SHOBHA.T

SOC Analyst

☎ 9019973299

✉ shobhabagalit@gmail.com

Bengaluru, Karnataka INDIA

https://www.linkedin.com/in/shobha-bagali-a0031030a

Education

2013-2016

- BSc (Computer Science)
  Davanagere University

Certifications

- Fundamentals of Mitre Attack
- Splunk Fundamentals
- Introduction To Cyber Security
  By CISCO

Tools

- SIEM : Splunk ES, Chronicle
- Firewall : Check Point , Fortinet
- ESA : MS365 Defender
- EDR :CISCO AMP, Sentinel One
- IPS : SNORT
- SOAR: Siemplify
- DDOS : Arbor
- AV : Systematic Antivirus
- Vulnerability Assessment :Qualys
- WAF: Cloudflare

Area of Interest

- Alert Analysis
- Malware Analysis
- Vulnerability Management
- Threat Intelligence
- SIEM Tool :Splunk ES, Chronicle

Languages

- English
- Kannada
- Hindi

Profile

Passionate Cyber Security Analyst with 4.3 years of experience as an incident responder, Certified Splunk ES Power User and good hands-on experience in various security technologies like IPS, AV, Email Security, Firewall, WAF, Proxy

Work Experience

SOC ANALYST

WEBAFFINITY TECHNOLOGIES PRIVATE LIMITED

Jan 2021-Present

- Working on Triggered Alerts using The SIEM tool-Splunk ES
- Rising tickets for validating incidents, followingup with the Incidents Response Team for ticketsclosures.
- Investigating and analyzing events in the EDRtool and taking required action.
- Working in a 24/7 SOC with a strong focus on meeting organizational SLAs.
- Analyzing events in Splunk for various types ofalerts from Firewall, IPS and servers.
- Participating in fine-tuning alerts, updating SOPs,and preparing reports as per client requirements.
- Blocking Malicious URL on Proxy Tools.
- Blocking the Blacklisted IP’s with bad reputationin Firewall.
- Daily Shift Handovers.
- Fine-tuning alerts of avoid false positives.
- Hands on Experience with some open-sourceThreat Intel Tools.
- In my role, I use Chronicle to analyze logs, identify anomalies, and create detection rules. Additionally, I work with tools like Splunk and other SIEM platforms for log correlation and reporting.