Security Analyst – Security Operations Center (SOC)

Name: **PEYYALA LOKESH**

Contact No: **8464094973**

Email ID: lokeshpeyyala94@gmail.com

YOE: 5

Professional Summary:

The Security Analyst – Security Operations Center (SOC) will work as part of the Information Security Operations team in the Technology Division (IT) to detect, prioritize, and triage any potential attacks or malicious activities involving intellectual property, networks, and sensitive data. The ideal candidate will have a thorough understanding of information security, cyber threats, cyber threat actors, and monitoring and detection. The SOC Analyst will be responsible for continuous monitoring, identifying, and investigating of security events and alerts, providing incident response and remediation support, and improving security posture.

Professional Experience:

SOC ANALYST

DIGIBOXX TECHONOLOGIES. PVT. LTD | Remote **02/2024 to Present**

- Define, identify, and classify information assets, assess threats and vulnerabilities regarding those assets, as well as recommend appropriate information security controls and measures.
- Detect, analyze, respond to, and lead security incidents, including Application and Network attempted and realized breaches. The incident response should include host and network-based log analysis, correlation of network indicators, PCAP data, incident timeline generation, and root cause analysis among other data sources.
- Correlate event data for IDS systems, Firewalls, Secure Web Gateways, SIEM, and other security systems for potential threats.
- Motivated team player and can adapt and learn new technologies, tools and applications Investigate Incidents using. Channels/Dashboards/Events/Graphs/Annotations/Cases and Reports.
- Perform Security SIEM Operational task - Analysis, Optimization, Filters, Active channels, Reports, Suggestion of fine tuning on existing rules.
- Monitoring and chasing for closure for security incidents like password getting attack, login failure from multiple hosts. Successful password guessing attack.

SOC ANALYST

JUST VFX STUDIOS PVT LTD | Hyderabad **12/2019 – 12/2023**

- Analyzing the vulnerability Scan report after remediation of the Specific Vulnerability. Monitoring and chasing for closure of NESSUS and remediation of vulnerability.
- Experience in Phishing emails and performing Malware analysis.
- Strong knowledge on Incident response process & good understanding of security solutions EDR Crowd Strike, Firewalls, IPS, WAF and Antivirus.
- Research and identify key indicators of compromise (IOC) on the network, servers, and end user workstations.
- Investigate and analyze causes, patterns and trends that can pose a risk to data integrity and information systems.
- Investigate security breaches and create actionable plans to address risks.
- Prepare detailed written analyses of incidents with remediation and prevention documentation.
- Provide briefing of findings to both technical and non-technical senior management audiences and business stakeholders.
- Maintain current knowledge on a wide range of security issues including architectures, firewalls, electronic data traffic and network access.
- Stays current with security news, attacks, threats, vulnerabilities, and technologies and implementing new defenses to secure the threat landscape.
- Document all incidents, investigations, and analysis activities accurately and thoroughly.
- Performing Log analysis & analyzing the crucial alerts at immediate basis.
- Preparing Daily, weekly, and Monthly reports as per client requirements.
- Experience in Phishing emails and performing Malware analysis.

Educational Qualification:

- Completed **B. TECH** at Paladugu Parvathi Devi College of Engineering with 58.41%, Which is affiliated to JNTU Kakinada during **2010-2015**

IT SKILLS:

- **Tools:** Seceon, CrowdStrike, EDR, Virus total, Jira, Darktrace, Nessus & IBM Q Radar
- **Technical Skills:** Dns, TCP/UDP, Osi &Tcp/Ip Layers, Nmap, Wireshark, Forti web, FortiGate, SIEM Backup.
- **Security Skills:** CIA, Hashing, Encryption, Threat, Vulnerability, Risk, IPS, VPN, IDS, Proxy Firewall, Routers, (TCPIP/DNS/HTTP/HTTPS), Root cause Investigation, Multifactor Authentication (MFA), Malware Analysis, Patch Vulnerability Management Life Cycle, Cyber Kill Chain, Phases of Hacking.