**Sai Ram Manda**

**Information Security Engineer**

**venkatesh.g@itechstack.com**

**+1-609-905-0827**

Vulnerability Management | Vulnerability Assessment | Policy compliance | Patch Management | Remediation | SOC | SIEM | Incident Management | Risk Management | Security Hardening

**Summary**

Information Security Technical Specialist and a result-oriented professional with over a decade of qualitative experience in Vulnerability Management, Policy Compliance, SOC, Patch Management, Risk Assessment and System Administration.

**Professional Summary**

* Experienced & understanding of process related to **Vulnerability management, Policy compliance, Patch management, SOC, Web Application scanning & Incident Response.**
* Experienced in complete **Vulnerability Management** program in **Discovering**, **Reporting**, **Verifying** the vulnerability and **Remediation** of vulnerabilities.
* Experienced in complete **Policy Compliance and Security Hardening** program, building the policies from scratch bases on different frameworks and implementing in entire environment.
* Implemented **policy & compliance assessments** based on company baseline standards.
* Hands on experience on implementing **CIS & NIST benchmark security compliance** for Windows, Unix (Red hat, Rocky Linux, AIX, HPUX, Solaris etc.) and Databases (MSSQL, Oracle, MySQL, Mango DB etc.).
* Demonstrated ability to research and track **Common Vulnerabilities and Exposures** (CVEs) relevant to the organization's technology stack.
* Strong knowledge of the **Common Vulnerability Scoring System** (CVSS) and its application in assessing the severity of vulnerabilities.
* Hands on Experience on both On-prem & Cloud environment (**AWS & Azure**) security.
* Knowledge on implementing regulatory frameworks like **PCI DSS, SOX, GDPR, HIPPA**
* Experienced in **Architecting and designing the infra VM scan setup** and closely worked with Architecture team on designing/implementation of **security policies**.
* Mentoring the team and providing the **technical training** to the team on different security technologies and tools.
* Working Experience on VM tools like Qualys, Rapid7 and Nessus.
* Data analysis and reporting of data through tools like Power BI and Tableau.
* Performed pathing on different technologies using Patch Management module and tools.
* Performed **Risk analysis** and **prioritization of vulnerabilities** using SKYBOX tool in helping teams to focus on the critical vulnerabilities.
* Collaborated in listing **Compensatory controls** to understand the risk of the organization.
* Prepared and presented all **Tech Risk** presentations to the Audit and executive management on Risk analysis of vulnerabilities.
* Managing critical vulnerability reports like **External, Internet Facing, SOX**, etc., and making sure that these vulnerabilities are mitigated within timelines (SLA)
* Extensively worked on **Authentication issues** with regards to different operating systems (E.g: Microsoft AD, Windows, Linux & VMware), Network devices and Databases.
* Providing support for **Incident response**, including evidence collection, documentation, communication, and reporting.
* Continuously researching the **end-of-life** versions and operating systems and communicating to the owners to patch/upgrade/migrate to the latest available versions as per **policies**.
* Involved in implementation of **SNOWVR** project.
* Managing **SOC**, across one or more of the following roles: Security Analysis, Incident Response, Security Monitoring, vulnerability management.
* In-depth knowledge of security concepts such as cyber-attacks and techniques, threat vectors, incident management etc.
* Performing penetration testing on internal systems with the use of popular penetration testing tools (**Metasploit, Nmap, net discover**).
* Creating alerts, updates, and notifications regarding new viruses, malware, and new patches using US-CERT, UK CERT, NVD in CSIRT team.
* Performing regular security monitoring to identify any possible intrusions. Providing support per request from various tower teams.
* Experienced in Creating scan template, Report template and providing vulnerability reports as per requirement.

**Education**

M.C.A (Master of Computer Applications) from JNT University, India

B.Sc. (Math’s & Computers) from Andhra University, India

**Awards and Honors**

* Certified Ethical Hacker V9(CEH|V9)
* Qualys Guard Certified Vulnerability Management Specialist.
* Qualys VMDR
* Qualys Certified Specialist – Web Application Scanning.
* Qualys Certified Specialist – Policy Compliance
* Microsoft security operations analyst (SC-200)
* Microsoft Azure security Engineer (AZ-500)

**Work Experience**

**Client Nokia Corporation**

**Duration August 2022 – Till date**

# Role Information Security Manager & Technical SME

**Project Description:**

It was founded as a pulp mill and had long been associated with rubber and cables, but since the 1990s has focused on large-scale telecommunications infrastructure, technology development, and licensing. Nokia made significant contributions to the mobile telephony industry, assisting in the development of the GSM, 3G, and LTE standards.

# ROLES AND RESPONSIBILITIES:

* Utilize Qualys Policy Compliance module to develop, implement, and manage policies, leveraging frameworks such as CIS, PCI DSS, and NIST, ensuring alignment with industry standards and internal security requirements.
* Employ scripting languages like Python or PowerShell to automate policy tuning and control adjustments in response to changes in corporate governance.
* Collaborate with teams using tools like SNOW and One trust to ensure Qualys policies align with regulatory requirements.
* Set up and manage scan schedules using Qualys Scanner Appliance (QSA) and create custom reports/dashboards using Qualys Reporting & Analytics.
* Configure and maintain Control IDs (CIDs) in Qualys Policy Compliance module, ensuring they accurately represent organizational security standards and are aligned with industry best practices.
* Utilize Qualys APIs and scripting languages to automate CID configuration updates based on security policy changes.
* Perform regular maintenance tasks on the Qualys platform, including applying software updates, patches, and making configuration adjustments using different tools.
* Monitor system performance using monitoring tools such as Nagios or Prometheus and troubleshoot issues to ensure the continuous and reliable operation of the Qualys tool.
* Collaborate with cross-functional teams using collaboration tools like Microsoft Teams or Slack, gathering organizational requirements and translating them into Qualys configurations.
* Maintain comprehensive documentation of Qualys policies, configurations, and procedures using tools like One trust, Archer Confluence for reference and audit purposes.
* Work with One Trust SME to integrate Qualys scan data into the One Trust tool using APIs and data transfer protocols.
* Provide technical training to internal teams on the use and best practices of the Qualys platform, utilizing tools like Zoom or Microsoft Teams for virtual training sessions.
* Foster a knowledge-sharing culture within the organization by sharing expertise through

platforms like Microsoft SharePoint or internal wikis.

* Customize policies, establish exception processes, and generate scorecard reports to provide insights into policy compliance status.
* Onboard assets into the Qualys platform and integrate CyberArk for privileged access management, ensuring secure authentication processes.
* Lead a team to discover vulnerabilities and threats in servers, endpoints, network device, and communicate to business owners.
* Responsible for defining and maintaining a formal Vulnerability Management Program.
* Used Rapid7 Insight VM for scanning and Qualys for Security Hardening.
* Creation of Sites and Deployment of scanners in InsightVM & Cloud Agent installation.
* Responsible for creating framework that defines the vulnerabilities priorities aligned with business criticality.
* Experience in managing and prioritizing vulnerabilities based on CVE identifiers.
* Skilled in assigning CVSS scores to vulnerabilities to prioritize remediation efforts.
* Created custom Azure Policy definitions to enforce security and compliance standards.
* Utilized AWS findings to enhance the overall security posture of cloud resources.
* Responsible for providing governance, guidance and setting priorities for remediation.
* Develop and present business case to Management to improve security posture to mitigate the critical vulnerabilities.
* Responsible for troubleshooting cloud agent issues and maintaining compliance.
* Responsible for creating script in MacAfee ePO for Qualys Cloud Agent related requirement (Deploying cloud agent, deploying certificates, configuring proxy for agent)
* Responsible for 1st level of approval for Exception and Extension of the vulnerabilities raised by the stake holders / Asset Owner.
* Publish patch governance reports to Windows, Unix, Oracle and end user computing team.

**Client Palo Alto Networks Duration April 2021 – August, 2022 Role Senior Technical Specialist**

# Project Description:

Palo Alto Networks is an American multinational cybersecurity company, The core product is a platform that includes advanced firewalls and cloud-based offerings that extend those firewalls to cover other aspects of security.

#  ROLES AND RESPONSIBILITIES:

* Responsible for defining, ratifying, and maintaining a formal Threat & Vulnerability Management Program and framework that defines the vulnerability priorities aligned with business criticality.
* Responsible for providing governance, guidance, and setting priorities for risk-based vulnerability management, mitigation, and remediation.
* Develop and present business cases to Management to improve security posture to effectively mitigate advanced threats.
* Proven expertise in integrating CVSS scores into risk management processes.
* Onboard the assets for target technologies in enterprise security tool. Create required authentication records for target technology assets in enterprise security tool.
* Deploy Qualys Cloud agent and ensure agent compliance.
* Perform infrastructure vulnerability management and ensure client environment is compliant.
* Gained understanding and knowledge of important Vulnerability Assessment tools – Qualys guard, Nexpose, IBM VMS.
* Utilized threat intelligence to enhance the accuracy of CVSS scoring and prioritization.
* Assisting the Information Security Risk Manager in the Risk analysis process, which is concerned with gathering information about exposure to risk so the organization can make appropriate decisions and manage risks appropriately. Assisting for risk procurement
* Interaction with Information Technology Team & all Staff to Perform risk analysis for all the raised queries by different stakeholders and Implementation of security products.
* Raising a PMR (project management review) call, to find a fix for security patches.
* Migration/Acquisition projects for vulnerability and Policy Compliance
* Experience in educating stakeholders on the importance of CVEs and CVSS scores.
* Responsible to run PCI scans on periodic basis.

**Client Sony Pictures Entertainment**

**Duration September 2017 – April 2021**

# Role Information Security Technical Lead Project Description:

Sony Pictures Entertainment is a division of Sony Corporation, a creative entertainment company built on a solid foundation of technology. Along with other sister companies, they make the movies, television, music, and games that engage billions of people, connecting creators and audiences around the globe.

# ROLES AND RESPONSIBILITIES:

* End to End deployment of New Business Subsidiaries to Qualys.
* Involved in Qualys-SNOW integration project.
* Overseeing Infra, Web & policy compliance activities.
* Developed and implemented a customized CVSS scoring model tailored to organizational needs.
* Creating the Dashboards in Qualys & Splunk, preparation of reports using Tools like Power BI
* Develop security baseline configurations for several operating system platforms (i.e., Windows, UNIX, Linux, Cisco, Juniper, etc.) and scan for compliance/vulnerabilities.
* Identify false positives, risk acceptance candidates, perform root cause analysis.
* Working on Cloud Agent issues & Troubleshooting.
* Providing periodic trending problem reports. Create and maintain a Security Incident log that is also provided to client Information Security to facilitate historical analysis.
* Diagnose and resolve issues and problems with the clients’ information technology systems

involving several processes. Investigating causes, analyzing, and diagnosing the problem and repairing or providing detailed alternative solutions.

* Identify vulnerabilities in the application and make recommendations on how to fix the issues and submit as documented report. Providing detailed reports for the developers to understand and fix the vulnerability found in the application.

**Client Time Warner, WB**

**Duration May, 2014 – September, 2017**

# Role Information Security Analyst Project Description:

The company is known for its film studio division, the Warner Bros. Motion Picture Group, which includes Warner Bros. Pictures, New Line Cinema, Warner Bros. Pictures Animation, Castle Rock Entertainment, and DC Studios. Among its other assets, stands the television production company Warner Bros. Television Studios.

# ROLES AND RESPONSIBILITIES:

* Scanning the servers using Qualys scanner and reporting the vulnerabilities to the appropriate teams for remediation.
* Created Qualys scan profiles for different project requirements.
* Generating customized Qualys reporting templates to explain the remediation status to the tower teams.
* Performing penetration testing on internal systems with the use of popular penetration testing tools (Metasploit, Nmap, net discover)
* Performed Manual/Automated weekly vulnerability assessment of 2500+ Servers, network devices which includes compliance servers and devices hosting PCI, SOX and DMZ compliance applications as the per defined scope.
* Worked with Platform team on mitigating WannaCry ransomware related Vulnerabilities on TW infrastructure servers.
* Implemented Qualys Cloud Agent on Windows Platform & AWS Instances as part of the new project.
* Conducted Weekly remediation follow-up meeting with the respective platform owners on the remediation status/challenges and documented it.
* Presented weekly vulnerability risk or compliance dashboard to higher management and client.