**Sathvik Vontela**

[satvontela@gmail.com](mailto:satvontela@gmail.com), +1.919.443.5512, [www.linkedin.com/in/sathvikvontela](http://www.linkedin.com/in/sathvikvontela)

**Professional Overview:**

* Overall, 9.5 years of work experience in the Information security field working in healthcare, banking, and computer networking sectors.
* Outstanding experience in implementing enterprise-level policies, procedures, processes, standards, and solid experience in auditing and reviewing the applications infrastructure, and SecOps such as Risk management, BCP, KMS, Patch, and Change management.
* Very good experience in threat surface reduction, Authentication, authorization, certificates, logging, auditing, Web Security, App Dev process, Privacy, and Data Security, SSO, OAuth, SAML, Cryptographic Support, Traffic and Protocol Protection, Sec Ops process, and Session management.
* Performed Threat modelling reviews, and code reviews after conducting the AppSec vulnerabilities such as SAST, DAST, and Pentest.
* SME for Asset management, Vulnerability management, security operations, and performing and executing recipes such as OAuth, DNSSEC, and vulnerability management.
* Good experience in Automated testing and manual testing with tools CheckMax, IBM/HCL App Scan, Rapid7, Burp suite, OWASP ZAP proxy.
* Good experience and understanding the security compliance/standards such as NIST, SOX, ISO-27002, OWASP Top 10, PCI, PII, HIPAA, and SAN 25.

**Certifications:**

* Token of Appreciation for living one of Cisco’s Principles: Takes Accountability.
* Certified Qualys – Vulnerability Management.
* Certified Cisco Security Ninja White and Advanced security programs.

**Education:**

* Master’s in Cyber systems and information security at Auburn University, Montgomery - 2017.
* Bachelor’s in Electrical and Electronic Engineering at Malla Reddy Engineering Collage – 2013.

**Technical Skills:**

* **Checkmarx** – SAST/Secure code
* **HCL/IBM App Scan** – DAST/Outside view testing
* **Burp Suite** - DAST/Outside view testing
* **Splunk** – SIEM Log monitoring and centralized logs
* **Qualys** – Vulnerability management for infrastructure scans.
* **Cloud** – Salesforce & Microsoft’s Azure.
* **Scripting** – Python, bash, sh, and CSH
* **SoapUI, and Postman** – Web API’s.
* **Application Platforms** – Linux (RedHat, CentOS, and Windows).
* **Compliance and Standards** - OWASP Top 10, CWE, NIST, ISO 27002, HIPAA, PTES, MITRE, SOC 2 and SAN 25.

**Professional Experience**

**Cisco Systems, Inc., RTP, Raleigh, North Carolina­ February 11th, 2019, to August 12, 2023.**

**Role:** Security Assessment Engineer / Qualys Admin / Application Security Auditor

**Partner Security Advocate – CX-IT Business Unit**

* As a partner Security Advocate cum Qualys Admin, I am responsible for the end-to-end application security lifecycle for the application from two portfolios.
* I perform security reviews and remediations of SAST and DAST scans.
* Closely work with InfoSec AppSec team on security compliance such as SSDLC.
* SAST(Gitlab), DAST, Pentest (If applicable) – Monitoring weekly to see any High and medium vulnerability issues.
* Help the developers with False positives and the remediation work.
* Keep track of all the application changes and deployments, including certifying the latest scans.
* Qualys – Work with the Continuous Security Buddy team and Developers to mitigate the High, Medium issues and Qualys Token in QQL.
* Make sure the apps meet the resiliency requirements and quarterly IT risk management.

**Program: CSDL For Enterprise**

* Worked on the CSDL4e - Cisco Secure Development Lifecycle (Similar to SDLC) PSB requirements, pulled out from the Cisco Enterprise level policies, process, standards, and guidelines.
* Assisted business units in securely architecting/operating their offerings by aligning to the Cisco Security Development Lifecycle (like SDLC), industry-standard methodologies, compliance, and privacy requirements.
* Leading multiple security assessments for enterprise applications and platforms within these business units (Supply Chain, IT, Customer Experience, SSBR) and working with them to identify gaps in compliance and propose remediation steps.
* Used in-depth knowledge of various security weaknesses and vulnerabilities and mitigations techniques to review technical documents and evidence provided by application teams to help them progress through the assessment process.
* Responsible for driving adoption, identifying, defining new CSDL requirements, and potentially helping our automated security validation development.
* Worked and contributed with other security engineers and architects to share lessons learned during assessments and identify best practices for future evaluations.
* Experience with Symantec DLP solutions such as identity and classifying the sensitive data, data encryptions, patch management strategies.
* Good experience with assessment of data protection standards, laws, and regulations like HIPAA, SOX and FISMA.
* Good experience with Infrastructure vulnerability scans and remediation such as Qualys.

**Program: Customer Assurance Program (CAP)**

* Worked on the build server hardening as being apart application security team.
* Worked with the build and release teams to migrate from LAB environment to Engineering -IT (Cisco managed Environment).
* Worked with the team on Operating System hardening and the infrastructure hardening based on the CIS benchmark.

**Program: CASPR / Cloud Vendor Security Assessment**

* Reviewing the business and systems architecture with the IT business team and Cloud service provider.
* Scoring an assessment questionnaire taken by the Cloud Security Provider.
* To protect Cisco and Customer's data to a level commensurate to its value and criticality.
* Engaging directly with an appropriate representative(s) of the CSP to remediate any outstanding findings.
* Collaborated with Cloud service provider (AWS, Salesforce, Azure) and performed risk management by considering SOC type 2, ISO27001 certifications.
* Thorough validation of policies and standards of Cloud service provider with Cisco compliance.

**McKesson - Tata Consultancy Services, USA, Scottsdale, Arizona­ August 2018 to January 2019 – 5 Months**

**Role:** Security Engineer / Qualys Admin / Security Test Engineer

* Worked on various projects at the client location, especially with Salesforce applications and traditional web applications.
* Worked on salesforce profile validation security testing manually on various programs such as Novartis ‘s COSENTYX, NPAF, PANO, AIMOVIG, Sun Pharma, TOBI.
* Worked on Mobile-based security testing on COSENTYX application which is a manually based and considering OWASP security standards.
* Very good experience with the Browser stack for functional testing in terms of security perspective.
* Tested the Copay application manually to find vulnerabilities and remediate them with a suitable solution.
* I have tested web services/Restful API’s security testing by using SoapUI and Postman desktop application.
* Identifying the critical, High, Medium, Low vulnerabilities and infrastructure vulnerability scans such as Qualys in the applications based on OWASP Top 10 and prioritizing them based on the hypercritical.

**BBVA, Dallas, Texas May 2017 to April 2018 – 12 Months**

**Role:** Penetration tester / Information security Analyst

* Worked on Web Application Vulnerability Assessment and Threat Modeling, Gap Analysis, Secure Code Review on the applications.
* Performing security analysis and identifying possible vulnerabilities in the essential derivation function, create Vulnerability Assessment report detailing exposures that were identified, rate the severity of the system & suggestions to mitigate any exposures & testing known vulnerabilities.
* Identified issues like SQL injection, XSS, CSRF using Burp Suite.
* Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and SANS 25 and prioritizing them based on the hypercritical.
* Conducting web application security scans using IBM App Scan, & Checkmarx.
* Perform periodic vulnerability assessments to identify weak systems and vulnerabilities.

**Omni Trust Technologies, Alpharetta, GA July 2016 to March 2017 – 9 months**

**Role:** Penetration tester

* Performed Manual Code Review to find logic flaws, which are not identified by Automated Tools.
* Well versed in Understanding Application-Level Vulnerabilities like SQL Injection, XSS, CSRF, Authentication Bypass, Authentication Flaws, Cryptographic Attacks, etc.
* Conducted Social Engineering Attacks using Backtrack and Kali Linux.
* Monitored, Analyzed, and responded to security incidents in the infrastructure. Investigate and resolve any security issues found in the infrastructure as per the security standards and procedures.

**Auburn University, Montgomery, AL March 2015 to April 2016 – 13 Months**

**Role:** Student Technician

* Responsible for installing and supporting network hardware, software, and applications on personal computers and Apple computers.
* Handled responsibilities of analyzing hardware and software problems and implement corrective measures.
* Skilled in MS Word, Excel and PowerPoint, Legal Solutions, Internet, and Email.
* Proficiency in handling network monitoring tools and packet capture tools.
* Adept skills in technical documentation and presentations using Microsoft Visio/ Office.

**Project-A**

* They are maintained and monitored by all the installed systems and the infrastructure.
* Installed, configured, tested, and maintained application software and system management tools.
* Maintained security, backup, and redundancy strategies.
* Installed, troubleshoot, repaired, and maintained Cisco VOIP/Call Manager/Unity/Network equipment on the LAN/WAN.
* I have configured VLANs with 802.1q tagging according to the server team's requirements.

**NetEnrich, Hyderabad, India July 2013 to November 2014 – 16 months**

**Role:** Jr. Network Engineer

* Performed network monitoring, provided analysis using various tools.
* I have worked with fundamental communication protocols like TCP/IP, UDP, Ethernet.
* Managed service providers/vendor's relationships from a project and technology perspective.
* Managed VPN, IPSec, Endpoint-Security, Status Policy, Application Control, IPS (Tipping Points), Monitoring, Anti-Spam, Smart Provisioning, DLP using Checkpoint Firewalls.
* Troubleshoot using various command tools on Cisco routers and network segments at different OSI layers.
* Performed troubleshooting of connectivity problems using Ping and Traceroute.