

Компонентный анализ программного обеспечения

SCA — фундамент безопасности
информационных систем

Алексей Смирнов
CodeScoring

DevSecOps #4, 22 марта 2022



whoami & howeare



Алексей Смирнов, основал profiscope.io

- проводим технический аудит
- выпускаем [CodeScoring](#) — первый российский SCA
- просвещаем в Code Mining [@ods.ai](#), tg: [@codemining](#)
 - 3 года ведем конференцию про анализ кода
 - делаем бесплатные курсы
 - публикуемся и выступаем

SNGGIDGERDCCDG
CSECGDNRREG
CGEEIICC
GICERGRNCGNCC
DINIECD CSC
NGRGINGCRC
EC CGIESEESGISR
DGC DG GCORNI
GGIDIGSCRC
NNRC DINIICC
EEECICNGRRRID
DSDCESGSCCCN
SSRGCSDRCC
SEERIRISSN
SRRRNRDDC
NE SERRR
CIRIDSIEENNS
ECNRCCCGCICGI
SCCECORISRN
DCCCD DCDR

Проблематика

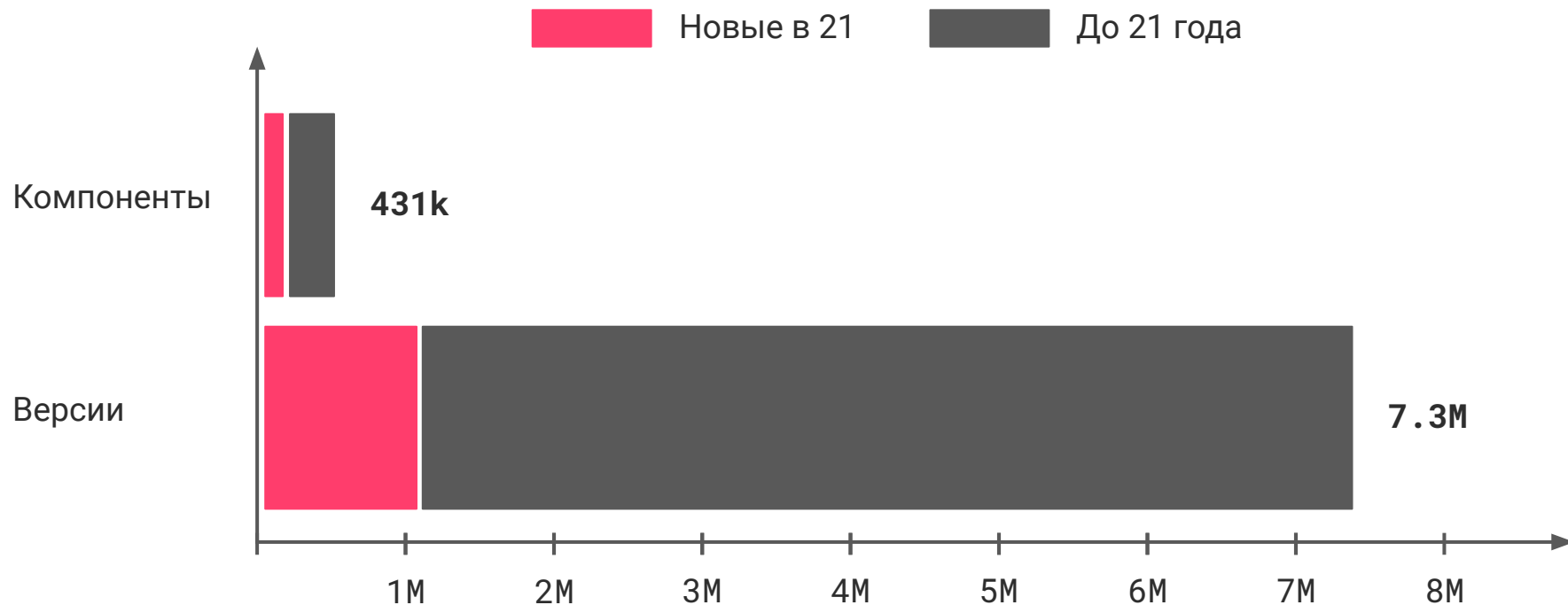
Open Source это благо и его очень много



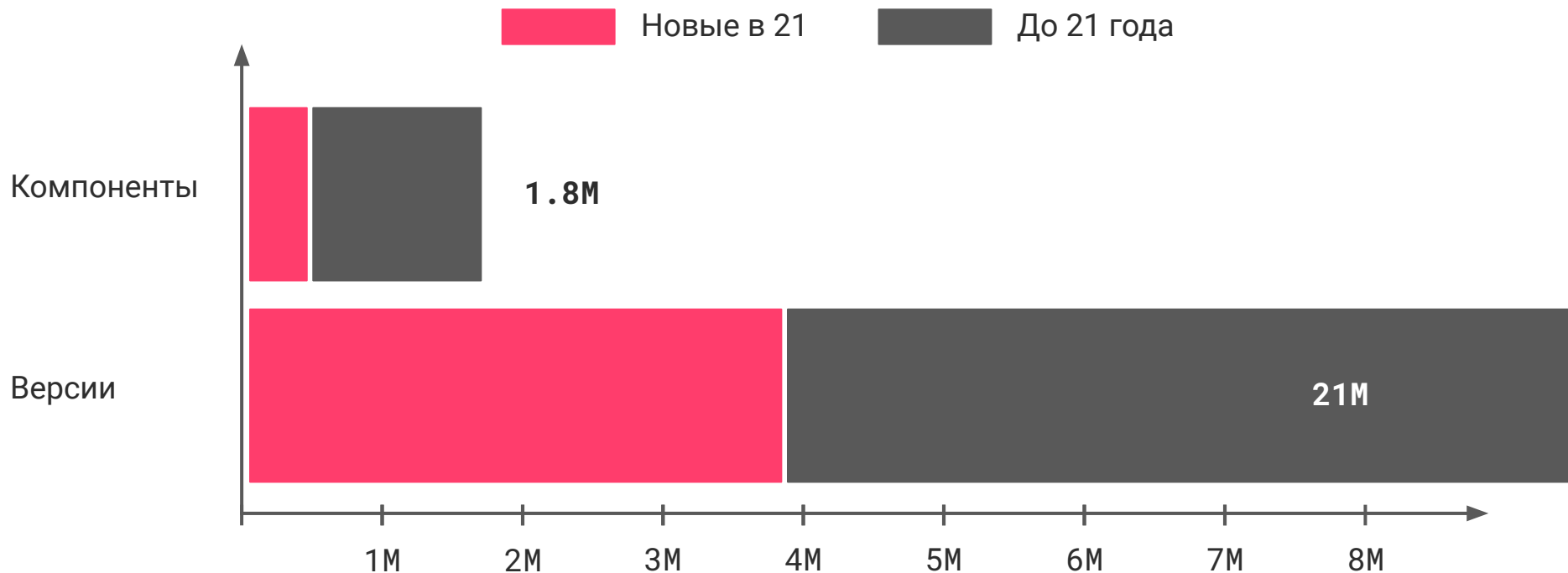
>200 млн.

Мировая база проектов с открытым кодом
от 70+ млн. разработчиков

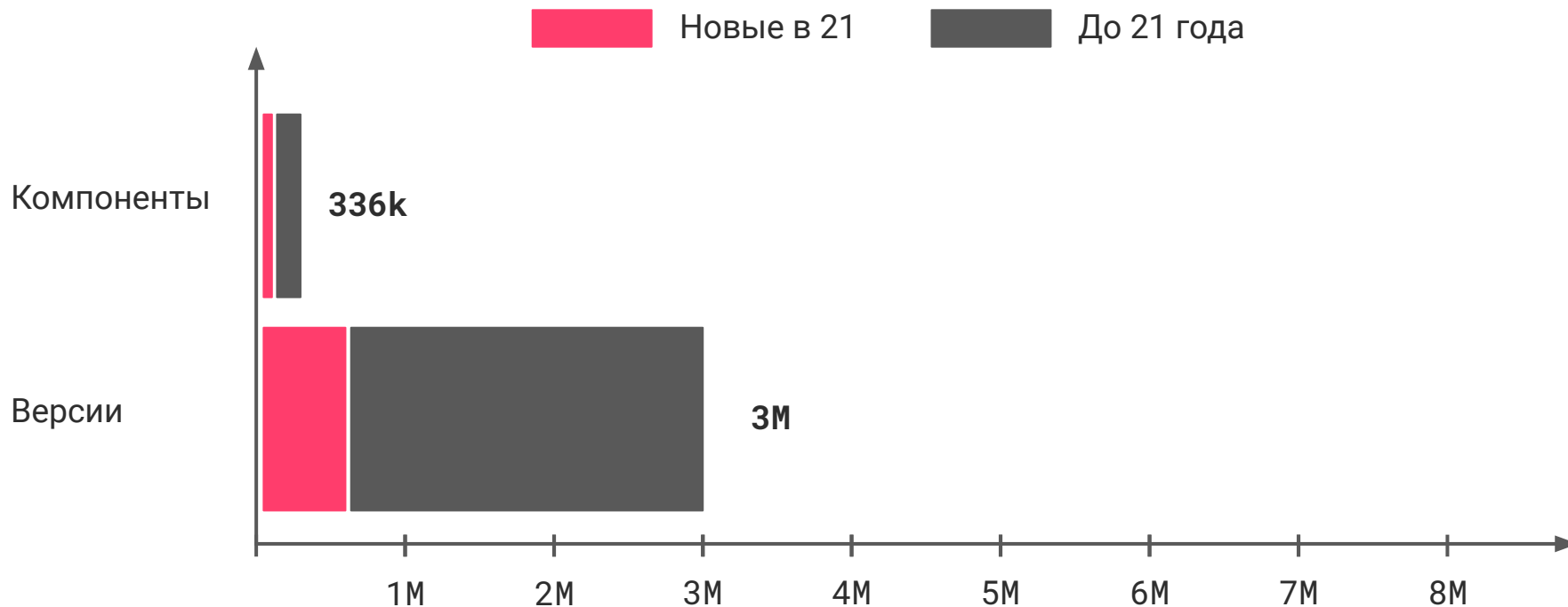
Рост Open Source'21 | Java



Пост Open Source'21 | JavaScript



Рост Open Source'21 | Python



на 72 %

выросло скачивание OSS компонент с 2020 по 2021 год

Supply chain attacks



x13

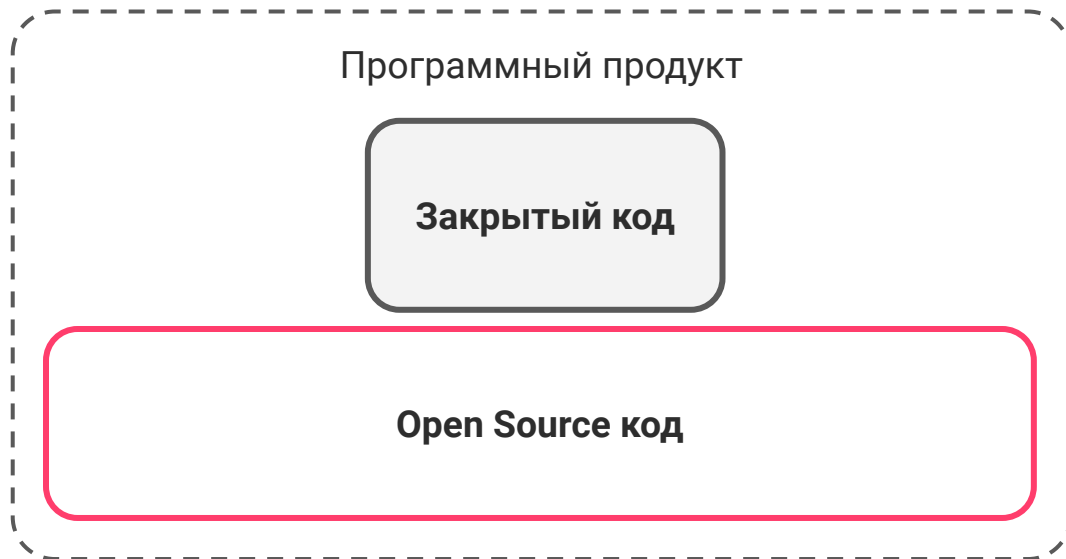
929 в 2020 году против 12k в 2021 году:
Dependency Confusion, Typosquatting, and Malicious Code Injection

Как правило,



OSS > Proprietary

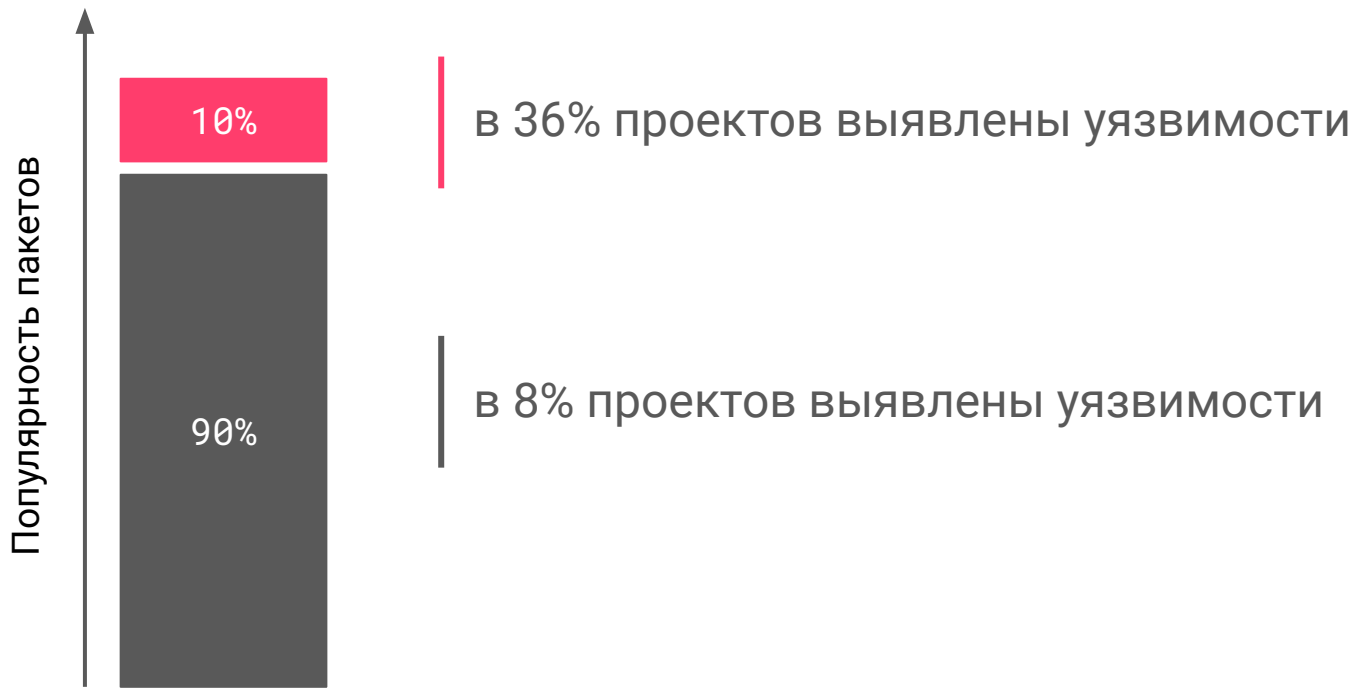
Как выглядит ваш продукт для «третьих» лиц



Неизвестен
Нужно сканировать
Сложно исследовать

Известен
Идентифицируем
Исследуем

Популярность не только у пользователей



Open Source небезопасен



- **Уязвимости**

Появляются каждый день. На многие уязвимости есть эксплоит на GitHub. Время подготовки атаки существенно сократилось.

- **Лицензии**

Их отсутствие, лицензионная (не)совместимость, риск смены лицензии на более строгую, риск введения экспортных ограничений.

- **Закладки**

Появление компонентов с вредоносными, особенно в последний месяц.

SNGGIDGERDCCDG
CSECGDNRG
CGEIIIDCC
GICRGRNCGNCC
DINIECD CSC
NGRGINGCRC
EC CGIESEESGISR
DGC DG GCRNI
GGIDIGSCRC
NNRC DINIIC
EEECICNGRRIDI
DSDCESGS CC CN
SSRG CSDRCC
SEERIRISSN
SRRRNRDDC
NE SERRRD
CIRIDS IENNS
ECNRCCCGCICGI
SCCECORISRN
DCCCD DCDR

Решение

Software Composition Analysis, SCA



Процесс определения компонентов,
составляющих программное обеспечение.

SCA инструменты помогают в управлении рисками,
связанными с безопасной разработкой.

Встраивание в жизненный цикл



Инструменты компонентного анализа могут применяться на различных этапах разработки программного обеспечения:

- проверка компонент добавляемых в проекты прямо сейчас (Shift Left)
- проверка сборок проектов в рамках CI/CD-конвейера
- непрерывное (continuous) отслеживание рисков в выпущенном ПО
- обеспечение приемки от подрядчика
- публикация в Inner Source / Open Source

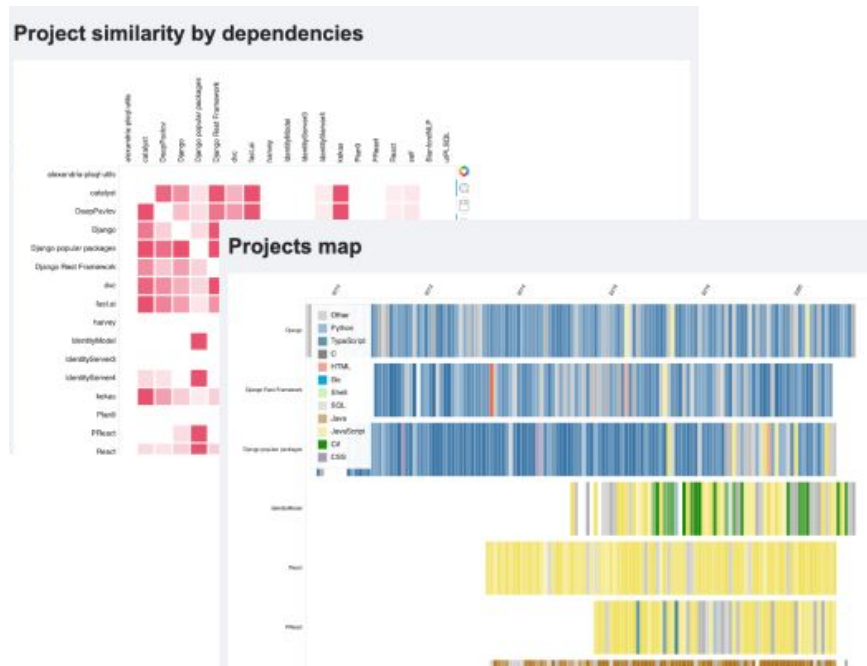
Базовая функциональность SCA



- композиционный анализ
- построение Software Bill of Materials (SBOM)
- определение уязвимостей и лицензий в open source компонентах
- оценка совместимости лицензий
- политики отслеживания рисков
- интеграция в CI/CD, Jira, почтовые уведомления

Инвентаризация ПО

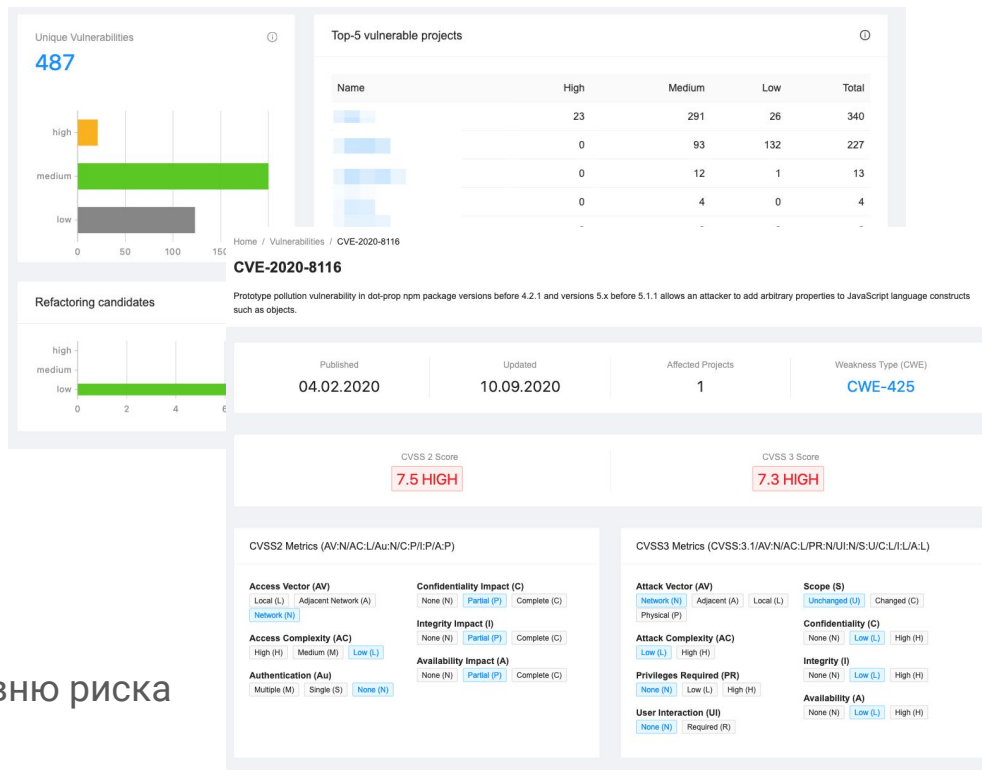
- Ведение реестра компонентных связей проектов (SBoM)
- Автообнаружение зависимостей
 - по файлам конфигураций (манифестам)
 - включений OSS
 - по мета-данным (хэшам): md5, sha1, sha2
- Отчеты:
 - Списки проектов
 - Карта всех проектов
 - Компонентный состав всех проектов
 - Компонентная база проекта
 - Матрица связей проектов



Уязвимости

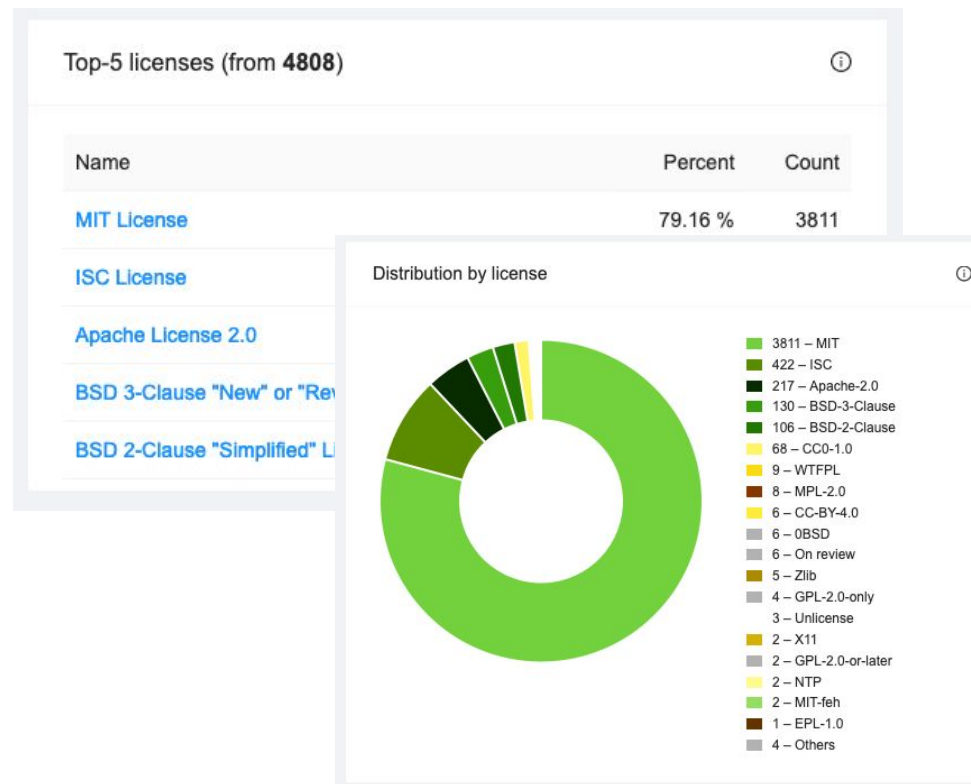


- Выявление уязвимостей: CVE, GHSA и т. п.
- Рекомендации по исправлению
- Ведение базы уязвимостей
- Классификация: CVSS2, CVSS3
- Автоматическое обновление
- Отчеты:
 - Новые уязвимости
 - Уязвимости по проектам
 - Уязвимости по компании
 - Наиболее уязвимые проекты
 - Распределение уязвимостей по уровню риска



Лицензии

- Определение лицензий
- Лицензионная совместимость компонент (license compliance)
- Ведение реестра лицензий
- Автоматическое обновление
- Отчеты:
 - Лицензионный состав проекта
 - Лицензионный состав всех проектов
 - Нарушения политик лицензирования
 - Лицензии по группам
 - База лицензий



Политики уведомлений



- Гибкая настройка политик
- Настройка отправки уведомлений:
 - выбор отчета для отправки
 - отправка по событию
 - выбор адресатов
- Отправка уведомлений на почту и в менеджер задач
- Отчеты:
 - нарушения политик по компании
 - нарушения политик по продукту
 - журнал сработки политик

Edit policy

Name: Vendor compliance policy

Scope: Project

Proprietor: OSS

Project:

Home / Policy Alerts

Policy Alerts [Export](#)

Event Repository Project Created

Start date End date

[Filter](#)

Actions Total 3 items [@](#) [1](#) 25 / page

By default all policies

Send email

Email

hello@codescoring

Scope	Event	Project	Repository	Event payload	Created
Project	Incompatible license found			Category: Copyleft License: GPL-2.0-only Dependency: fraction.js@4.1.1	20.08.2021 12:57
Project	Incompatible license found			Category: Copyleft License: GPL-2.0-or-later Dependency: fraction.js@4.0.13	20.08.2021 12:57
Project	Incompatible license found			Category: Copyleft License: GPL-2.0-or-later Dependency: fraction.js@4.1.1	20.08.2021 12:57

Total 3 items [@](#) [1](#) 25 / page

IF This

- Нарушена лицензионная чистота (найдена неподходящая лицензия)
- Найдена критическая уязвимость
- Найден компонент из Blacklist
- Появилась новая технология

Then

Тогда

Тогда

Тогда

Тогда

That

Поставить задачу на замену библиотеки и уведомить юристов

Заблокировать сборку, поставить задачу на третью линию

Заблокировать компонент

Уведомить Tech & HR

**Кто из разработчиков
может исправить
проблему?**

SNGGIDGERDCCDG
CSECGDNRG
CGEIIIDCC
GICERGRNCGNCC
DINIECD CSC
NGRGINGCRC
EC CGIESEESGISR
DGC DG C RNI
GGIDIGSCRC
NNRC DINIIC
EEECICNGRRIDI
DSDCESGS CC CN
SSRG CSDRCC
SEERIRISSN
SRRRNRDDC
NE SERRR
CIRIDS IENNS
ECNRCCCGCICGI
SCCECORISRN
DCCCD DCDR

Заклучение

SCA обеспечивает



Быструю, важную и **понятную** ценность:

- компонентный состав, включая OSS-заимствования
- информированность об уязвимостях в фундаменте
- понимание лицензионной чистоты
- регулярный контроль ситуации
- понимание, что с этим делать дальше

SAST, DAST & SCA



Спасибо за внимание

alexey@codescoring.ru

codescoring.ru