DevSecOps & Secure Code Review Consultant | Mitigating Security Risks Through Seamless Integration of Security in the Development Cycle

Madhu Nandyala

Hyderabad, India.
91 9966869555
MADHUNANDYALA@HOTMAIL.COM
LinkedIn: https://www.linkedin.com/in/madhunandyala/

Professional Summary

Results-driven Application Security Consultant with 13+ years of experience in DevSecOps, Secure Code Review, and Application Security Tooling. Expertise in Vulnerability Assessment, Threat Modeling, Component Lifecycle Management, and Security Automation. Proven track record of integrating security into CI/CD pipelines and leading Application Security initiatives.

Core Competencies

- **Application Security**: SAST, DAST, SCA, Risk Management
- **Security Tools**: Fortify, Checkmarx, Veracode, IBM AppScan, Sonatype IQ Server, Blackduck, Snyk, OWASP Dependency Checker, Sonarqube, JFrog X-Ray
- **DevSecOps & CI/CD Integration**: Jenkins, GitHub Actions, GitLab CI, AWS CodePipeline
- **Threat Modeling**: Secure by Design, MS Threat Modeller, IriusRisk
- **Cloud Security**: Docker, Kubernetes, AWS Cloud.
- **Programming**: Java, NodeJS, Python (Beginner)
- **Version Control**: SVN, Github, Gitlab, Nexus Repository, JFrog Artifactory
- **Leadership & Mentorship**: Security Focal, Security Program management, Tooling Evaluation, Training & Development, Secure coding training.
- **Vulnerability Management Tools**: Orca Security, Seemplicity, DAZZ (WiZ)

Professional Experience

Oct 2024 – Till date

Alteryx – *Staff Application Security Engineer*

- **SAST (Static Application Security Testing)**:
    - Performed SAST by onboarding of applications into Sonarqube tool.
    - Networked with 30+ teams to onboard, identify vulnerabilities, remediate findings till now. Planning to collaborate more in upcoming quarters.
    - Contributed to integrate Sonarqube with Wiz (DAZZ) vulnerability aggregator tool and successfully completed.
- **SCA (Software Composition Analysis)**:
    - Performed SCA by onboarding of applications into Blackduck tool.
    - Networked with 30+ teams to onboard, identify vulnerabilities, remediate findings till now. Planning to collaborate more in upcoming quarters.
    - Contributed to integrate Blackduck with Wiz (DAZZ) vulnerability aggregator tool and successfully completed.

- Performed a POC to get rid off an ongoing issue with Blackduck scans with the thick client applications. Written a python script to automate identifying non modified open source components in the code base.

- **Cloud Security**:
  - Performed 25+ Orca scans for different cloud accounts and coordinated with the development teams to mitigate the findings.
  - Completed Orca integration with GITLAB to achieve Shift left security.
  - Scanned 60+ containers in Snyk and collaborated with Product teams for remediation efforts.

March 2022 – Oct 2024

Cadence Design Systems – *Staff Information Security Analyst*

- **SAST (Static Application Security Testing)**:
  - Built entire Fortify tool from scratch including Fortify SCA Engine, Fortify SSC and all the Jenkins/GITHUB actions integrations.
  - Responsible for Fortify server availability and Scan efficiency.
  - Networked with 80+ teams to onboard, identify vulnerabilities, remediate findings.
  - Contributed to integrate Fortify with Seemplicity vulnerability aggregator tool and successfully completed.
- **SCA (Software Composition Analysis)**:
  - Built the Sonatype Nexus repository and IQ Server from scratch with High availability.
  - Responsible for Nexus Repository manager and IQ Server availability and Scan findings.
  - Performed SCA by onboarding of applications into Sonatype Nexus IQ Server tool.
  - Networked with 100+ teams to onboard, identify vulnerabilities, remediate findings.
  - Contributed to integrate Nexus IQ Server with Seemplicity vulnerability aggregator tool and successfully completed.
- **On-Premises GITHUB administration**:
  - Providing administrative support by managing new user accounts, permissions, issues, storage, licenses etc.
  - Helped around nearly 100 tickets related to account creation, repository access, licenses, GitHub action workflow issues, implementing Infosec policies etc

February 2021 – March 2022

IBM, Hyderabad – *Senior Advisory Consultant/Security Consultant*

- **Cloud and Application Security**:
  - Successfully completed Cloud migration/modernization of 35 applications for Travel and Transport industry where the targeted platform is AWS.
  - Acted as a Security focal where I handheld the Application Development teams to Path2PROD route. I have provided guidance to the teams to adhere to the Controls/Mandates to get the required approvals from the Client's GRC team.
  - Completed 35 application SAST scans, finding analysis, mitigation of the findings before those applications are deployed to UAT environment.

- Primary contact from Offshore team for DevSecOps. Good knowledge on AWS Code pipeline, Jenkins JTE, Tekton pipeline and integration of Security tools into the pipelines.

- **DevSecOps:**
  - Implemented shift left using DevSecOps practices. Integrated 50+ pipelines with Security tools.
  - Tool stack used AWS Code Piepline, Jenkins JTE, Tekton pipelines.
- **Data and Application Security Practice Level initiatives**:
  - Handled a team of 7 interns 2021 batch for Data and Application Security(DAS) practice. Guided the interns wherever needed for smoother internship completion and success at IBM.

September 2019 – February 2021

HSBC, Hyderabad – *Consultant Specialist on Secure Development Lifecycle (previously Application Security Tooling SME).*

- **Secure Development**:
  - Responsible for Secure Coding using Threat Modelling, SAST, DAST tools and thereby enabling Secure Development Life Cycle.
  - Weekly 3-5 Trainings provisioned for Development communities on how best to utilize the tools. Weekly scheduled sessions on tools like Checkmarx, NetSparker, IriusRisk etc.
  - Security remediation recommendations to development communities across the GB/GF BUs of HSBC.
- **Application Security Tooling:**
  - Responsible for Application Security related tools Evaluation, Implementation and Maintenance. The tools used were Checkmarx SAST, Contrast IAST, NetSparker DAST and IriusRisk threat modelling.
  - Developed an API which is internally used across HSBC through which Automation of User onboarding to Checkmarx SAST tool using REST API in NodeJS language.
  - Involved in support activities for the entire Application Security related tools.
  - Helped development teams to understand the tools better and make use of the tools efficiently.

October 2014 - September 2019

IBM, Hyderabad - *Application Security Consultant*

- **SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) remediation**:
  - Responsible for SAST from Offshore delivery perspective. Completed 300+ SAST scans, reviews and guided for remediation over a 2.5 year tenure.
  - Brought down the SLA for mitigation of vulnerabilities to 18 calendar days from 90 calendar days(Industry standard)
  - Fixed DAST identified issues within the SLAs agreed with the client. Approximately over 1000 issues remediated and successfully deployed the fixes to Production.
- **SCA (Software Composition Analysis)**:

  - Scan the applications for SCA using Nexus IQ Server. Over 600+ applications scans performed, findings analyzed, supported remediation.
  - Coordinated with Release teams to push these changes whenever there is a deployment. Given utmost priority to SCA findings as these impact direct risk towards the application.
- **DevSecOps:**
  - Worked with the DevOps teams to integrate security tools (Fortify, IQ Server) with the pipelines. Achieved almost 100+ pipelines integration with the Security tools.
- **Team Lead activities:**
  - Lead a team of 15 people from offshore and responsible for Offshore delivery. Coordinated with multiple stake holders from Client and Onshore counterparts to ensure smoother Security processes.
  - Helped the junior resources by giving functional KT and technical help wherever needed.

November 2012 - October 2014

Infosys, Hyderabad - *Process Specialist*

- **Development activities:**
  - Involved in complete cycle of the project execution (Design, Build, Test, Production release and Postproduction support).
  - Part of implementation, owned 2 modules completely.
  - Primary point of contact from offshore in System Integration Testing (SIT), SOCT, and SVP phases as project was completely led by onshore lead.
  - Involved in documenting changes; Support handover documents, updating current state documents etc...
  - Investigating and resolving issues found in testing phase.
  - Analyzing and tweaking (if necessary) batch jobs scripts.

Education

2008 - 2010

Anna University, Chennai, TN - *Master of Engineering with 8.11 CGPA*

Awards

- Got Technical Excellence Award Q4 2021 for ideating Security Automation in Application Security competency.
- Service Excellence award for the contribution of Mentoring and training the Interns (2021 batch) on DevSecOps at IBM.
- Excellence award for the Automation of Tooling onboarding efforts in HSBC.

(Madhu Nandyala)