DerScanner

Комплексное устранение известных и неизвестных
уязвимостей приложений на протяжении всего цикла разработки

DerSecur

Цифровая трансформация сделала разработку приложений в 10 раз более гибкой

Частые изменения и быстрый темп

Agile-разработка ориентирована на быстрые итерации и частые изменения в коде. Такая динамичная среда может привести к тому, что что в спешке безопасность отодвигается на второй план.

Отсутствие комплексного планирования

В Agile-методологиях часто отсутствует долгосрочное планирование, характерное для традиционных моделей разработки. Это может привести к тому, что соображения безопасности окажутся не в приоритете и не будут интегрированы в первоначальный проект.

Интеграция сторонних компонентов

Agile-разработка часто предполагает быструю интеграцию множества сторонних компонентов. Эти компоненты могут создавать уязвимости, если их не проверять и не обновлять должным образом.

DerSecur

Безопасность едва ли успевает за быстрыми темпами разработчиков

Безопасность

Разработчики

DerSecur

Из-за сжатых сроков разработчики предпочитают легкие пути

Жестко закодированные секреты

Встраивание паролей, ключей API или ключей шифрования непосредственно в исходный код, которые могут быть легко извлечены злоумышленниками.

Небезопасное хранение и передача данных

Игнорирование необходимости шифрования конфиденциальных данных как в состоянии покоя, так и при транспортировке.

Бэкдоры

Реализация в коде скрытых точек входа для облегчения доступа или отладки, которые могут быть использованы злоумышленниками.

Недостаточная валидация ввода

Отсутствие проверки вводимых пользователем данных может привести к таким уязвимостям, как SQL-инъекции, межсайтовый скриптинг (XSS) и переполнение буфера.

Непроверенные сторонние или open source компоненты

Встраивание пакетов, загруженных из Интернета, без предварительной проверки безопасности, что может привести к появлению уязвимостей или вредоносного кода в приложении.

DerSecur

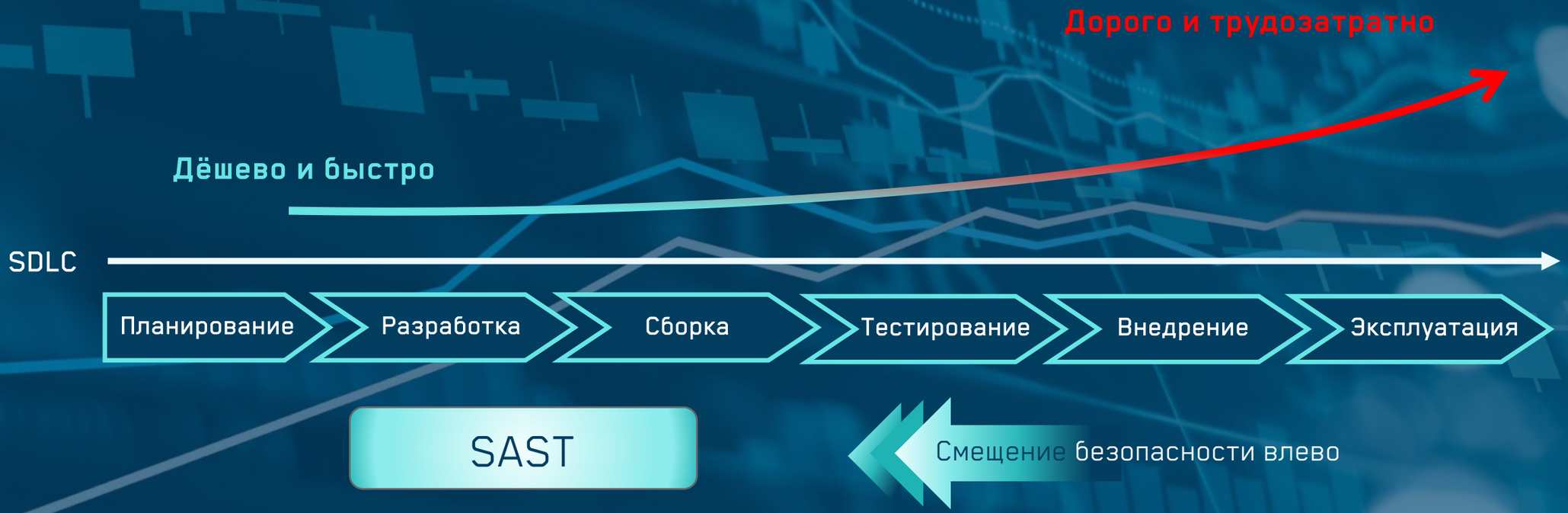
Вам неизбежно придется все это исправлять.

Вопрос только в том, что лучше - начать устранять последствия после утечки данных или до нее.

DerSecur

DerSecur

Стоимость устранения уязвимости приложения



DerSecur

Начните с раннего обнаружения известных уязвимостей

Смещайте безопасность влево (Shift Left), внедрив статический анализ (SAST) на ранних этапах.
Сканируйте исходный код приложения, чтобы выявить шаблоны, соответствующие известным уязвимостям.

- ✓ Жестко закодированные секреты
- ✓ Бэкдоры
- ✓ SQL-инъекции
- ✓ Межсайтовый скриптинг (XSS)
- ✓ Переполнение буфера
- ✓ и т.д.

DerSecur

Единое решение для 43 популярных языков программирования

Java, JSP, JS, TS, PASCAL, T-SQL, salesforce APEX, SAP ABAP, BASH THE BOURNE-AGAIN SHELL

python, GO, HTML, php, Visual Basic, SOLIDITY, xml

Visual Basic, VB, Microsoft VBScript, Delphi, ORACLE PL SQL, IBM Notes and Domino, [T]

1С, Microsoft Visual Basic for Applications, Dart, COBOL, YAML

LotusScript, Scala, Kotlin, ASP.NET, android, Perl

Swift, RUBY, Objective-C, SQL, Groovy, TSX

Исходный код можно анализировать из загруженных файлов или непосредственно из репозитория.

Интегрируйте проверку безопасности в жизненный цикл разработки программного обеспечения

Интеграция DerScanner с основными инструментами разработчика позволяет выполнять проверку исходного кода на ранних этапах работы.

Репозитории

git

SUBVERSION

VCS хостинги

GitHub

GitLab

Bitbucket

Среды разработки

eclipse

Visual Studio

IJ

IDE

RAD

Скоро!

Xcode

GNU (Autotools, Make)

sbt

Maven

CMake

Gradle

Visual Studio

CI/CD сервера

Jenkins

TeamCity

Azure DevOps Server

Отслеживание ошибок

Atlassian JIRA

Анализ кода

sonarqube

Open API (включая JSON API и CLI) обеспечивает мощную интеграцию и возможности автоматизации

DerSecur

Избавление от ложных срабатываний

Мы знаем, как может обескуражить получение отчета с тысячами уязвимостей.

Трудно сосредоточиться и понять реальный риск.

Наша собственная технология Confi AI поможет вам определить приоритеты и снизить уровень шума от ложных срабатываний, чтобы вы могли сосредоточиться на важной информации.

DerSecur

Сканирование бинарных файлов, когда исходный код недоступен

Устаревшие приложения

Устраняйте уязвимости, когда исходный код может быть утерян, устарел или плохо документирован

Соответствие нормативным требованиям и аудит

Убедитесь, что приложение соответствует нормам безопасности в отраслях с жестким регулированием

Выявление экзотических уязвимостей

Выявляйте опасные уязвимости, которые не могут быть обнаружены при анализе исходного кода

DerSecur

Раскройте невидимое, защитите неизведанное

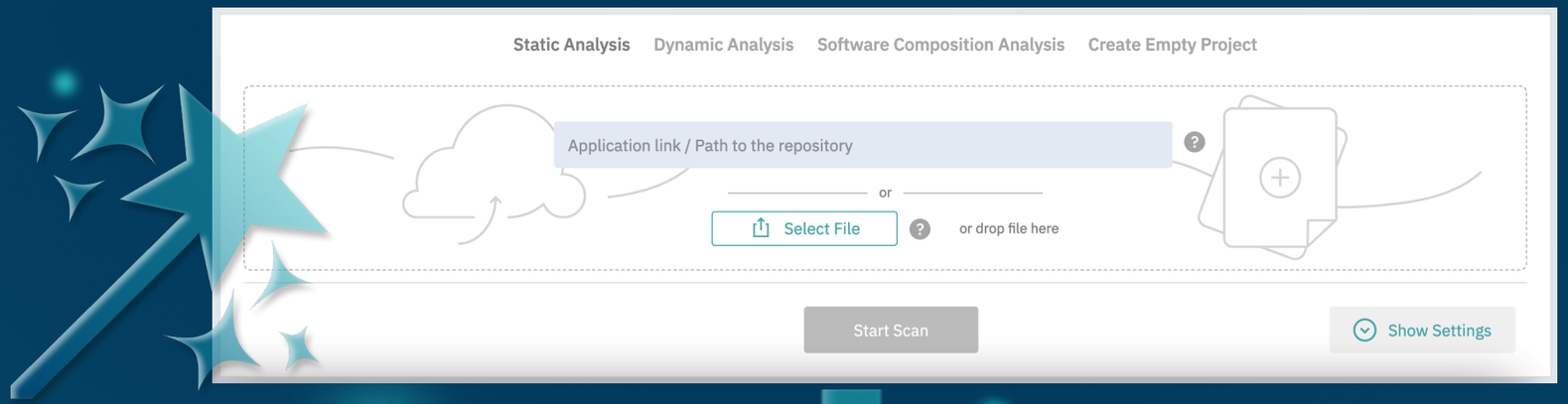
1. Загрузите свое приложение в любом доступном формате

EXE DLL JAR WAR APK IPA APP EAR AAR AAB

https://play.google.com/store/apps/AppName

https://apps.apple.com/en/app/AppName

2. Наука и Магия



3. Получите результаты оценки безопасности

DerSecur

Тестируйте веб-приложения извне

DAST имитирует действия внешнего атакующего, как при тестировании на проникновение, чтобы обнаружить уязвимости, которые могут эксплуатироваться после запуска приложения.

DerSecur

Тестируйте веб-приложения извне - IAST

Интерактивный анализ IAST (Interactive Application Security Testing) объединяет усилия SAST и DAST и находя уязвимости, которые SAST может пропустить, особенно те, которые связаны со средой выполнения и взаимодействием с пользователем

DerSecur

Тестируйте веб-приложения извне – чёрный ящик

Как метод тестирования “черного ящика”, DAST не требует доступа к исходному коду, что делает его идеальным для тестирования веб-приложений.

DerSecur

Пройдите оценку соответствия с легкостью

В зависимости от вашей отрасли, различные нормативные стандарты требуют тестирования безопасности рабочих приложений.

Получите отчет об уязвимостях, чтобы убедиться, что ваш код соответствует специальным стандартам:

- PCI DSS
- OWASP
- HIPAA
- CWE/SANS Top 25

PCI Security Standards Council

HIPAA COMPLIANCE

OWASP

SANS CWE

DerSecur

Требования к SBOM в мире

Регулирующие органы требуют более глубокого понимания спецификаций программного обеспечения (SBOM) для защиты ПО от рисков, связанных с открытым исходным кодом

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.

Вы не можете запретить разработчикам использовать компоненты сторонних производителей

Но вы все равно можете предотвратить риски, связанные с открытым исходным кодом

Видимость открытого исходного кода

Получите доступ к компонентам с открытым исходным кодом и зависимостям, чтобы обнаружить известные уязвимости до того, как они смогут быть использованы против вас.

Соответствие лицензиям

Убедитесь, что лицензии на используемые компоненты с открытым исходным кодом совместимы с условиями лицензирования проекта, чтобы избежать юридических проблем.

Software Composition Analysis (SCA) для

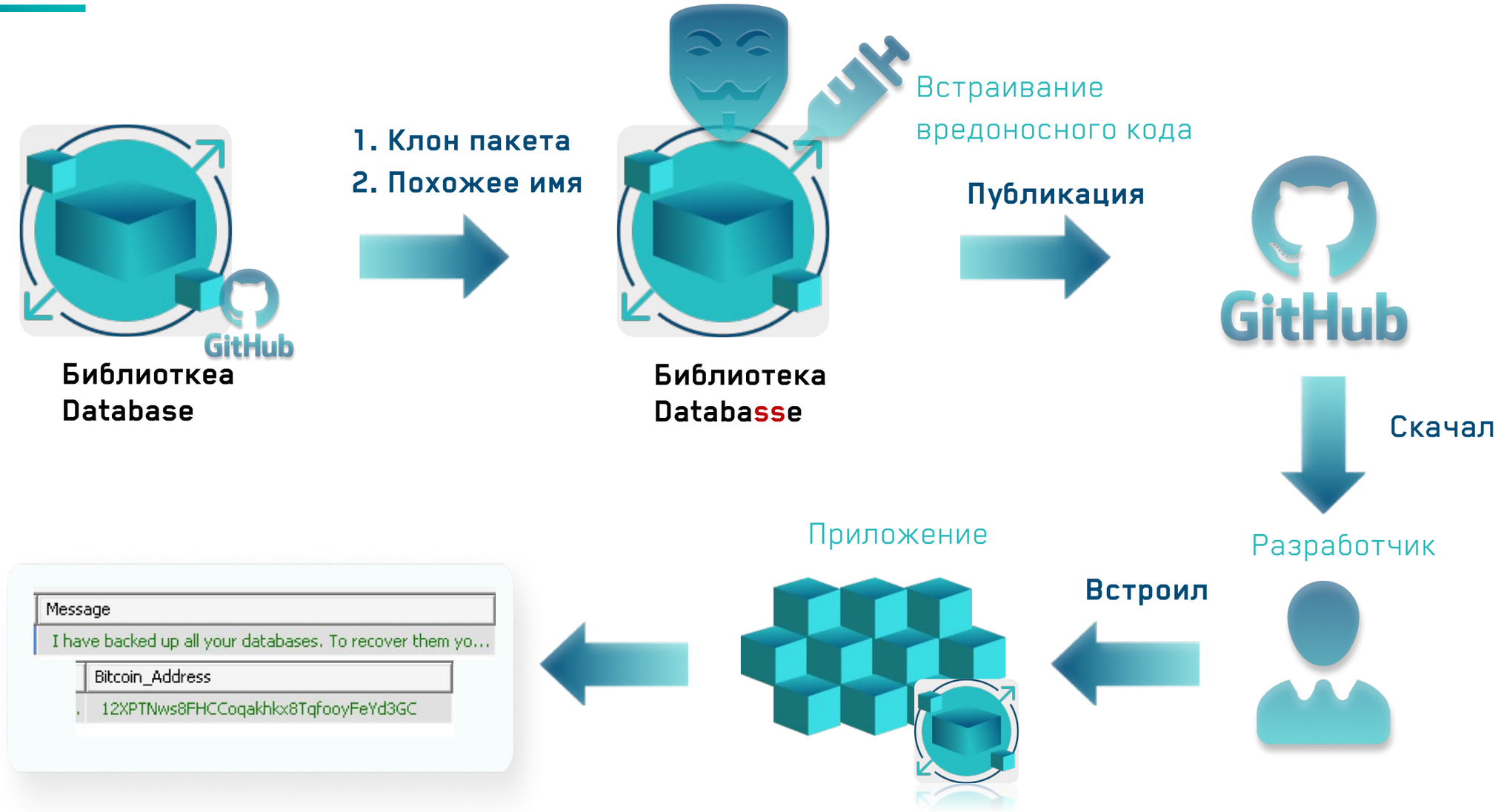
Устраняйте риски цепочки поставки ПО

Предотвращение угроз, направленных на цепочки поставок, включая такие атаки как typosquatting, starjacking и MavenGate.

Проверяйте репутацию

Выбирайте библиотеки с высокими показателями “репутации”, чтобы избежать проектов с историей уязвимостей или плохих практик безопасности.

Атака Typosquatting (подмена имени)



DerSecur

Starjacking Attack (воровство звёзд рейтинга)

Цель

npm yarn python Package Index RubyGems

Проблема

Эти пакетные менеджеры не проверяют связь между пакетом и ссылкой на репозиторий GitHub, указанной при публикации. Таким образом, можно претендовать на репутацию любого популярного проекта на GitHub и наслаждаться рейтингом в 100 500 звезд. Такая репутация может создать ложное положительное впечатление о пакете и убедить разработчиков использовать такую библиотеку.

Сценарий

Воровство популярности («звездочек») у очередного известного пакета.

Источник изображения How to Steal a Star (and put it back) Paperback – 13 July 2022

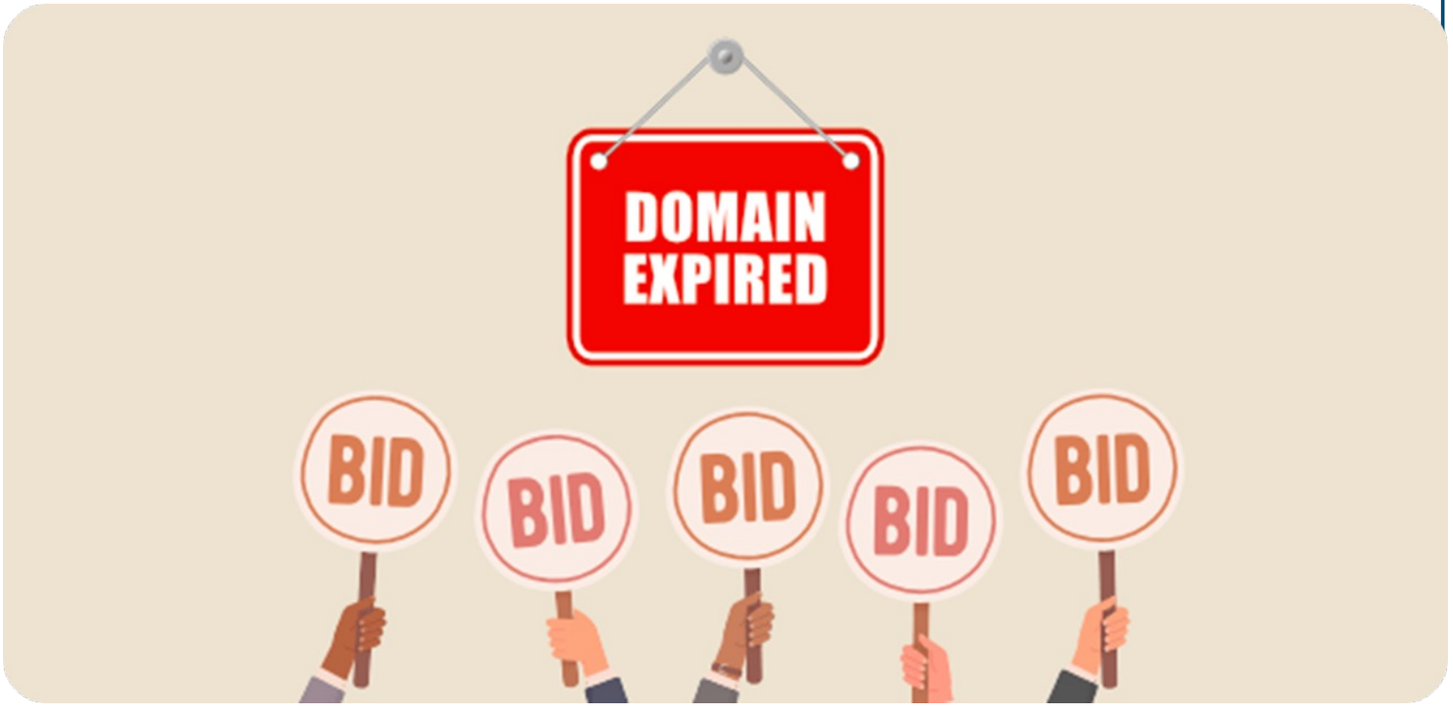
Атака MavenGate

Цель

JVM

Сценарий

Злоумышленники перехватывают просроченные домены, связанные с библиотеками, и начинают контролировать распространение кода под их именами. Это позволяет им внедрять вредоносное ПО в проекты разработчиков.



Атака

Атака осуществляется путем загрузки вредоносных пакетов в центральный репозиторий Maven, где разработчики могут случайно скачать их и использовать в своих проектах.

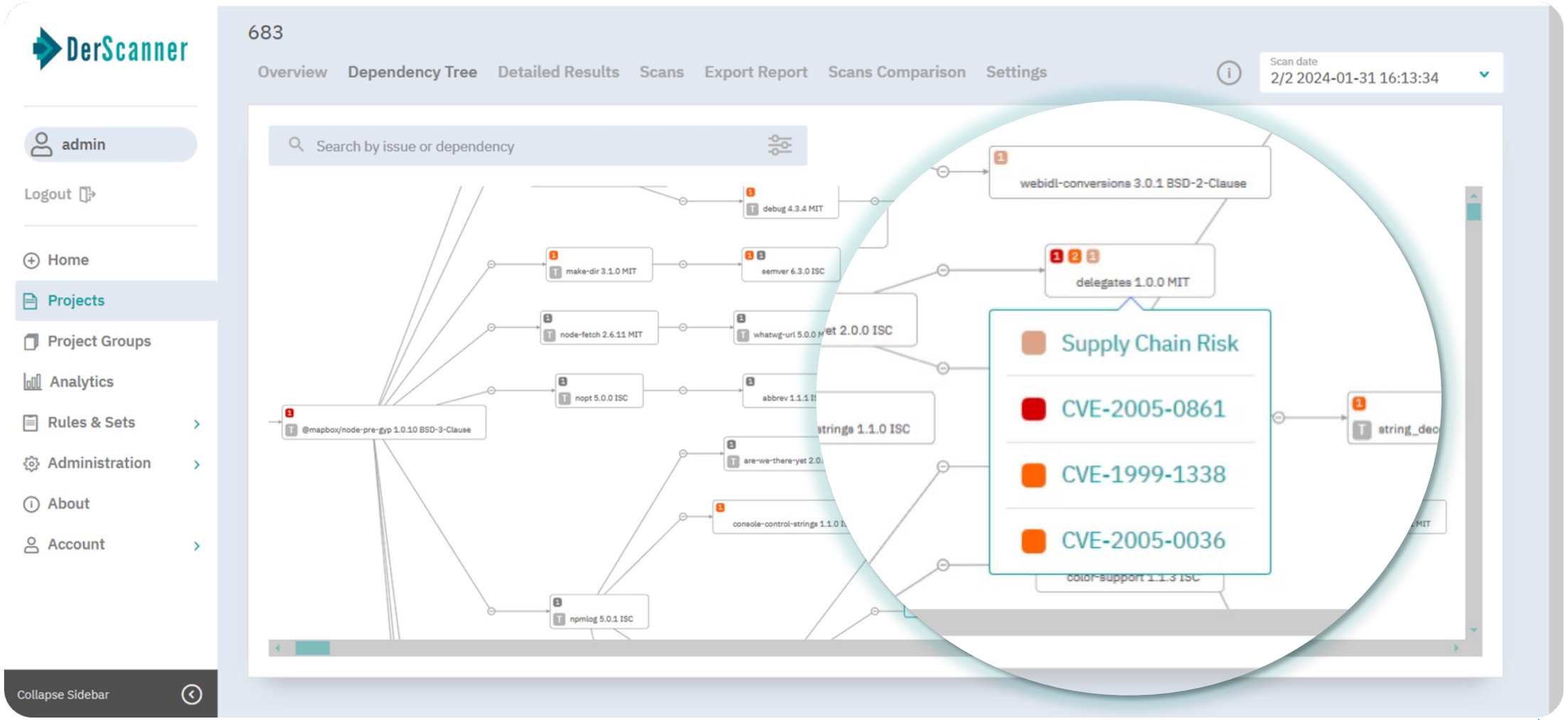
DerSecur

От создания SBOM до устранения рисков

DerSecur

Выявление рисков с помощью графа дерева зависимостей

Визуализируйте всю структуру проекта, чтобы точно увидеть, где находятся уязвимые пакеты



DerSecur

Оценивайте репутацию библиотек

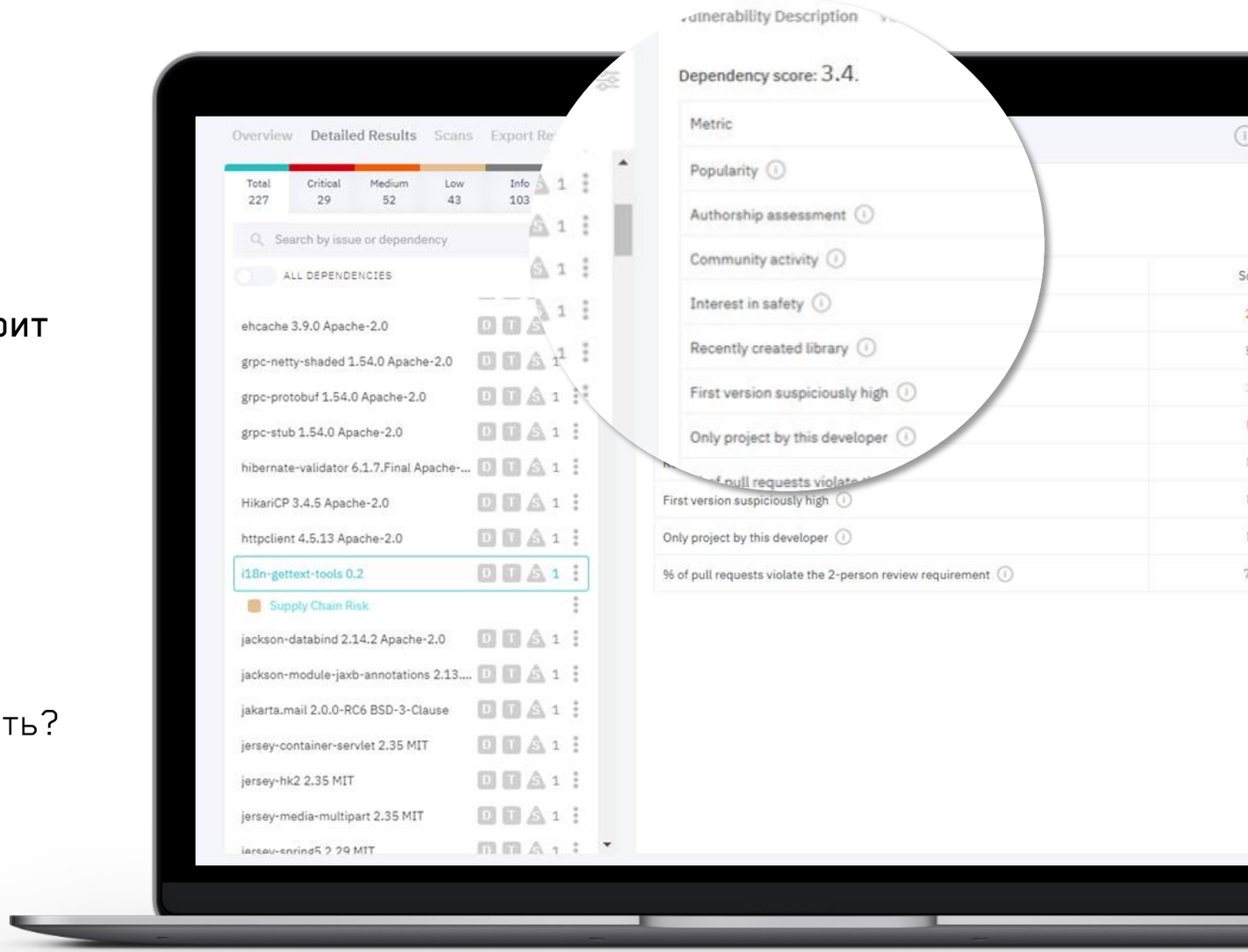
GitHub

DerScanner непрерывно оценивает пакеты с открытым исходным кодом в различных репозиториях.

Проверьте репутацию любого пакета и принимайте обоснованное решение о том, стоит ли использовать его в своем проекте.

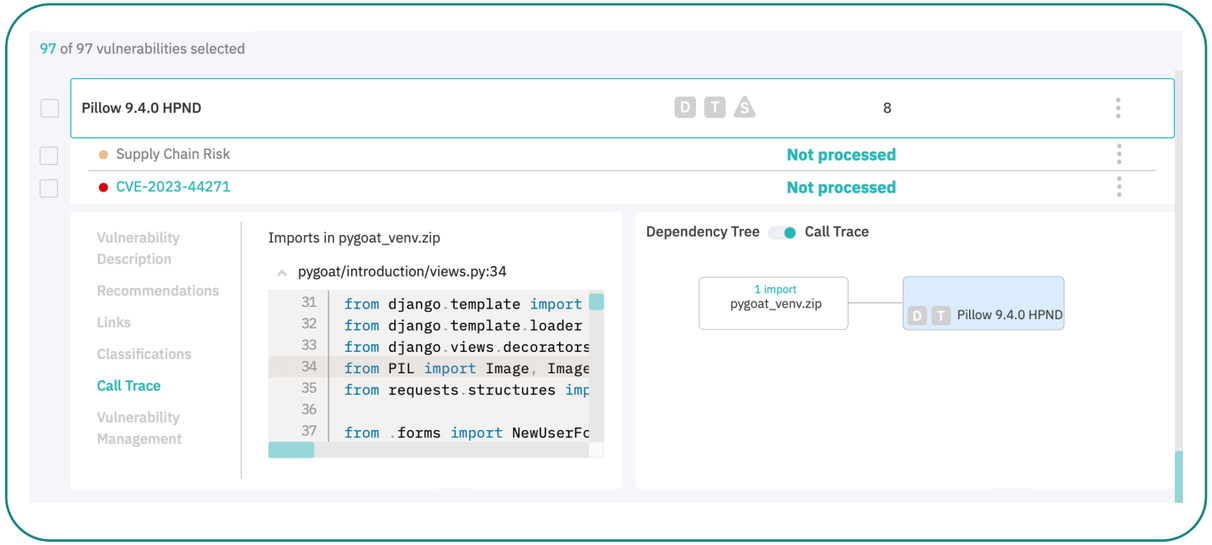
Получите оценку любого пакета и узнайте:

- Насколько популярен пакет?
- Доверяют ли автору?
- Насколько активно поддерживается сообщество?
- Включил ли автор базовую безопасность?
- Когда была создана библиотека?
- Была ли первая версия библиотеки подозрительно высокой?
- Это единственный проект автора?
- Проходят ли запросы на исправление ошибок авторизацию от двух человек?



DerSecur

Фокусируйтесь на действительно важных уязвимостях



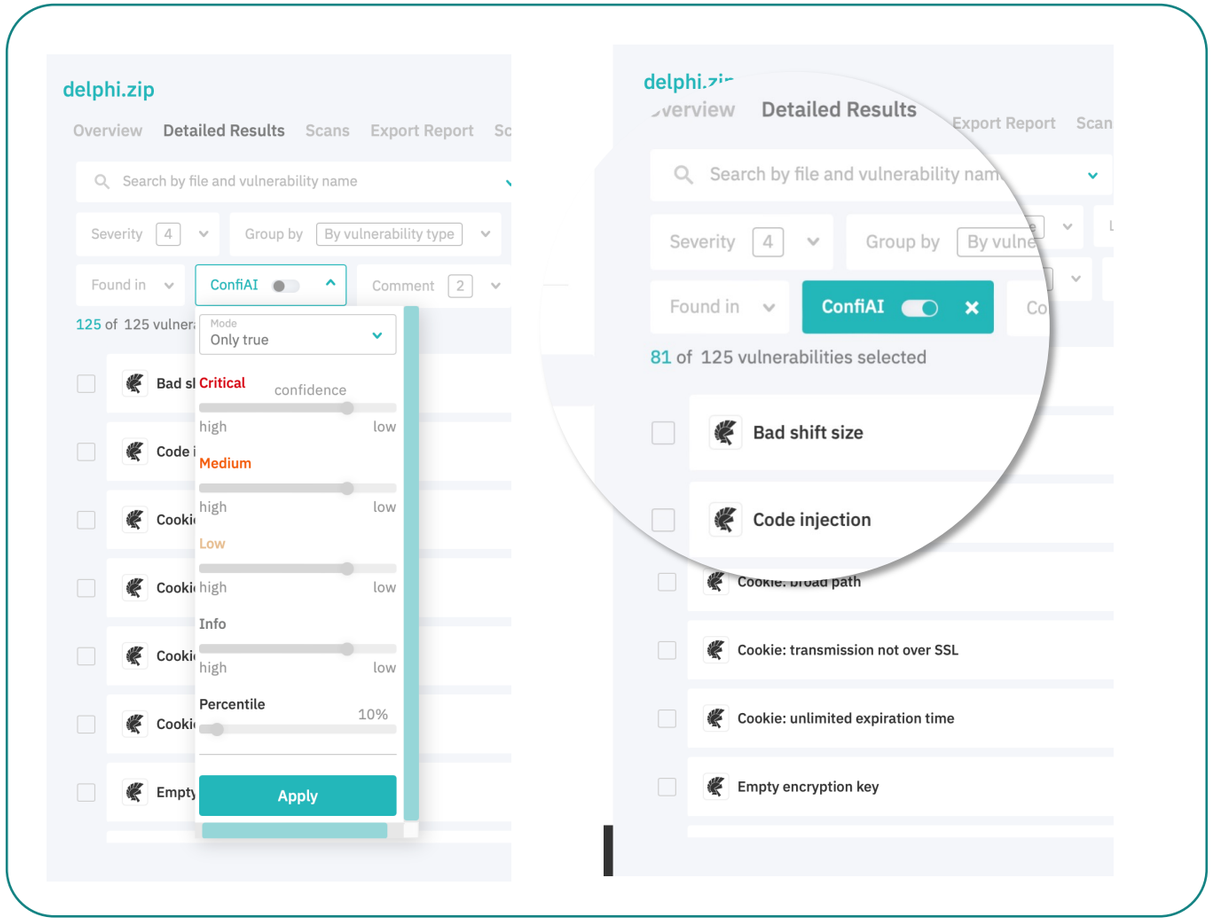
SAST

Гибридный анализ

SCA

Merely identifying a CVE in a dependency doesn't necessarily mean the entire package is at risk. DerScanner pinpoints which method calls could lead to vulnerability exploitation.

Confi AI filters out false negatives/positives



DerSecur

Обеспечьте уверенность в компонентах с открытым исходным кодом

Если бы во время знаменитых атак проводился анализ состава программного обеспечения (SCA)

Ошибка Heartbleed в OpenSSL (2014 год): Это была серьезная уязвимость в криптографической библиотеке OpenSSL, затронувшая миллионы веб-сайтов.

SCA могла бы определить уязвимую версию OpenSSL, используемую в приложениях, и предложить обновить ее до исправленной версии.

Взлом данных Equifax (2017 год): Эта утечка произошла из-за непропатченного фреймворка Apache Struts, используемого Equifax.

SCA могла бы выявить устаревшую систему и своевременно обновить ее, что позволило бы предотвратить взлом.

Взлом программного обеспечения SolarWinds Orion (2020 год): В ходе атаки на цепочку поставок вредоносный код был внедрен в процесс сборки программного обеспечения.

SCA отследила бы изменения в поведении или целостности компонентов и сигнализировала о несанкционированных изменениях.

Уязвимость Apache Log4j (2021): Известная под названием Log4Shell, эта уязвимость в широко используемой библиотеке протоколирования Log4j позволяла удаленно выполнить код.

SCA бы выявила уязвимые версии Log4j в реестрах программного обеспечения и рекомендовала их срочное обновление.

DerSecur

Почему выбирают DerScanner SCA

Высокая точность благодаря PURL

Гибридный анализ SCA+SAST для проверки эксплуатации

Меньше «фолзов» с Confi AI для SCA

Обширная база уязвимостей

DerScanner

Собственная база

+

Github Advisory

GitLab Advisory

Google OSV Database

EPSS Exploit Prediction Scoring System

EPSS (Exploit Prediction Scoring System)

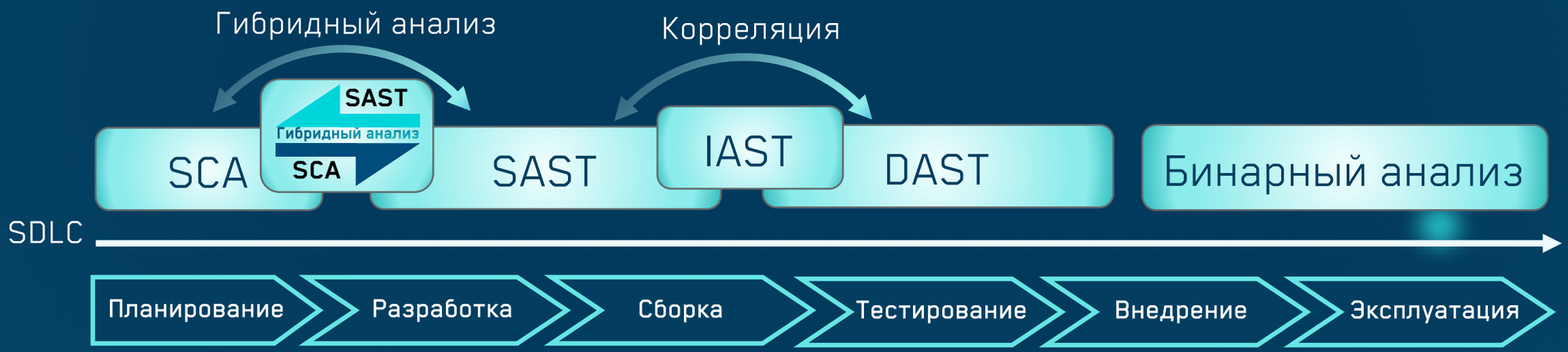
NIST NATIONAL VULNERABILITY DATABASE NVD

NVD

DerScanner

Устраняйте известные и неизвестные угрозы в коде на протяжении всего SDLC

- Защитите любое приложение от известных и неизвестных уязвимостей
- Интегрируйте проверки безопасности в SDLC, чтобы синхронизировать усилия по разработке и обеспечению безопасности



DerSecur

Варианты использования

On-premise

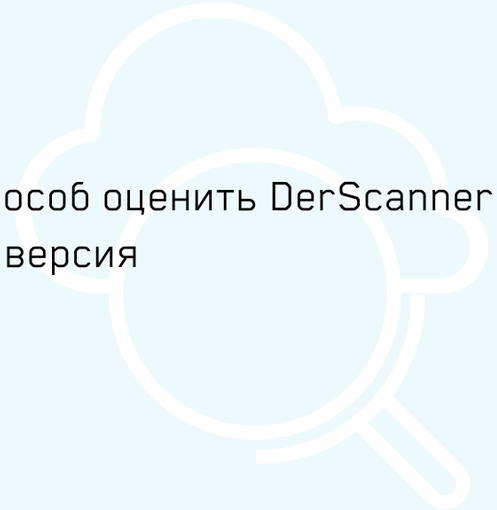
Хранится у вас

- Абсолютная конфиденциальность

SaaS

Хранится у нас

- Самый быстрый способ оценить DerScanner
- Всегда последняя версия



DerSecur

Почему клиенты выбирают DerScanner

Единая платформа безопасности приложений

- ✓ Эффективная комбинация технологий для безопасности приложений
- ✓ Корреляция результатов для получения полного представления о том, какие угрозы действительно опасны

Низкий уровень ложных срабатываний

- ✓ Собственная технология ИИ для установки порога предупреждений, который наилучшим образом соответствует вашим приоритетам

Отраслевое признание

- ✓ Отмечен FORRESTER® в числе заметных поставщиков SAST и SCA
- ✓ Сертифицирован MITRE
- ✓ Высокая оценка пользователей

Удобные отчеты

- ✓ Отчеты написаны простым языком, который может понять специалист по безопасности, не имеющий опыта разработки

Лучшее решение для аудита безопасности

- ✓ Даже если исходный код недоступен, проверьте работающие веб и мобильные, или устаревшие приложения с помощью комбинации бинарного SAST и DAST

Традиционная техническая поддержка

- ✓ Никаких ботов. Только классическая поддержка с помощью людей
- ✓ Поддержка в мессенджерах для крупных клиентов

DerSecur

DerScanner пользуется доверием

JUST EAT Takeaway.com

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

athena dynamics

nexagate

PARASOFT

DCU Ollscoil Chathair Bhaile Átha Cliath Dublin City University

Consequor Integrando Tecnologias e Negócios

RS Security

Bsecure

AST Cyber Lab

Modern Solutions LTD

DerSecur

DerSecur

Спасибо за внимание!

Узнать больше: https://derscanner.com/

Напишите нам: partner@dersecur.com