FARUKH ATTAR

INFORMATION SECURITY ANALYST

Pune, Maharashtra, India.

+91 9168422007 |farukhattar11@gmail.com

Professional Summary

A highly skilled Information Security Analyst with around 4 years of experience in Cyber Security domain with online security research, planning, execution and maintenance. Worked in multiple domains and across multiple teams to build and safeguard the organization from external and internal threat actors.

Exposure to MSSP and Financial organizations and am very well versed with the environment they operate in. I have been the ace performer and a quick learner in my journey and continue to do so. I enjoy cybersecurity as a domain and try to learn new accomplishments going on all across the globe. Trained staff members on the best cyber security procedures.

Experience

ASSOCIATE INFORMATION SECURITY ANALYST

Global Payments | Pune, Maharashtra, India

2022 – PRESENT

- Working in a financial sector, providing support to the Global Security Operations Centre to protect against the threat actors.
- Have exposure to the different SIEM technologies like Splunk and ELK.
- Worked on the endpoint protection systems like Carbon Black, Symantec Endpoint Protection, Trend Micro.
- Worked on data loss prevention tools like Symantec DLP and Forcepoint.
- Had exposure to Email Security like Proofpoint and Email Admin center for email analysis and protection.
- Worked on the ELK stack and used Kibana to monitor multiple applications in a Graphical Manner.
- Had the chance to handle the centralized mailbox for GSOC and be the primary point of response for all the security incidents that were reported.
- Worked on multiple Investigations, from Malware to DLP, and multiple Security Incidents that had the capability to impact the organization in terms of Security.
- Created and improved the Playbooks that were being used with the correct and up to date procedures.
- Tuned the alerts for reducing the noise being generated for the False Positive alerts on Endpoint Tool and SIEM tool.
- Worked in shifts to support the business.

- Well documented the Incidents in the Ticketing tools like Jira, Service Now.
- Identified the IOCs and implemented the security measures required to neutralize them in the organization.
- Worked with cross functional teams to get the work done in terms of policies or any security incidents.
- Reached out to managers whenever required to highlight and escalate the necessary incidents for visibility.
- Good knowledge of security frameworks like NIST, HIPAA, PCI-DSS, ISO 27001.

INFORMATION SECURITY ANALYST

Connectwise LLP | Pune, Maharashtra, India
2022 – 2022

- Worked in a MSSP environment.
- Handled the pressure and responsibilities that are present in the MSSP environment.
- Worked on Sentinel One Endpoint Detection Response Tool.
- Worked on Confluence Custom templates and Anti-Virus tool.
- Handled the ever-expanding endpoint and servers data base of ConnectWise for its clients and partners with over 5000 active endpoints to monitor in real time.
- Faced the security incidents including the normal malware like PUP and PUA, and advanced malwares like the Ransomware, example lock bit, black cat, and many more.
- Investigated these malwares to determine the impact and conclusion and contacting the Partner to further remediate on their side as well.
- Analyzed the malwares based on their behavior and Escalating to the management if required the same.
- Trained new hires on handling the alerts and analyzing the malwares in depth.
- Worked in shifts.

ASSOCIATE PROFESSIONAL NETWORK

Dxc Technologies | Bangalore, Karnataka, India.
2021 – 2021

- Experience working with the Networking Devices like, Routers, Switches, Firewall, F5 Load Balancer.
- Worked on the Security side by designing and troubleshooting the firewall rules as per the issue and business requirements.
- Worked on Service Now ticketing tool to resolve the issue assigned to my team.
- Worked on an on call-based environment.
- Worked on the requirements from clients with changes from my end.
- Engaging the required teams and doing escalations across multiple teams to get things resolves was daily task of my work.
- Allocating the tickets to other team members accordingly.
- Worked on DR activity, single handedly and got appreciated for the same.

INFORMATION SECURITY ANALYST

Link Networks| Pune, Maharashtra, India
2019 – 2021

- Worked on the threats and incidents on multiple platforms like SIEM, EDR and AV.
- Worked on SEP AV, Symantec Endpoint Protection Manager AV, to monitor for any threats present on the system based on the alerts triggered.

- Worked with the Proxy, Bluecoat and Zscalar to monitor for malicious activities and to analyze the logs for further investigations.
- These also provided with an extra layer of protection against internet browsing to protect organization from external or unknown websites that are visited.
- Used Service Manager to Log in the tickets and resolve any tickets that are assigned to my team on a real time basis.
- Worked on the Sentinel EDR to work with the alerts getting triggered on the Endpoint side.
- Updated and created SOPs for the team against the alerts and procedures to access or work upon different tools that were present.
- Worked on Qualys for automated scanning for vulnerabilities. Created the reports and escalated to the respective Point Of Contacts to get them remediated in a timely manner.
- Worked on the Cisco Amp to remediate the alerts for Endpoints and servers. Escalating to the user for finding the conclusion.
- Worked on the alerts that were being generated by the IDS like Suricata and resolving them further.
- Educating the users on security awareness, risk and controls.
- Worked on Firepower to find the malicious IPS that are being flagged and resolved those issues also.

Education

Bachelor of Engineering in Electrical Engineering - NBN Sinhgad School of Engineering, vadgaon, Pune. (2015-2019)

12th standard - Kendriya Vidyalaya Railway, Gandhidham, Gujarat. (2015)

10th Standard - Kendriya Vidyalaya Railway, Gandhidham, Gujarat. (2013)

Professional Skills

Adaptability	Teamwork	Quick Learner
Team Leadership	Problem Solving	Creativity
Public Speaking Management	Effective Communication	Resource

Technical Skills

EDR (Sentinel One, Carbon Black, Cisco AMP)	IDS (Suricata, Firepower)
Networking devices (Routers, Switches, Firewalls, F5 Load Balancers)	SIEM (Splunk, Netwitness)
Anti-Virus (SEP, Trend Micro)	Email pSecurity (Proofpoint)
Ticketing Tool (Jira, Service Now, Confluence, Service Manager)	DLP (SEP, Forcepoint)

Extra Achievements

Part of the Social Committee for my current organization.

Organized multiple events and SSR for employee's engagement.

Part of the Robin Hood Army NGO for food distribution

Active trekker, enjoy trekking forests and mountains on weekend.