SHAFIULLA J DODDAMANI

Mobile : 8105434720

SOC Analyst (cybersecurity)

Mail : shafiulla371jd@gmail.com

STATEMENT OF PURPOSE:

A dynamic professional seeking challenges and willing to exhibit technical skills looking forward to being associated with a progressive organization where there is scope to utilize the skills and be part of a team works towards the growth of myself and organization

WORK EXPERIENCE :

Company Name : Molex India Pvt Ltd Bangalore
Period : Dec 2018 to June 2020 (1.6 years)
Designation : Trainee Engineer

Experience :

My Experience includes diligently monitoring of the company's network for Security threats. As it a point to stay update on all the latest news and information in order to provide the best protection possible I believe my skills and Experience will allow me to make an impact in your Organization.

KNOWLEDGE IN :

- Use of the Security information Event Management **(SIEM – SPLUNK ENTERPRISE SECURITY & IBM QRadar)** tool
- Perform Security SIEM Operational task – Analysis, Filters, Active channels, Reports.
- reating dashboards in **SPLUNK** and **QRadar**
- Investigating on the reputation of **IP** addresses, suspicious URL's, files, and hash files with the help of **IBM X- Force Exchange, CISCO TALSO,** virustotal.

- Knowledge on **penetration testing** to find the vulnerability and make a recommendation for fixing the problem in order to assess the vulnerability using tools such as **Nessus, Zenmap, Metasploit.**
- Knowledge on the Incident response activities like **Malware analysis, Phishing analysis**
- Analysis of Phishing mail with the help of **Force Point, MxToolbox.**
- Basic static analysis of malware with help of **Exeinfope, strings, pestudio**,
- Basic Dynamic analysis of malware with the help of **RegShot, Procmon, Autoruns, FakeNet.**
- Using Sysinternal tools such as **Process explorer, process monitor,tcplog view**, and **sysmom** for monitoring and peeking under the hood to see what files and register keys your application are accessing
- Diagnosing the traffic of infected machines with the help of **WIRESHARK**
- Managing the **McAfee ENS** (end point security) products with the help of **McAfee EPO**
- Good understanding of various alerts .
- Good understanding of various attacks such as **XSS, SQL injection, Phishing, Spoofing, MITM, Sniffing, Brute force, DOS, DDOS, ARP Spoofing, etc.**
- Good understanding of various malware such as **Virus, Worm, Trojan horse, Ransomware, Rootkit, Adware, spyware, scareware, etc.**
- Knowledge of architecture and components of **SPLUNK ENTERPRISES SECURITY & IBM QRadar.**
- Good understanding of security concepts and networking concepts.

TOOLS:

SIEM: 1. SPLUNK. 2.IBM QRadar.
VAPT: Nessus. Zenmap .Metasploit.
FIREWALL: Cisco ASA
ENS: McAfee
Security Management : EPO(McAfee)
Network Analyzer : Wireshark
Email : Mxtoolbox

ANALYSIS TOOLS:

IBM X-Force Exchange , CISCO TALOS, VIRUSTOTAL,

CVE MITRE, NVD, US – Cert, Symantec Site review.

SYSINTERNAL TOOLS:

Process Explorer, Process Monitor (Procmon) , tcplog view, Sysmon, Autoruns, PeStudio, Exeinfope, Strings, Regshot, Fake Net.

EDUCATIONAL QUALIFICATION:

B.E in ELECTRICAL & ELECTONICS ENGINEER.
College: H.K.B.K College of engineering Bangalore.
Board : Visvesvaraya Technological University, Belgaum, Karnataka.

Place : Bangalore Yours Faithfully
Date : (SHAFIULLA JD)