log monitoring of network traffic, intrusion/malware events and device health checkup in IPS/IDS.
- Investigating, analyzing events in Endpoint Detection and Response Tool, and then taking required action.
- Providing a list of required actions when analysis confirms malicious, suspicious, or actionable incidents.
- Monitoring Manage Engine for various auto-generated requests and user reported requests(tickets).
- Blocking Malicious URL on proxy tools.
- Fine-Tuning of alerts to avoid false positives.
- Analyzing the events in Splunk (SIEM) for various types of alerts from Firewall, IPS, Servers.
- Monitoring for the alerts like DOS, Malware, Network Security, IPS.
- Blocking the blacklisted IPS with bad reputation in Firewall.
- Produce security incident reports and briefings to the team lead and manager.
- Daily Shift Handovers.

Certifications

- Security Operations And Defense Analyst
- Foundations of Operationalizing MITRE ATT&CK
- Understanding Threats And Attacks
- Network Fundamentals.

Declaration

I hereby declare that the above information is true and correct to the best of my knowledge and belief.