Name: Shaik Ameer
Mobile: 9440891662
Email: shaik.ameer234@gmail.com

Career Objective:

To occupy a leading role in a **Cyber Security/ SOC domain** with a leading organization that recognizes and encourages innovative thinking and play an active role in achieving the organizations business and financial goals.

Tools & skills:

- Security Devices: Firewall, IPS, IDS, Endpoint Security, Email Security (ESA), WAF and other cyber security devices.
- Malwares: Virus, worms, Trojan horse, spyware, adware, ransomware
- Protocol Suits: TCP/IP, DNS, DHCP, Syslog, RDP, HTTP, HTTPS, SSH, SSL, FTP etc.
- Attacks: Email Phishing, DOS, DDOS, Malware and other cyber security attacks.
- Cyber security essentials: IOC, CIA, AAA, hashing, encryption, encoding, use cases.
- Networking: OSI layers, Flags, TCP, UDP, IP header, NAT, PAT,
- Operating Systems: Linux, Windows
- Tools: Office 365, windows Defender ATP, Splunk, Any run, Record future, Azure

Professional Experience:

Grapple Info Solutions Pvt LTD, Hyderabad (Soc Analyst)
November 2018 - Current

- SIEM Monitoring and SOC Operations - analyzes security event data from SIEM tool Splunk and WDATP, to get the right balance between caution, false positives and incidents, while providing effective security monitoring and incident response through triage, investigation, communication, reporting and escalation
- Analyzed systems on client's network to identify vulnerabilities, anomalous network behavior, compromised network hardware, and advanced malware.
- Work with supervisor to resolve issues and follow documented escalation procedures
- Analyze security event data from the network (IDS, SIEM).
- Conduct proactive monitoring, investigation, and mitigation of security incidents
- Conduct log analysis and Security monitoring using Splunk &WDATP
- Investigate malicious phishing emails, domains and IPs using Open-Source tools and recommend proper blocking based on analysis.
- Review internal logs and alerts to determine and detect potential cybersecurity events. Triage cases based on output from automated alerts, and determine when to escalate to tier 2/3 resources
- Document actions in tickets to effectively communicate and track information with team members and internal customers

- Document, follow and improve policies, procedures, and best security practices
- Monitor events, respond to incidents, and report findings and escalate critical tickets if need.
- Prioritize and differentiate between potential intrusion attempts and false alarms.
- Use Service Now to create tickets for third party supports in resolving SOC issues.
- Responsible for investigating suspicious and potentially malicious activity within the networks and systems.
- Performed Header analysis, Blacklist check for IP, Hyperlinks, analyze encoded html files etc.
- Work with legal team to take down fake domains that impersonate the real client domain.
- Identify suspicious/malicious activities or codes
- Worked in a 24x7 Security Operations Center
- Alongside supervisor, interface with customers to consult with them on best security practices and help them mature their security posture

Certificate:

- Splunk 7.x Fundamentals

Education:

- B.Sc. in Computer Science