DerScanner

Комплексное решение для контроля безопасности ПО
(SAST, DAST, SCA)

DerSecur

Современные вызовы

Все приложения уязвимы

Переход на быстрые методы разработки и публикации кода (CI/CD) не оставляет времени на вдумчивый анализ кода. Результат: уязвимости и закладки.

Приложения – главная цель злоумышленников

С ростом квалификации и опыта киберпреступников дыры в приложениях стали основным вектором атак на информационные системы – они используются в 90% успешных атак.

Распространение атак через уязвимости в общедоступных библиотеках

Участились случаи внедрения недекларированных возможностей в open-source-код из общедоступных библиотек, бесконтрольное использование которых может привести к инцидентам ИБ.

От безопасности приложений зависит безопасность бизнеса

DerSecur

Чего стоит опасаться?

Уязвимости

Неумышленные ошибки, нестыковки, неточности, которые ведут к возможности взлома системы

Недекларированные возможности (НДВ)

Скрытая функциональность, умышленно внесенная в код

DerSecur

Откуда берутся уязвимости и НДВ?

Особенности разработки

- Использование небезопасных языковых конструкций
- Использование сторонних компонентов (СПО, библиотеки)
- Встраивание закладок для ускорения разработки

Дефицит времени

- Сжатые сроки разработки технического задания
- Сроки разработки ПО сокращаются (CI/CD, DevOps, Agile, SCRUM)
- Задержка в разработке – это потеря денег

Унаследованное ПО

- Содержит общеизвестные уязвимости (Heartbleed и т. д.)
- Сложно или невозможно обновить

DerSecur

Современный подход к анализу кода

1

Статический анализ кода (SAST)

Проверяет исходный или бинарный код
на наличие уязвимостей как на ранних,
так и на более поздних этапах разработки.

2

Динамический анализ кода (DAST)

Проверяет работающее приложение
в конце жизненного цикла разработки ПО
или когда оно уже установлено в инфраструктуре.

3

Анализ состава ПО (SCA)

Проверяет сторонние компоненты в коде
приложения и выявляет в них уязвимости
и закладки.

Для более полного контроля безопасности ПО необходимо зрелое комплексное решение, включающее разные виды анализа кода:

- SAST
- DAST
- SCA

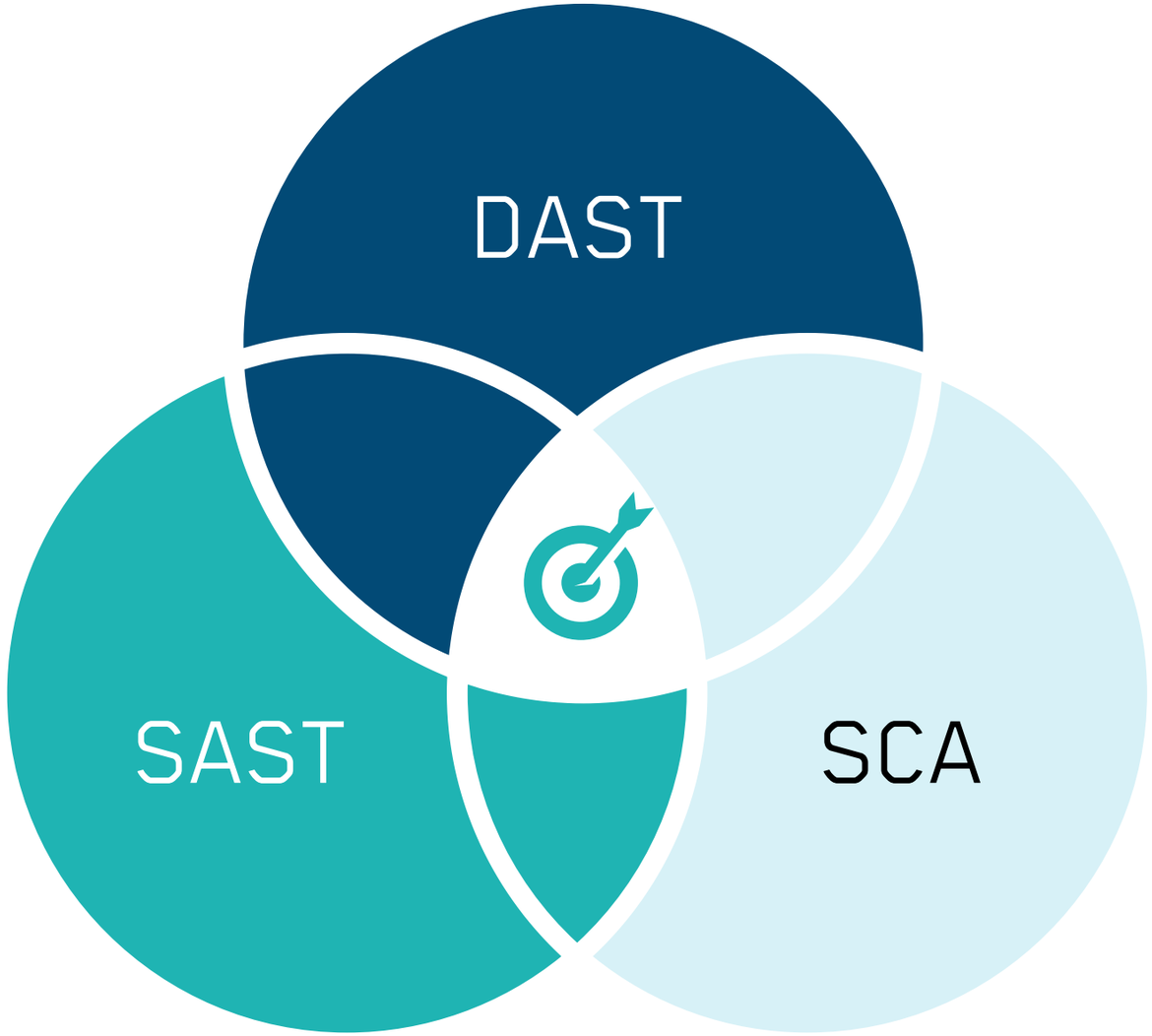
DerSecur

Что мы предлагаем

DerScanner – комплексное решение для контроля безопасности ПО, включающее технологии статического (SAST), динамического анализа (DAST) и анализа состава ПО (SCA).

- Сочетает преимущества всех трех методов анализа в одном решении
- Позволяет быстро и удобно управлять сканированиями из единого интерфейса
- Предоставляет возможность корреляции результатов разных видов анализа

Одно из крупнейших аналитических агентств Forrester включило DerSecur в свой отчет среди других SAST-вендоров



DerSecur

Статический анализ кода (SAST)

Статический анализ кода (SAST) позволяет выявить уязвимости и недекларированные возможности в коде приложений.

- 36 языков программирования
- Анализ исходного и бинарного кода
- Технология Fuzzy Logic Engine для сокращения ложных срабатываний

Анализ исходного кода. 36 языков

Java, JSP, JS, TS, PASCAL, T-SQL, salesforce APEX, SAP ABAP, python, GO, HTML, php, Visual Basic, SOLIDITY, Visual Basic, VB, Microsoft VBScript, Delphi, ORACLE PL SQL, C++, C#, 1С, Microsoft Visual Basic for Applications, Dart, COBOL, R, C, LotusScript, Scala, Kotlin, ASP.NET, ANDROID, Perl, Swift, RUBY, Objective-C

Мировой лидер по количеству поддерживаемых языков программирования

Анализ бинарного кода

Если исходный код приложения недоступен, можно загрузить исполняемые файлы в следующих форматах:

Приложение будет автоматически:

1. Скачано
2. Декомпилировано и деобфусцировано
3. Проверено

Для анализа мобильных приложений достаточно скопировать ссылку из Google Play или App Store

DerSecur

Динамический анализ кода (DAST)

Динамический анализ кода (DAST) – это способ анализа программы при ее выполнении.

DAST имитирует вредоносные внешние атаки, использующие распространенные уязвимости для компрометации приложения.

DerSecur

DAST. Проведение анализа

1 Для запуска анализа из интерфейса DerScanner введите локальный адрес (IP) или URL приложения

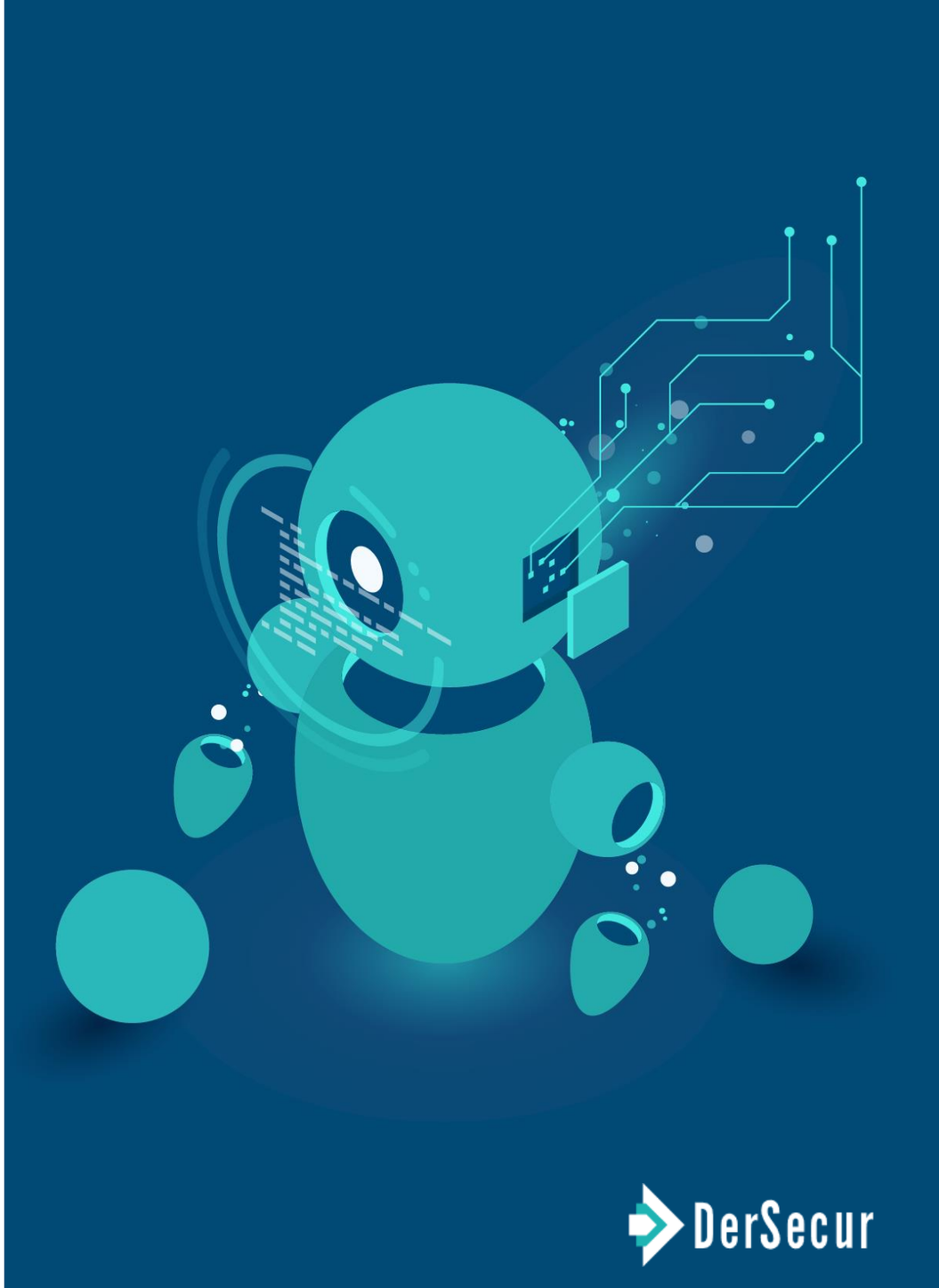
2 По итогам анализа получите детальный отчет с перечнем и описанием обнаруженных уязвимостей и их уровнем критичности

Анализ состава ПО (SCA)

Анализ состава ПО (SCA) – метод, который позволяет выявлять уязвимые компоненты и зависимости в сторонних библиотеках, используемых разработчиками в своем ПО.

Решаемые задачи:

- Обнаружение и отслеживание всех сторонних компонентов в ПО
- Выявление уязвимостей и закладок в сторонних библиотеках
- Предотвращение угроз и снижение рисков ИБ из-за заимствования кода



DerSecur

SCA. Проведение анализа

1. Для запуска проверки в интерфейсе DerScanner загрузите исходный код проекта, ссылку на репозиторий или SBOM

2. DerScanner проведет анализ на основе баз уязвимостей и выявит все заимствованные компоненты кода в проекте

3. Получите полный отчет со списком зависимостей и уязвимостей в сторонних компонентах кода

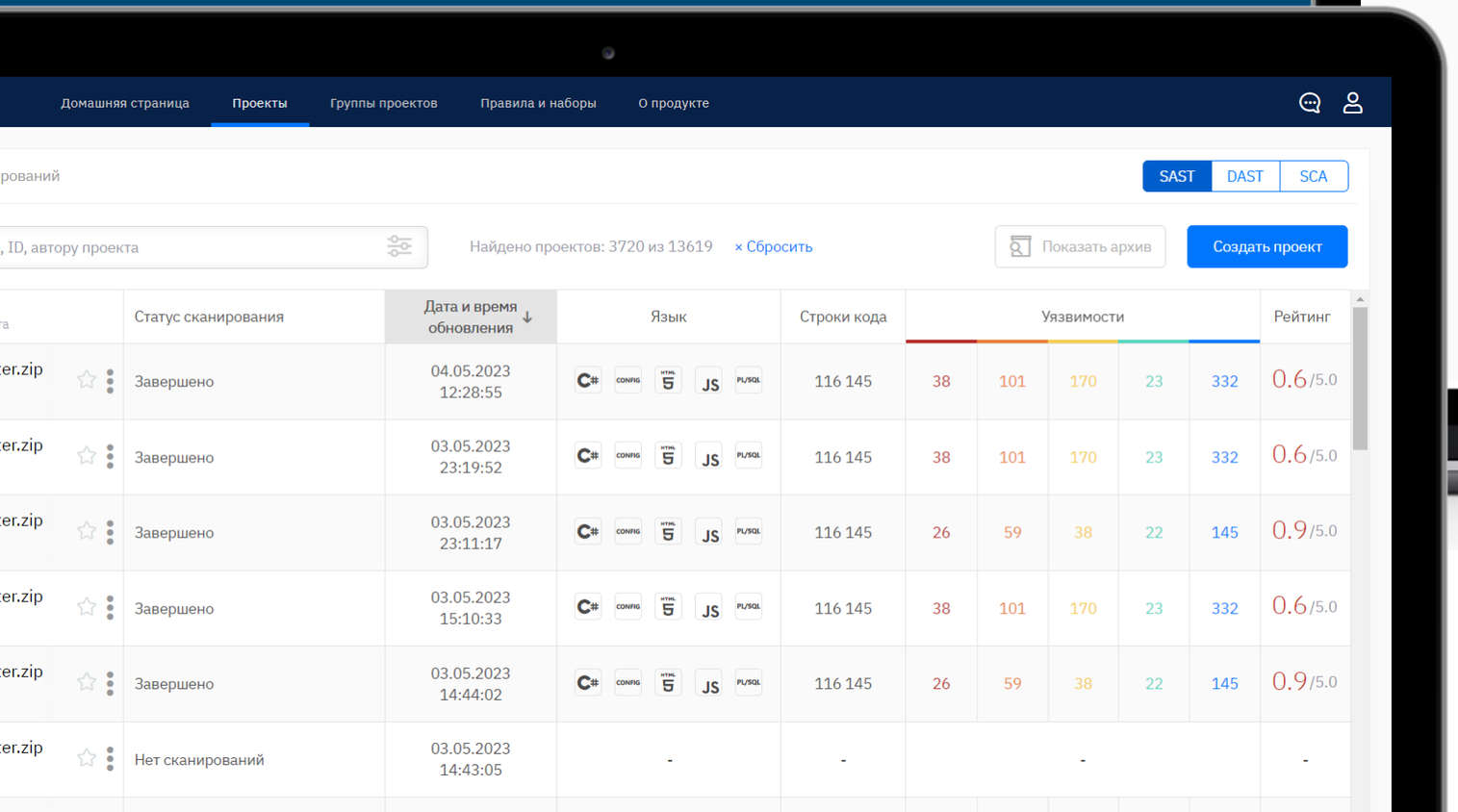
Анализ состава ПО в DerScanner проводится с применением нескольких источников:

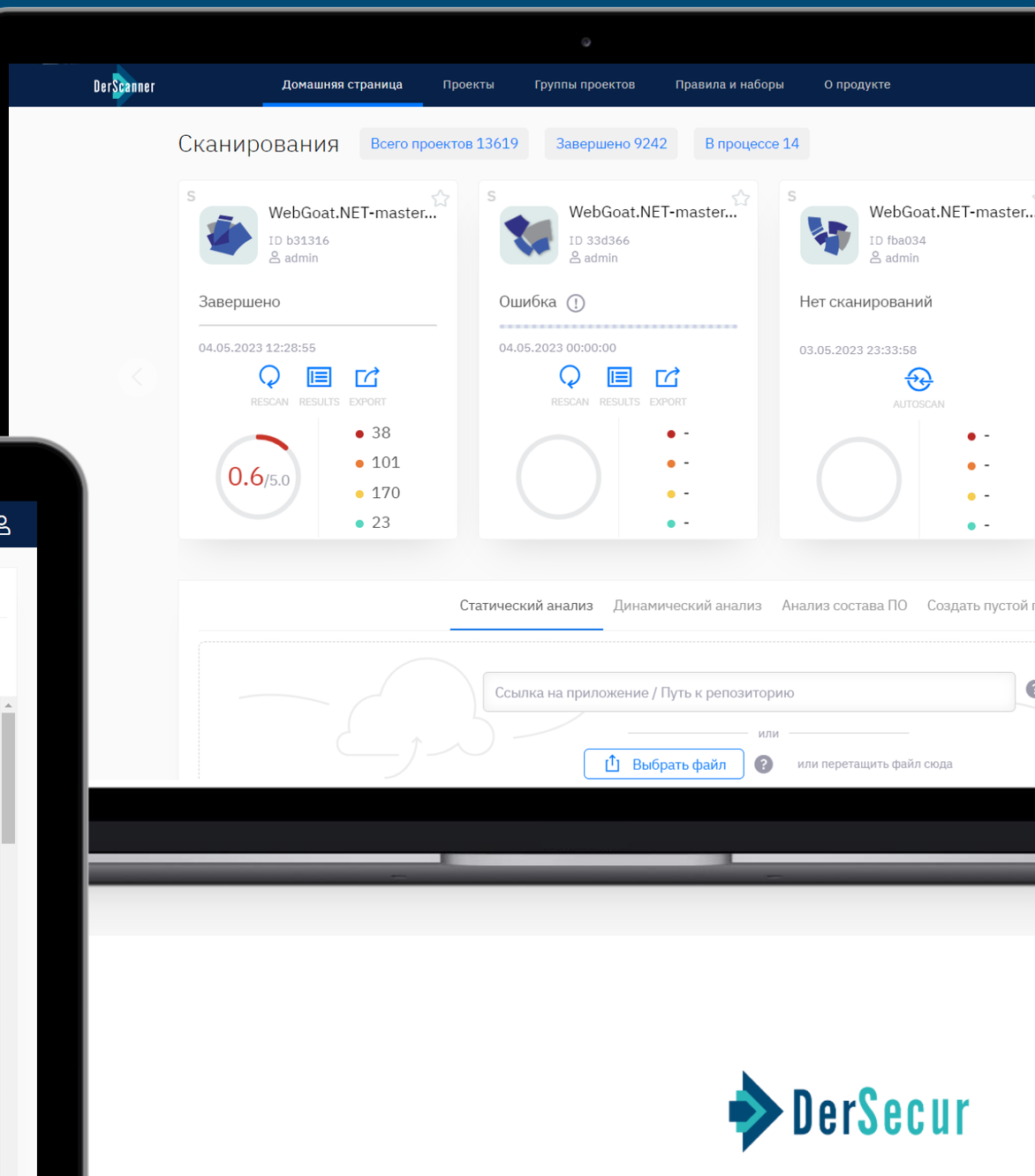
- стандартных баз уязвимостей
- собственной базы от экспертов DerSecur

DerSecur

Понятный интерфейс

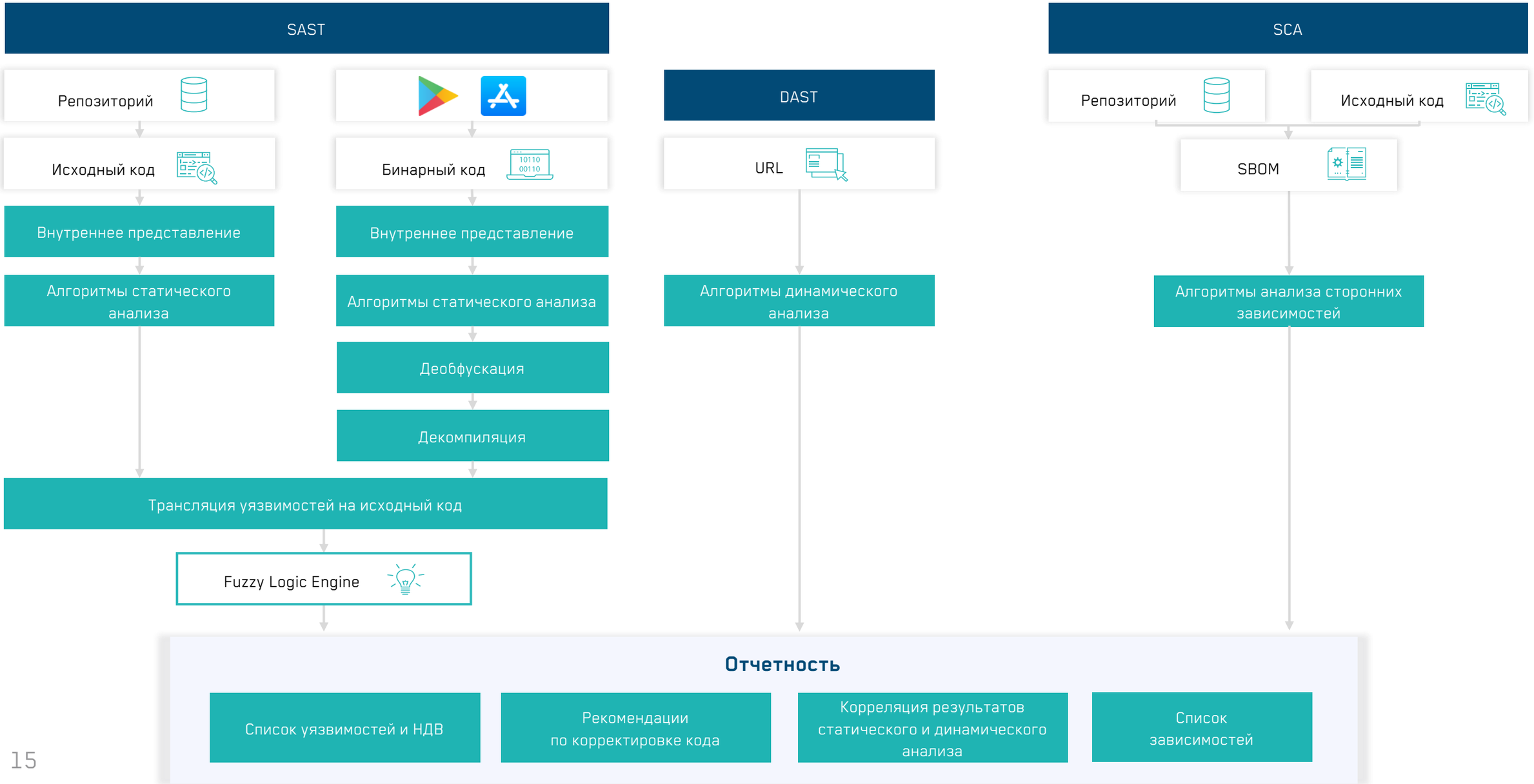
- Запуск сканирования в два клика
- Быстрое переключение между вкладками статического, динамического анализа и анализа состава ПО
- Единообразие отображения результатов разных видов анализа ПО





DerSecur

Принцип работы DerScanner



Преимущества DerScanner

Комплексное решение для анализа кода

Универсальный продукт, комбинирующий ключевые
виды анализа кода – статический, динамический и анализ состава ПО

Умеет работать без исходных кодов

Не надо просить исходные коды у разработчиков – можно загрузить
исполняемый файл или дать ссылку на Google Play или App Store

Удобный инструмент SSDLC / DevSecOps для разработчиков

Интеграция с Git и Subversion, средствами разработки, серверами CI/CD
и другими инструментами позволяет удобно встраивать решение в цикл
безопасной разработки

Признание в отрасли

DerSecur был включен в отчет Forrester среди других SAST-вендоров,
а решение DerScanner обладает сертификатом CWE-Compatible

DerSecur

Преимущества DerScanner

Минимизирует ложные срабатывания

Запатентованная технология Fuzzy Logic Engine
сокращает процент ложных срабатываний

Целостная аналитика результатов

Корреляция результатов статического
и динамического анализа и полноценная отчетность
по итогам всех трех видов анализа кода

Удобен для службы ИБ, т.к не требует опыта разработки

DerScanner обладает интуитивно понятным интерфейсом
и не требует специальных навыков для работы с ним

DerSecur

Ключевые заказчики

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

Возможности интеграции

Репозитории

git

SUBVERSION

VCS-хостинги

GitHub

GitLab

Bitbucket

Средства разработки

eclipse

Visual Studio

IJ

Средства сборки

Xcode

GNU (Autotools, Make)

sbt

Maven

Gradle

CMake

Visual Studio

Серверы CI/CD

Jenkins

TeamCity

Azure DevOps Server

Отслеживание задач

Atlassian JIRA

Анализ кода

sonarqube

Открытый API предоставляет широкие возможности по дополнительной интеграции и автоматизации. Включает в себя JSON API и CLI.

DerSecur

Соблюдение стандартов

Отчеты доступны в форматах в соответствии со стандартами:

- PCI DSS
- OWASP
- HIPAA
- CWE/SANS

План действий

Получить демо, написав на **company@dersecur.com**

Совместно оценить потребности компании в анализе кода

Инициировать пилотный проект

Успешно реализовать пилот

DerSecur

DerSecur

Адреса международных офисов:

- Israel, Haifa, Khuri 2
- Spain, Madrid, Paseo de la Castellana 200
- Singapore, 8 Penjuru Ln.
- Canada, Ontario, Toronto, 16 Dallimore Circle Unit 818, M3C4C4
- UAE, Abu Dhabi, 16-02 Office Tower, Capital Plaza
- Brazil, Sao Paulo, 1437, Al. Itu, 141
- Republic of Kazakhstan, Astana, Anatoly Khrapaty street 25, office 17
- Azerbaijan, Baku, R. Aliyev 12/14, office 15

company@dersecur.com