SHIVASHANKAR MH

7676947025 ◇ Shimoga, Karnataka
shiva.shankar.syat@gmail.com ◇ https://www.linkedin.com/in/shivashankar-mh-142b9217b/ ◇

OBJECTIVE

In close to 3 years of my career, I have acquired and exhibited extensive Network Security and Palo Alto TAC skill-set and provided Security solutions and delivered Comprehensive threat analysis. Being passionate in Security Analyst I look for an opportunity to contribute in developing effective security strategies to protect critical infrastructure.

EDUCATION

M.C.A (Master of Computer Application), KLE Technological University 2018 - 2021

SUMMARY

- Good knowledge of Networking Devices like Hub, Switch, Repeaters, Router, Firewall and it's types.
- Good knowledge on different types of Cyber attacks.
- Working level knowledge on security solutions like Firewall, IPS, IDS, EDR, Antivirus, VPN etc.
- Good learning of Network fundamentals, TCP/UDP, NAT, IP Address, IPsec protocol, TLS handshake, TCP flags.
- Sound knowledge about the OSI (Open Systems Interconnection) model, ARP protocol, IP (Internet Protocol) header and it's fields, TCP (Transmission Control Protocol) header and its fields, DHCP process, DNS process.
- Security concepts: CIA, AAA, Hashing, Encryption, MFA, Three-Way handshake, Threat, Vulnerability and Risk, System hardening, ZERO trust model.
- Proficient in the Cyber Kill Chain model, understanding the stages of an attack from reconnaissance to actions on objective.
- Familiarity with the Mitre Attack framework, recognizing the tactics, techniques, and procedures used by attackers
- Knowledge of OWASP guidelines for securing web applications.
- Sound knowledge on Port numbers and protocols such as Http/s, FTP, DNS, DHCP, SMTP.
- Keeping updated with the latest developments in the cyber security landscape.

EXPERIENCE

Network Security Engineer MAY 2023 - Current
Movate Technologies Pvt Ltd *Chennai*

- Configured Paloalto firewall interface deployment in L3, L2, Virtual-wire, HA and Tap modes also Performed PAN-OS upgrades using PANORAMA.
- Managed features such as Firewall Policies, IPsec VPN, Global-Protect SSL-VPN, SSL Decryption (Forward Proxy and Inbound Inspection), Authentication (local database and other protocols), Threat Prevention, URL Filtering, High Availability (Active-Passive and Active-Active), Panorama and Log Collector.
- Also Assist in configuration and troubleshooting in Security profiles like Antivirus, Anti-spyware, Vulnerability protection, URL filtering, File blocking, and DOS protection.
- Responsible for analyzing customer tech-support files and logs of Palo Alto devices to their respective Daemon.
- Provide technical support, configurations, troubleshooting to customers via phone, e-mail, and web for the next generation firewall customers.
- Hands-On experience tools - Palo Alto Firewall, Palo Alto PANORAMA, PANTS, SHORTS, PPGraph, QUEST Console, JIRA, Salesforce, Velocity, Strata Troubleshooting Playbook, Genesys cloud, GP parser.

Network Security Analyst SEP 2021 - MAY 2023
Genex Technologies Pvt Ltd *Hyderabad*

- Performed real-time monitoring security incident handling, investigation, analysis, reporting and escalation of security events from multiple log sources.
- Acknowledging and closing false positives and raising tickets for validated incidents.
- Investigating security incidents, preparing IR report and assigning to higher team and follow up with incident response team for remediation.
- Build daily/weekly reports as per client requirements.
- Used Microsoft Word and other software tools to create documents and other communications.
- Create reports that will allow experts to make changes in the security policies as per the needs of the organization.
- Real time log analysis from different network devices such as SIEM, Firewall, etc
- Knowledge working in 24/7 with strong focus on agreed SLAs.
- Drafting shift hand overs.
- Good understanding of various SOC processes like monitoring, analysis, playbooks, escalation, incident documentation, SLAs, client meetings, report walk through, bridge calls, etc.
- Hands-On experience tools - FortiSIEM, SNOW, VirusTotal, AbuseIPDB, Shodan, Microsoft Office (MS Word, MS Power Point), Phishing Email analysis, WireShark.

LANGUAGES

Kannada, English, Hindi, Tamil

CERTIFICATIONS

- Certified Security Analyst by SOC Experts.
- Foundations of Operationalizing MITRE ATTACK by ATTACK IQ Academy