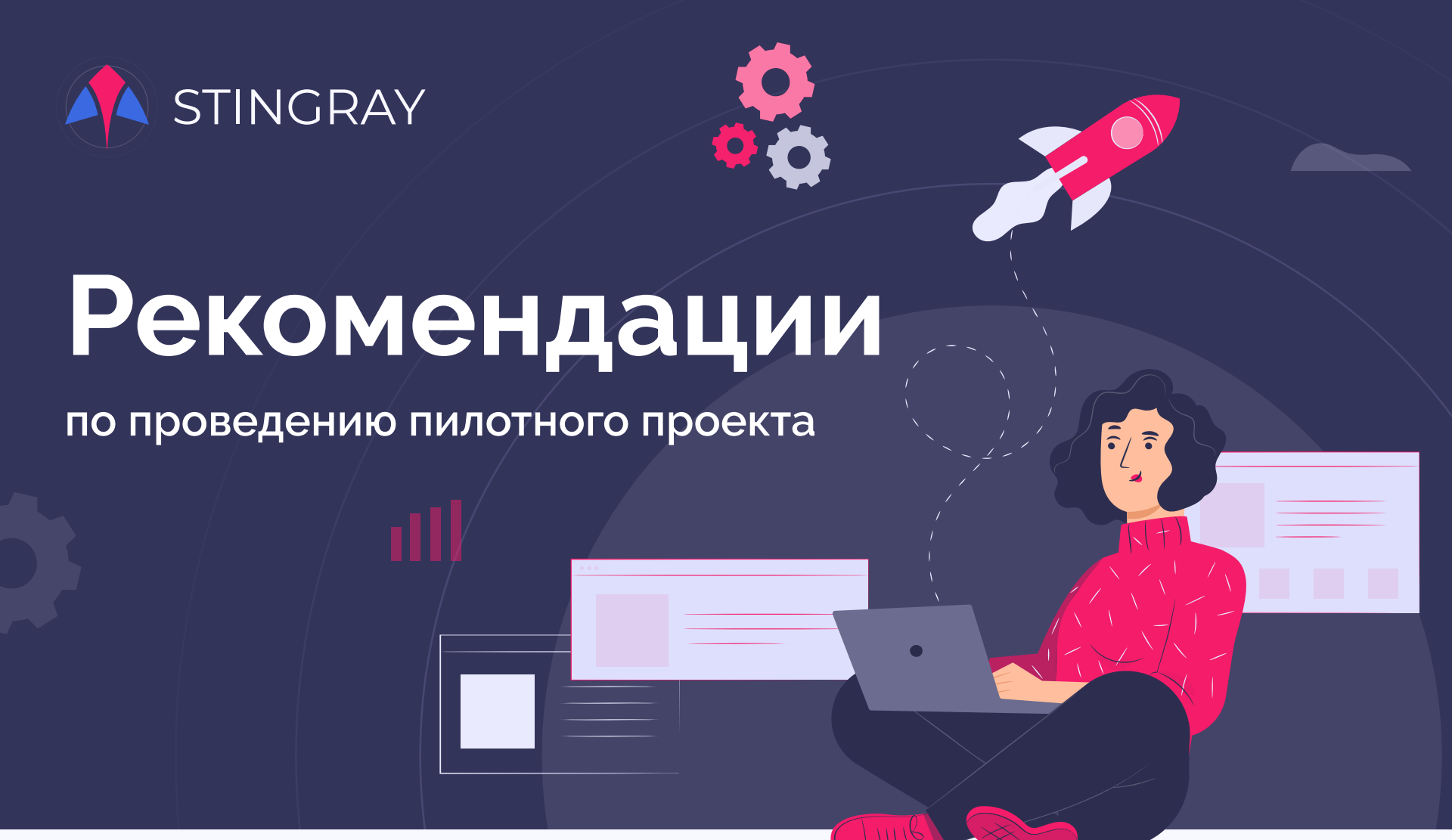
STINGRAY

Рекомендации

по проведению пилотного проекта



Основные рекомендации

При проведении пилотного проекта в формате On-premise убедитесь, что выделенные мощности поддерживают технологию виртуализации Intel Virtualization Technology (VT, VT-x, vmx) или AMD Virtualization (AMD-V, SVM).

При проведении тестирования системы в формате Cloud убедитесь в доступности тестовых серверов мобильного приложения из сети интернет. Если тестирование будет проходить на Production среде, при необходимости создайте специальную учетную запись.

x86

Для лучшей производительности рекомендуется использовать приложения на архитектуре x86.

Для проведения анализа не рекомендуется использовать приложения, зашифрованные при помощи DexProtector или DexGuard.

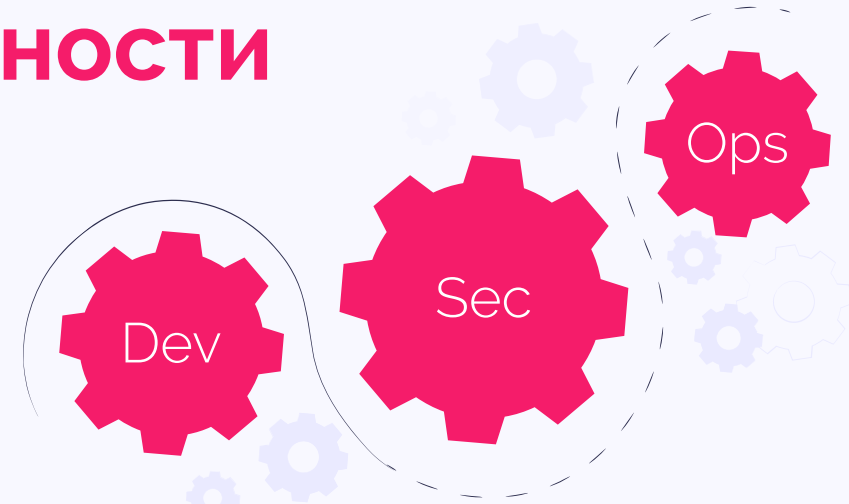
TEST

При записи автотестов полезно использовать сценарии, которые уже применяются для ручного тестирования приложения.

Ключевые особенности

Различные режимы сканирования

В системе Stingray есть несколько режимов анализа безопасности приложений, которые подходят для различных сценариев.
Ручной анализ для быстрой проверки приложения и автоматический режим для встраивания в процесс разработки.



Гибкое изменение правил анализа

Дополняйте правила анализа под ваше приложение, чтобы получить максимальную эффективность при поиске дефектов.
Компоненты системы, отвечающие за сбор данных, представлены в виде модулей с простой и понятной конфигурацией. Модификация правил анализа сделана в виде конструктора, благодаря которому изменение не займет много времени.

Встраивание в процесс CI/CD

Помимо полноценного REST API, предусмотрены интеграции с системами дистрибуции мобильных приложений. Максимальная гибкость и разнообразие настроек позволяет использовать Stingay в том процессе, который уже выстроен для разработки приложения и информировать разработчиков о наличии уязвимостей еще на этапе первых сборок.

Проверка на соответствие стандартам Безопасности

При анализе приложения вы получите не только описание и рекомендации о выявленных уязвимостях, всю собранную информацию о работе приложения, но и детальный отчет о соответствии вашего приложения всем актуальным мировым стандартам информационной безопасности.

Вся собранная информация о работе приложения

Все данные, собранные во время работы приложения на устройстве, сохраняются, структурируются, анализируются и предоставляются в качестве артефактов сканирования.

Детальные рекомендации о выявленных уязвимостях

Stingray позволяет обнаруживать более 30 типов уязвимостей. Технология поиска базируется на наблюдении за поведением приложения на устройстве во время совершения бизнес-операций.
После всех этапов анализа выявленные в ходе работы приложения уязвимости отображаются в интерфейсе с подробной информацией о месте возникновения, критичности, детальными рекомендациями по исправлению и, самое главное, предотвращению появления подобных уязвимостей в дальнейшем.
Рекомендации постоянно обновляются согласно новейшим способам защиты и лучшим мировым практикам. Ваши разработчики всегда будут в курсе самых надежных методов защиты!

Рекомендации для интеграции в непрерывный процесс разработки

Для интеграции с системам сборки (CI/CD) возможно использование REST API или специально разработанного инструмента для интеграций с системами дистрибуции.

Для использования REST API напрямую – необходимо зайти на страницу «Настройки» - «CI/CD», выбрать необходимые параметры и скопировать строку запуска в ваш конвейер разработки.

Советы для интеграции с системами дистрибуции мобильных приложений HockeyApp и AppCenter

Для запуска инструмента интеграции необходимо указать обязательные параметры:

stingray_url – сетевой адрес Stingray (путь до корня без последнего /), при использовании cloud версии – https://saas.mobile.appsec.world;
profile – идентификатор профиля для которого проводится анализ;
testcase – идентификатор автотеста, который будет воспроизведен во время анализа; возможен запуск нескольких автотестов, для этого их id перечисляются через пробел;
token – CI/CD токен для доступа (как его получить можно посмотреть в документации);
distribution_s ystem – способ загрузки приложения, возможные опции: file, hockeyapp или appcenter. Более подробно про них написано в соответствующих разделах;

Опциональные параметры:

report – тип отчета, который будет сформирован по результатам проведенного анализа.

Возможные опции:
separate – одиночный отчет по проведенному сканированию, является отчетом по умолчанию при указании одного testcase id, При нескольких testcase id создаст отдельный отчет для каждого запуска;
standard – отчет по умолчанию при указании нескольких testcase id, совмещает дубликаты дефектов из нескольких сканирований в один (id сохраняются);
grouping – отчет, группирующий дефекты одного типа с указанием всех деталей.
Можно указывать сразу несколько опций для создания отчетов нужных типов, например: “report separate grouping standard”. Для сканирований с одним тесткейсом возможно создание отдельных и группирующих отчетов.

HOCKEYAPP

Для загрузки приложения из системы дистрибуции HockeyApp при запуске необходимо указать параметр distribution_system = hockeyapp. Также необходимо указать обязательные параметры:

hockey_token (обязательный параметр) – API токен для доступа. Как его получить можно узнать из официальной документации системы HockeyApp.

hockey_version (необязательный параметр) – при указании данного параметра будет скачана конкретная версия приложения по коду его версии (поле version в API). При отсутствии данного параметра будет загружена последняя доступная версия приложения (latest).

hockey_bundle_id или **hockey_public_id** (обязательный параметр)

- **hockey_bundle_id** – идентификатор Android приложения или, по другому, имя пакета (com.stingray.app.example). При указании данной опции будет осуществлен поиск по всем приложениям внутри HockeyApp и выбрано приложение с соответствующим идентификатором. Поле в API - bundle_identifier;
- **hockey_public_id** – идентификатор приложения внутри системы HockeyApp. При указании данного параметра будет загружено приложение с соответствующим идентификатором. Поле в API - public_identifier.

AppCenter

Для загрузки приложения из системы дистрибуции AppCenter при запуске необходимо указать параметр distribution_system = appcenter. Также необходимо указать обязательные параметры:

appcenter_token – API токен для доступа. Как его получить можно узнать из официальной документации системы AppCenter.

appcenter_owner_name – владелец приложения, как узнать имя владельца можно посмотреть в официальной документации AppCenter.

appcenter_app_name – имя приложения в системе AppCenter.

appcenter_release_id или **appcenter_app_version**

- **appcenter_release_id** – идентификатор загружаемого релиза в системе AppCenter для конкретного приложения. Возможно выставить значение latest – тогда будет загружен последний доступный релиз приложения.
- **appcenter_app_version** – при указании данного параметра будет найдена и скачана конкретная версия приложения по коду его версии (указанной в Android Manifest) (поле version в документации).

Примеры запуска

HockeyApp по public_identifier и с последней доступной версией

Для запуска анализа последней версии приложения из системы **HockeyApp** по его публичному идентификатору:

```
python3.6 run-stingray-scan.py --distribution_system "appcenter" --appcenter_token
"18bc81146d374ba4b1182ed65e0b3aaa" --appcenter_owner_name "stingray_test_org_or_user"
--appcenter_app_name "Stingray_debug_version_of_test" --appcenter_release_id 710 --stingray_url
"https://saas.mobile.appsec.world" --profile 2 --testcase 3 --token
"eyJ0eXA4OiJKA1QiLbJhcGciO5JIU4I1NiJ1.eyJzdaJqZWNcX2lkIj53LCJle5AiOjf1OTM5OTU3MjB1.hfI6c
4VN_U2mo5VfRoENPvJCvpxhLzjHqI0gxqgr2Bs"
```

В результате в системе **HockeyApp** будет найдено приложение с уникальным публичным идентификатором **1234567890abcdef1234567890abcdef** и последней доступной версией. Файл приложения будет скачен и для него будет проведен автоматизированный анализ с профилем с **id 2** и будет запущен автотест с **id 3**.

AppCenter по id релиза

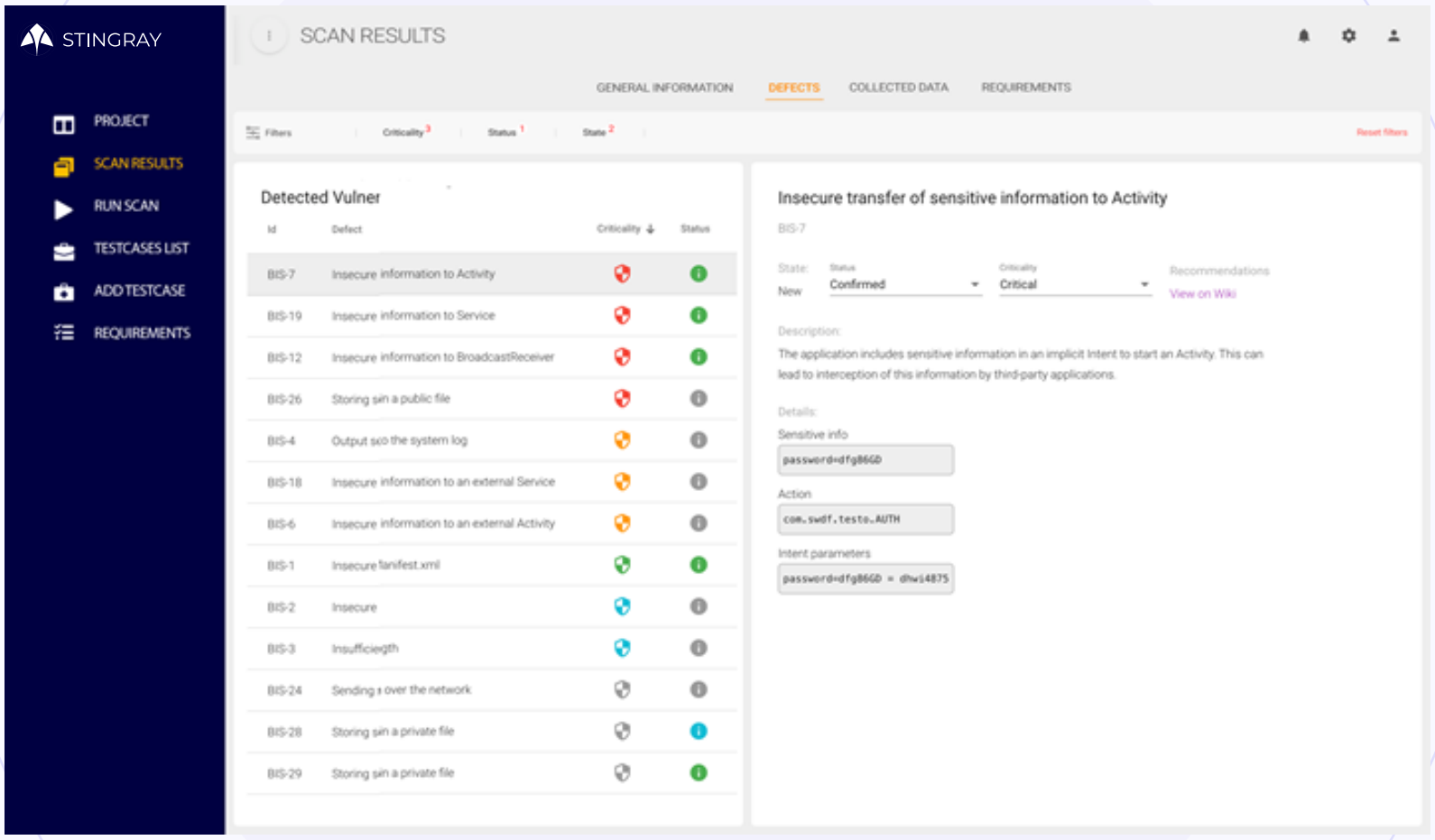
Для запуска анализа приложения по известному имени, владельцу и ID релиза необходимо выполнить следующую команду:

```
python3.6 run-stingray-scan.py --distribution_system "hockeyapp" --hockey_token
"18bc81146d374ba4b1182ed65e0b3aaa" --public_id "1234567890abcdef1234567890abcdef"
--stingray_url "https://saas.mobile.appsec.world" --profile 2 --testcase 3 --token
"eyJ0eXA4OiJKA1QiLbJhcGciO5JIU4I1NiJ1.eyJzdaJqZWNcX2lkIj53LCJle5AiOjf1OTM5OTU3MjB1.hfI6c
4VN_U2mo5VfRoENPvJCvpxhLzjHqI0gxqgr2Bs"
```

В результате у владельца (пользователя или организации **test_org_or_user**) будет найдено приложение **Stingray_debug_version_of_test** с ID релиза **710**. Данная версия релиза будет загружена и передана на анализ безопасности в **Stingray**.
Для загрузки релиза с последней версией необходимо указать параметр **appcenter_release_id = latest**. Тогда команда будет выглядеть следующим образом:

```
python3.6 run-stingray-scan.py --distribution_system "appcenter" --appcenter_token
"18bc81146d374ba4b1182ed65e0b3aaa" --appcenter_owner_name "stingray_test_org_or_user"
--appcenter_app_name "Stingray_debug_version_of_test" --appcenter_release_id latest
--stingray_url "https://saas.mobile.appsec.world" --profile 2 --testcase 3 --token
"eyJ0eXA4OiJKA1QiLbJhcGciO5JIU4I1NiJ1.eyJzdaJqZWNcX2lkIj53LCJle5AiOjf1OTM5OTU3MjB1.hfI6c
4VN_U2mo5VfRoENPvJCvpxhLzjHqI0gxqgr2Bs"
```

Результатом выполнения будет загрузка и автоматический анализ последнего доступного релиза для указанного приложения.



При возникновении любых вопросов, связанных со сканированием или возможными ошибками, пришлите нам снимок экрана с появившейся ошибкой или результатами сканирования и опишите последовательность действий, которая привела к этому.

О компании Stingray

В Stingray работает профессиональная команда экспертов по безопасности мобильных приложений, готовых помочь в выявлении нестандартных уязвимостей в ваших приложениях, которые потребовали бы существенных затрат при обычном ручном анализе.

Продуктовая команда Stingray является одной из самых высококвалифицированных в отрасли кибербезопасности и обладает богатым опытом и знаниями в разработке и тестировании мобильных приложений. Чтобы узнать больше об услугах анализа безопасности мобильных приложений, автоматизации этого процесса и других возможных опциях, заполните контактную форму на сайте и мы обязательно с вами свяжемся.

Контактная информация

+7 916 287 72 78
stingray@appsec.global

Адрес:
121205, Москва,
территория Сколково инновационного центра,
улица Нобеля, дом 5, этаж 1, помещение 5,
рабочее место 4.