S.Venkatesulu

MOB: +91-9108236532 **EMAIL: srmvenkey7@gmail.com**

CAREER OBJECTIVE:

Information Security professional seeking a career position within an organization, where my professional experience, education and abilities would be an advantage for the growth of employer and myself.

CORE QUALIFICATIONS:

- IBM QRadar,McAfee Nitro, LogRhythm,Arcsight,Splunk SIEM Tools
- Threat Hunting
- Email Security
- Vulnerability assessment
- Proof point Email Security
- Incident response
- Security Advisories
- Malware Analysis
- Symantec Antivirus, DLP.
- Data Loss Prevention
- Tenable & QualysGuard
- McAfee Web gateway &ATD

ORGANIZATIONAL EXPERIENCE:

- **3.6 years** of experience in Information Security/ Cyber Security/SOC.
- Experience in Monitoring and Administration of IBM Qradar, HP Arc sight and McAfee Nitro SIEM Tools.
- Experience in Monitoring of McAfee IPS and Symantec Endpoint Protection (SEPM).
- Experience in Symantec Antivirus and DLP.
- Experience in working on identifying phishing emails by using Proof point Email security solution.
- Experience in Monitoring of Snort IDS, McAfeeIPS.
- IBM QRADAR, Tenable Security Center, QualysGuard Vulnerability assessment tools.
- Experience in Malware Analysis, Phishing Email Analysis.
- Experience in Cisco Iron Port Tracker Email Security.
- Experience in ServiceNow and Jira Ticketing Tools.

EXPERIENCE:

❖ Working as **Security Engineer** with **Fincare Small Finance Bank** (May 2020 Till date)

- Working on identifying **IOC's** in the client network and performing **Sandbox** analysis.
- Analysis Web attacks and Malware Alerts and Working on remediation actions.
- **SIEM** consultant for log & event analysis, incident investigation, reporting, remediation & also develop new rules, policies for incident detection.

- Determine the scope of security incident and its potential impact to Client network, assessment of risk; recommend steps to handle the security incident with all information and help them to Mitigate the risks and threats.
- Responsible for end to end security, ensuring that the confidentiality, integrity and availability of all enterprise data is not breached, infected or compromised in anyway by outside malicious users.
- By utilizing a defense in depth approach and identifying areas of potential weakness.
- IBM QRADAR SIEM Deployment, Integration of logs from various across vendor network and security devices and application specific servers; Case study and Implementation of basic to advanced correlation rules; Custom parsers and Dashboards
- Creation of reports, dashboards and rules fine tuning.
- Real Time log Monitoring and Analysis in **SOC**, Incident tracking, incident Investigation, incident analysis and Reporting.
- Scan Status, Asset discovery, Configuration Assessment of SIEM Clients.
- Threat management, Security advisories & compliance audits.
- Auditing the rules based on security standards and refining it.
- Perform deep packet analysis to identify DDoS/DoS attack vectors and security threats. Implement security countermeasures to mitigate security related threats (DDoS/DoS/Attacks).
- Create and coordinate attack response based on security product.
- Performed full application security assessments and analysis on newly built and existing applications. Because of these efforts, many potential security Threats were identified before being released into a production environment.
- Existing production security vulnerabilities were promptly remediated upon discovery, thus greatly reducing the overall security risk.
- Continuous monitoring of the authority network and internal systems for malicious activity. Numerous attacks and security threats targeted at company.
- Responsible for scan running and Analyzing Symantec AV risk reports and recommending for required actions.
- Reviewing and Analyzing different security advisories to provide recommendation for latest emerging threat in context of the Client infrastructure.
- Preparing trends, notifications, daily reports and security advisory for customer devices.
- Monitoring individual device logs – **Arbor, F5 WAF, Symantec HIPS, Source fire IPS, Tenable Security Center**.
- Experience in configuration and administration of **McAfee ePO, HIPS, DLP; McAfee NSP, McAfee NGFW**.
- Linux experience and competence.
- Ability to work in a dynamic and rapidly changing environment.
- Validate Daily / Weekly / Monthly security operations reports
- Configured reports & dashboards in SIEM product for various security devices i.e: firewalls & IDS and network devices.
- Preparing the Knowledge Transfer document of Process and Technical specifications guide for the Transition/Internal purpose.
- Conducting Training for the Team Members.

❖ Worked as Junior Security Engineer with IIFL (AUG 2018 – Apr 2020)

- Experience in Network traffic and log analysis: identifying and classifying attempted security incidents, suspicious traffic to client networks using **McAfee Nitro and Logarithm SIEM** tools.
- Experience in performing scans in **Symantec Endpoint Protection** management.
- Skilled in identification of emerging security threats, intrusion investigations, Vulnerability assessment and troubleshooting.

- Real time log monitoring in the **Security Operations Center (SOC)** from different devices such as **Firewalls, IDS, IPS and Windows Servers** received from the client and segregating and correlating the logs of that device.
- Configuring Reports, Dashboards, Notifications and Real time alerts.

- Preparing Vulnerability Assessment reports and remediation steps post assessment.
- Preparing daily reports, trends, notifications and security advisory for customer devices.
- Reviewing and Analyzing different security advisories to provide recommendation for latest emerging threat in context of the Client infrastructure.
- Reviewing quarantined DLP email and escalating to customers for critical data theft.
- Experience in SPAM mailbox monitoring and identifying and mitigating phishing campaigns.
- Responsible for running scans on Symantec and moving host to block mode policy to contain the host.
- Real Time log Monitoring and Analysis in **SOC**, Incident tracking, incident Investigation, incident analysis and Reporting.
- Scan Status, Asset discovery, Configuration Assessment of SIEM Clients
- Responsible for daily and weekly client meeting and sharing risk reports with management.

CERTIFICATIONS:

- QualysGaurd Vulnerability Assessment
- McAfee SIEM Certification

TRAININGS:

- IBMQRADAR
- ITIL
- Proof point Email Security

INTERESTS:

- Attending Security forums.

ACADEMIC DETAILS :

- ✓ **MBA** from, JNT University Hyderabad.
- ✓ **B.Com** from, Sri Krishnadevaraya University Anantapur.
- ✓ **Intermediate** from, Govt Junior College Kambadur, Anantapur.
- ✓ **SSC** from Zillah Parishad High School Sevamandir, Anantapur.

PERSONAL INFORMATION:

Full Name	:	S. Venkatesulu
Date of Birth	:	01/07/1983
Sex	:	Male.
Marital Status	:	Married.
Nationality	:	Indian.
State	:	Bangalore, Karnataka.
Languages	:	English, Hindi, Kannada, and Telugu.
Contact Number	:	91-9108236532
Email Address	:	srmvenkey7@gmail.com

DECLARATION:

I hereby declare that the above written particulars are true to the best of my knowledge and belief. If provided an opportunity, I will utilize it with all my determination to be a committed professional dedicated to the cause of the organization.

PLACE:

BANGALORE

NAME:

S. Venkatesulu