CODE SCORING

КСБ-СОФТ

Безопасное применение Open Source

О процессах и инструментах

Алексей Смирнов, Основатель CodeScoring

Степан Харитонов, Руководитель направления безопасной разработки КСБ-СОФТ

CODE SCORING

КСБ-СОФТ

План вебинара

- Актуальная проблематика
- Способы решения
- Кейсы
- Ответы на вопросы

Обменивайтесь сообщениями во вкладке «Чат»

Запись вебинара направим всем участникам на указанный при регистрации e-mail

Задавайте вопросы во вкладке «Вопросы»

За лучший вопрос подарим корпоративный мерч

Чаще всего, ваш продукт выглядит так:

CODE SCORING

КСБ-СОФТ

Сторонний код	Собственный код
~80% заимствованных компонентов из открытых источников	~20% собственного кода
Известен	Неизвестен
Идентифицируем	Нужно сканировать
Исследуем	Сложно исследовать

CODE SCORING

КСБ-СОФТ

Сторонние компоненты — ваши компоненты

Практически все открытые лицензии содержат уведомление об отказе от ответственности и гарантий

Немного статистики про сторонний код

CODE SCORING

КСБ-СОФТ

> 250 млн

проектов с открытым исходным кодом, а также:
8 млн. готовых пакетов;
100 млн. их версий

~90 млн

разработчиков хотя бы раз поучаствовали в разработке, а регулярно участвует ~6 млн.

protestware

саботаж и закладки
Пакеты: es5-ext, node-ipc, colors, faker, и ещё немного.
И Палестина.

x2.5

увеличилась скачиваемость открытых компонентов с 2022 на 2023

x13

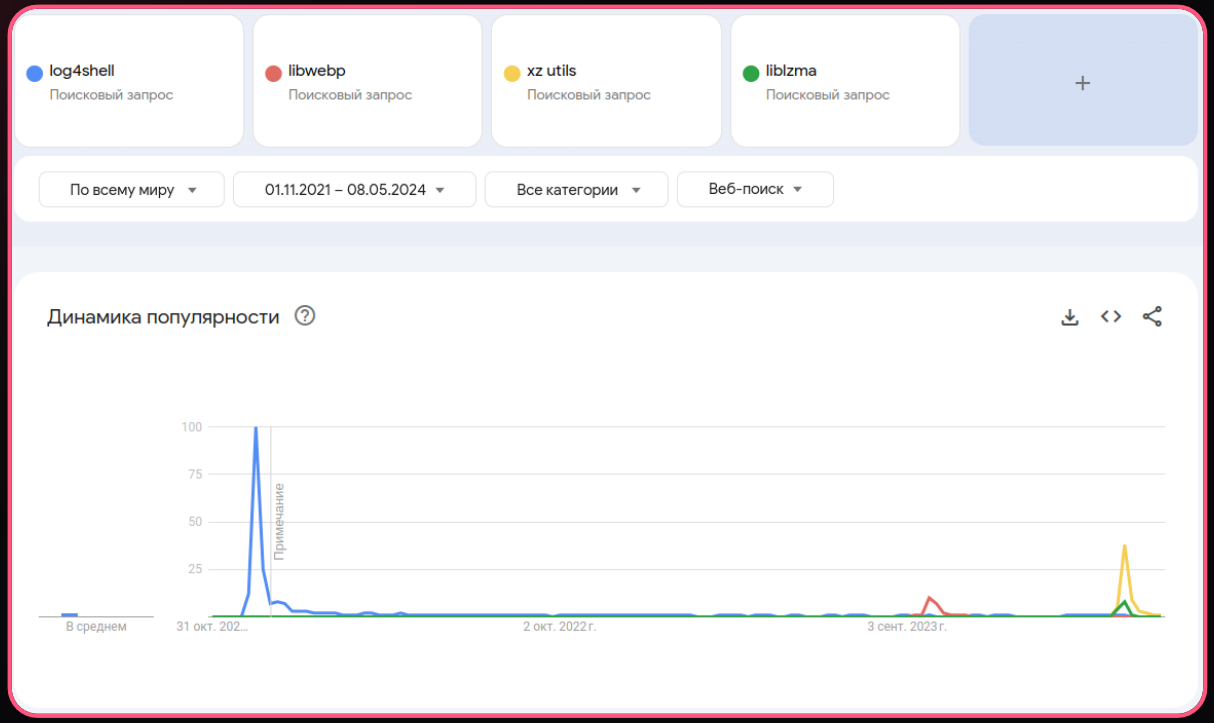
выросло количество известных атак на цепочки поставки: Dependency Confusion, Typosquatting, Namesquatting, Brandjacking, Malicious Code Injection и др.

> 700/мес

вредоносных пакетов выявляется экспертами по безопасности каждый месяц: кража параметров окружения, бэкдоры, шифровальщики и др.

log4shell RCE

Затронула 8% maven экосистемы в конце 2021 года



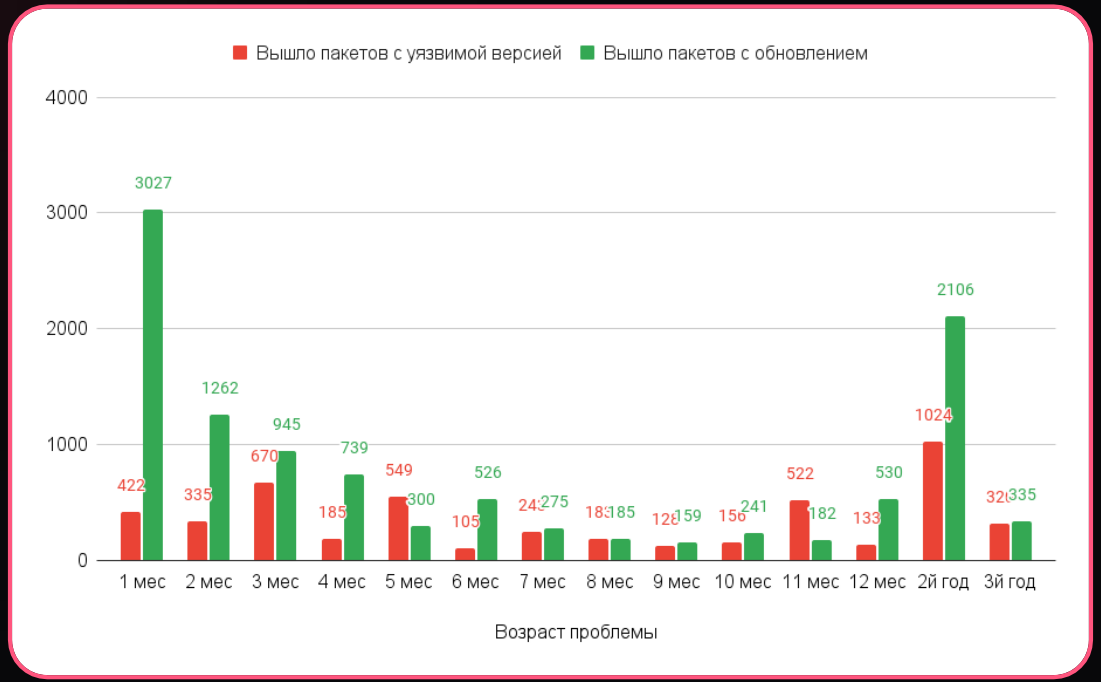
Google trends

Переход сообщества на безопасный log4j-core

CODE SCORING

КСБ-СОФТ

Окружения:
compile, runtime, provided



Итоги перехода сообщества на безопасный log4j-core

CODE SCORING

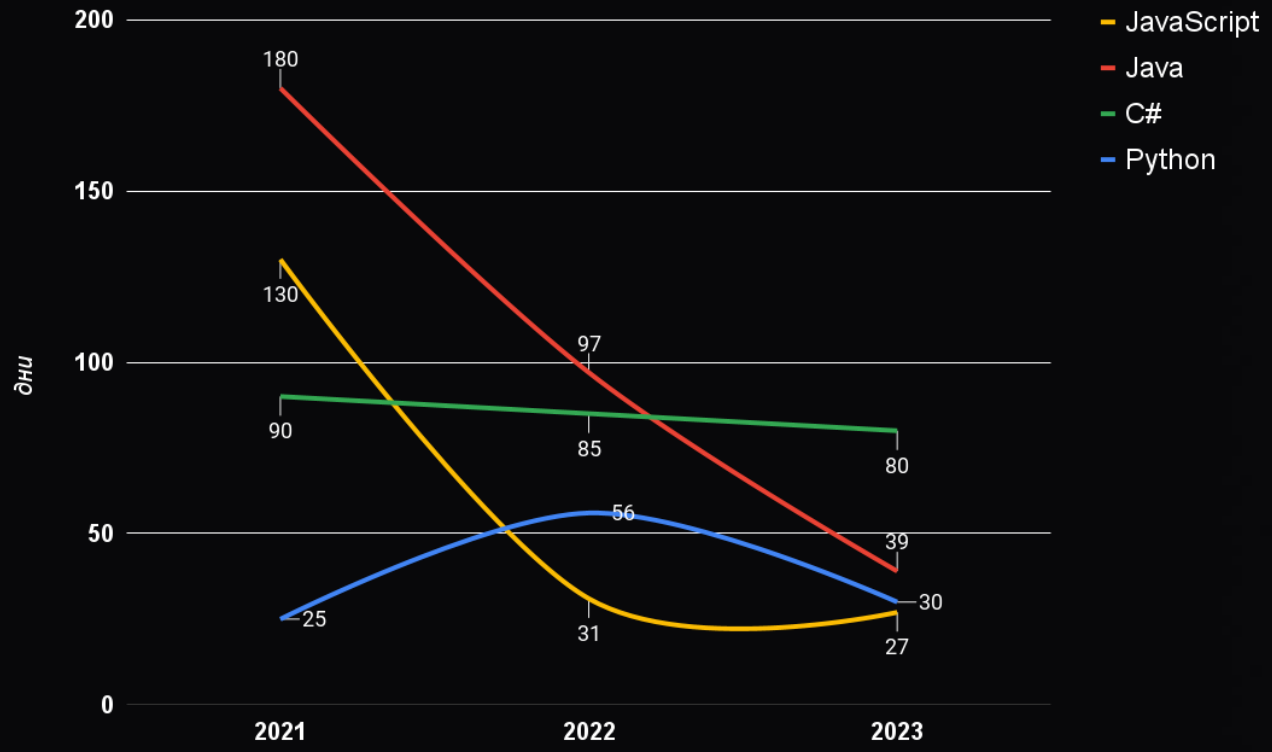
КСБ-СОФТ

затронуто:
20 588 версий пакетов

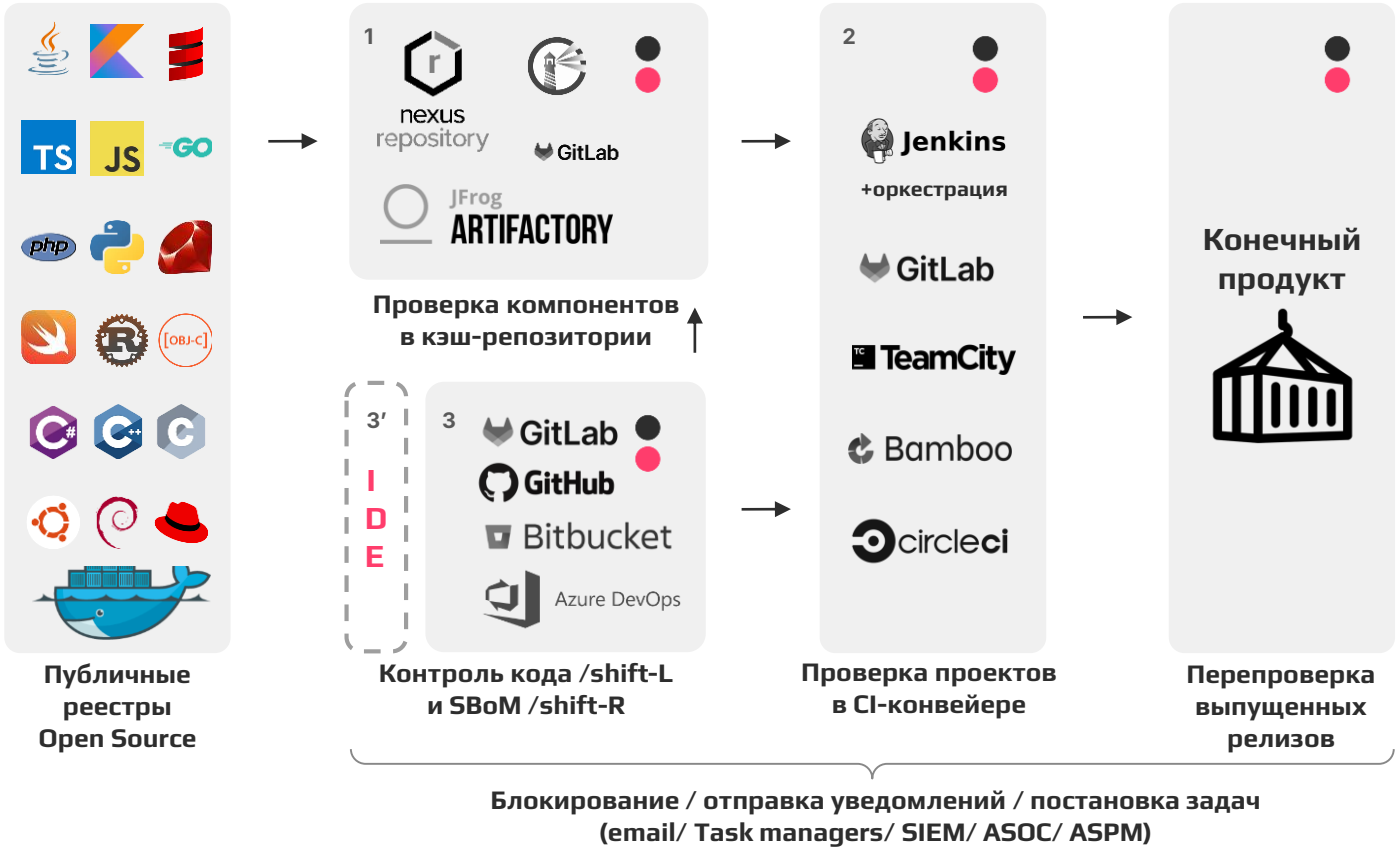
исправлено 28%:
5 837
не исправлено 72%:
14 751

Окружения: compile, runtime, provided

Скорость выхода патча после раскрытия уязвимости (дни)



Проверка на каждом этапе



Перечень программных компонентов (ппк)

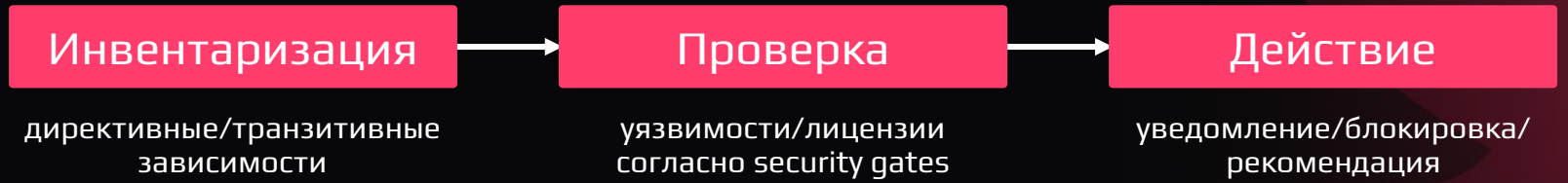
Машиночитаемый документ, содержащий в себе структурированную информацию о сторонних компонентах программного обеспечения и отношениях между ними.

SBoM, Software bill of materials.

Композиционный анализ

Анализ, основанный на инвентаризации сторонних компонентов ПО, определении особенностей их использования, составлении перечня известных уязвимостей и/или иных недостатков компонентов. (англ. Software Composition Analysis, SCA)

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

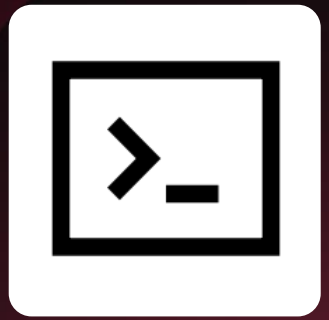


Открытые инструменты SCA

CODE SCORING

КСБ-СОФТ

- Trivy /trivy.dev
- Dependency check /owasp.org/www-project-dependency-check
- Dep scan /owasp.org/www-project-dep-scan
- CDXGen /github.com/CycloneDX/cdxgen
- Grype /github.com/anchore/grype
- OWASP tool Center /cyclonedx.org/tool-center



Открытые инструменты SCA

CODE SCORING

КСБ-СОФТ

- Dependency Track /dependencytrack.org
- ByteSafe /bytesafe.dev
- OpenSCA /opensca.xmirror.cn

SCA бывает разным

CODE SCORING

КСБ-СОФТ

SCA tooling

- Решает задачу проверки проекта
- Проверка в одной точке на конкретный язык и локальную политику
- Обновление легаси зависимостей и обнаружение уязвимостей
- Рекомендации по исправлениям

Effective SCA

- Сокращение издержек на анализ зависимостей и уязвимостей
- Работа с инвентарем, массовые исправления
- Кросс-языковой анализ проектов
- Действенная аналитика о проблемах
- Гибкие политики отслеживания проблем и рекомендации по исправлениям

CodeScoring /возможности

CodeScoring создан в 2019 году и выведен на рынок в 2021.
Решение вобрало в себя опыт:

- проведения ИТ/ИБ-аудитов
- разработки анализаторов кода
- анализа мирового Open Source

Сегодня включает в себя функциональность:

- OSA /защита цепочки поставки
- SCA /композиционный анализ
- TQI /анализа качества ПО
- Secrets /идентификация секретов в коде

CodeScoring /сегодня

- 20+ интегрированных баз уязвимостей
- собственная база знаний про мировой open source
- собственная база знаний про open source лицензии
- интеграция на всех этапах разработки ПО
- широкий набор политик отслеживания и блокирования рисков
- защита цепочки поставки от популярных атак (+интеграция с **Kaspersky**)
- вся ключевая функциональность собственной разработки
- применение машинного обучения для удобства пользователей

CodeScoring

CODE SCORING

КСБ-СОФТ

Заказчики:

- Банки и Финансовые компании
- Нефтяные и Энергетические компании
- Телеком и Медиа
- Государственные учреждения (госпорталы)
- Разработчики ПО

Решение является лидером российского рынка — многие десятки боевых внедрений
и мы непрерывно получаем обратную связь от заказчиков для регулярного улучшения продукта.

Безопасность цепочки
поставки программного
обеспечения

Проверка проектов
при приёмке заказного ПО

Анализ проектов
в разрезе авторов

CODE SCORING

КСБ-СОФТ

Выводы

Польза для безопасности

CODE SCORING

КСБ-СОФТ

- Знание своих продуктов
- Информированность об уязвимостях
- Понимание что делать дальше
- Контроль ранее выпущенных продуктов
- Автоматизация процесса защиты цепочки поставки

Варианты использования #1

CODE SCORING

КСБ-СОФТ

- **Внедрение платформы композиционного анализа CodeScoring**

Для больших команд разработки (> 50 разработчиков)

Если есть потребность выстраивания собственного процесса SDL

Возможность вести постоянный контроль в отношении применяемых компонентов

Пилотирование решения

- Бесплатное тестирование платформы
- Самостоятельное ознакомление с продуктом
- Сопровождение в процессе пилота

Варианты использования #2

CODE SCORING

КСБ-СОФТ

Промо от КСБ-СОФТ

Анализ одного разрабатываемого проекта Заказчика

Срок исполнения
1 день

Стоимость
69 тыс. руб.

Подключение к платформе CodeScoring по сервисной модели

Для небольших команд (до 50 разработчиков)

Если в штате нет собственных специалистов AppSec

Гибкое решение конкретной проблемы клиента с учетом его потребностей

Варианты использования #3

CODE SCORING

КСБ-СОФТ

- **Комплексный аудит кода с применением платформы CodeScoring**

  Глубокое изучение особенностей конкретного продукта профессиональной командой по безопасной разработке

Полезные материалы

CODE SCORING

КСБ-СОФТ

01 Композиционный анализ (SCA)

Проблема отцов и детей: аналитика и триаж транзитивных зависимостей, PHD'24

Построить SBoM, вырастить SDL- политики, воспитать культуру безопасной разработки, IT IS Conf'23

Protestware. Как много в этом слове! Devopsconf'22

02 Защита цепочки поставки (OSA)

Таксономия атак на цепочку поставки ПО: тренды и предпосылки новых трендов, GigaConf'24

Мифы и факты о цепочке поставки программного обеспечения, CyberCamp'23

PyPI сегодня — радости статистики и печали безопасности, PyCon'22

Спасибо

CODE SCORING

КСБ-СОФТ

@codescoring

@ksb_security_group

hello@codescoring.ru

info@ksb-soft.ru

codescoring.ru

ksb-soft.ru