Anusha

Sr. Security Analyst

7702443838
anushanadukuru8@gmail.com
India, Visakhapatnam
http://www.linkedin.com/in/anusha-sirra-1b129a122

PROFILE SUMMARY

Overall 7.8 years of experience into IT and 4.11 years of experience into Information Security. Currently working as a Sr. Security Analyst (Security Operation Center team).

TOOLS AND TECHNOLOGIES

SIEM Tool	:	Azure sentinel, AlienVault, Splunk.
Endpoint protection	:	Cybereason, Crowd Strike, TrendMicro
Ticketing Tool	:	Service Now, OTRS, BMC Remedy, Service Desk, Jira
Email Gateway	:	Mimecast
Firewall	:	Palo Alto Panorama, Zscaler
Antivirus	:	Symantec Endpoint Protection and McAfee.
Web Filtering Tool	:	Cisco umbrella
WAF	:	Akamai, Panorama

TECHNICAL SKILLS

- **Networking** (TCP/IP Suite, OSI Model, LAN & WAN, Router, Switch, Protocols & Ports, TCP (Three-way Handshake), SSL/TLS Handshake, DNS, DHCP).
- **Industry Recognized analysis frameworks** (Cyber Kill Chain, MITRE ATT&CK, NIST Incident Response)
- **Security Solutions** (Antivirus, Firewalls, SIEM, IDS/IPS, SSL/TLS, VPN, Cryptography, CIA Triad)

PROFESSIONAL EXPERIENCE

Tech Mahindra | Hyderabad | June 2022 – Present

Role: Sr. Security Analyst

- Overall 7.8 years of experience in IT industry and 4.8 years of experience as Information Security Analyst (Security Operation Centre team).
- Proficiency in using various security tools and technologies, such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, proxy, SIEM (Security Information and Event Management), and threat intelligence platforms
- Experience of working in 24x7 operations of SOC team, offering log monitoring, security information management, global threat monitoring.
- Handling critical alerts from Endpoint Protection and working for resolution.

- Analyses the nature and source of security threats, understanding their tactics, techniques, and procedures (TTPs)
- Handling alerts from Crowd strike EDR and investigation.
- Perform Malware analysis using different types of web-based tool such as Hybrid Analysis, Virus Total.
- Investigate phishing emails, domains and IP's using open source tools and recommend proper blocking based on analysis
- Creating suppression rules for the false positive alerts in order to avoid unnecessary noisy alerts.
- Strong knowledge on Incident management, Event Life Cycle and its Phases.
- Good understanding of OWASP Top 10, IDS, IPS, cyber Attacks like DOS, DDOS, MITM, SQL,XSS and CSRF.
- Ensure compliance with industry-specific regulations and security standards (e.g., GDPR,HIPAA, NIST). Participate in audits and assessments.
- Ability to conduct vulnerability assessments and penetration testing to identify weaknesses and vulnerabilities in the organization's systems and networks.
- Skill in responding to security incidents, including identifying, containing, and mitigating the impact of security breaches.
- Knowledge of security architecture best practices and the ability to design and implement security measures to protect critical assets.
- Keeping up to date with the latest threats and trends in the cybersecurity landscape and utilizing threat intelligence to proactively defend against emerging threats.
- Understanding of cryptographic concepts and their application in securing data and communication.
- Configure and fine-tune security technologies to enhance detection and prevention capabilities.
- Maintain detailed records of security incidents, investigations, and response activities.
- Prepare incident reports and recommendations for improving security practices.
- Provide guidance and mentorship to junior SOC analysts.
- Participate in threat hunting to proactively identify potential security threats.
- Hands on experience into KQL quires.
- Hands on experienced to AWS security.
- Experience into Incident response and end to end life cycle.

UST GLOBAL | Bangalore | Feb 2019 –

June 2022 Role: SOC Analyst L1

- Worked in a 24x7 Security Operations Centre Environment.
- Experience in handling multiple clients as a part of MSSP.
- Involved in deployment of Windows NXLog agent on servers.
- Experience of working in 24x7 operations of SOC team, offering log monitoring, security information management, global threat monitoring.
- Monitor and acknowledge alerts in the console as per the internal OLAs (Low and Medium)
- ensure that all incidents were investigated and resolved in a timely manner.
- Inform L2 s about high severity alerts
- Email forwarding for alerts, timely acknowledge and forwarding email alerts.
- SOP Adherence for email alerts.
- Ensure all tickets owned by L1 team are followed up and resolved on time.
- Tickets status to be updated on daily basis.
- Experience on performing log analysis and analyzing the crucial alerts at immediate basis through SIEM.
- Experience in generating Daily, Weekly & Monthly Reports.
- Attend SOC meetings and escalations calls.
- Strong in team coordination and managing tasks.
- Good communication, problem solving skills and the ability to acquire new skills in a timely manner.
- Preparation of Shift Handover reports at the end of the shift to provide situational awareness to the incoming shift.

Birla Soft | Bangalore | Jan 2016 to Jan 2019

Role: System Analyst

- Performed analysis and design including investigations, documentation, recommendation, and problem-solving.
- Wrote user requirements into technical specifications.
- Extensive knowledge of IT procedures and available technology solutions.
- Strong ability to coordinate with external or internal clients.
- Ability to analyze clients' existing systems and business models.
- Solid understanding of software development lifecycles.
- Produced project feasibility and cost analysis reports.
- Provided troubleshooting for internal and external users while working on help desk.
- Ability to meet strict deadlines & Strong analytical skills.

EDUCATION

Name of College: (Pydah Degree College)

Graduation: B Com Computers

Years: 2010 -2013

City, State: Visakhapatnam, AP

CERTIFICATIONS/LICENSES

- Certification AZ-900
- Certification CEBC (Code of Ethical Business Conduct)
- Certification AI101
- Certification SOC fundamentals
- Certification AWS Level 1
- Certification SECEON (XDR, MSSP, SIEM, SOAR, MITRE ATT&CK)

DECLARATION:

I hereby declare that the information furnished above is true to the best of my knowledge and if selected, would put in my best efforts for the growth of the organization.

Anusha S
Visakhapatnam