Faris Sheikh Moosa Avulan

9 June 1994

avulanfm@gmail.com

+971-503550823
+91-9526333343

Darrussalam House
Othukkungal Post Manoor,
Malappuram-676528

linkedin/Faris SheikhMoosaAvulan

Education

B.Tech.Information Technology PSG College of Technology Coimbatore| 2017 | GPA:7/10

Class XII
Sree Saraswathi Vidhyamandir Mettupalayam- CBSE| 2013 | 75 %

Class X
Farook English Medium Higher Secondary School Kottakkal| 2010 | 85%

Skills

SIEM : Splunk
Vulnerability Management: Beyondtrust Retina,Qualys, Checkpoint, Nessus

Email/AV security: Microsoft O365, Ironport, McAfee ePo

Network Monitoring : Akamai, Shape

Ticketing Tools : Service Now, HP SAW, Assyst, BMS Remedy, Marval

Operating System : Windows, Linux(Kali)

Other Tools : CSC, Digital Shadows, Falcon Crowdstrike, Tanium, LaTeX

Resume Summary

Cybersecurity Analyst

Skilled Security Analyst specializing in Splunk and well-versed in Phishing analysis, vulnerability management and a strong aspiration to explore in cyber security world. Insightful professional ready to apply 2 years of experience to a new role with room for growth and advancement.

Work Experience

2017 Jul - SOC Analyst - IAG - TCS | Chennai 2.5 Years

SIEM Analysis
- Continuously monitored, analyzed and identified security alerts information from Splunk
- Creating dashboards, new rules and alerts fine-tuning to reduce time and effort
- Acting on security alerts and following up for mitigation
- Proactiveness in creation of alerts
- Currently in knowledge transfer process with client for Falcon Crowdstrike and Tanium ESP

Phishing Analysis
- Conducting analysis to determine the legitimacy of files, domains, and emails reported by end users using Windows Powershell and online resources like Virustotal, urlscan.io, IPVoid, MX toolbox, Brightcloud URL/IP lookup to name a few
- Hands-on in Microsoft O365 console and Ironport for obtaining audit/email trace logs
- Working with the Network Teams, IT Support ,End user Computing to block malicious sender addresses/embedded domains and resetting of credentials for compromised client accounts.
- Communicating and educating the end users on how not to fall prey to phishing attacks

Vulnerability Management
- Audit scans carried out on weekly basis for new vulnerabilities within the client network
- Working with the respective teams for remediation/patching of existing vulnerabilities
- Hands-on in using Beyondtrust Retina, Qualys, Checkpoint VM, and currently in knowledge transfer for Nessus Professional
- Hands-on in scanning ports and services using Nmap and monitoring network traffic using Wireshark Network Analyzer

Firewall Rule Approval and Certificate Management
- Having the judgemental decision of opening new ports for new services required by end users
- Approving rules after analysis for safe ports/protocols usage
- Certificate generation/renewal/cancellation using GlobalSign, currently in knowledge transfer process for Venafi
-Good knowledge on certificates, cryptography and ports/protocols

Others
- Hands-on in analyzing network traffic using Akamai Security Monitor and Shape for botnet/DDoS attacks
- Preparing and sharing threat advisory reports on a regular basis with the AntiVirus teams on the latest malware/threats detected globally
-Hands-on in CSC and Digital Shadows tools for handling incidents like brand infringement,anti-phishing,certificate mismanagement and permanent takedown of domains
-Good understanding on Penetration Testing and self-learned ethical hacking tools with hands-on in Kali Linux.

Accomplishments

- Recipient of "On the Spot Award" and "Star of the Month" by the project management
- Managed and took ownership of tasks originally assigned to peers to decrease their workloads, completing them within expected time constraints.
- Orchestrated as alternate shift lead as necessary and mentored new associates on process and procedure
- Resolved several incidents which leads to leads to threat for security and got appreciated by team and Clients
- Learned the Management structure and deliverable constraints in an organisation.

Certifications

- EC- Council Certified Security Analyst v10
- Certification in Agile
-Internal Certification in Cybersecurity Practices and Data Security

Strengths

- I am committed and dedicated to my work from start to finish, with a high level of concentration.
Always prioritize task and finishes within the deadlines
-I always focus on being productive in my tasks and believe in working smart rather than working hard.
- I am adaptive and a quick learner - since in our project we have a plethora of tools to work with, hence I am always quick on my toes for any new tool/technology to be implemented.
- -I am flexible to work in 24x7 shifts and weekend support.
-I have excellent communication skills and have proven this in a number of elocutions and debates I participated in school/college level.
-I am a punctual and a disciplined person in both personal and professional life.
-Having a good commitment to society and had served in Bharath Scout and Guides in school
-Organized several events in school and college.

Hobbies

-Tech-savvy and keeping interest in the latest gadgetry and technology
-Watching Movies
-Playing football and video games
-Acting in dramas and short films
-Trekking

Languages Known

-Malayalam (mother tongue)
-English
-Tamil
-Hindi
-Arabic