Анализ состава программного обеспечения (SCA): все, что вам нужно знать в 2024 году

Описание

Анализ состава программного обеспечения (SCA) – это техника, которую современные ИТ-команды могут использовать для поиска всех компонентов с открытым исходным кодом и управления ими. Предприятиям необходимо знать все об используемом приложении и его составе, чтобы решить, безопасно ли оно и соответствует ли нормативным требованиям. Если вы используете приложение со взломанным или уязвимым компонентом с открытым исходным кодом, оно всегда подвержено риску эксплуатации злоумышленниками. И когда это произойдет, вы можете потерять все конфиденциальные данные о вашем бизнесе и клиентах, хранящиеся в приложении. Это может привести к потере доверия клиентов, утечке деловой информации, финансовым рискам и штрафам, связанным с соблюдением нормативных требований. Поэтому вы должны знать, что вы используете, а также все лицензионные обязательства и ограничения приложения с открытым исходным кодом. Однако делать все это вручную – довольно сложная задача. В большинстве случаев код и его уязвимости могут быть пропущены, если вы пойдете таким путем. Инструменты SCA упрощают и облегчают этот процесс, автоматически анализируя компоненты с открытым исходным кодом. В этой статье я расскажу все о SCA и о том, почему он важен для безопасности приложений. Следите за новостями!

Что такое анализ состава программного обеспечения (SCA)?

Анализ состава программного обеспечения (SCA) – это процесс, который позволяет обнаружить компоненты с открытым исходным кодом, используемые в кодовой базе приложения. Этот автоматизированный процесс является частью тестирования безопасности приложений, которое оценивает безопасность приложения, качество кода и соответствие требованиям. На рынке представлено множество инструментов SCA, способных выполнить этот процесс. Эти инструменты помогут вам обнаружить и управлять компонентами с открытым исходным кодом, их косвенными и прямыми зависимостями, вспомогательными библиотеками, устаревшими зависимостями, потенциальными эксплойтами и уязвимостями.

Сканирование приложения с помощью SCA-инструмента позволит создать полный перечень материалов, в котором будут указаны все активы приложения. Это поможет вам лучше понять, что было сделано при создании приложения и безопасно ли оно для использования. Тем не менее, концепция SCA не совсем нова. С ростом популярности инструментов с открытым исходным кодом, в первую очередь благодаря доступности и экономичности, SCA стал необходимым процессом для программ безопасности приложений. Решение SCA предоставляет разработчикам более совершенные средства разработки и направляет их на обеспечение безопасности на протяжении всего жизненного цикла разработки приложений.

Как работает SCA?

Чтобы выполнить SCA с помощью решения SCA, вы должны направить его на файлы

сборки вашего приложения. Эти файлы можно найти на сервере сборки, рабочем столе разработчика или в каталоге сборки CI/CD-конвейера. Инструменты SCA сканируют кодовую базу приложения, чтобы распознать файлы, которые могут быть получены из стороннего продукта. Инструменты могут использовать различные тактики идентификации, например уникальный предварительно вычисленный список хэшей файлов известного приложения. Итак, когда инструмент SCA запускается, он вычисляет хэши файлов в вашем приложении и сопоставляет их со списком. Если хэши совпадают, инструмент SCA найдет продукт и его версию, которую вы используете, и разберет исходный код, чтобы обнаружить фрагменты проприетарного кода, используемые в вашем коде. Инструменты SCA также поддерживают и обновляют свой список уязвимостей, чтобы вы могли использовать его для поиска проблем в вашем приложении спустя годы после выпуска. Они могут проверять открытый код, менеджеры пакетов, бинарные файлы, файлы манифеста, образы контейнеров и т. д. После выявления компонентов с открытым исходным кодом инструмент соберет их в спецификацию материалов (BOM) и сравнит ее с различными базами данных, которые могут быть коммерческими или государственными, например с Национальной базой данных уязвимостей (NVD), содержащей данные о распространенных и известных уязвимостях в программном обеспечении. Кроме того, инструмент SCA может дать различные результаты, такие как:

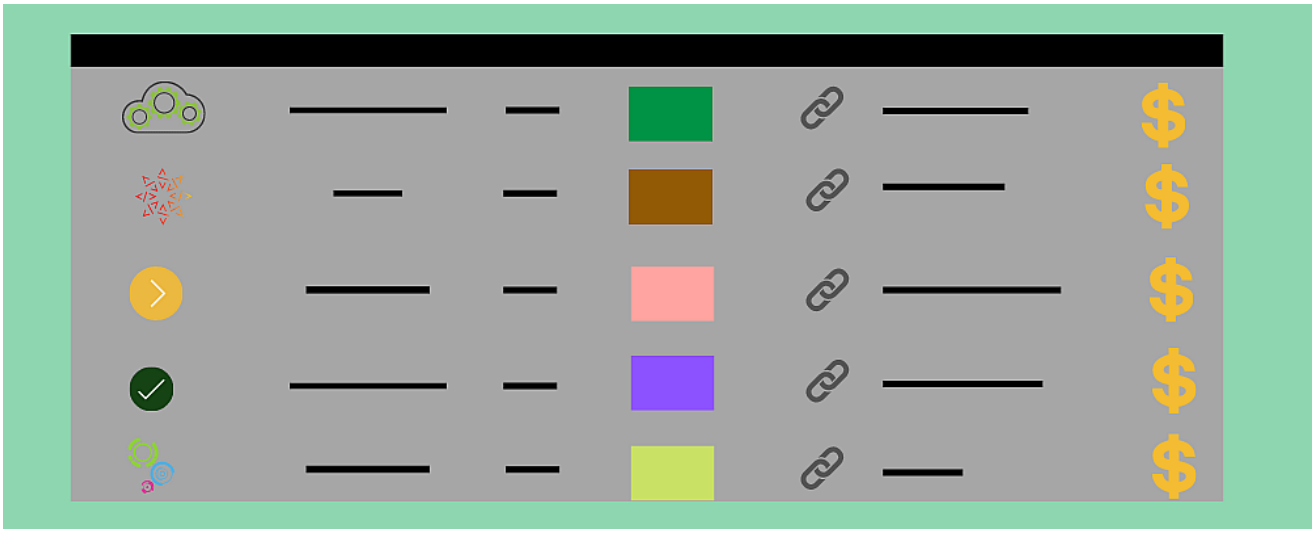
- **Список лицензий:** Это список лицензий, связанных с компонентами сторонних разработчиков, используемых в вашем приложении. Они могут иметь высокие ограничения и представлять риск для бизнеса, которого вы можете избежать, чтобы оставаться в безопасности.
- **Ведомость материалов (BOM):** Это перечень программных пакетов, созданных третьими сторонами для обеспечения безопасности и соответствия требованиям.
- **Известные уязвимости:** Это критические недостатки безопасности в компонентах сторонних приложений, позволяющие определить степень серьезности и тип уязвимости в файлах.

Таким образом, инструменты SCA могут обнаружить лицензии, проанализировать качество кода с помощью контроля версий, истории вкладов и т. д. Эта информация поможет разработчикам выявить потенциальные уязвимости в области безопасности и соответствия нормативным требованиям и быстро устранить проблемы.

Ключевые особенности SCA

Некоторые из ключевых особенностей SCA таковы:

Точная спецификация



Инструмент SCA точно создаст спецификацию материалов (BOM) для ваших приложений. В ней будут описаны компоненты приложения, используемые версии и тип лицензии. Цель BOM – помочь разработчикам и командам безопасности лучше понять компоненты приложений и оценить их лицензионность и безопасность. Таким образом, если инструмент обнаружит какие-либо уязвимости, они смогут быстро их устранить и защитить свое приложение и данные от злоумышленников.

Поиск и отслеживание компонентов

Отслеживать компоненты вручную очень сложно, а иногда и невозможно, поскольку предприятия работают с различными цепочками поставок, включая сторонних поставщиков, партнеров, проекты с открытым исходным кодом и т. д. Инструмент SCA найдет все компоненты с открытым исходным кодом приложения,

зависимости сборки, контейнеры, подкомпоненты, двоичные файлы и компоненты ОС.

Обеспечение соблюдения политик

Оценка соответствия лицензиям и безопасности полезна везде в организации, учитывая всех, от разработчиков до топ-менеджеров. SCA показывает необходимость создания политик безопасности, предоставления знаний об ОС и обучения членов вашей команды, а также быстрого реагирования на события безопасности и соблюдения лицензионных требований. Кроме того, с помощью инструментов SCA можно автоматизировать процессы утверждения, настраивать использование и выпускать нормы исправления.

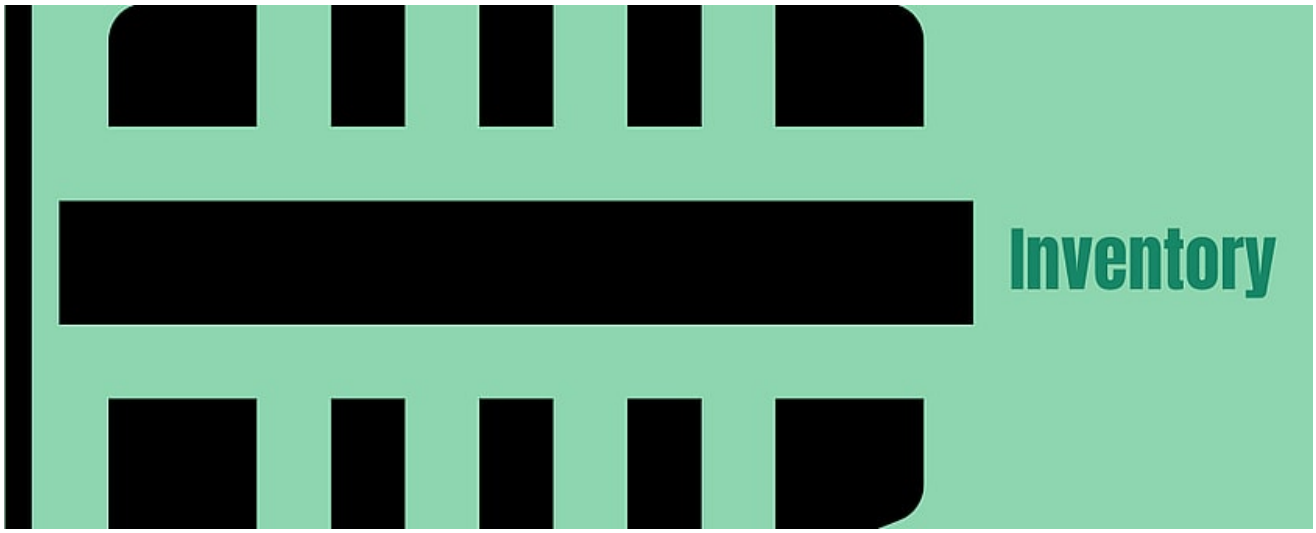
Непрерывный мониторинг

Если вы сможете эффективно управлять рабочими нагрузками, это поможет повысить производительность всей вашей команды. Используя SCA-инструмент, вы сможете добиться и того, и другого, поскольку он предлагает непрерывный мониторинг вашего приложения для обнаружения проблем и уязвимостей безопасности. Эти инструменты позволяют настраивать оперативные оповещения, чтобы вы могли получать немедленную информацию о новых обнаруженных уязвимостях в поставляемых и текущих продуктах.

Всеобъемлющая база данных

Каждое SCA-решение имеет базу данных, которую необходимо обогатить данными, собранными из нескольких источников. Чем полнее эта база данных, тем лучше инструмент SCA справляется с обнаружением компонентов с открытым исходным кодом и связанных с ними рисков. Но если вы не поддерживаете подробную базу данных, которая постоянно обновляется, то точное обнаружение компонентов и их нужных версий становится сложной задачей. В результате вам будет сложно обновлять лицензии, применять исправления и обновления, а также вовремя устранять проблемы безопасности.

Инвентаризация



Процесс SCA начинается со сканирования для создания реестра, содержащего все компоненты приложений с открытым исходным кодом, включая переходные и прямые зависимости. Подробный перечень компонентов вашего приложения позволит вам с легкостью управлять им и выполнять все процессы без путаницы, будь то контроль версий или внесение исправлений. Она также необходима для обеспечения соответствия каждого используемого компонента, что невозможно, если вы не знаете, какой компонент вы используете.

Обширная отчетность

Хороший инструмент SCA включает в себя широкий спектр отчетов для различных случаев использования, от инвентаризации и лицензирования до отслеживания ошибок и уязвимостей, а также комплексной проверки. Это облегчает получение информации на каждом этапе, чтобы вы могли принимать обоснованные решения. Они полезны для управления компонентами приложения, контроля версий, соблюдения требований и безопасности. Кроме того, они полезны для DevSecOps и DevOps.

Соблюдение лицензионных требований

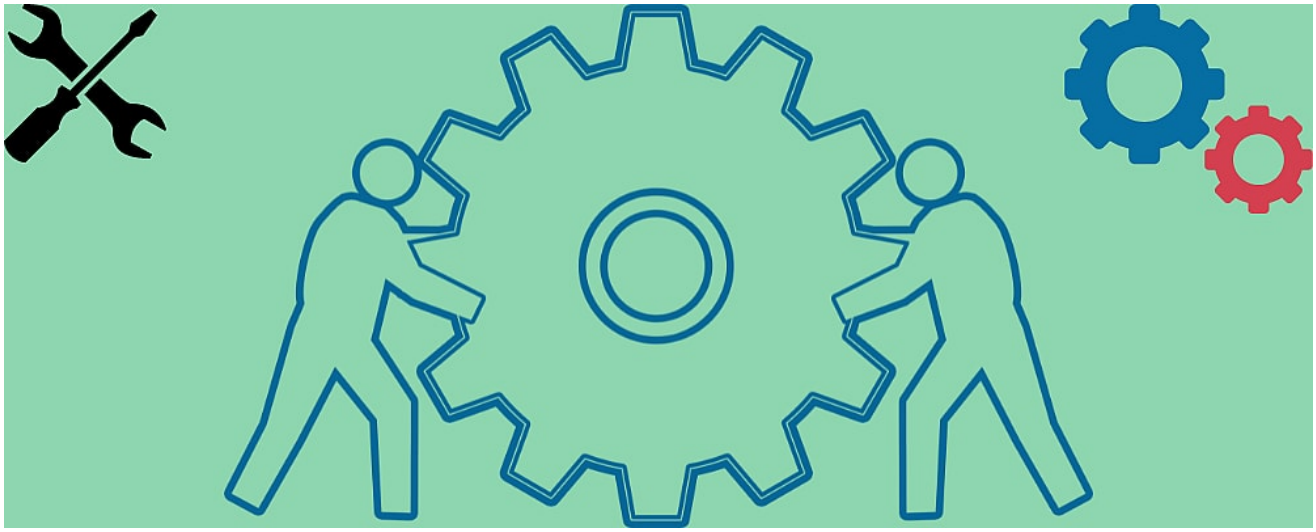
После идентификации всех компонентов с открытым исходным кодом в вашем приложении с помощью инструмента SCA он предоставит вам полную информацию о каждом компоненте. Она может включать данные о лицензии с открытым исходным кодом каждого компонента, совместимости лицензии с вашей бизнес-политикой и требованиях к авторству. Это необходимо для соблюдения

лицензионных требований и предотвращения использования компонентов, которые не соответствуют вашим политикам или представляют собой риски, связанные с соблюдением требований.

Поддержка нескольких языков

Решения SCA поддерживают множество языков и совместимы с широким спектром приложений и проектов.

Интеграция



Инструменты SCA легко интегрируются с различными средами сборки на разных этапах жизненного цикла разработки приложений. Они могут легко интегрироваться с вашими репозиториями, CI-серверами, менеджерами пакетов, IDE и инструментами сборки. В результате это дает разработчикам возможность выбрать наиболее подходящую среду сборки для вашего проекта и облегчает им процесс.

Преимущества SCA

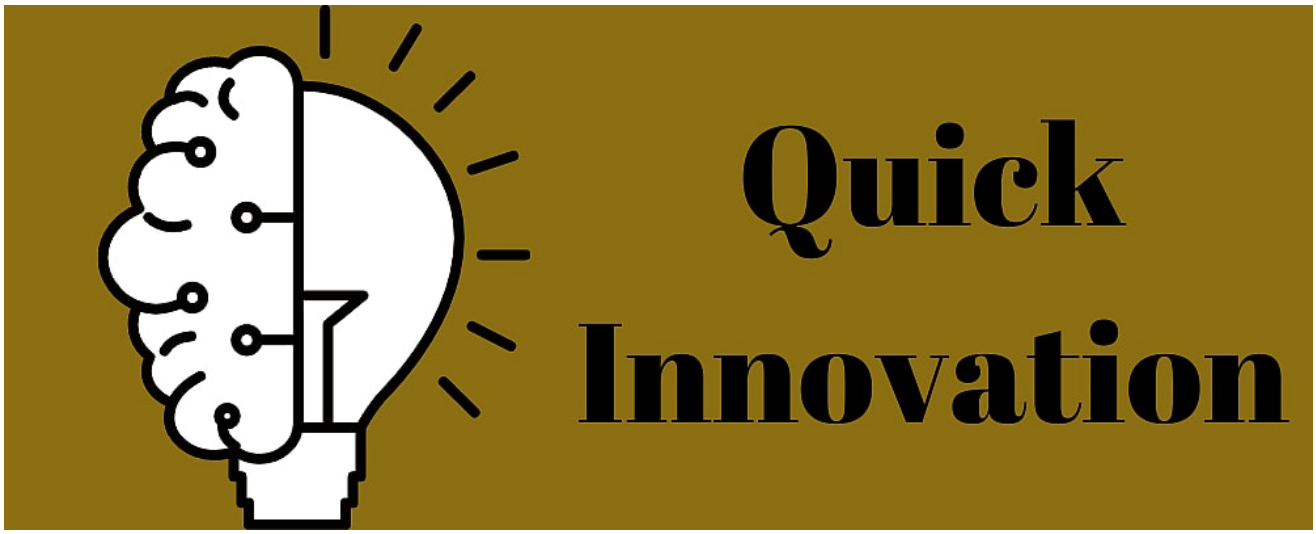
Организации, от небольших до крупных, разрабатывают приложения для решения различных задач. Но все не могут вкладывать столько средств в их разработку, особенно индивидуальные разработчики и малые предприятия. Таким образом, они могут использовать компоненты с открытым исходным кодом, которые можно свободно применять и изменять в соответствии с требованиями. Разработчики и команды используют все больше и больше компонентов с открытым исходным

кодом для создания своих приложений. Но не все из них безопасны. Здесь им на помощь приходят инструменты SCA, позволяющие найти все компоненты с открытым исходным кодом в вашем приложении и определить, насколько они безопасны и соответствуют требованиям безопасности. Это помогает быстрее находить проблемы с лицензированием и уязвимости, снижать затраты на исправление и выполнять автоматическое сканирование для обнаружения и устранения проблем безопасности с меньшими затратами человеческих усилий. Вот подробная информация о преимуществах:

Устранение рисков для бизнеса

Большинство компаний не знают всего обо всех компонентах, используемых в их приложениях. Возможно, компонент поставляется сторонним поставщиком или по другой причине. Но если вы не знаете, что входит в состав вашего приложения, всегда существует риск, связанный с количеством кибератак, происходящих каждый день. Выполняя анализ состава программного обеспечения (SCA), они могут понять все используемые компоненты с открытым исходным кодом. Таким образом, если возникнет какая-либо проблема, вы сможете быстро устранить ее с помощью правильной автоматизации и процессов и обезопасить себя от рисков, связанных с безопасностью и соблюдением лицензионных требований.

Инновации



Использование компонентов с открытым исходным кодом обеспечивает большую гибкость и свободу, а также экономит деньги и время. Таким образом, вы можете посвятить свое время инновациям, чтобы удовлетворить потребности рынка. SCA

позволяет сделать инновационные продукты более безопасными и совместимыми, обеспечивая эффективное управление лицензиями.

Приоритезация уязвимостей

Современные решения SCA сокращают разрыв между обнаружением проблем и их устранением. Хороший SCA-инструмент предлагает возможности для определения приоритетности уязвимостей в открытых источниках. Это возможно благодаря проактивному и автоматическому выявлению уязвимостей в системе безопасности. Получив эти данные, можно определить приоритетность проблемы, которую следует устранить в первую очередь, на основе отчета о степени серьезности. Это избавляет разработчиков и других специалистов по безопасности от необходимости тратить время на просмотр страниц с предупреждениями и попытки определить, какие уязвимости в приложении более серьезны и могут быть использованы.

Быстрое устранение уязвимостей

Помимо расстановки приоритетов, инструменты SCA помогают компаниям и частным лицам быстро устранить уязвимости в приложении. Они могут автоматически определять местоположение уязвимости и предлагать способы ее устранения. Он также предоставит вам информацию о том, как реализация исправления может повлиять на вашу сборку. Инструменты SCA могут запускать автоматический процесс устранения уязвимостей на основе степени тяжести уязвимости, обнаружения уязвимости, оценки степени тяжести, выпуска новой версии и политик уязвимостей, созданных на основе этих факторов. Этот инструмент также поможет вам поддерживать компоненты приложений с открытым исходным кодом в актуальном состоянии, что является отличной стратегией снижения рисков.

Ускоренный выход на рынок

В большинстве приложений сегодня используются компоненты с открытым исходным кодом, поскольку они экономически эффективны и легкодоступны. Это позволяет быстрее разрабатывать код и выводить приложение на рынок, чтобы удовлетворить запросы клиентов. А чтобы убедиться, что вы используете безопасный компонент с открытым исходным кодом, полезно использовать инструменты SCA. Это поможет убедиться, что ваши приложения соответствуют юридическим обязательствам и что вы устранили все уязвимости.

Кто и почему использует инструменты SCA?

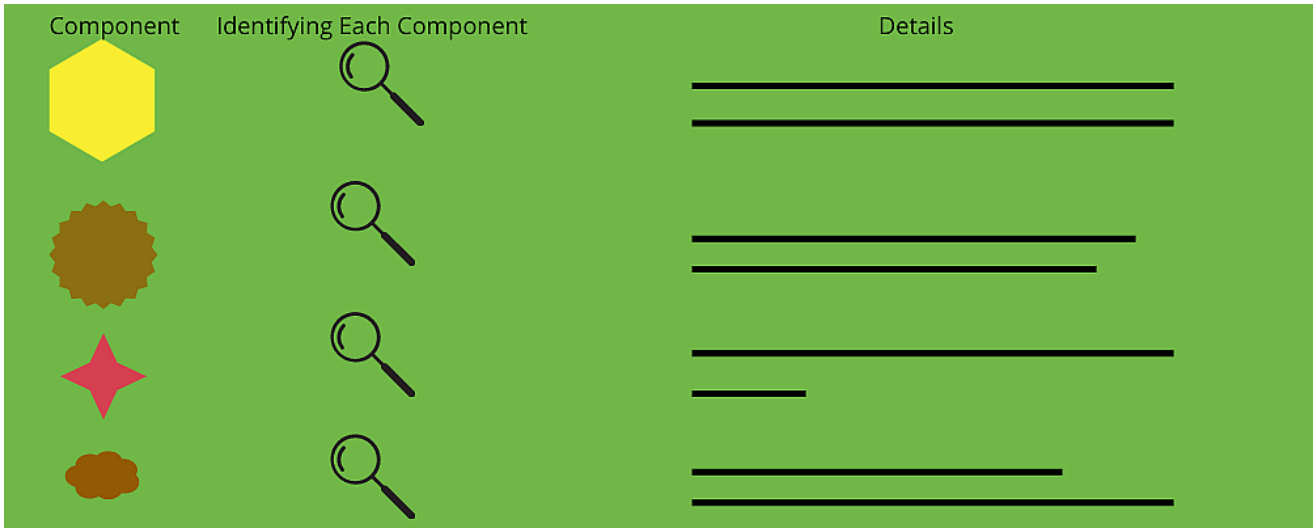
Предприятия различных отраслей используют те или иные виды программного обеспечения для ускорения работы персонала, обеспечения бесперебойной связи и повышения производительности. Поэтому повсеместно растет спрос на приложения, которые разработчики и предприятия стремятся реализовать. Чтобы удовлетворить этот огромный спрос, им требуются решения, способные ускорить их работу и обеспечить более быстрое развертывание услуг и продуктов. В то же время они должны обеспечить безопасность своих развертываний от киберзлоумышленников, распространенных в наши дни. Таким образом, инструменты SCA помогают компаниям и отдельным разработчикам находить компоненты с открытым исходным кодом, используемые в их приложениях, и обеспечивать их безопасность. Инструменты SCA используются командами разработчиков в различных отраслях и сферах, от ИТ, маркетинга и электронной коммерции до здравоохранения, финансов, EduTech и многих других. Кроме того, растет спрос на сложные и “облачные” приложения, что увеличивает потребность в надежных инструментах SCA. Они также помогают командам DevOps ускорить процессы разработки с упором на безопасность.

На что обратить внимание при выборе инструмента SCA?

Выбор лучшего инструмента SCA может оказаться непростой задачей, поскольку на рынке представлено множество вариантов. Поэтому необходимо учитывать ваши конкретные требования. Давайте рассмотрим некоторые ключевые факторы, которые необходимо учитывать при выборе инструмента SCA.

Удобен ли он для разработчиков?

Ваши разработчики будут заниматься созданием кода, основываясь на конечной цели, требованиях к дизайну и потребностях пользователей. Они должны быстро выполнять итерации, когда это необходимо, и создавать код лучшего качества. Если инструмент SCA не ориентирован на разработчиков, им будет сложнее принять его и потребуется больше времени, чтобы понять и использовать его, что снизит их производительность. Однако если вы предоставите им инструмент SCA, дружественный разработчикам, то есть простой в настройке и использовании, это повысит их производительность и сэкономит время и силы.



Как происходит обнаружение компонентов?

Хороший SCA-инструмент должен обладать обширной базой данных для выявления компонентов с открытым исходным кодом, используемых в приложении. Чем больше компонентов он сможет обнаружить, тем больше шансов обнаружить уязвимости и устранить их. Поэтому, прежде чем выбрать инструмент SCA, проверьте, насколько полно он обнаруживает компоненты, сравнив его с другими инструментами.

Как насчет выявления и устранения уязвимостей?

Выбранный вами инструмент SCA должен также обеспечивать комплексное обнаружение уязвимостей всех выявленных компонентов с открытым исходным кодом. Чем больше, тем лучше. Это позволит выявить большее количество проблем

в компонентах, которые вы сможете немедленно устранить и защитить свое приложение от эксплойтов. Также будет полезно, если инструмент предоставит рекомендации по устранению уязвимостей в системе безопасности.

Каково качество отчетности?

Поскольку отчетность является обязательной функцией инструмента SCA, вам необходимо сравнить возможности отчетности различных инструментов SCA, которые вы выбрали. Возможности создания отчетов могут отличаться в зависимости от инструмента. Для этого проверьте качество получаемых отчетов, насколько они подробны и понятны. Вы можете сделать это, попробовав БЕСПЛАТНУЮ пробную версию, предоставляемую большинством SCA-решений.

Сколько ложных срабатываний?

Инструменты SCA, как правило, не выдают больше ложных срабатываний, чем инструменты DAST. Однако вероятность этого все же существует. Поэтому выполнение пробной версии может помочь оценить соотношение сигнал/шум инструмента. Поэтому сравнивать инструменты SCA следует по среднему количеству ложных срабатываний.

Как насчет интеграций?

Выберите SCA-инструмент, который может легко интегрироваться с вашей текущей средой сборки, чтобы избавиться от проблем. Кроме того, он должен подключаться к другим инструментам и сервисам, таким как контейнеры, системы безопасности,

инструменты CI/CD, IDE, SCM и т. д., чтобы расширить функциональность вашего приложения.

Несколько хороших инструментов SCA

Вот некоторые из хороших инструментов SCA, которые вы можете рассмотреть для своих приложений:

Veracode: Veracode упрощает выполнение SCA. Вы можете начать работу в своей среде разработки, запустив сканирование из командной строки. Это обеспечит более быструю обратную связь в вашей IDE и конвейере. Этот инструмент позволит сократить время тестирования приложения на наличие компонентов с открытым исходным кодом. Он обладает функциями автоматического исправления, позволяющими создавать автоматические запросы на исправление, минимизировать сбои и рекомендовать интеллектуальные исправления для повышения скорости и точности исправления.

Revenera: Продукты Revenera для анализа состава программного обеспечения – от полных пакетов программ до фрагментов кода – проверяют исходный код, двоичные файлы и зависимости на наличие уязвимостей в программном обеспечении и проблем с соблюдением лицензионных требований. Кроме того, он интегрируется с распространенными инструментами сборки и предоставляет одну из крупнейших в отрасли баз знаний с открытым исходным кодом, насчитывающую более 14 миллионов компонентов. Их команды аудиторов также поддерживают базовые аудиты и мероприятия по комплексной проверке, такие как слияния и поглощения.

Другие известные инструменты SCA – Black Duck, Snyk, Checkmarx и другие.

Некоторые лучшие практики SCA

Даже если вы используете высококлассный инструмент SCA, вы не сможете достичь высокого уровня безопасности и удовлетворенности. Причина кроется в том, как вы его используете.

Вот некоторые из лучших практик, которым вы можете следовать, чтобы добиться успеха с помощью инструмента SCA:

- **Быстрое внедрение**: Внедрите инструмент SCA на ранней стадии жизненного цикла разработки программного обеспечения. Кроме того, ознакомьте свою команду с рисками безопасности и их последствиями, чтобы мотивировать их на принятие ответственных и взвешенных решений.
- **Юридическое руководство**: Проконсультируйтесь с юристом, чтобы определить, какие лицензии с открытым исходным кодом в вашем приложении слабее или неприемлемы в соответствии с политикой вашего бизнеса. Будьте быстры в исполнении этих решений.
- **Автоматизируйте сканирование**: Необходимо автоматизировать сканирование с помощью инструмента SCA в конвейере CI/CD. Устраняйте уязвимости в зависимости от степени их серьезности, начиная с уязвимостей с наивысшим риском. После их устранения вы можете заблокировать сборки со средними по серьезности уязвимостями.
- **Постоянные обновления**: Убедитесь, что используемый вами инструмент SCA регулярно обновляет данные об уязвимостях и возможности обнаружения компонентов. Таким образом, он сможет обнаружить больше компонентов и проблем, лежащих в их основе, которые вы сможете устранить и сделать приложение более безопасным.
- **Выбирайте компоненты сторонних разработчиков с умом**: Прежде чем добавлять компоненты с открытым исходным кодом от сторонних разработчиков в свое приложение, необходимо грамотно подойти к их выбору. Проверьте их на надежность, частоту обновлений, количество исправлений и историю уязвимостей.
- **Не используйте устаревшие компоненты**: Вы должны заменять компоненты, которые их производитель больше не поддерживает. Если вы используете компоненты, которые никогда не обновляются, это создает угрозу безопасности.

Заключение

Анализ состава программного обеспечения (SCA) помогает повысить уровень безопасности и соответствия приложений требованиям, обнаруживая уязвимые компоненты с открытым исходным кодом и позволяя вовремя их исправить. Это защитит ваши приложения и данные от кибератак. Это также помогает сократить расходы, повышает гибкость бизнеса и позволяет разработчикам узнать, как обеспечить безопасность приложений на этапе планирования и проектирования. Достичь всего этого можно, внедрив лучший инструмент SCA в соответствии с

потребностями вашего бизнеса. Вы также можете следовать некоторым лучшим практикам, чтобы добиться большего успеха в своей деятельности в области SCA.

Дата Создания
05.03.2024