SHIVAKUMARA P J

Security Analyst

Contact

Davanagere
pjshivakumara@gmail.com
8660145014
linkedin.com/in/shivakumarapj

Objective

Enthusiastic Fresher eager to contribute to team success through hard work, attention to detail, and good organizational skills. Seeking an entry-level position in a reputable organization to begin and to build a career in the corporate environment that will explore new horizons, thus enhancing my knowledge about new and emerging trends in the sector.

Tools and Technologies

- Splunk
- Wireshark
- Virus Total
- MX Toolbox
- URL Void
- IP Void
- Linux

Education

Jain Institute of Technology
Davanagere

Certifications

- Completed SOC Analyst training
- Completed NSE-1 and NSE-2 Certifications from NSE Training Institute (Fortnite)
- Certification of completing SPLUNK fundamentals by splunk learning portal.
- Certification of completion on SOC Analyst Level 1 Career Path by CYBRARY
- CISCO Certification on Introduction to CyberSecurity

Proffessional Summary

- Good Knowledge on the Network Devices, OSI Layers, TCP/IP protocols, different Ports and Protocols.
- Understanding of security concepts like AAA, CIA.
- Knowledge on TCP 3-way handshake.
- Knowledge on different types of Malware and Cyberattacks and their Mitigations.
- Better understanding of concepts like DNS, DHCP, ARP, Encryption and Decryption, Threat and Risk, Hashing.
- Knowledge on Defence in Depth, DMZ.
- Good understanding of OWASP top 10 Vulnerabilities, online Threat Intelligence.
- Knowledge on incidence response process/life cycle.
- Good understanding of Security solutions like EDR, IPS, IDS, Antivirus.
- Knowledge on commonly used Logon types, Windows Event Logs and IDs.
- Knowledge on SIEM and the Functionality of different Components used.
- Good Knowledge on Cyber kill chain and understanding of Mitre ATT@CK framework and TTPs.
- Better understanding on use cases of Malware, Firewall, AD and Windows logs.
- Knowledge on networking concepts and log analysis.
- Able to develop new skills to keep up with the advances in Information security.

Roles and Responsibilities

- Monitoring, Analyzing and Investigating the security alerts generated by SIEM
- Analysis of triggered alerts using various analysis tools
- Creation of dashboards for visualization
- Raising tickets for validated security incidents using organization defined ticketing tools
- Follow up with incident response team for remediation
- Drafting shift hand-overs