DerScanner

DerScanner Software Composition Analysis
Анализ компонентов и сторонних библиотек

В современных условиях как никогда важно обеспечить безопасность и прозрачность программного обеспечения. По всему миру регулирующие органы требуют более глубокого понимания спецификаций программного обеспечения (SBOM), чтобы обезопасить программное обеспечение от рисков, связанных с открытым исходным кодом, на протяжении всего жизненного цикла. Эти нормы обязывают производителей документировать и сообщать о компонентах и уязвимостях программного обеспечения, повышая ответственность и прозрачность для потребителей.

Постановление Правления Национального Банка № 48 обязывает тестировать приложения с применением анализа компонентов и (или) сторонних библиотек (SCA)

Исполнительный указ 14028 о повышении кибербезопасности страны требует наличия SBOM для всего программного обеспечения, продаваемого федеральным агентствам.

Закон ЕС о киберустойчивости (CRA) требует использования SBOM для повышения безопасности программного обеспечения.

Закон Германии об информационной безопасности 2.0 (IT-SiG 2.0) включает требования к использованию SBOM для обеспечения безопасности и прозрачности программного обеспечения.

В японском документе Cybersecurity Framework, разработанном под руководством Агентства по развитию информационных технологий (IPA), особое внимание уделяется прозрачности компонентов программного обеспечения.

В Стратегии кибербезопасности Австралии до 2020 года подчеркивается важность защиты цепочки поставок программного обеспечения.

Получите глубокое представление о SBOM и защитите свою кодовую базу от рисков, связанных с открытым исходным кодом, с помощью DerScanner Software Composition Analysis. DerScanner позволяет специалистам по кибербезопасности и разработчикам проактивно выявлять и устранять уязвимости в компонентах сторонних разработчиков. Не ограничиваясь базовым сканированием уязвимостей, он оценивает соответствие лицензиям и выдает оценку состояния каждого пакета с открытым исходным кодом на основе данных. Это позволяет принимать взвешенные решения, определять приоритеты действий по исправлению ситуации и избегать потенциальных юридических последствий. С помощью DerScanner SCA вы можете с уверенностью создавать безопасное, соответствующее требованиям программное обеспечение, сводя к минимуму риск использования уязвимостей "нулевого дня" и атак на цепочки поставок.

FORRESTER®

DerSecur вошла в число заметных поставщиков в аналитическом обзоре The Software Composition Analysis Landscape Q2 2024

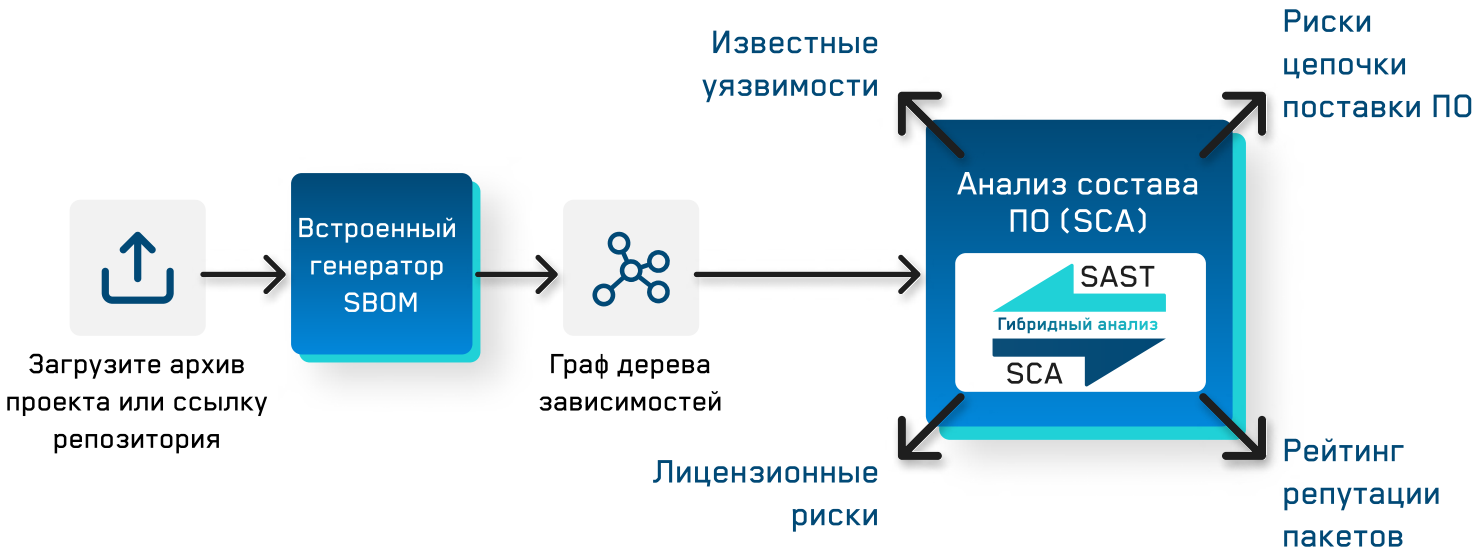
Оптимизация управления SBOM с помощью DerScanner

Упростите процесс создания SBOM

Управление спецификацией программного обеспечения (SBOM) может быть сложной и трудоемкой задачей. Традиционные внешние генераторы SBOM часто требуют сложной конфигурации и настройки, что приводит к разочарованию и задержкам в обеспечении безопасности ваших проектов с применением Open Source.

Лёгкая генерация SBOM

С DerScanner вам больше не нужно работать с внешними инструментами для создания SBOM. Наш встроенный генератор SBOM упрощает этот процесс, позволяя вам без труда создавать подробные SBOM. Просто загрузите свой проект в DerScanner, и наш инструмент автоматически сгенерирует SBOM, готовый для всестороннего анализа состава программного обеспечения (SCA).



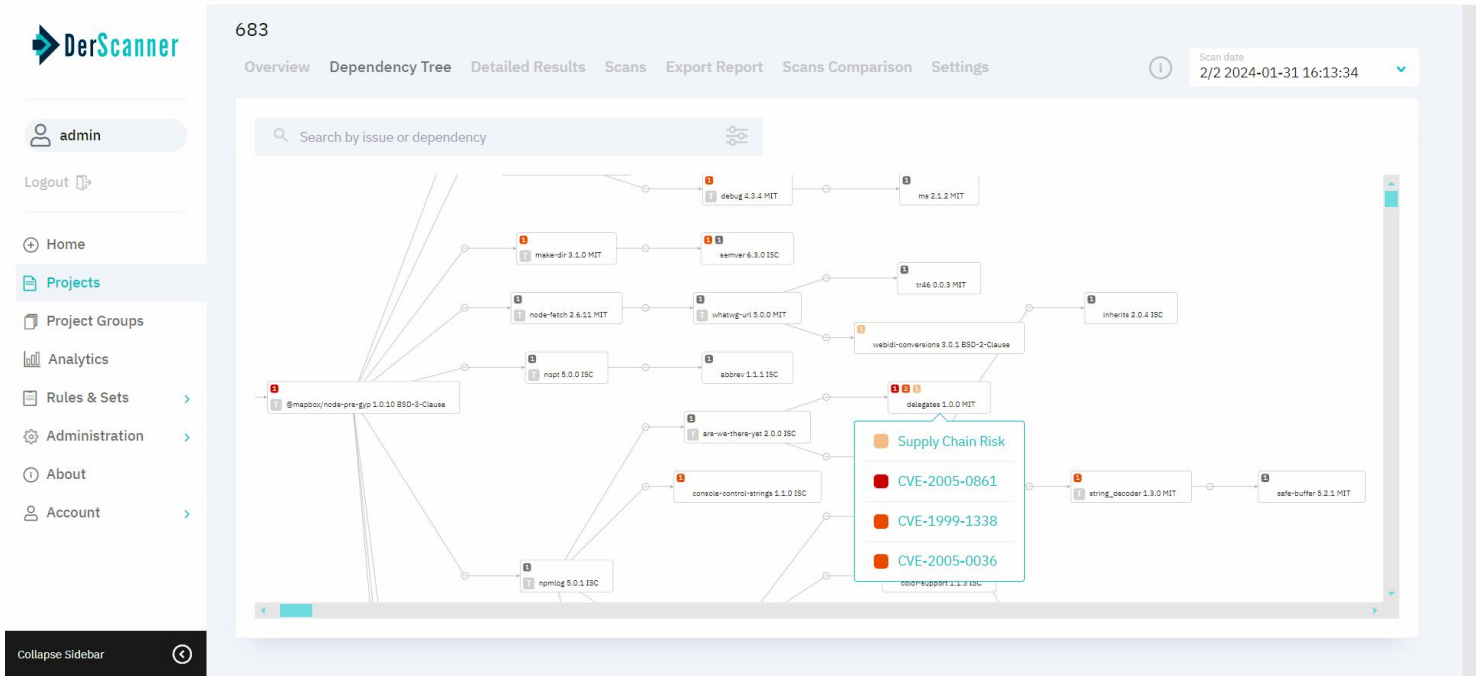
Визуализация и управление зависимостями с помощью графика дерева зависимостей DerScanner

Комплексная визуализация зависимостей для повышения безопасности

Управление сложными зависимостями проекта может оказаться непростой задачей. Проекты часто включают в себя глубокие структуры прямых и транзитивных зависимостей, что затрудняет понимание всего масштаба и выявление скрытых уязвимостей.

Ясность через визуализацию

Граф дерева зависимостей DerScanner упрощает управление зависимостями проекта. Он визуализирует всю структуру проекта, позволяя вам увидеть, где именно находятся уязвимые пакеты. Благодаря такому наглядному представлению вы сможете быстро и эффективно выявлять и устранять риски безопасности.



Взгляните внутрь состава открытого ПО для предотвращения известных уязвимостей

DerScanner SCA поддерживает обширные базы данных известных уязвимостей в программном обеспечении с открытым исходным кодом, взятые из различных рекомендаций по безопасности и баз данных. Путем перекрестного сопоставления SBOM с базой данных уязвимостей DerScanner SCA выявляет уязвимости, которые непосредственно влияют на ваше приложение. Он даже может выявить уязвимости, скрытые в глубине дерева зависимостей.

Ценность видимости открытого исходного кода

Проактивная безопасность: Обнаруживая уязвимости до того, как они будут использованы, вы можете поставить заплатку или обновить уязвимые компоненты, снизив риск нарушения безопасности.

Соответствие требованиям: Многие отрасли и нормативные акты, такие как Постановление Правления Национального Банка Казахстана № 48, требуют отслеживать и управлять использованием открытых исходных кодов и уязвимостями. SCA помогает обеспечить соответствие таким требованиям.

Принятие взвешенных решений: Понимание того, как вы используете открытый исходный код, помогает вам принимать взвешенные решения о том, какие компоненты использовать и в какой последовательности обновлять.

Сокращение затрат на устранение уязвимостей: Устранение уязвимостей на ранних этапах разработки гораздо менее затратно, чем их устранение после взлома.

Проверяйте “репутацию” пакетов для предотвращения рисков в цепочке поставки ПО

Скоринг репутации открытого исходного кода в DerScanner - это метрика, оценивающая общее благополучие и уровень безопасности проекта с открытым исходным кодом. Она объединяет различные факторы в единый балл, облегчая оценку потенциальных рисков и преимуществ использования конкретного пакета.

Как скоринг репутации с открытым исходным кодом помогает избежать уязвимостей Zero-Day

Раннее предупреждение: Учитывая оценку состояния пакета, вы можете избегать проектов с историей уязвимостей или плохими практиками безопасности. Это снижает риск внедрения известных уязвимостей или неосознанного использования пакетов, которые могут быть подвержены будущим эксплойтам нулевого дня.

Сокращение поверхности атаки: Ограничение использования рискованных пакетов минимизирует потенциальную поверхность атаки для уязвимостей нулевого дня.

Проактивный выбор: Выбор пакетов с высокими показателями репутации означает, что вы с большей вероятностью выберете хорошо обслуживаемые и безопасные компоненты.

Более быстрая реакция: Если уязвимость обнаруживается в хорошо поддерживаемом проекте, сообщество и сопровождающие, скорее всего, быстро отреагируют на это исправлениями и обновлениями, снижая риск атак "нулевого дня".

Гибридный анализ SCA+SAST

Точная оценка уязвимостей в проектах с открытым исходным кодом

Понимание истинного риска уязвимостей в зависимостях имеет решающее значение. Простое обнаружение CVE в зависимости не обязательно означает, что весь пакет находится под угрозой. Важно точно определить, какие вызовы методов могут привести к эксплуатации уязвимости.

Комплексный гибридный анализ

Гибридный анализ DerScanner SCA+SAST сочетает в себе сильные стороны анализа состава программного обеспечения (SCA) и статического тестирования безопасности приложений (SAST) для точной оценки безопасности вашего приложения. Благодаря этому передовому гибридному подходу вы точно знаете, какие пакеты содержат CVE, к которым можно обратиться и которые можно эксплуатировать

Не позволяйте лицензиям открытого исходного кода привести к юридическим последствиям

DerScanner SCA определяет лицензии, связанные с каждым идентифицированным компонентом с открытым исходным кодом. Это очень важно, поскольку лицензии на открытый исходный код имеют различные условия использования, модификации, распространения и атрибуции.

> *"Обеспечение соответствия лицензиям с открытым исходным кодом было сложной задачей, пока мы не начали использовать DerScanner. Их решение упростило этот процесс, позволив нам сосредоточиться на инновациях без постоянного беспокойства о юридических проблемах".*
>
> **Александр Слободчиков, генеральный директор, CT Mobility Solutions**

DerScanner SCA оценивает, соответствует ли использование каждого компонента с открытым исходным кодом условиям лицензии. Это включает в себя:

Проверка наличия обязательств по авторскому праву

Некоторые лицензии, например GPL, содержат положения об "авторском леве", которые требуют, чтобы вы выпускали свои программы под той же лицензией, если вы распространяете измененную версию. DerScanner SCA отмечает эти компоненты и обеспечивает их соответствие.

Определение ограничений

Некоторые лицензии могут ограничивать коммерческое использование или требовать указания авторства. DerScanner SCA подчеркивает эти ограничения и помогает вам избежать юридических проблем.

Мониторинг зависимостей

DerScanner SCA отслеживает зависимости ваших компонентов с открытым исходным кодом, поскольку они также могут иметь лицензионные обязательства, которые необходимо соблюдать.

Сокращение числа ложных срабатываний в проектах по безопасности с открытым исходным кодом с помощью Confi AI

Точность и эффективность в управлении зависимостями с открытым исходным кодом

Управление безопасностью открытого кода может оказаться непосильной задачей, особенно если речь идет о большом количестве зависимостей. Ложные срабатывания в проектах SCA (анализ состава программного обеспечения) не только тратят драгоценное время, но и отвлекают внимание от настоящих уязвимостей, требующих немедленных действий.

Confi AI для точного управления уязвимостями

Включив Confi AI в своих проектах SCA, вы сможете использовать комплексный механизм, основанный на искусственном интеллекте и предназначенный для минимизации ложных срабатываний. Обученный на основе системы Exploit Prediction Scoring System (EPSS), а также результатов SAST и SCA в DerScanner, Confi AI помогает сосредоточиться на уязвимостях, которые действительно важны.

Предотвращение угроз MavenGate с помощью обнаружения просроченных доменов

Защитите свои приложения от атак на цепочки поставок

Домены с истекшим сроком действия представляют собой серьезную угрозу безопасности при атаках на MavenGate. Когда срок действия домена, связанного с легитимным пакетом Maven или разработчиком, истекает, злоумышленники могут перерегистрировать его и получить контроль. Этот перерегистрированный домен, ранее указанный в метаданных пакета, профилях разработчиков или в качестве URL репозитория в файлах Maven POM, затем используется для загрузки вредоносных пакетов. Разработчики и системы CI/CD, все еще доверяя теперь уже вредоносному домену, неосознанно интегрируют эти вредоносные пакеты в свои проекты. После включения вредоносный код запускается на выполнение, что приводит к потенциальной утечке данных, компрометации системы и другим вредоносным действиям. Эта угроза в первую очередь затрагивает проекты, использующие Java, но также распространяется и на другие языки JVM, такие как Kotlin, Scala, Groovy и Clojure, все из которых полагаются на Maven для управления зависимостями.

Как DerScanner защищает от атак MavenGate

Постоянно отслеживая и анализируя состояние доменов, DerScanner гарантирует, что вы будете предупреждены о любых зависимостях, связанных с просроченными или устаревшими доменами, которые могут быть использованы злоумышленниками.

Почему стоит выбрать DerScanner SCA?

DerScanner SCA обеспечивает непревзойденную точность и действенные подходы для обеспечения безопасности в проектах с открытым исходным кодом. Используя именование пакетов PURL вместо CPE, мы минимизируем ошибки и обеспечиваем точную идентификацию уязвимостей. Наше уникальное сочетание баз данных GitHub Advisory, GitLab Advisory, Google OSV Database, EPSS и NIST NVD обеспечивает наиболее полный охват уязвимостей с наименьшим количеством ложных срабатываний, позволяя вам принимать обоснованные решения и эффективно устранять риски.

DerScanner Hoy-xay +

Github Advisory

GitLab Advisory

Google OSV Database

EPSS (Exploit Prediction Scoring System

NVD

О компании DerSecur

Компания DerSecur, основанная в 2011 году, занимает передовые позиции в области безопасности приложений. Команда из 70 экспертов разработала DerScanner - универсальное решение для защиты приложений, которое поддерживает 43 языка программирования и обеспечивает статический, динамический и анализ состава программного обеспечения. DerSecur стремится развивать исследования и разработки в области кибербезопасности, обеспечивая более безопасное цифровое будущее.

https://derscanner.com/