**GONDHI SESHU**

Mobile:8985365045

Email ID: gseshu2006@gmail.com

# P R O F I L E

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.

# P R O F E S S I O N A L S U M M A R Y

* Over all 3.8 years of IT Experience with Information Security as Security Analyst (Security Operation Centre team).
* Good understanding of security solutions like Anti-virus, DLP, Proxy, Firewall filtering/monitoring, IPS, Email Security, EPO, WAF etc. Hands on experience with Log rhythm, HP ArcSight, Splunk, Q radar.
* SIEM tool for logs monitoring and analysis, Service now ticketing tool. Hands on experience on Endpoint Detection and Response (EDR).
* Good knowledge on networking concepts including OSI layers, Subnet, TCP/IP, ports, DNS, DHCP, Firewall monitoring, content filtering, checkpoint etc.

# T E C H N I C A L S K I L L S

* SOC (Security Operation Center)
* SIEM (Security Information and Event Management) Tool: Log rhythm, HP ArcSight, Splunk, Q radar.
* Vulnerability Assessment (Nessus), Symantec endpoint (EDR)
* Phishing Email Analysis
* Create, Modify and Update Security Information Event Management (SIEM) Tools.
* Perform Cyber and Technical Threat Analysis
* Networking: Switches, Routers, OSI layers, TCP/IP model, Security Solutions, Malware,
* LAN & WAN support. Hardware installation. Network IP configuration. Routing and switching.
* Hardware/software trouble shooting, System & software installation.
* Basic knowledge in CCNA(Cisco certified network associate), MCSE(Microsoft certified solution expert) ,LINUX.

# WORKING EXPERIENCE

Security Analyst with Varutra (Mumbai) July 2019 to till Date.

* Served as Security Analyst in SOC operations for real-time monitoring, analyzing logs from various security/Industrial appliances by using ArcSight ESM console, ArcSight Logger and troubleshooting of logging issues.
* Administrating various incidents/security alerts triggered in SIEM tool.
* Monitoring 24x7 for Security Alerts and targeted phishing sites by using SIEM tool with the help of technologies such as Watermark, Referrer, Abuse mailbox and similar sounding domains.
* Website Anti-Malware and Defacement monitoring and real-time alerting based on anomalies detected.
* Created filters, active channels, queries, Rules, Dashboard in ArcSight for monitoring purpose.
* Configured reports in ArcSight ESM and ArcSight Logger as per the requirement.
* Maintenance of HP’s ArcSight Products (ESM and Logger) like its Health check which also includes ArcSight content developments i.e. rules, reports, dashboards.
* Knowledge of Installation, Configuration and up gradation of various connectors, and its troubleshooting.
* Conduct analysis of network traffic and host activity across a wide array of technologies and platforms.
* Assist in incident response activities such as host triage and retrieval, malware analysis, remote system analysis, end-user interviews, and remediation efforts.
* Recognize cyber-attacks based on their signatures. Differentiate the false positives from true intrusion attempts and help remediate/prevent cyber-attacks.
* Analyze malicious campaigns and evaluate effectiveness of security technologies.
* Develop advanced queries and alerts to detect adversary actions.
* Lead response and investigation efforts into advanced/targeted attacks.
* Identify gaps in IT infrastructure by mimicking an attacker’s behaviors and responses.
* Provide expert analytic investigative support of large scale and complex security incidents.
* Direct prior experience with core security technologies.

# EDUCATION

BSC(C/S) RAYALASEEMA UNIVERSITY 76%, 2015.

MBA BHARATHIYAR UNIVERSITY 72%, 2019.

# DECLARATION

I Seshu.G declare that the above information given is correct and true to the best of my knowledge.

Seshu.G.