SECURE DEVELOPMENT PLATFORM

SOLIDLAB SDP — ИНТЕЛЛЕКТУАЛЬНАЯ ПЛАТФОРМА ДЛЯ РАЗРАБОТКИ ЗАЩИЩЕННЫХ ПРИЛОЖЕНИЙ

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

Анализ защищенности приложений: SAST, DAST, OST, анализ описаний инфраструктуры, анализ контейнеров.

Потребность: разовый или периодический поиск недостатков.

Решение: однократное или периодическое сканирование приложения инструментами Платформы и разбор результатов.

Построение процессов защищенной разработки с использованием инструментальных проверок защищенности.

Потребность: построение процессов защищенной разработки в соответствии с требованиями регуляторов и лучшими практиками.

Решение: исследование текущих процессов разработки, подготовка рекомендаций и внедрение Платформы для реализации автоматизированного анализа защищенности.

ОСНОВНЫЕ КОМПОНЕНТЫ РЕШЕНИЯ

SAST **Static Application Security Testing**

Подбираем эффективные инструменты для проведения статического анализа кода Заказчика с учетом специфики анализируемого приложения. Платформа содержит решения партнеров и open source инструменты, в том числе средства поиска секретов и анализа инфраструктуры. Набор инструментов Платформы может быть расширен.

DAST **Dynamic Application Security Testing**

Платформа использует динамические методы анализа для поиска недостатков в приложениях. Платформа включает собственное решение по анализу защищенности SolidPoint DAST. Для поиска входных точек в веб-интерфейсах используется уникальный статико-динамический анализатор JavaScript-кода.

DT **Defect Track**

Платформа включает систему управления находками, которая позволяет обрабатывать большое количество недостатков.

OST **Анализ защищенности используемых компонентов**

Анализ программных и системных компонентов, а также образов контейнеров выполняется с использованием собственной базы уязвимостей SolidLab OST.

AST **Обучение практикам защищенной разработки**

Учим разработчиков учитывать возможные недостатки ИБ при написании кода и знакомим с мерами противодействия им.

РЕЗУЛЬТАТЫ ИСПОЛЬЗОВАНИЯ ПЛАТФОРМЫ

Рост числа обнаруженных недостатков на этапе разработки ↑

Снижение количества уязвимостей в приложениях ↓

Обучение разработчиков защищенной разработке ↑

СТАТИЧЕСКИЙ АНАЛИЗ (SAST)

Анализ исходного кода

Платформа предоставляет возможность использования широкого набора как коммерческих, так и решений с открытым исходным кодом. Все доступные инструменты используются в унифицированном процессе анализа. Результаты сканирований различных инструментов коррелируются между собой. В качестве дополнительной услуги оказывается помощь в выборе и настройке инструментов под специфику анализируемого кода.

Анализ конфигураций

Решение позволяет анализировать конфигурации разрабатываемого ПО, включая конфигурации инфраструктуры, описанной в виде кода. При использовании подхода Infrastructure as Code в разработке это позволит контролировать инфраструктуру приложения еще на этапе его разработки.

Поиск секретов

Платформа включает в себя модули анализа, обнаруживающие оставленные секреты в исходном коде и в истории коммитов. Правила поиска секретов могут быть адаптированы под специфику использования секретов у Заказчика.

ДИНАМИЧЕСКИЙ АНАЛИЗ (DAST)

Широкий набор инструментов

Платформа содержит широкий набор инструментов динамического анализа: SolidPoint DAST собственной разработки дополняется набором инструментов с открытым исходным кодом.

Выявление точек ввода данных

Поддерживается максимально широкий спектр технологий по обнаружению точек ввода данных, как традиционных (crawling, dirbusting), так и альтернативных (статико-динамический анализ JavaScript, FAST, загрузка описаний Open API).

Обнаружение различных классов уязвимостей

Модули сканирования в составе Платформы позволяют выявлять различные классы уязвимостей, в том числе инъекции, недостатки десериализации и парсинга форматов передачи данных, уязвимости аутентификации и авторизации и другие.

КОМПОНЕНТНЫЙ АНАЛИЗ (OST)

Анализ используемых компонентов

Платформа включает в себя инструменты собственной разработки для качественной инвентаризации компонентов. Также поддерживается интеграция с популярными инструментами инвентаризации используемых программных компонентов.

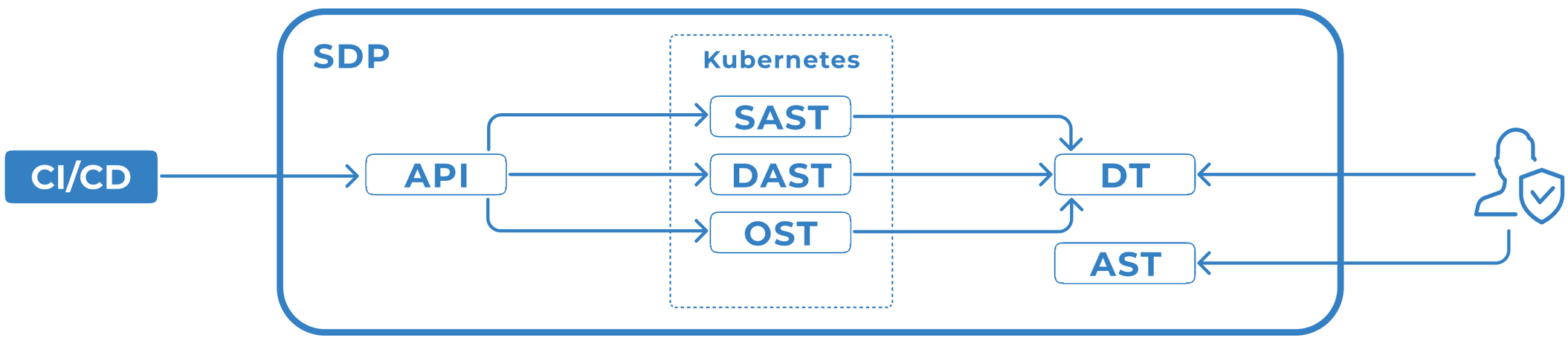
Анализ собранных приложений и контейнеров

Анализ зависимостей на уязвимости может быть выполнен и для собранных приложений. В том числе поддерживается анализ упакованных в контейнеры приложений, включая контейнеризованное окружение.

Интеграция с инструментами разработки

Предоставляются плагины для интеграции в инструменты разработки: для репозитория компонентов и для IDE. Плагин для Nexus позволяет оставлять в репозитории только те внешние компоненты, которые прошли проверку на отсутствие уязвимостей.

АРХИТЕКТУРА ПЛАТФОРМЫ



УПРАВЛЕНИЕ НАХОДКАМИ (DEFECT TRACK)

Все результаты анализа в одном интерфейсе

Результаты работы всех инструментов анализа на Платформе попадают в единый интерфейс, который позволяет отслеживать метрики качества и динамику исправления недостатков. Единый интерфейс предоставляет возможности по интеграции с привычными для разработчика системами, такими как Jira и GitLab.

Возможность работы с большими объемами находок

Система управления находками позволяет работать с несколькими миллионами записей о находках при использовании вычислительных ресурсов обычного ноутбука.

Удобные процессы

В системе управления находками реализованы механизмы, упрощающие типовые задачи управления недостатками защищенности при разработке ПО. Например, отслеживание статуса находки между различными ветками или агрегация однотипных находок при генерации отчетов.

ОБУЧЕНИЕ (AST)

Обучение практикам защищенной разработки

С использованием Платформы можно организовать полноценное обучение практикам защищенной разработки: от поиска недостатков различными методами анализа до их исправления. Для обучения предоставляются уязвимые приложения и методические материалы.

Очное обучение

В дополнение к обучению практикам защищенной разработки опытные преподаватели могут провести курсы по разработке защищенных приложений, на которых расскажут теорию и на практике покажут, как реализовать приложения с учетом требований к их защищенности. Курсы могут быть адаптированы под технологический стек Заказчика.

ПРОФЕССИОНАЛЬНЫЕ СЕРВИСЫ

- ✓ Выбор подходящих инструментов анализа
- ✓ Консультации по найденным недостаткам
- ✓ Тонкая настройка инструментов анализа
- ✓ Подготовка аналитических отчетов
- ✓ Встраивание в процессы разработки
- ✓ Разработка типовых CI/CD-процессов

ПРЕИМУЩЕСТВА ПЛАТФОРМЫ ДЛЯ РАЗОВЫХ ПРОВЕРОК

Все необходимые проверки в одном интерфейсе

На Платформе есть все необходимые инструменты для выполнения разовой проверки защищенности приложения. Сканирования можно запускать без необходимости разбираться в инструментах, а результаты всех проверок отобразятся в едином интерфейсе, который позволяет отслеживать статистику по найденным недостаткам.

Экспертное мнение опытной команды специалистов ИБ

Результатом разового сканирования являются не только сырые находки инструментов, но и мнение экспертов по каждой находке, с оценкой ее критичности и рекомендациями по исправлению с учетом специфики анализируемого приложения.

ПРЕИМУЩЕСТВА ПЛАТФОРМЫ В ОБЛАКЕ

Управляемая услуга (managed service)

Облачное решение с расширенным набором услуг по внедрению и сопровождению процессов защищенной разработки. Доступен широкий набор инструментов для построения процессов защищенной разработки и услуг по анализу результатов. Возможность выбрать только те инструменты и услуги, которые нужны.

Интегрируется с процессами разработки

Облачная версия Платформы позволяет интегрировать проверки защищенности в процессы разработки на стороне Заказчика. Доступны типовые шаблоны автоматизированных процессов и типовые интеграции с системами разработки.

ПРЕИМУЩЕСТВА ЛОКАЛЬНОЙ УСТАНОВКИ ПЛАТФОРМЫ

Работа в закрытом контуре без потери функциональности

Все необходимые базы знаний, в том числе базы уязвимостей, поставляются вместе с Платформой.

Возможность кастомизации состава инструментов под нужды клиента

Состав компонентов и инструментов Платформы оптимизируется по запросу. Возможно добавление новых или сторонних инструментов.

Оптимизация потребления вычислительных ресурсов

Вычислительные ресурсы для инструментов анализа выделяются только при необходимости выполнения анализа. По завершении анализа ресурсы высвобождаются.

Дополнительные возможности для локальной установки

Возможность обогатить встроенную базу недостатков уязвимостями внутренних компонентов Заказчика, обучение разработчиков на основе выявленных уязвимостей и другие возможности.

МЕТОДЫ ЛИЦЕНЗИРОВАНИЯ

T0 - разовые сканирования в общем облаке

SAST и OST - количество строк кода.
DAST - количество целей сканирования.

T1 - периодические проверки в облаке (общая система управления и сканеры)

SAST и OST - количество репозиториев.
DAST - количество целей сканирования.

T2 - регулярные проверки в облаке (общая система управления, выделенные сканеры)

SAST и OST - количество репозиториев.
DAST - количество целей сканирования.
SAST, OST, DAST - количество параллельных потоков анализа.

T3 - выделенная инсталляция Платформы

SAST и OST - количество репозиториев.
DAST - количество целей сканирования.
SAST, OST, DAST - количество параллельных потоков анализа.

117312, г. Москва, ул. Вавилова, д. 47А
+7 (499) 705-76-57
info@solidlab.ru

Группа компаний SolidLab работает в области информационной безопасности более 10 лет, защищая организации от киберугроз, предупреждая атаки, минимизируя риски финансовых и репутационных потерь. SolidLab предлагает полный комплекс услуг: от пентестов до защиты приложений, реагирования на инциденты и организации процессов SDLC.