Satyanarayana Chirumamilla

+91-8073068242

chsn5803@gmail.com

Bangalore, India

SUMMARY

Highly accomplished Information Security Architect with 5+ years of experience in support of project vision, road map and business objectives. Exceptional skills in Information Security, Threat modeling & Architecture Review, Cloud Security Risk Assessments, Vulnerability assessment, Vulnerability Management, Coordinated Penetration tests with Third-party vendors and Azure CI/CD pipeline Integrations w.r.t to the CIA Triad

EDUCATION

JNTU University | Hyderabad
Master's in Computer Science & Engineering

JNTU University | Hyderabad
Bachelor's in Information Technology

SKILLS

- Threat Modeling & Architecture Review
- Cloud Security (Azure, AWS)
- Vulnerability Assessment & Penetration testing
- Risk Assessment & Risk Management
- Coordinating Penetration tests with Third-party vendors

TOOLS

DAST : Appscan Standard, Enterprise, BurpSuite
SAST : Checkmarx, Veracode
API: Postman, SoapUI
Threat Modeling: Microsoft Threat Modeling, Visio, SD Elements (POC)
Network & Vulnerability Management: QualysGuard, NMAP, NESSUS, VMDB

CERTIFICATIONS

- EC-COUNCIL CERTIFIED SECURITY ANALYST V10
- CompTIA Security +
- AWS Certified Security Specialty
- Certified ISO/IEC 27001:2013 Information Security Management Lead Auditor
- Microsoft Certified Azure Fundamentals (AZ-900)

EXPERIENCE

02/2022 - Current
Information Security Architect
Daimler Truck Innovation Center India Private Ltd | Bangalore

1. Performing the Cyber architecture reviews in alignment with Daimler Truck AG, IT Global Enterprise Architecture and engaging with other senior technical leaders throughout the organization for the implementation.
2. Working closely with the development teams to understand the applications in depth to document the application details including the security architecture, Cloud security controls, attack surface, trust boundaries and data flows for vendor offerings (SAAS/ PAAS/ IAAS) services.
3. Developed the Threat Models involving the public cloud stacks (e.g. Azure, AWS) and internal cloud platforms that enumerate cybersecurity threats by attack surface.
4. Analyzing the existing cloud security controls, SOC 2 report gathered from the project team with reference (ISO/IEC 27001; ISO/IEC 27017; SOC 2 Type 2, ISO 22301, NIST CSF), identifying the gaps and generated the vulnerabilities as per Threat category.
5. Prepared security profile summary report with potential vulnerabilities, Countermeasures, shared with project team/Business and articulated the vulnerabilities and countermeasures in awareness session.

08/2021 - 02/2022
Assistant Manager
KPMG Assurance and Consulting Services LLP | Hyderabad

1. Worked on technical IT risk assessments, architectural security reviews involved complex architectures associated client's cloud applications.
2. Integrated the vulnerabilities from all the penetration tests, performed the vulnerability management execution, effectively communicating security risks, and developed meaningful action plans and tracking issues to resolution.
3. Researched standards such as ISO 27001, CIS, CSA CCM and NIST 800-53 to provide a comprehensive control catalog and identify gaps in alphabets use of the Azure cloud environment.
4. Maintained and updated process steps, service documents in Atlassian confluence pages and available to global team members.

- Microsoft Azure Security Technologies (AZ-500)

TICKETING SYSTEM

- ServiceNow
- Jira Service Desk
- Azure Boards

5. Participated in IT Information Risk Management (IRM) team and community meeting held in KPMG and contributed applying setting standards and policies for the group and the business.

11/2019 - 08/2021
Technical Solutions Architecture Specialist
NTT DATA Information Processing Services Pvt Ltd | Bangalore
1. Conducted Vulnerability Assessment & Penetration Tests for web applications using IBM Appscan standard and enterprise to evaluate attack vectors, Identify application vulnerabilities and Performed manual assessment of the results from the Appscan to eliminate false positives using Burp Suite.
2. Integrated new repos/URL's in CI/CD pipeline, performed static (SAST, DAST) &Open Source Analysis (OSA) scans using Checkmarx, Appscan and eliminated false positives against the secure coding baseline and practices.
3. Raised the defects in qTest, prepared executive summary reports for every assessment and conducted meetings with respective application teams, explained the vulnerabilities listed and provided recommendations to fix the issues.
4. Performed retest, verifying the fixes applied by dev team passing the test runs and defects to go to the production.
5. Acquainted with various approaches to Grey & Black box security testing based on the OWASP top 10 standards and scored the vulnerabilities based on the criticality.

04/2018 - 11/2019
Senior Analyst - Data & Cyber Security
Societe Generale Global Solution Centre Pvt Ltd | Bangalore
1. As part of ROCS (Regulatory, Oversight and Cyber Security), team responsible for security governance, including Application Security Risk Analysis, Control execution, follow-ups and dashboard generation.
2. Coordinated end-to-end Application Security activities (Vulnerability Assessment, Penetration Testing) globally with different stakeholders in organizing the Pentest and follow-up with project teams to fix the vulnerabilities discovered during Pentest audit.
3. Coordinated with external vendors on a regular basis for the security assessment and penetration testing activities.
4. Conducted the kickoff meeting with the pen testers & Application Managers to define the scope, functionalities and ensures pre-requisites are ready for the pen test.
5. Performed analysis of vendor audit reports on the vulnerabilities identified and imported to vulnerabilities database. Executed the VM control, prepared action plans, and sent alert emails to the Application Owner, Application Manger timely to remediate the vulnerabilities.
6. Performed Application Sensitivity Assessment (ASA), Risk exception management, on the SGGSC Paris applications to assess the criticality of an application.
7. Created SOP for new activities, on boarded new activities with minimal support from the extended team Paris.
8. Produced the security dashboards regularly to monitor the activity and reported the trends to the management.