Наливайте чай/кофе
Скоро начинаем!

Начало вебинара в 12:00 (мск)

Rostelecom
Solar

Спикер вебинара

Сергей Деев

Менеджер продукта appScreener

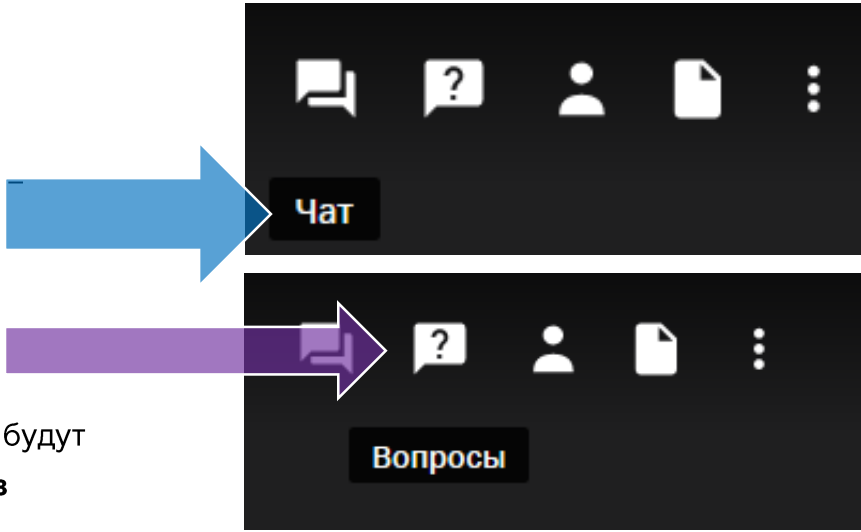
Центр разработки решений по контролю безопасности ПО «Ростелеком-Солар»

s.deev@rt-solar.ru

Rostelecom Solar

Организационные детали

- Длительность вебинара – **1 час**
- Если вы хотите пообщаться с другими участниками вебинара, – **добро пожаловать в чат!**
- Свои вопросы спикерам мероприятия просьба задавать **в специальном разделе «Вопросы»**
- Запись вебинара, презентации спикеров и другие материалы будут отправлены участникам на указанные при регистрации email **в течение 2–3 дней после мероприятия**



Rostelecom
Solar

Solar appScreener

Анализ кода приложений при выполнении требований Банка России 683-П и 684-П

Деев Сергей
менеджер продукта appScreener
s.deev@rt-solar.ru

Rostelecom
Solar

Сегодня мы поговорим...

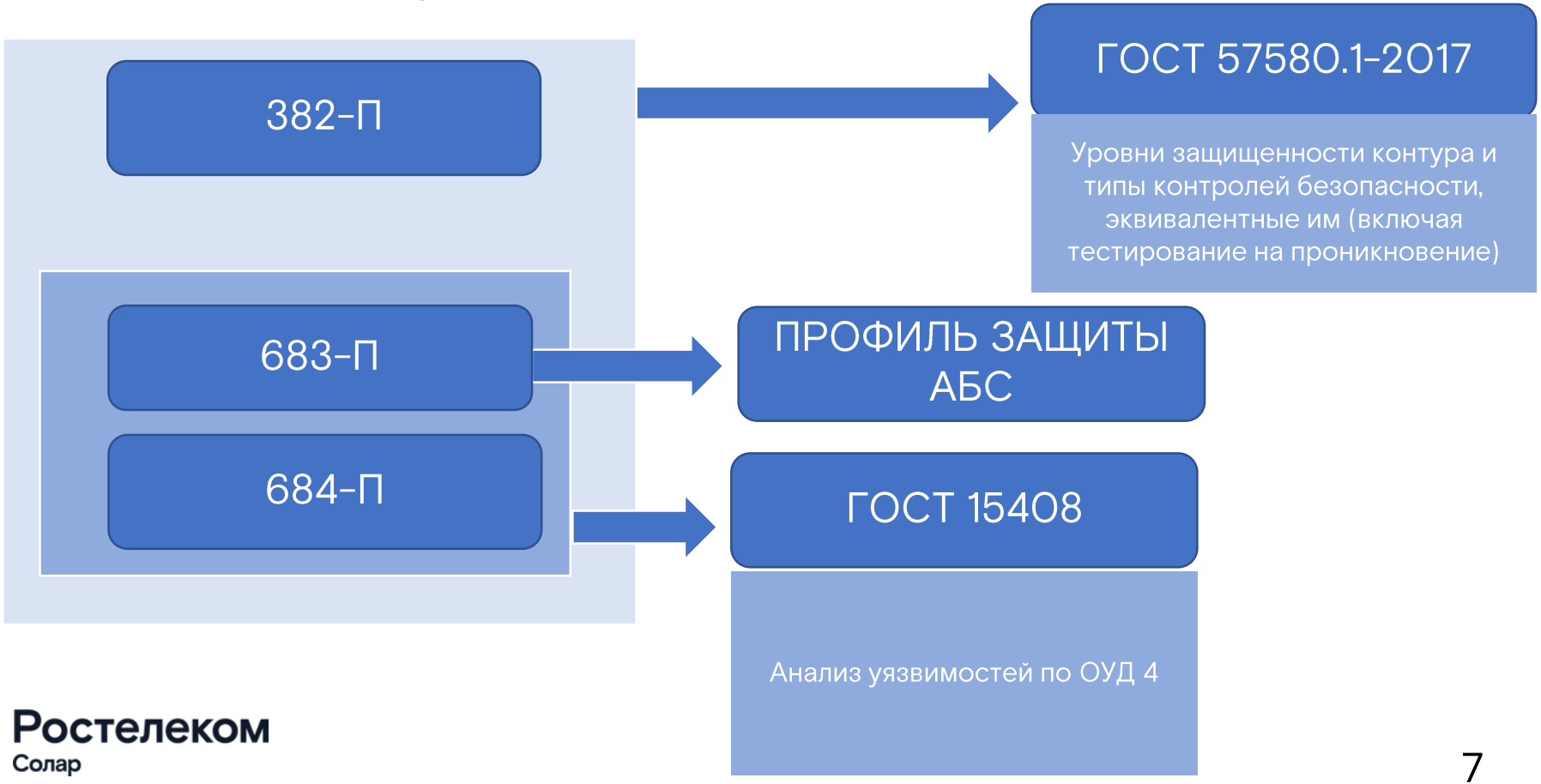
- О безопасности финансовых организаций: анализируем и разбираем ключевые аспекты
- Почему важен контроль безопасности в организациях финансового сектора?
- Что возможно выявить с помощью анализа кода?
- Об оценке ПО по ГОСТ Р ИСО/МЭК 15408 и сертификации на отсутствие НДВ
- Solar appScreener – современный инструмент анализа кода и выявления уязвимостей
- Ответим на ваши вопросы!

Rostelecom
Solar

Роль требований регулятора в деятельности организаций по обеспечению ИБ

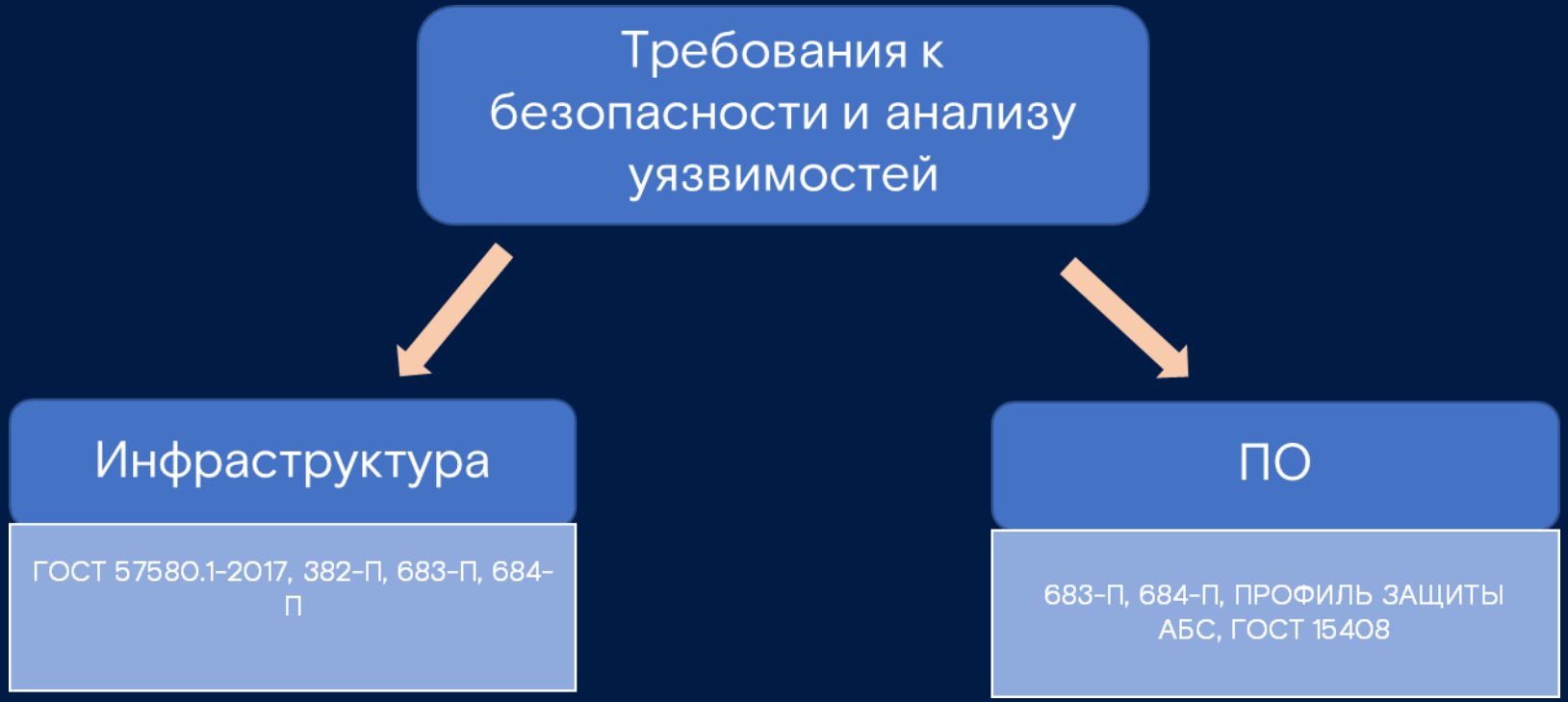
Ростелеком
Солар

Роль НПА при аудите БР



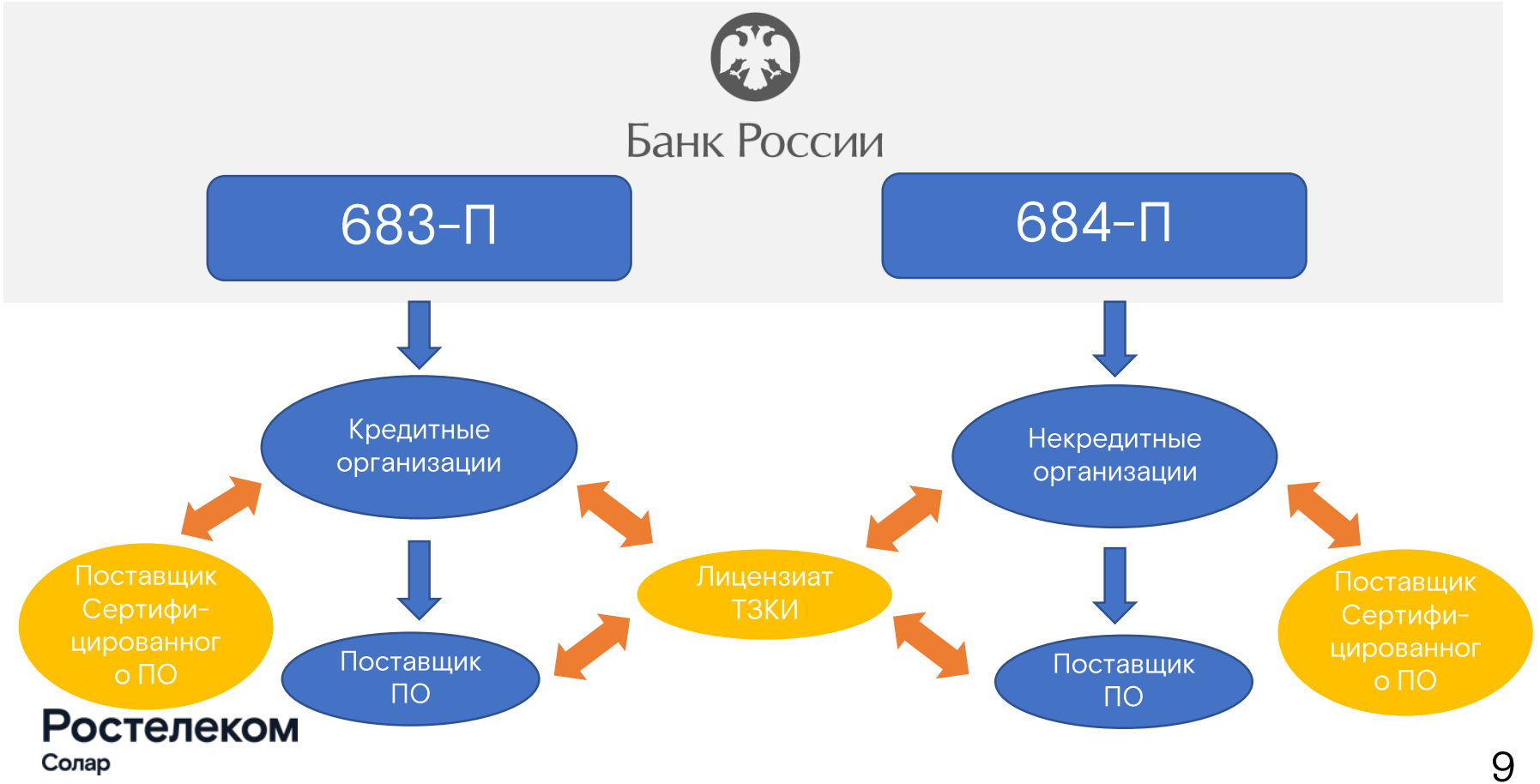
Ростелеком
Солар

Требования БР к безопасности



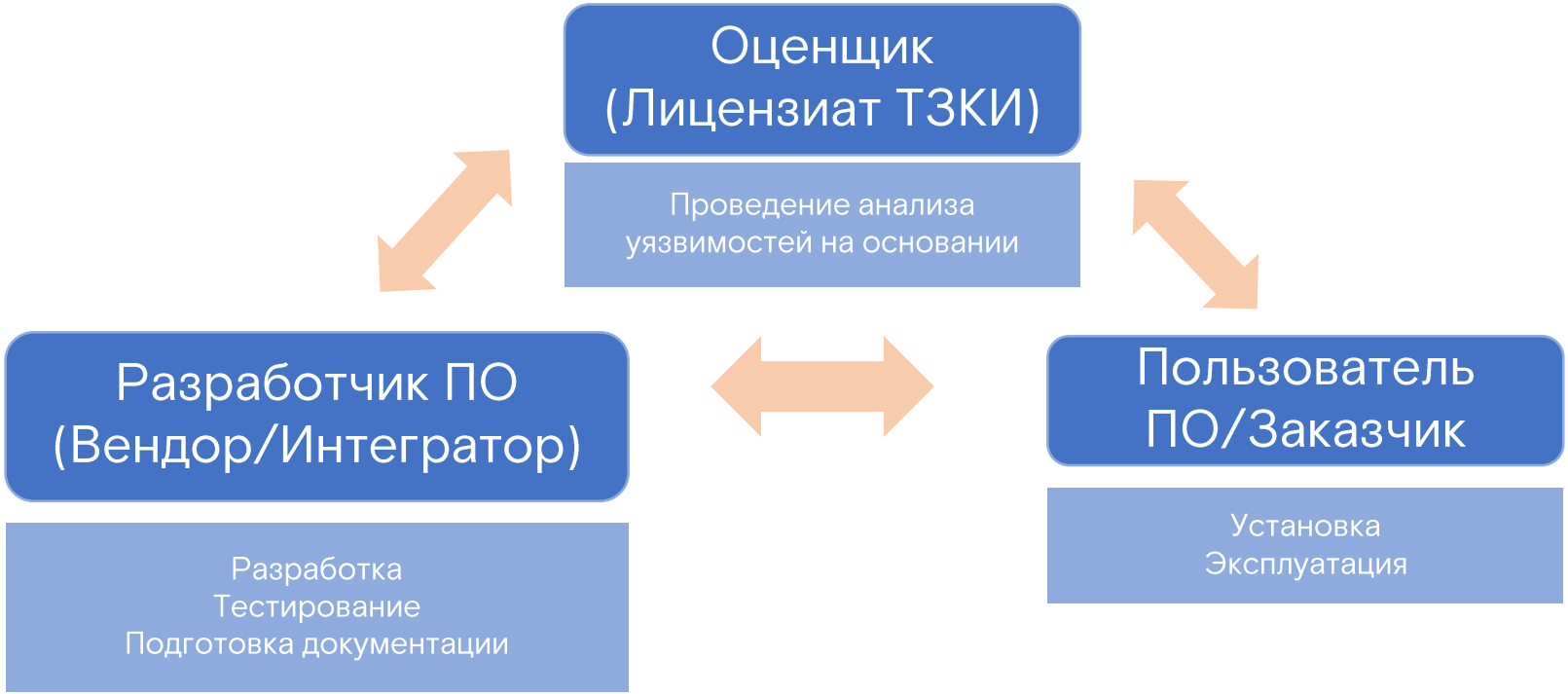
Ростелеком
Солар

Организации, подотчетные БР



Ростелеком
Солар

Роли при оценке защищенности



Ростелеком
Солар

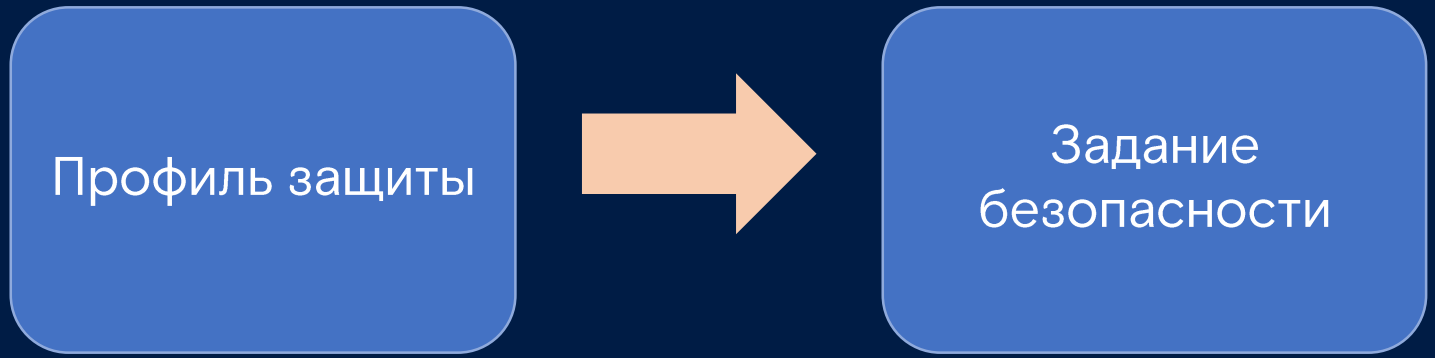
Что передает Разработчик для оценки

Описание архитектуры безопасности

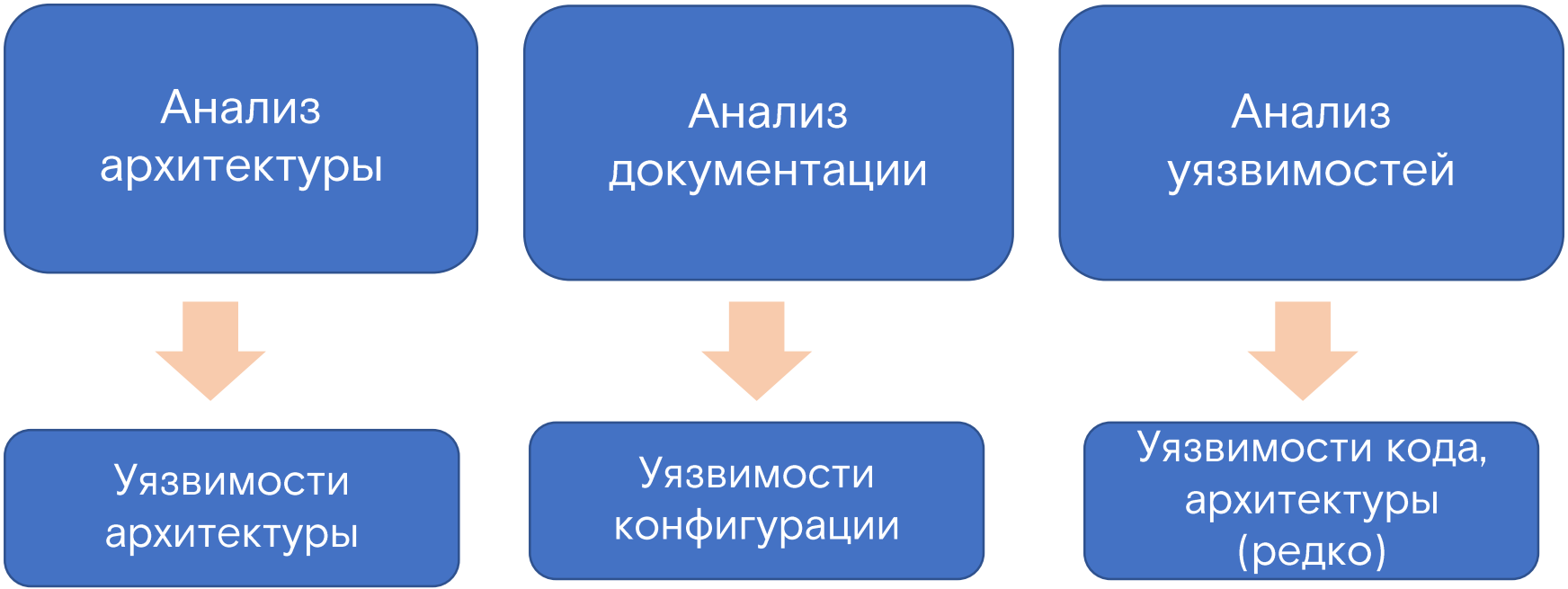
Пользовательскую и проектную документацию

Исходный код, экземпляр ПО

Описание архитектуры безопасности (выполняет разработчик ПО)



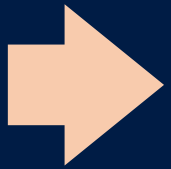
Типы контроля
(Выполняет оценщик/Лицензиат ФСТЭК)



Ростелеком
Солар

Критерии оценки

Функции безопасности и условия доверия



Оценочный уровень доверия

Ростелеком
Солар

Оценка по общим критериям

Классы требований к функциям безопасности (15408-2)

FAU (аудит безопасности)
FCO (связь)
FDP (защита данных пользователя)
FIA (идентификация и аутентификация)
FPR (секретность)
FPT (защита функций безопасности)
FRU (использование ресурса)
FTA (доступ к ОО)
FTP (надежный маршрут/канал)

Классы требований доверия (15408-3)

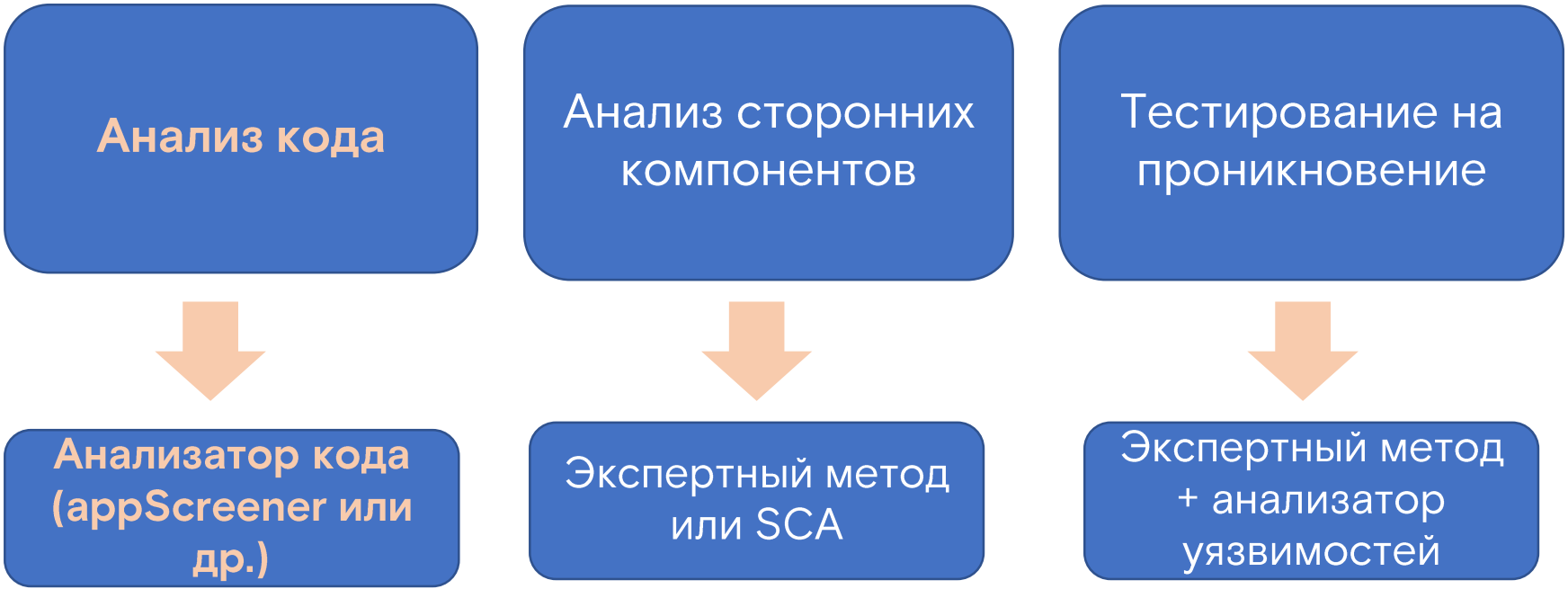
ACM (управление конфигурацией)
ADO (поставка и эксплуатация)
ADV (разработка)
AGD (руководства)
ALC (поддержка жизненного цикла)
ATE (тестирование)
AVA (оценка уязвимостей)

Оценочные уровни доверия

ОУД 1 - функционально проверенный проект
ОУД 2 - структурно проверенный проект
ОУД 3 - методически проверенный и оттестированный проект
ОУД 4 - методически разработанный и проверенный проект
ОУД 5 - полуформально разработанный и проверенный проект
ОУД 6 - полуформально верифицированный и проверенный проект
ОУД 7 - формально верифицированный и проверенный проект

Ростелеком
Солар

Анализ уязвимостей ПО (Выполняет оценщик/Лицензиат ФСТЭК)

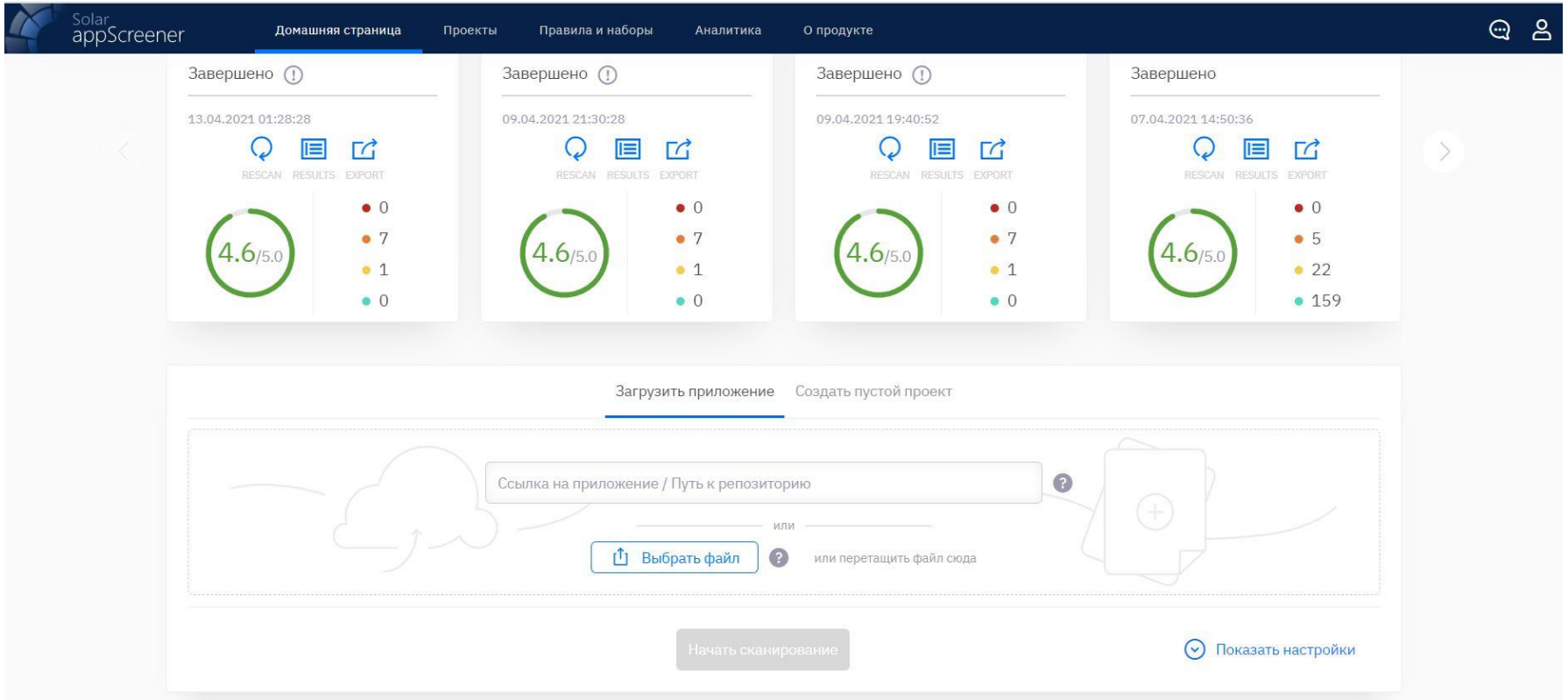


Ростелеком
Солар

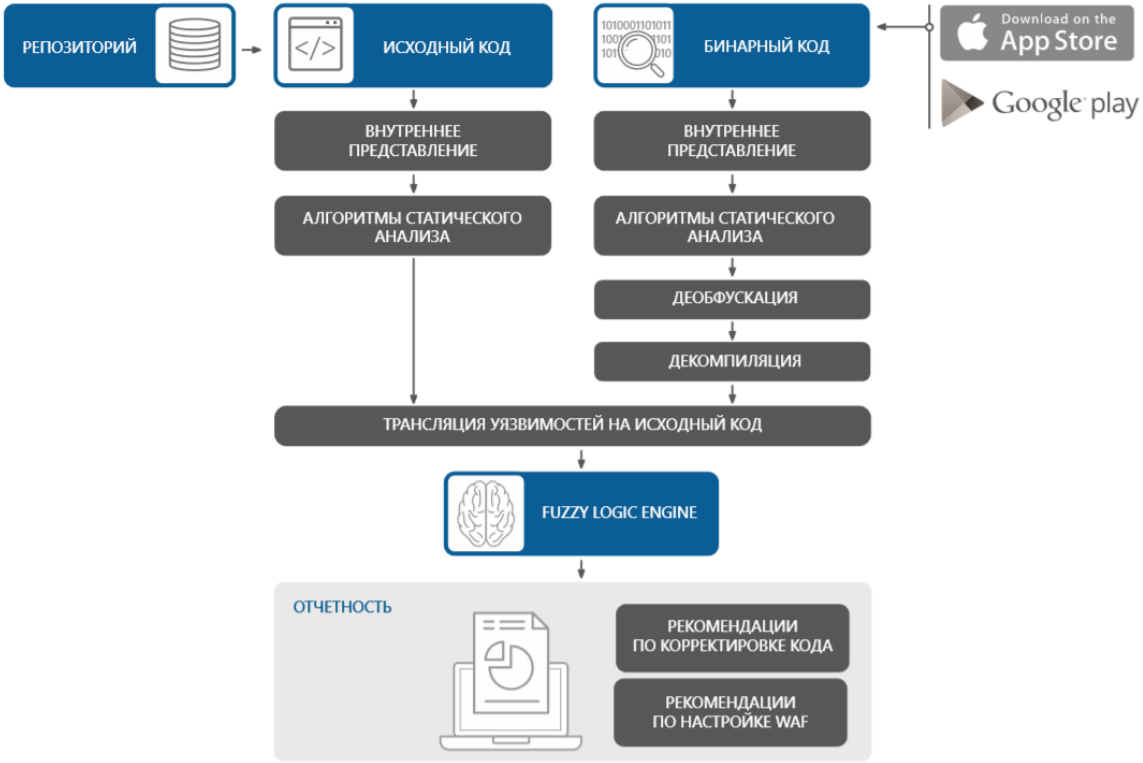
Роль статического анализа

Ростелеком
Солар

Графический интерфейс

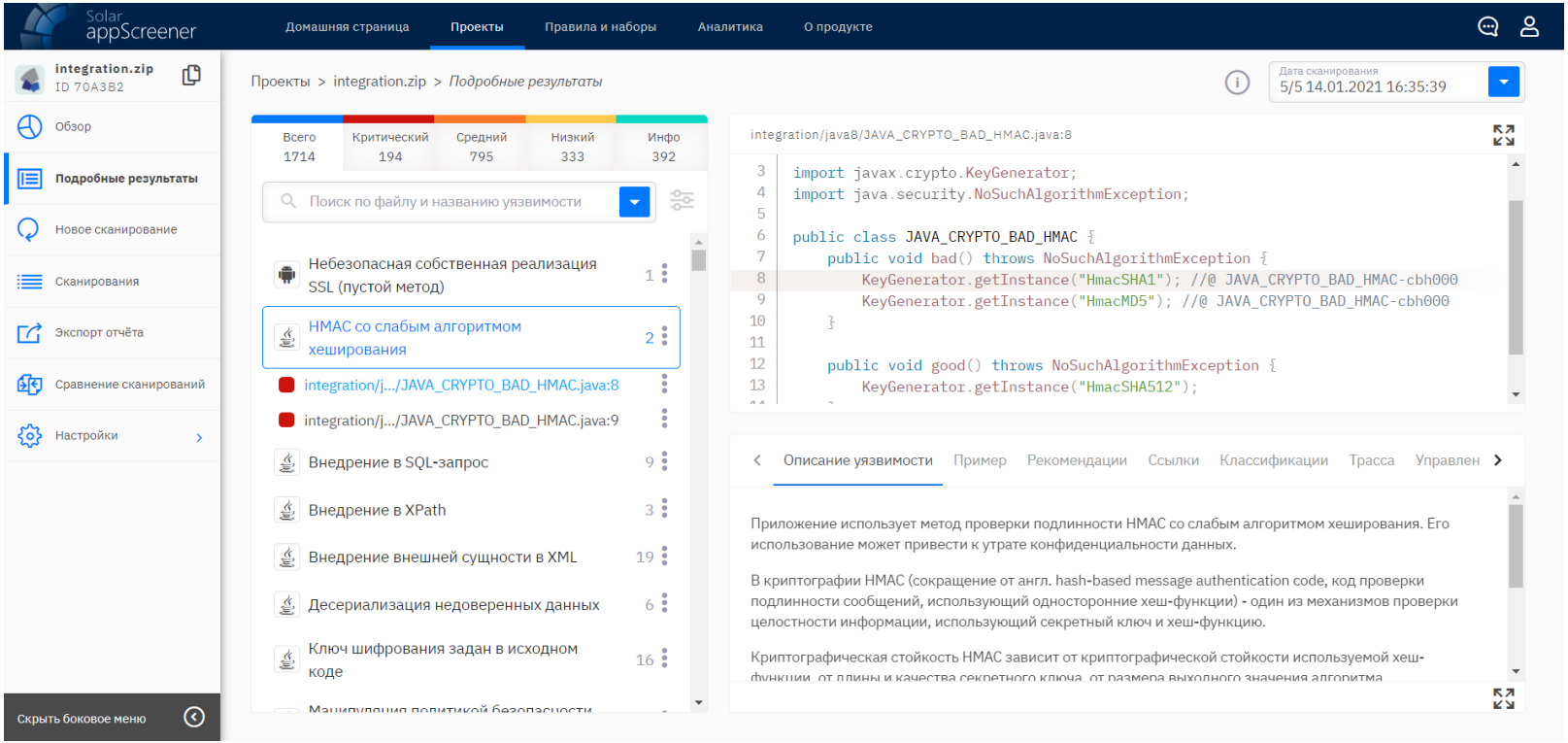


Принцип работы



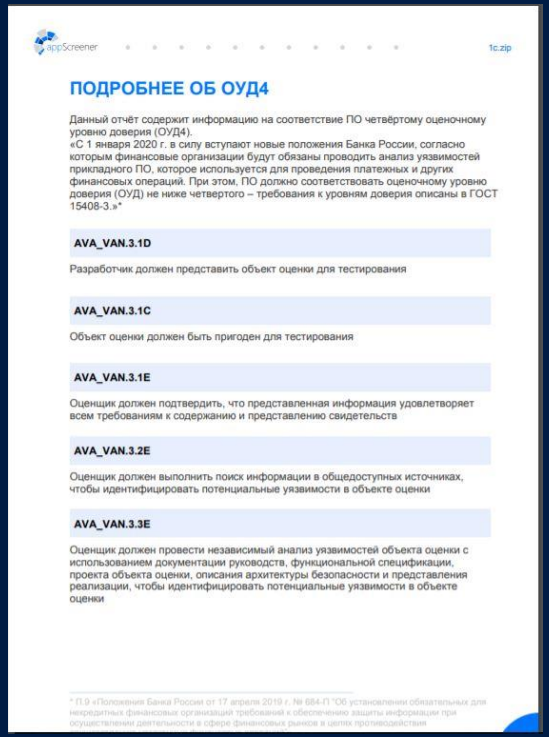
Результаты анализа

Реализован в виде **веб-сервиса.** Соединение защищено с помощью протокола **HTTPS**



Ростелеком
Солар

Отчет по ОУД4



appScreener 1c.zip

ПОДРОБНЕЕ ОБ ОУД4

Данный отчёт содержит информацию на соответствие ПО четвёртому оценочному уровню доверия (ОУД4).
«С 1 января 2020 г. в силу вступают новые положения Банка России, согласно которым финансовые организации будут обязаны проводить анализ уязвимостей прикладного ПО, которое используется для проведения платежных и других финансовых операций. При этом, ПО должно соответствовать оценочному уровню доверия (ОУД) не ниже четвертого – требования к уровням доверия описаны в ГОСТ 15408-3.»*

AVA_VAN.3.1D

Разработчик должен представить объект оценки для тестирования

AVA_VAN.3.1C

Объект оценки должен быть пригоден для тестирования

AVA_VAN.3.1E

Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств

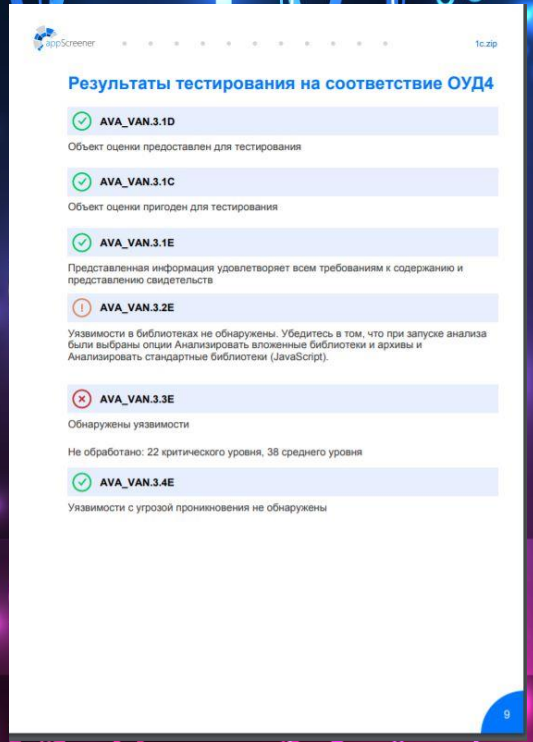
AVA_VAN.3.2E

Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в объекте оценки

AVA_VAN.3.3E

Оценщик должен провести независимый анализ уязвимостей объекта оценки с использованием документации руководств, функциональной спецификации, проекта объекта оценки, описания архитектуры безопасности и представления реализации, чтобы идентифицировать потенциальные уязвимости в объекте оценки

* П.9 «Положения Банка России от 17 апреля 2019 г. № 684-П "Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия



appScreener 1c.zip

Результаты тестирования на соответствие ОУД4

AVA_VAN.3.1D

Объект оценки предоставлен для тестирования

AVA_VAN.3.1C

Объект оценки пригоден для тестирования

AVA_VAN.3.1E

Представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств

AVA_VAN.3.2E

Уязвимости в библиотеках не обнаружены. Убедитесь в том, что при запуске анализа были выбраны опции Анализировать вложенные библиотеки и архивы и Анализировать стандартные библиотеки (JavaScript).

AVA_VAN.3.3E

Обнаружены уязвимости

Не обработано: 22 критического уровня, 38 среднего уровня

AVA_VAN.3.4E

Уязвимости с угрозой проникновения не обнаружены

9

Ростелеком
Солар

Анализ бинарного кода – 9 форматов файлов

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

Приложение будет **автоматически:**

1. Скачано
2. Декомпилировано и деобфусцировано
3. Проверено

Ростелеком
Солар

Анализ исходного кода – 36 языков

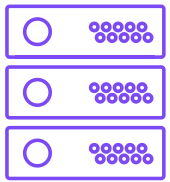
appScreener соответствует требованиям к отечественному ПО

1 Включен в Единый реестр отечественного ПО

2 Проходит сертификацию ФСТЭК России

Ростелеком
Солар

Лицензирование и поставка



Установка на собственный сервер (On-premise)

- Лицензирование осуществляется по количеству пользователей, которые имеют доступ к системе
- Подходит при необходимости постоянного анализа ПО (крупные вендоры и компании)

Сервис из облака «Ростелеком-Солар» (SaaS)

- Оплачивается количество произведенных проверок
- Подходит, если потребность в проверке приложений возникает время от времени (небольшие вендоры, использование заказного ПО, «перестраховка»)

Ростелеком
Солар

Возможности интеграции

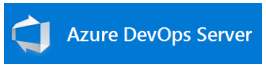
Репозитории

VCS-хостинги

Средства разработки

Средства сборки

Серверы CI/CD



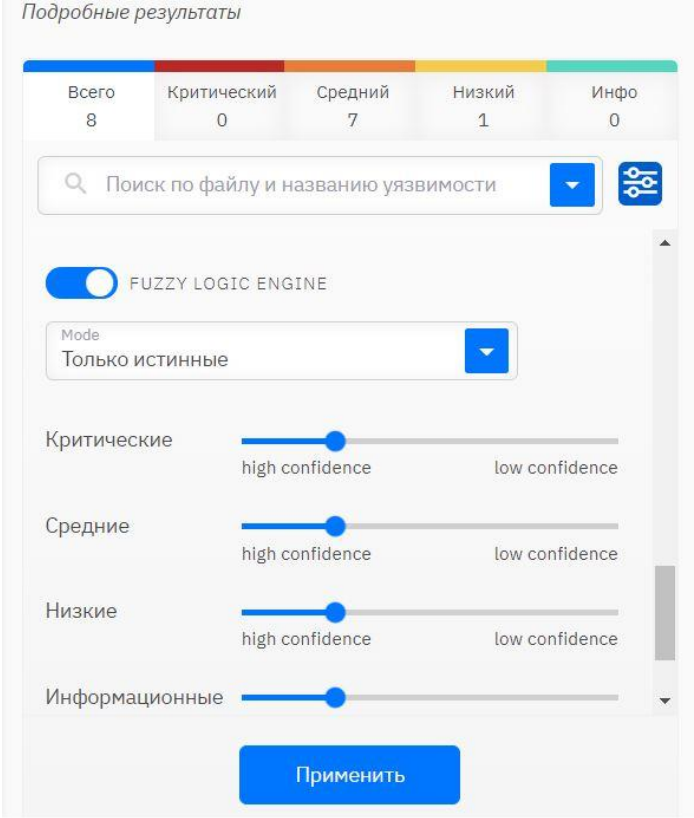
Отслеживание задач

Анализ кода

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

Ростелеком
Солар

Гибкая настройка выводимых результатов об уязвимостях



Ростелеком
Солар

Контроль безопасности ПО как часть безопасности организации

На основе Solar appScreener можно реализовывать проекты по внедрению практик безопасной разработки. Отдельным примером таких практик может служить построение **Центра контроля безопасности ПО (ЦКБ ПО)**

Услуга ЦКБ ПО = Безлимитная лицензия Solar appScreener + Аудит процессов разработки ПО +

Разработка ролевой модели + Адаптация методологии анализа ПО и обучение + Запуск процесса непрерывного анализа ПО

Ростелеком
Солар

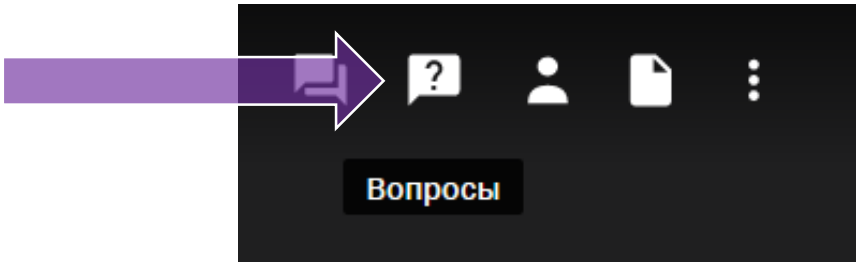
Попробуй Solar appScreener!

Как возможно познакомиться с решением?

1. Получить доступ к демостенду Solar appScreener, написав на presale@rt-solar.ru
2. Совместно оценить потребности организации в анализе кода
3. Инициировать пилотный проект
4. Успешно реализовать пилот

Ростелеком
Солар

Ваши вопросы?



Сергей Деев
Менеджер продукта appScreener
s.deev@rt-solar.ru

Rostelecom
Solar

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Ростелеком
Солар