Checkmarx CxSAST

Proof of Concept (POC) Plan

# CxSAST POC Plan



Table of Contents

[General Information 3](#_Toc16777426)

[Stakeholders 3](#_Toc16777427)

[POC Owners 3](#_Toc16777428)

[POC Team 3](#_Toc16777429)

[Business Needs 4](#_Toc16777430)

[POC Technical Aspects 4](#_Toc16777431)

[Success Criteria 4](#_Toc16777432)

[POC Owners 4](#_Toc16777433)

[Support of Languages & Frameworks 5](#_Toc16777434)

[Customization 5](#_Toc16777435)

[Timeline 5](#_Toc16777436)

[Customer Responsabilities 5](#_Toc16777437)

[IT Infrastructure 5](#_Toc16777438)

[On-Premise POC 5](#_Toc16777439)

[Cloud POC 5](#_Toc16777440)

[Resources 5](#_Toc16777441)

[Participants from Customer 6](#_Toc16777442)

[Facilities 6](#_Toc16777443)

[Appendix: CxOSA 6](#_Toc16777444)

[CxOSA Success Criteria 6](#_Toc16777445)

[Appendix: Prodcution Envioronment Description 7](#_Toc16777446)

[Checkmarx Implementation Discovery Questionnaire 7](#_Toc16777447)

[Program Overview and Goals 7](#_Toc16777448)

# General Information

Company Name:

Company Description:

# Stakeholders

## POC Owners

* AppSec Manager:
* CISO:
* Development Manager:
* DevOps Manager:

## POC Team

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| First name | Last name | Position | Email | Phone |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Business Needs

Main AppSec challenges to address in the POC:

# POC Technical Aspects

* Installation location (on premise or Checkmarx cloud):
* Named users (number):
* Duration (limited to 2 weeks):
* Maximum project size (limited to 500,000 lines of code):

# Success Criteria

The Customer and Checkmarx will agree on some of the Success Criteria below:

## POC Owners

* Installation
* Usage
* Integrations:
* IDE : Eclipse, IntelliJ, Visual Studio, other
* Source repository : GIT, PERFORCE, SVN, TFS, other
* Build management : Bamboo, Jenkins, TeamCity, TFS, VSTS, other
* Bug tracking : HP ALM, JIRA, other
* Dashboard : SonarQube, other

## Support of Languages & Frameworks

Scan projects in following environments:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Project name | Language | Framework | Lines of Code | Remarks |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Customization

Easily remove False Positives & False Negatives:

# Timeline

* Start date (dd/mm/yyyy):
* End date (dd/mm/yyyy):

# Customer Responsibilities

## IT Infrastructure

### On-Premise POC

* Hardware and software requirements are specified in [Server Host Requirements](https://checkmarx.atlassian.net/wiki/display/KC/Server+Host+Requirements)
* Hardware ID will be provided by customer to get a POC license

### Cloud POC

* Address will be provided by Checkmarx

## Resources

Prepare the code of the projects to scan

## Participants from Customer

* Developers to scan, review the results and fix the code
* Project lead
* AppSec owner

## Facilities

* Room
* Projector
* Internet access for WebEx sessions

# Appendix: CxOSA

During the CxOSA POC how will open source libraries be submitted for scanning?

* Upload of a zip file containing libraries via Cx UI (Yes/No)
* Upload of a package manager file (e.g. pom.xml) to CxUI (Yes/No)
* Which package manager is being used?
* Is this package manager installed on the Cx server? (Yes/No)
* Use of build Server (e.g. Jenkins)? (Yes/No)
* Is package manager used as part of build process? (Yes/No)
* Which package manager is being used?
* If the package manager file references internally hosted libraries and will this repository be accessible from CxServer? (Yes/No)

### 

### CxOSA Success Criteria

How will you define success for your POC of CxOSA?

Notes to Cx SE:

* Please accept the CxOSA EULA prior to OSA scanning
* Is QF1 installed ( for new systems) OR
* Is system migrated (for existing OSA customers using old OSA engine)
* Does POC license include CxOSA (and date)
* Send Organization Token to OSA Team and Regional OSA Champion

# Appendix: Production Environment Description

It is important to understand the production environment characteristics:

* How many developers will be using the system
* Development method (Waterfall /Agile / CI-CD):
* Information about the code:
* Languages used
* Frameworks used
* Hosting or on premise. In the case of hosting, AWS / Azure / and are they using SQL DB as-a-Service
* SDLC / DevOps environment and integrations:
* IDEs used:
* Source Repositories:
* Build Servers:
* Dashboards and bug tracking:

# Checkmarx Implementation Discovery Questionnaire

Answer the following questions to the best of your ability. If you don’t know the answers to all of the questions, that’s alright, we can talk through them with you to help you find the best path forward.

## Program Overview and Goals

1. What are the overarching goals for your Checkmarx deployment?
2. Describe in as much detail as possible your existing AppSec program. Do you consider your program to be mature?
3. Do you have application security policies that govern software development, which may drive how Checkmarx is implemented and used within your organization?
4. Are there certain types of vulnerabilities you want to find (E.g., specific severity, CWE, etc.) with Checkmarx?
5. How will you measure the success of your Checkmarx implementation?
6. What metrics are you looking to derive from your Checkmarx implementation and how will you report those metrics?

## Organizational Structure, Teams, and User Management

1. Describe the roles and responsibilities of your AppSec team, DevOps team, Developers, and Managers as it pertains to Checkmarx.
2. Describe the roles and responsibilities of your AppSec team, DevOps team, Developers, and Managers as it pertains to Checkmarx.
3. Describe the roles and responsibilities of your AppSec team, DevOps team, Developers, and Managers as it pertains to Checkmarx.
4. Describe the roles and responsibilities of your AppSec team, DevOps team, Developers, and Managers as it pertains to Checkmarx.

## SDLC Integration

1. What CI/CD technologies are you using (Jenkins, TeamCity, Bamboo, CircleCI, etc.)?
2. What SCM technologies are you using (Git, Perforce, TFS, SVN, etc.)?
3. What defect tracking system are you using (Jira, etc.)?
4. What IDEs are the developers using (JetBrains, Eclipse, VS, etc.)?
5. What programming languages are most commonly used in your organization?
6. Are there any other systems besides those mentioned above that you would be interested in integrating with?
7. How will developers consume Checkmarx results?

## Checkmarx Capacity and Scanning

1. How many different applications do you plan to scan with Checkmarx?
2. How frequently do you want to scan your applications with Checkmarx?
3. How many of applications of the following sizes do you plan to scan with Checkmarx?

1 – 100K LOC:

100K – 500K LOC:

500K – 1.5M LOC:

> 1.5M LOC:

1. Given a choice, would you scan from CI/CD, IDE, SCM, Ad hoc, or via other automation?
2. Are there any circumstances where you would choose scan speed over scan accuracy?

## Checkmarx Management

1. Who will manage and maintain Checkmarx after it has been implemented?
2. Who will have access to CxAudit to reduce FPs and FNs, and who manage and maintain Checkmarx queries?
3. What are your data retention requirements? How much scan history is your organization required to maintain?
4. Who will triage Checkmarx results (mark results as confirmed, not exploitable)?