Анализ безопасности приложений
Инструмент для разработчиков

CHECKMARX

Что делает CHECKMARX

Checkmarx CxSAST является высокоточным и гибким инструментом для анализа исходного кода, который позволяет в автоматическом режиме сканировать не скомпилированный код, обнаружить и идентифицировать сотни уязвимостей в наиболее распространенных языках программирования.

CxSAST доступен в установке как самостоятельно, так и эффективно интегрирован в цикл разработки (SDLC) для сокращения времени на обнаружение и устранение уязвимостей.
CxSAST может быть развернут как внутри корпоративной сети заказчика, так и использоваться как облачный сервис.

О CHECKMARX

Checkmarx является лидером в области решений для тестирования безопасности приложений. Клиентами компании являются 4 мировых производителя программного обеспечения из топ-10 и сотни Fortune 500 и SMB организаций из всех отраслей промышленности.

ПОЧЕМУ CxSAST

Для крупных организаций, которые хотят свести к минимуму риски информационной безопасности, CxSAST предоставляет возможность устранения уязвимостей на ранних этапах разработки. В отличии от других решений для статического анализа кода CxSAST получил широкое распространение у разработчиков, так как легко вписывается в их существующие процессы разработки.

Gartner

The only vendor to score a perfect 5.0 for "Static Analysis Product," AST Critical Capabilities Report 2014.

ПОДДЕРЖИВАЕМЫЕ ЯЗЫКИ ПРОГРАММИРОВАНИЯ

Java | JS | php | python | Groovy | Apex | android | perl
Microsoft .net | HTML 5 | Windows Mobile | C++ | Scala | Ruby | Microsoft ASP.net | VB.NET | Microsoft Visual Basic 6.0 | PL/SQL

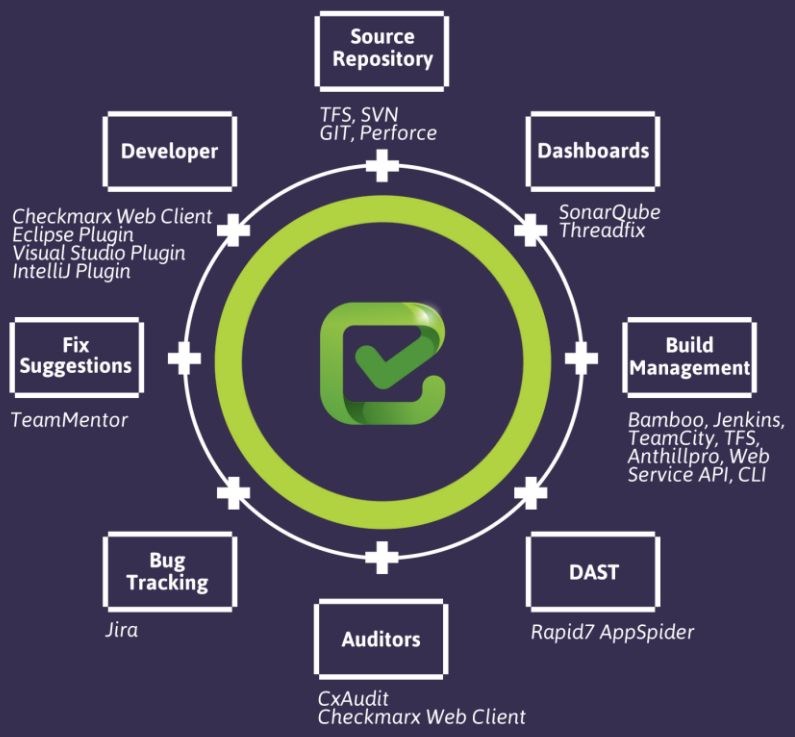
info@iitdgroup.ru | www.iitdgroup.ru| www.checkmarx.com

БЕЗОПАСНЫЙ SDLC

Checkmarx позволяет интегрировать статический анализатор кода в SDLC. Платформа интегрируется с наиболее распространенными репозиториями, серверами сборки, системами баг-трекинга и имеет плагин для сред разработки. В случае отсутствия интеграции с каким-либо специфичным компонентом SDLC из коробки, то это возможно поправить с помощью встроенных API.

Преимущества полностью интегрированной модели SAST:

- Checkmarx выполняет проверку автоматически исходя из заданных параметров;
- Инкрементальное сканирование – сканирование только измененных частей кода. Позволяет значительно сократить время сканирования и, как следствие, быстрее приступить к устранению проблем.



ПОДДЕРЖИВАЕМЫЕ ТИПЫ УЯЗВИМОСТЕЙ:

- SQLInjection
- Cross-SiteScripting
- Code Injection Buffer
- Overflow
- ParameterTampering
- Cross-SiteRequestForgery
- HTTP Splitting Log
- Forgery Denial of
- Service Session
- Fixation Session
- Poisoning
- UnhandledExceptions
- Unreleased Resources
- Unvalidated Input
- DangerousFilesUpload
- Hardcoded Password And
- more...

ПОДДЕРЖИВАЕМЫЕ СТАНДАРТЫ

OWASP Top 10 2013 | OWASP Mobile Top 10 | SANS 25 | HIPAA | Mitre CWE | FISMA | PCI DSS | MISRA | BSIMM

FAQ

Какие виды отчетов поддерживает CHECKMARX?

Checkmarx предоставляет конфигурируемые отчеты о выполненном сканировании в форматах PDF, RTF, CSV или XML..

Поддерживает ли CHECKMARX сканирование мобильных приложений?

Да, Checkmarx полностью поддерживает приложения для Android, IOS, Windows, и гибридные мобильные приложения.

Как работает CHECKMARX?

Checkmarx разбирает исходный код (который не нуждается в компеляции), мапирует его, сохраняет в базу данных, и далее, запускает запрос по базе данных, в котором и заложены сотни правил для нахождения уязвимостей.

Предоставляется ли Checkmarx в виде сервиса?

Да, предоставляется 2 варианта поставки: как лицензия для заказчика, так и в виде облачного сервиса от партнера.

Можно ли использовать Checkmarx, чтобы понять, какие изменения в коде привели к уязвимости ?

Да, Checkmarx обеспечивает сравнение сканирований одного и того же проекта и указывает на отличия от версии к версии.

info@iitdgroup.ru | www.iitdgroup.ru| www.checkmarx.com

Что делает CHECKMARX уникальным?

CHECKMARX сканирует не компилируемый код

Возможность платформы сканировать сырой исходный код означает, что пользователь может начинать сканирование на самых ранних этапах разработки в том случае, когда это является самым эффективным моментом для устранения ошибок, связанных с безопасностью.
Checkmarx позволяет сканировать фрагменты кода в любое время, в том числе когда код еще является не скомпилированным.

CHECKMARX не сканирует повторно код, который не был изменен

Checkmarx использует свою собственную запатентованную технологию инкрементального сканирования, которая избавляет от необходимости повторно полностью сканировать весь код: сканируются только те ветки, которые были изменены. Такое сканирование позволяет быстро получить результаты и очень удобно при agile подходе.

CHECKMARX прозрачен и прост в настройке

Продукт Checkmarx SAST был разработан с использованием открытого языка запросов, которые могут быть легко изменены в зависимости от потребностей пользователя. Также можно указать методы санитации, которые не являются частью фреймворка, что позволит уменьшить количество ложных срабатываний. Существует возможность добавления своих собственных проверок для обеспечения соответствия кодирования лучшим практикам, внутренним политикам компании для решения специфичных задач.

CHECKMARX интегрируется в процесс сборки

Checkmarx является достаточно гибким инструментом и интегрируется в существующий SDLC, поэтому может автоматически применять существующие политики безопасности. Платформа поддерживает самые широко используемые репозитории, серверы сборки, системы баг-трекинга, среды разработки и системы отчетности, что позволяет оптимизировать процесс тестирования безопасности и максимально обеспечить его эффективность.

CHECKMARX оптимизирует Ваши затраты на исправление

Checkmarx имеет более широкие возможности, чем просто проверка кода на уязвимости. С помощью данной платформы можно оптимизировать рабочий процесс по исправлению ошибок. Checkmarx оценивает направление потока данных в приложении и определяет критические узлы, в которых можно закрыть сразу несколько уязвимостей всего лишь одним исправлением.

CHECKMARX поддерживает большое количество языков программирования

Checkmarx поддерживает на данный момент 20 языков программирования и самые используемые фреймворки. Каждый год добавляется по 2-3 новых языка!

OUR AWARDS

Deloitte.
2nd Fastest Growing Security Company in EMEA

CIOReview
Top 20 Security Products

RED HERRING WINNER 100 EUROPE
Red Herring EMEA Top 100 Winners

Best Application Security Product in 2014 by Cyber Defense Magazine

FAQ

Есть ли интеграция с серверами сборки?
Да, сейчас мы поддерживаем плагин Jenkins, Bamboo, TeamCity, TFS, Anthill Pro и другие.

Как часто выпускаются обновления?
Новая версия продукта выходит каждый год, текущие обновления происходят каждый квартал. Срочные исправления происходят по запросу.

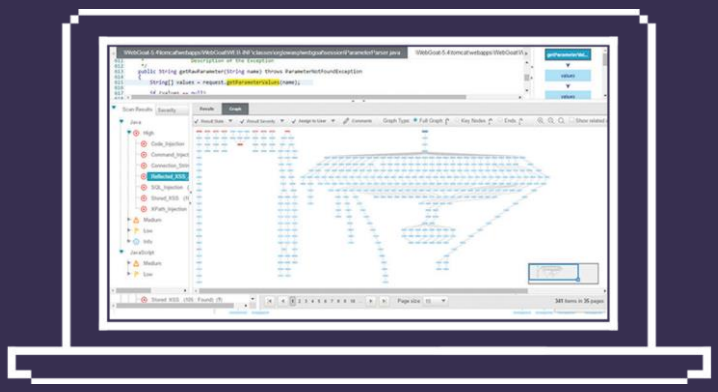
Какой процент ложных срабатываний ?
Checkmarx имеет низкий уровень ложных срабатываний (менее 5%). Достигается это путем пометки данного срабатывания как ложного прямо в интерфейсе программы, а так же адаптацией правил проверки к вашей среде разработки. В этом также могут помочь наши инженеры.

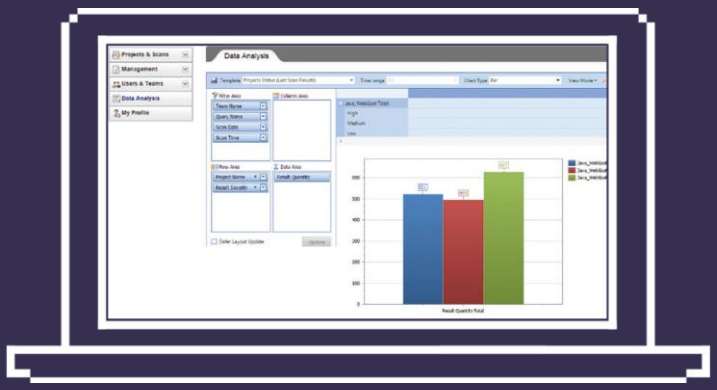
Нужно ли каждый раз сканировать весь код?
Нет. функция инкрементального сканирования будет автоматически сканировать только обновленные ветви кода.

CxSAST панель просмотра результатов

Окно просмотра результатов предоставляет удобный интерфейс для специалиста в области информационной безопасности и разработчиков, позволяя им исследовать уязвимость и принять решение об устранении. Так же интерфейс показывает вектор атаки и путь прохождения данных по приложению от их ввода до вывода.

При нажатии на прямоугольник с функцией в основном окне с кодом будет подсвечиваться соответствующая строка или фрагмент кода



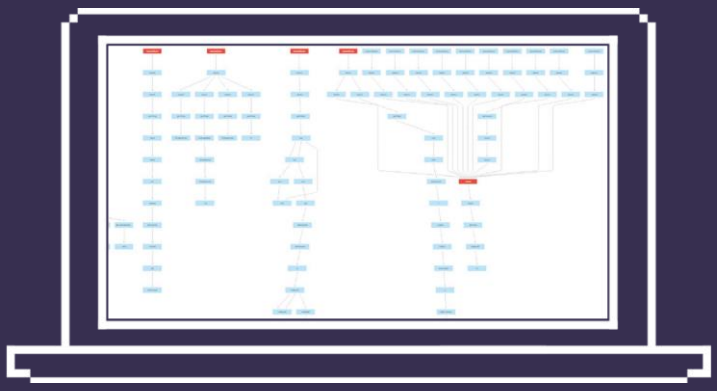


ГРАФИКИ & ОТЧЕТЫ

Анализировать данные и создавать отчеты с Checkmarx очень просто. Есть возможность использовать предустановленные шаблоны отчетов или изменять их, создавая свои с помощью интуитивно понятного интерфейса, просто перетаскивая нужные элементы на экране, указать желаемые параметры, по которым необходимо провести аналитику. Можно изменять и вид графиков отчетности. Все изменения вступают в силу в режиме реального времени и можно сразу выгрузить PDF или Excel файл.

ОПТИМИЗАЦИЯ ЗАТРАТ на устранение ошибок

Checkmarx – это нечто большее, чем просто выявление уязвимостей. В дополнение ко всему перечисленному ранее, Checkmarx использует методику графов – алгоритм, который позволяет консолидировать векторы атак и показать конкретные точки, в которых они сходятся, это и будет самой удобной точкой для исправления сразу нескольких векторов атак!
Данная диаграмма позволяет разработчику сократить объем работ по исправлению, показывая минимальное количество мест для работы, при этом покрывая все имеющиеся уязвимости.



Atlassian

"Using Checkmarx is easier than other tools. Important - you do not need to integrate it into your build process, just throw source code at it. The team was extremely happy with the levels of support they received. It was both professional and timely despite the time zone differences."
Vitaly Osipov, Information Security Expert, Atlassian

playtech SOURCE OF SUCCESS

"Checkmarx is loved by both our InfoSec team and our developers. It is easy to use and provides highly accurate results combined with the flexibility we need to enforce our application security policy."
Kobi Lechner, Information Security Manager, Playtech

LIVEPERSON

"Checkmarx's technology is highly accurate and easy to use. It offers great performance and the ability to scan incomplete code samples. Checkmarx was agile enough to support special requests we had for our secure SDLC and was the most sensible decision commercially."
Security Specialist, LivePerson

salesforce

Salesforce.com selected Checkmarx's Static Code Analysis tool as the official Force.com Security Code Scanner. With over 2.5 billion LoC scanned to date and 2 million vulnerabilities detected, Checkmarx ensures all AppExchange applications are secured to the highest standards.

info@iitdgroup.ru | www.iitdgroup.ru| www.checkmarx.com