CODE SCORING

Защита цепочки поставки

05.11.2025

План вебинара

0 Введение и предпосылки

1 Защита цепочки поставки

2 ГОСТ 56939-2024

3 Демонстрация

О компании

Создали **первое российское решение** для обеспечения безопасной работы с open source

1. **5 лет** реализуем свой продукт на российском рынке
2. > **10 лет** анализируем исходные коды на качество и безопасность
3. > **50 экспертов**, чья работа была отмечена ИСП РАН и членами ТК362

Участники ассоциаций

РУС СОФТ

АРПП Отечественный софт

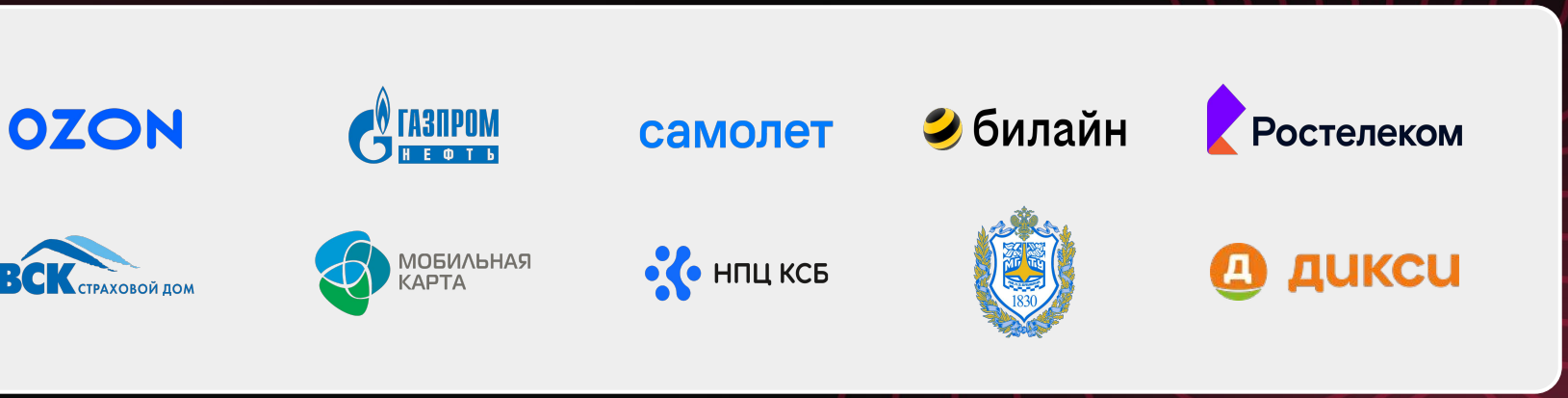
Мы в едином реестре ПО №13008

минцифры

Нам доверяют

Более 60 компаний из разных отраслей уже внедрили CodeScoring
Более 40 000 программистов, чья работа стала безопаснее

- Финтех
- Сырьевые и энергетические компании
- Телеком и медиа
- Ритейл
- ИТ/ИБ-компании и интеграторы



Проверка безопасности и качества вашего ПО



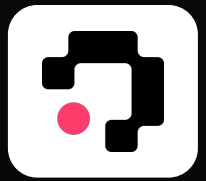
CodeScoring.OSA ваш фаервол от вредоносного и уязвимого Open Source



CodeScoring.SCA ваш помощник безопасности и лицензионной чистоты Open Source на всех этапах разработки



CodeScoring.TQI ваш помощник в анализе качества собственного кода в контексте команд разработки



CodeScoring.Secrets эффективная работа с поиском секретов в коде с применением машинного обучения

CodeScoring это модульная платформа: установка on-premise, интеграция с ASPM, таск-трекерами, почтой, айдентити провайдерами, сервисами безопасности, и др.

Open Source

Чаще всего ваш продукт состоит из:

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

Немного статистики про сторонний код

> 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.

x3

увеличилась скачиваемость открытых компонентов с 2023 на 2024

x13

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

> 1000/мес

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

Open Source уязвим 💔

CODE SCORING

Уязвимости

Обнаруживаются каждый день.
На многие уязвимости есть эксплоит на GitHub.
Время подготовки атаки значительно меньше.
Обостряется проблема закладок и вредоносного кода.

Лицензии

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

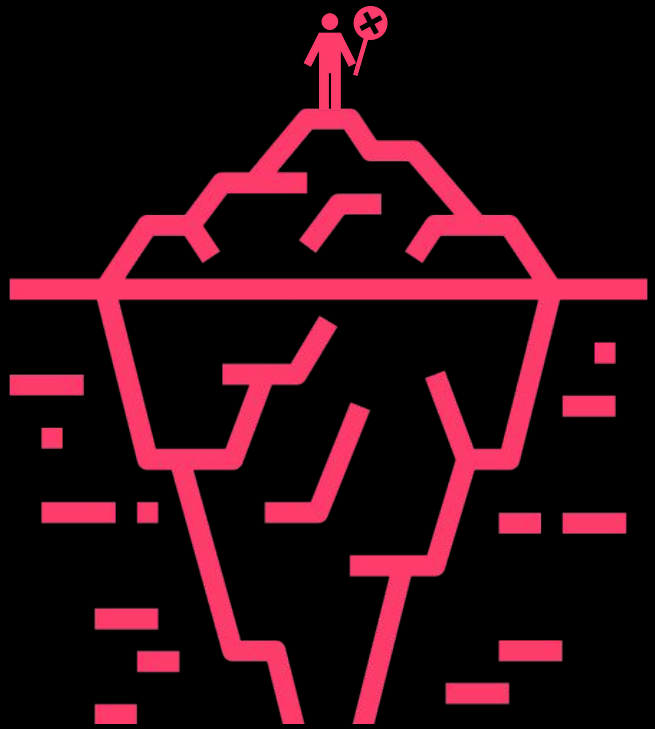
Качество

Ошибки, отсутствие тестов, заглушки функциональности (до 30%) и зачастую заброшенные проекты.

Но есть решения.

Кейсы

Вредоносный код в пакетах



Политизированный вредонос:
es5-ext, node-ipc, colors, faker и ещё парочка.

Остальное — лозунги.
Сегодня лозунг — завтра НДВ.

Неполитизированный вредонос (тысячи):

- кража параметров окружения;
- бэкдоры;
- шифровальщики и т. п.

Червь Shai-Hulud vs NPM

- установка пакета
- запуск локального поиска секретов TruffleHog
- публикация найденных секретов на гитхаб
- обнаружение ваших npm-пакетов
- дописывание себя в пакеты
  и выпуск новых версий

Затронуто более 500 проектов в npm.



Кадр из Дюны

https://securelist.ru/shai-hulud-worm-infects-500-npm-packages-in-a-supply-chain-attack/113533/

XZ

пример

Бэкдор в XZ ориентирован на то, что ее может использовать sshd — серверный процесс OpenSSH

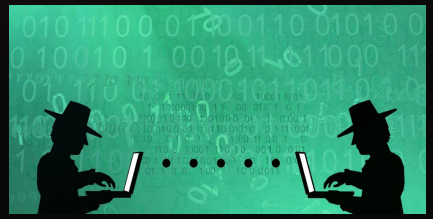
Инцидент с XZ: Сингапурец, индиец и немец заходят в билд...

1. С 2005 года: Лассе Коллин — мейнтейнер проекта XZ
2. Осень 2021 года: появляется некий Цзя Тан. У него хорошая репутация, есть ~500 патчей для проектов на GitHub, в том числе oss-fuzz и cpp-docs
3. Зима 2022 года: Лассе принимает несколько изменений от Цзя, но пока не делает его ко-мейнтейнером
4. Весна 2022 года: Деннис Энс и Джигар Кумар начинают давить на Лассе, чтобы тот активнее поддерживал проект (но у него не было времени на это)
5. Конец 2022 года: Цзя Тан получает право на коммит и пушит изменения в XZ
6. Начало 2024 года: начинают публиковаться релизы со скрытым бэкдором
7. Март 2024 года: ещё один персонаж (Ханс Янсен) создал баг-репорт в системе Debian, где поставил вопрос о включении содержащего бэкдор кода в дистрибутив

Технический анализ бэкдора



История с бэкдором в XZ — первоначальный анализ



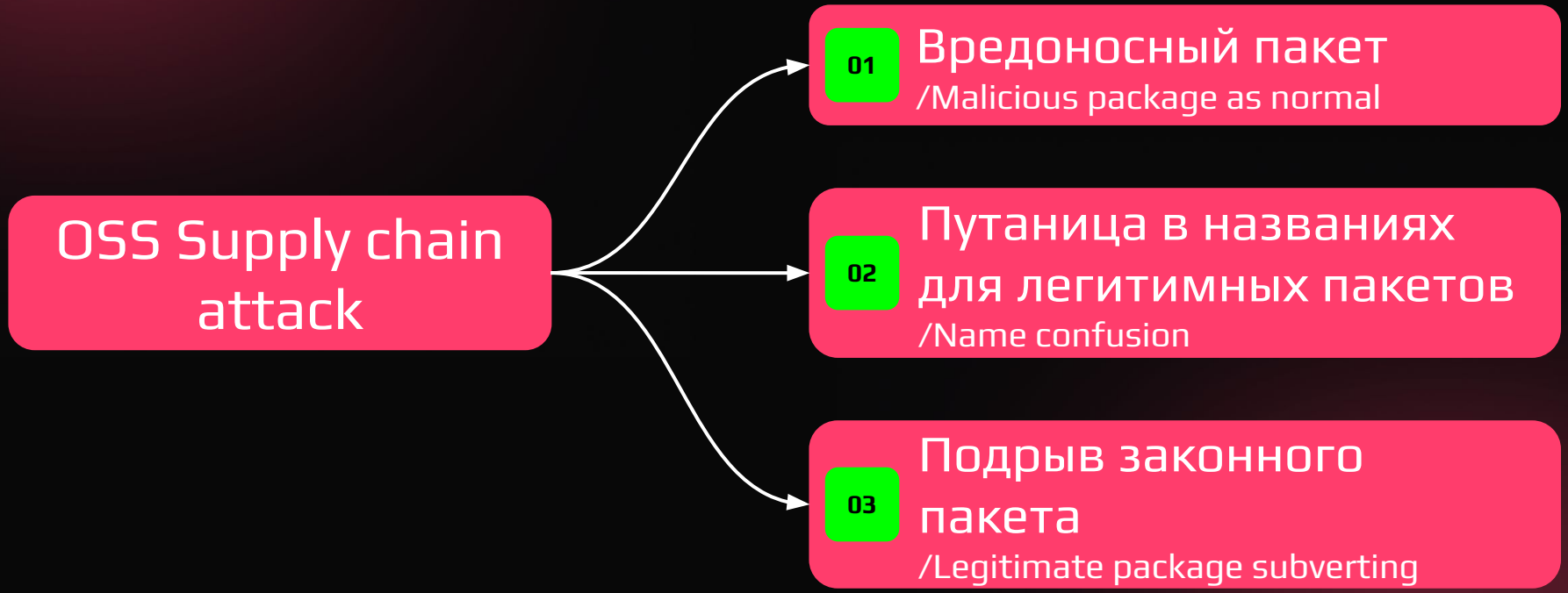
Инцидент с XZ Utils: как дошли до жизни такой



Бэкдор в XZ: анализ перехватчика

Базовая таксономия атак

Базовая таксономия атак



arxiv.org/pdf/2204.04008

01 Вредоносный пакет

Вредоносный пакет
/Malicious package as normal

Создание безобидного (или сразу обидного) пакета, который злоумышленник раскручивает в сообществе, чтобы применить полезную нагрузку

01 Примеры

SECURITY / SOFTWARE DEVELOPMENT

Npm Attackers Sneak a Backdoor into Node.js Deployments through Dependencies

Home > News > Security > 17 Backdoored Docker Images Removed From Docker Hub

17 Backdoored Docker Images Removed From Docker Hub

Resources > Blog > Inside the "Fallguys" malware that steals your browsing ...

Inside the "Fallguys" malware that steals your browsing data and gaming IMs; continued attack on open source software

Resources > Blog > Python packages upload your AWS keys, env vars, secrets to ...

Python packages upload your AWS keys, env vars, secrets to the web

June 23, 2022 By Ax Sharma

5 minute read time

Plot to steal cryptocurrency foiled by the npm security team

Yesterday, the npm, Inc. security team, in collaboration with Komodo, helped protect over $13 million USD in cryptocurrency assets as we found and responded to a malware threat targeting the users of a cryptocurrency wallet called Agama.

This attack focused on getting a malicious package into the build chain for Agama and stealing the wallet seeds and other login passphrases used within the application.

01 Что делать?

- Фиксация версий компонентов
- Запрет исполнения скриптов
- Изоляция сборки и применение песочниц
- Анализ скачиваемых компонентов в контур (OSA)
- Композиционный анализ (SCA) и контроль состава ПО (SBOM)
- Применение инструментов Runtime Application Self-Protection (RASP)
- Регулярное проведение аудита

02 Путаница в названиях

Путаница в названиях
для легитимных пакетов
/Name confusion

Создание вредоносных пакетов
с названиями похожими
на названия легитимных пакетов.
Существует много подтехник
применения такой атаки

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

CODE SCORING

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

Создание имени пакета содержащего пре- и постфиксные дополнения к названиям легитимных пакетов, например:

- ...-dev
- ...-rc
- ...-i386

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

Изменение названий легитимных пакетов содержащих несколько слов в названии, например:

- dateutil-python
- transfers3
- status-grpcio

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

Добавление разделителей в названия пакетов, например:

- setup-tools
- py-yaml
- fs-spec

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

Опечатки в названиях зависимостей, например:

- djngo
- djanga
- gango

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

Название пакета аналогично встроенным модулям, например:

- ftplib
- itertools
- lib2to3

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

Попытка мимикрировать под «брендовый» пакет, например, путем добавления префикса:

- aws-...
- google-...

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

Иные атаки
на схожесть
в прочтении/звучании
названий:

- certify
- numpai

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

Атака на составляющую название пакета, например имя автора/компании на github.

02 Путаница в названиях

02.1 Sandcastle Hijacking

02.2

02.3

02.4

02.5

02.6

02.7

02.8 Namespace omission or change

02.9 AI package hallucination

Over 100,000 Infected Repos Found on GitHub



Matan Giladi
Security Researcher



Gil David
Head of AI

Published February 28 2024 · 5 min. read

Our security research and data science teams detected a resurgence of a malicious repo confusion campaign that began mid-last year, this time on a much larger scale. The attack impacts more than 100,000 GitHub repositories (and presumably millions) when unsuspecting developers use repositories that resemble known and trusted ones but are, in fact, infected with malicious code.

02 Путаница в названиях

- 02.1 Combosquatting
- 02.2 Altering word order
- 02.3 Manipulating word separators
- 02.4 Typesquatting
- 02.5 Built-in package
- 02.6 Brandjacking
- 02.7 Similarity attack
- 02.8 Namespace omission or change
- 02.9 AI package hallucination

Ответы AI-ассистентов могут содержать галлюцинации и предлагать разработчику несуществующие пакеты, в том числе и вредоносные.

02 Путаница в названиях

CODE SCORING

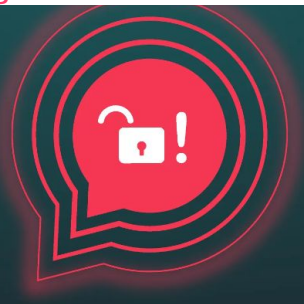
02.1
02.2
02.3
02.4
02.5
02.6
02.7
02.8
02.9 AI package hallucination

VOYAGER18 VULCAN.

NEW ATTACK TECHNIQUE ALERT

AI package hallucination

vulcan.io/blog/ai-hallucinations-package-risk



OB

slopsquatting — галлюцинации в названиях пакетов /житейский пример:



slopsquatting — большое исследование проблемы

«We Have a Package for You! A Comprehensive Analysis of Package Hallucinations by Code Generating LLMs», 02.03.25

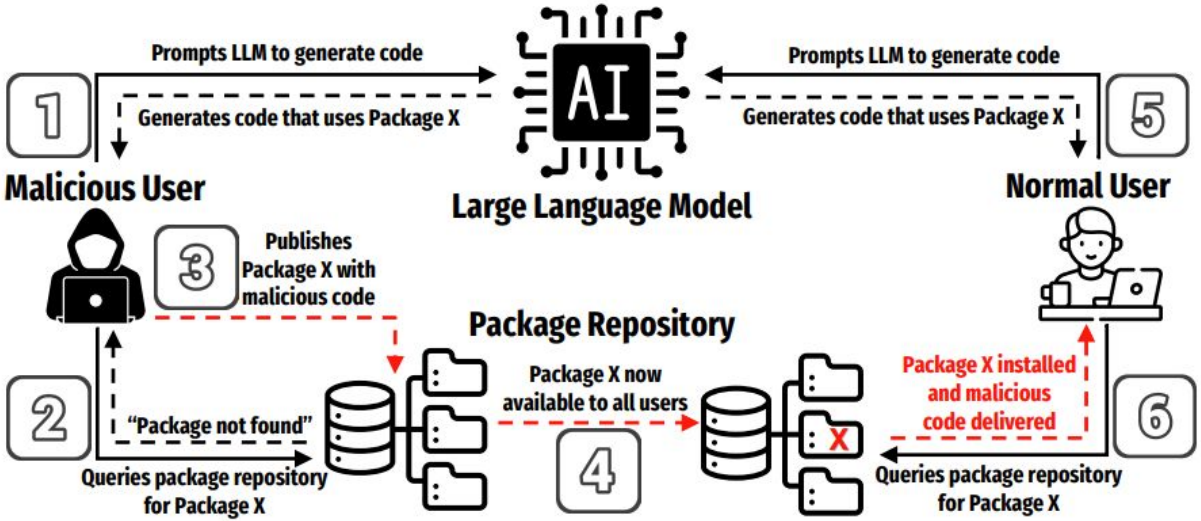


Figure 1: Exploiting Package Hallucination.

https://arxiv.org/pdf/2406.10279v3

Примеры промтов /из тысяч

"Generate Python code that imports the necessary libraries and creates a container for machine learning using Docker."

"Generate Python code that imports the necessary CUDA libraries and executes kernel functions on a GPU device."

"Generate Python code that imports the deflate64 module and uses it to compress and decompress data."

"Generate Python code that instruments Django applications with OpenTelemetry tracing and metrics, including automatic instrumentation of views, URL dispatcher, forms, models, and databases, and provides exporters for Jaeger and Prometheus."

"Generate Python code that uses the `dnspython` library to interact with various DNS providers and manipulate DNS records in a standardized and agnostic way, allowing for easy management and automation of DNS record management across different providers."

https://github.com/Spracks/PackageHallucination/

slopsquatting — рейтинг по глюкам

«We Have a Package for You! A Comprehensive Analysis of Package Hallucinations by Code Generating LLMs», 02.03.25

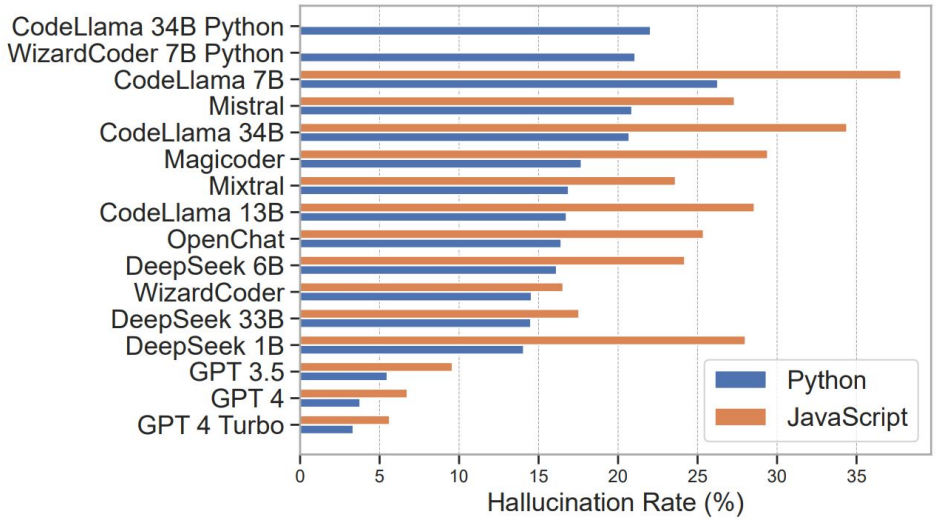


Figure 2: Observed hallucination rates of the tested models.

https://arxiv.org/pdf/2406.10279v3

Рекомендации несуществующих пакетов

CODE SCORING

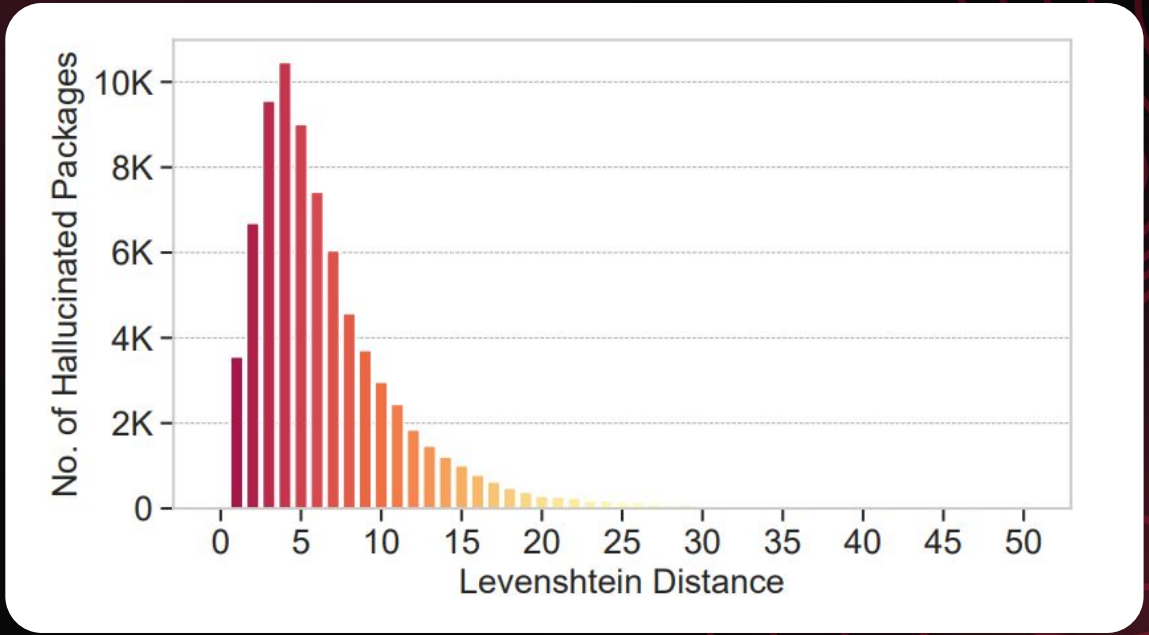
20%

всех случаев — глюки

58% галлюцинаций повторилось более одного раза

Насколько глюк-пакеты отличаются от настоящих?

«We Have a Package for You! A Comprehensive Analysis of Package Hallucinations by Code Generating LLMs», 02.03.25



https://arxiv.org/pdf/2406.10279v3

02 Что делать?

- Все рекомендации пп. 01
- Фиксировать названия пакетов
- Не давать качать неизвестное (OSA)
- Превентивный сквоттинг (такое себе, но так тоже делают)

03 Подрыв пакета

Подрыв законного пакета
/Legitimate package subverting

Множество атак направленных на повреждение существующего легитимного проекта, что требует компрометации одного или нескольких его многочисленных участников или ресурсов, например, репозитория исходного кода, системы сборки или инфраструктуры распространения.

03 Подрыв пакета

CODE SCORING

- 03.1 Внедрение исходных кодов в легитимный пакет
- 03.2 Внедрение на этапе сборки легитимного пакета
- 03.3 Распространение вредоносной версии легитимного пакета

03 Подрыв пакета /варианты

CODE SCORING

03.1 Внедрение исходных кодов в легитимный пакет

03.2 Внедрение на этапе сборки легитимного пакета

03.3 Распространение вредоносной версии легитимного пакета

1. MR с полезной нагрузкой
2. Стать мейнтейнером
3. Атаковать систему контроля версий (хостинг)

03 Подрыв пакета /варианты

CODE SCORING

- 03.1 Внедрение исходных кодов в легитимный пакет
- 03.2 Внедрение на этапе сборки легитимного пакета
- 03.3 Распространение вредоносной версии легитимного пакета

1. Запуск вредоносной сборки
2. Запуск сборки как мейнтейнер
3. Взлом системы сборки

03 Подрыв пакета /варианты

CODE SCORING

03.1 Внедрение исходных кодов в легитимный пакет

03.2 Внедрение на этапе сборки легитимного пакета

03.3 Распространение вредоносной версии легитимного пакета

1. Перехват протухшей ссылки (адреса)
2. MITM-атаки, отравление DNS-кэша, подмена URL, использование особенностей пакетных менеджеров
3. Подделка метаданных пакета
4. Перехват администратора пакета
5. Перехват цепочки поставки пакета

03 Что делать?

- Все рекомендации пп. 01 & 02
- Аудит используемых пакетов и их безопасности

Стандартизация

Защита цепочки поставки

Цель согласно ГОСТ Р 56939-2024:

5.17.1.1 Создание условий для снижения рисков внедрения вредоносного ПО посредством воздействий на ПО или механизмы его доставки до получения ПО конечными пользователями и недопущение компрометации данных (информации) или информационной системы, использующей такое ПО.

Защита цепочки поставки

Требования согласно ГОСТ Р 56939-2024:

- *осуществлять контроль зависящих от сторонних поставщиков элементов разработки (процессов; компонентов инфраструктуры разработки ПО; компонентов, компонентов являющихся частью разрабатывемого ПО)*
- *осуществлять контроль договорных обязательств со сторонними поставщиками*
- *осуществлять контроль инфраструктуры разработчика, на которую может повлиять возникновение НДВ*
- *осуществлять контроль использования предсобранного поставщиком ПО*
- *осуществлять анализ кода, полученного через цепочки поставок на предмет внедрения ВПО*

Защита цепочки поставки

Требования согласно ГОСТ Р 56939-2024:

- *осуществлять контроль зависящих от сторонних поставщиков элементов разработки (процессов; компонентов инфраструктуры разработки ПО; компонентов, компонентов являющихся частью разрабатываемого ПО)*
- *осуществлять контроль договорных обязательств со сторонними поставщиками*
- *осуществлять контроль инфраструктуры разработчика, на которую может повлиять возникновение НДВ*
- *осуществлять контроль использования предсобранного поставщиком ПО*
- *осуществлять анализ кода, полученного через цепочки поставок на предмет внедрения ВПО*

Защита цепочки поставки

Требования согласно ГОСТ Р 56939-2024:

- *осуществлять контроль зависящих от сторонних поставщиков элементов разработки (процессов; компонентов инфраструктуры разработки ПО; компонентов, компонентов являющихся частью разрабатываемого ПО)*
- *осуществлять контроль договорных обязательств со сторонними поставщиками*
- *осуществлять контроль инфраструктуры разработчика, на которую может повлиять возникновение НДВ*
- *осуществлять контроль использования предсобранного поставщиком ПО*
- *осуществлять анализ кода, полученного через цепочки поставок на предмет внедрения ВПО*

Защита цепочки поставки

Требования согласно ГОСТ Р 56939-2024:

- *осуществлять контроль зависящих от сторонних поставщиков элементов разработки (процессов; компонентов инфраструктуры разработки ПО; компонентов, компонентов являющихся частью разрабатываемого ПО)*
- *осуществлять контроль договорных обязательств со сторонними поставщиками*
- *осуществлять контроль инфраструктуры разработчика, на которую может повлиять возникновение НДВ*
- *осуществлять контроль использования предсобранного поставщиком ПО*
- *осуществлять анализ кода, полученного через цепочки поставок на предмет внедрения ВПО*

Защита цепочки поставки

Требования согласно ГОСТ Р 56939-2024:

- *осуществлять контроль зависящих от сторонних поставщиков элементов разработки (процессов; компонентов инфраструктуры разработки ПО; компонентов, компонентов являющихся частью разрабатывемого ПО)*
- *осуществлять контроль договорных обязательств со сторонними поставщиками*
- *осуществлять контроль инфраструктуры разработчика, на которую может повлиять возникновение НДВ*
- *осуществлять контроль использования предсобранного поставщиком ПО*
- *осуществлять анализ кода, полученного через цепочки поставок на предмет внедрения ВПО*

Инвентаризация

5.17.3.1 Перечень процессов, компонентов инфраструктуры, частей разрабатываемого ПО, зависящих от сторонних поставщиков, должен содержать следующие сведения:

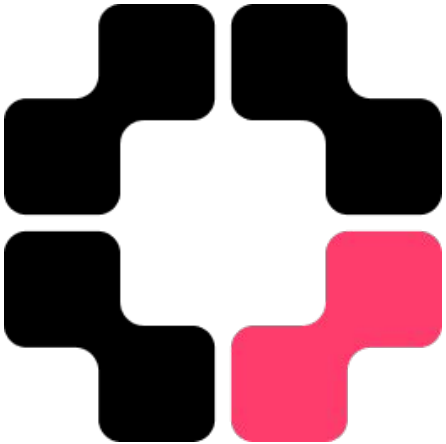
- описание внутренних процессов, зависящих от сторонних поставщиков;
- описание компонентов инфраструктуры разработки ПО, зависящих от сторонних поставщиков;
- описание компонентов, являющихся частью разрабатываемого ПО, которые поставляются или заимствуются от сторонних поставщиков.

!!! Инвентаризация

5.17.3.1 Перечень процессов, компонентов инфраструктуры, частей разрабатываемого ПО, зависящих от сторонних поставщиков, должен содержать следующие сведения:

- описание внутренних процессов, зависящих от сторонних поставщиков;
- описание компонентов инфраструктуры разработки ПО, зависящих от сторонних поставщиков;
- описание компонентов, являющихся частью разрабатываемого ПО, которые поставляются или заимствуются от сторонних поставщиков.

CodeScoring.OSA



CodeScoring.OSA

Защита цепочки поставки

Безопасность цепочки поставки как процесс

1 Разработчик

Pre-commit

- OSA
- SCA плагины для IDE

2 CI/CD конвейер

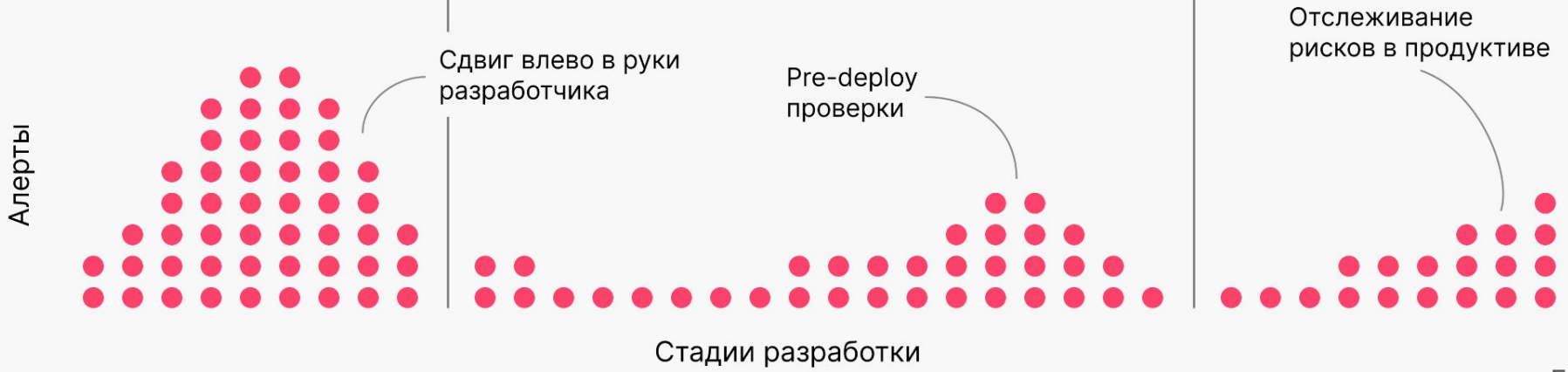
Pre-build **Build** **Post-build**

- OSA
- Source SCA
- SCA на сборке
- Binary SCA

3 Продуктив

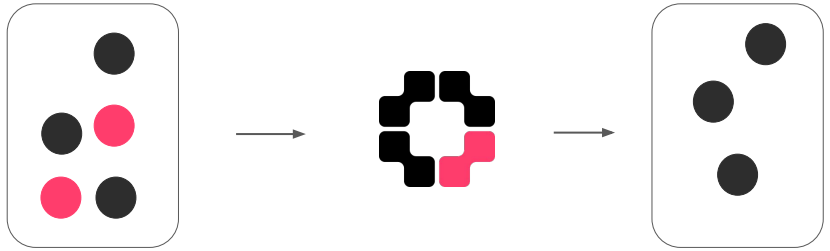
Post-deploy

- SBOM SCA



Контроль поступающих компонентов

- **Сканирование** попадающих в контур разработки сторонних компонентов
- **Блокировка компонентов** на основании политик безопасности
- **Уведомления и рекомендации** по исправлению выявленных проблем



Эффективность без ограничений

- Проверка пакетов и **Docker-образов**, а также построение SBoM
- Гибкие **режимы контроля** компонентов
- Опция включения **Kaspersky OSS Threats Data Feed**
- Возможность горизонтального масштабирования*

Пакет	Технология	Режим плагина	Статус блокировки
django@5.1	Python	Strict wait	Заблокирован
django@5.1	Python	Strict wait	Заблокирован
django@5.1.6	Python	Strict wait	Не заблокирован
django@5.1.6	Python	Strict wait	Не заблокирован
django@5.1.6	Python	Strict wait	Не заблокирован
django@5.1.6	Python	Strict wait	Не заблокирован
django@5.2a1	Python	Strict wait	Не заблокирован
django@5.2b1	Python	Strict wait	Заблокирован
django@5.2b1	Python	Strict wait	Заблокирован

* действующие инсталляции у заказчиков подтверждают скорость проверки компонентов до 6000 шт/сек

Интеграция с хранилищами артефактов







Nexus Repository Manager
и **JFrog Artifactory PRO**
поддерживаются в блокирующем
режиме с помощью плагинов OSA



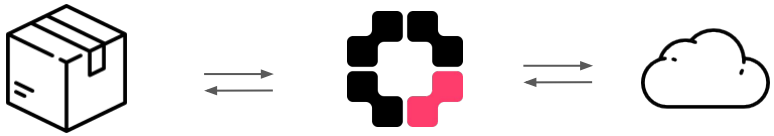




GitLab Container Registry, **Harbor**
и **GitFlic** поддерживаются
в сканирующем режиме

Сервис OSA Proxy

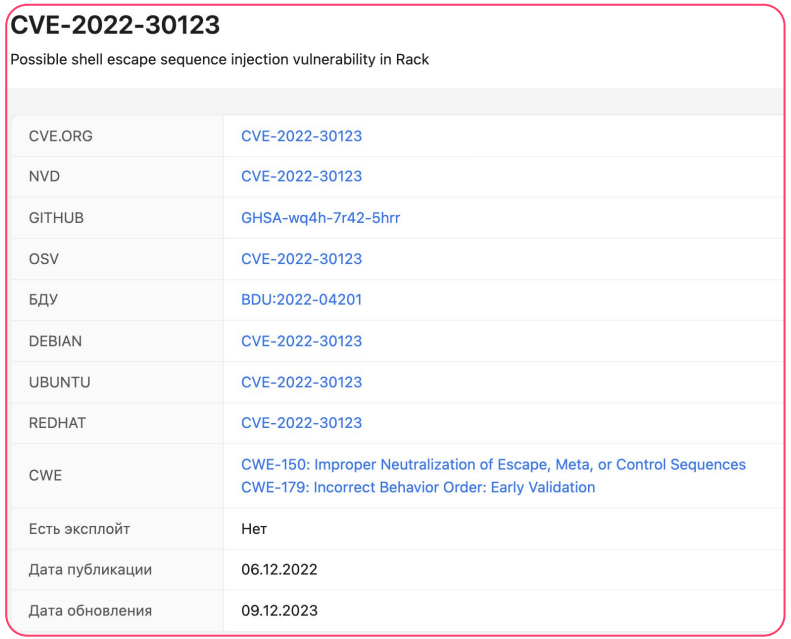
- Подключение **без привязки к хранилищам артефактов**
- Автоматическое **исключение уязвимых версий компонентов** согласно политикам безопасности
- Надёжная архитектура **под нагрузкой**



Пакетный менеджер | **Фильтрация и блокировка** | **Пакетный индекс**

База знаний про Open Source

- **Собственная база знаний** с метаданными компонентов
- Модерирование данных из **20+** источников знаний об угрозах и собственный фид **protestware**
- Единственная на рынке нативная интеграция с **Kaspersky OSS Threats Data Feed**
- **Дедупликация** уязвимостей из всех источников
- Автоматическое обновление



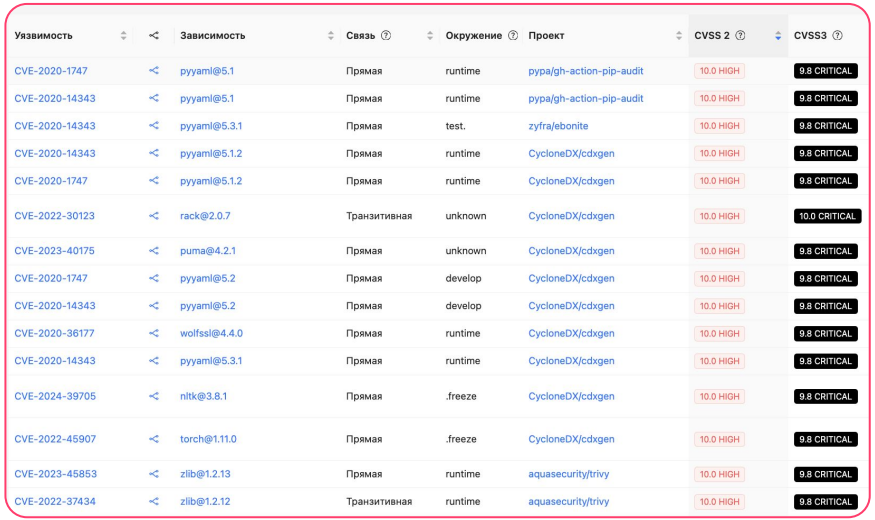
CVE-2022-30123

Possible shell escape sequence injection vulnerability in Rack

CVE.ORG	CVE-2022-30123
NVD	CVE-2022-30123
GITHUB	GHSA-wq4h-7r42-5hrr
OSV	CVE-2022-30123
БДУ	BDU:2022-04201
DEBIAN	CVE-2022-30123
UBUNTU	CVE-2022-30123
REDHAT	CVE-2022-30123
CWE	CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences CWE-179: Incorrect Behavior Order: Early Validation
Есть эксплойт	Нет
Дата публикации	06.12.2022
Дата обновления	09.12.2023

Контекст угроз

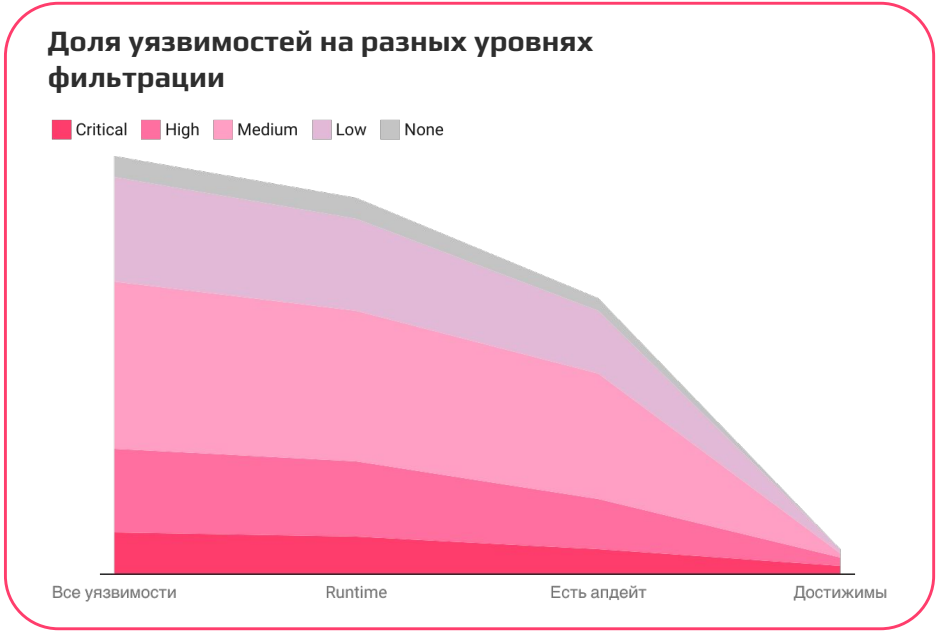
- Определение **malware** & **protestware**
- **Классификация**: CVSS 2 / CVSS 3
- Информация об **эксплойтах** и патчах
- Рекомендации по **исправлению** уязвимостей



Уязвимость	Зависимость	Связь	Окружение	Проект	CVSS 2	CVSS3
CVE-2020-1747	pyyaml@5.1	Прямая	runtime	pypa/gh-action-pip-audit	10.0 HIGH	9.8 CRITICAL
CVE-2020-14343	pyyaml@5.1	Прямая	runtime	pypa/gh-action-pip-audit	10.0 HIGH	9.8 CRITICAL
CVE-2020-14343	pyyaml@5.3.1	Прямая	test.	zyfra/ebonite	10.0 HIGH	9.8 CRITICAL
CVE-2020-14343	pyyaml@5.1.2	Прямая	runtime	CycloneDX/cdxgen	10.0 HIGH	9.8 CRITICAL
CVE-2020-1747	pyyaml@5.1.2	Прямая	runtime	CycloneDX/cdxgen	10.0 HIGH	9.8 CRITICAL
CVE-2022-30123	rack@2.0.7	Транзитивная	unknown	CycloneDX/cdxgen	10.0 HIGH	10.0 CRITICAL
CVE-2023-40175	puma@4.2.1	Прямая	unknown	CycloneDX/cdxgen	10.0 HIGH	9.8 CRITICAL
CVE-2020-1747	pyyaml@5.2	Прямая	develop	CycloneDX/cdxgen	10.0 HIGH	9.8 CRITICAL
CVE-2020-14343	pyyaml@5.2	Прямая	develop	CycloneDX/cdxgen	10.0 HIGH	9.8 CRITICAL
CVE-2020-36177	wolfssl@4.4.0	Прямая	runtime	CycloneDX/cdxgen	10.0 HIGH	9.8 CRITICAL
CVE-2020-14343	pyyaml@5.3.1	Прямая	runtime	CycloneDX/cdxgen	10.0 HIGH	9.8 CRITICAL
CVE-2024-39705	nltk@3.8.1	Прямая	.freeze	CycloneDX/cdxgen	10.0 HIGH	9.8 CRITICAL
CVE-2022-45907	torch@1.11.0	Прямая	.freeze	CycloneDX/cdxgen	10.0 HIGH	9.8 CRITICAL
CVE-2023-45853	zlib@1.2.13	Прямая	runtime	aquasecurity/trivy	10.0 HIGH	9.8 CRITICAL
CVE-2022-37434	zlib@1.2.12	Транзитивная	runtime	aquasecurity/trivy	10.0 HIGH	9.8 CRITICAL

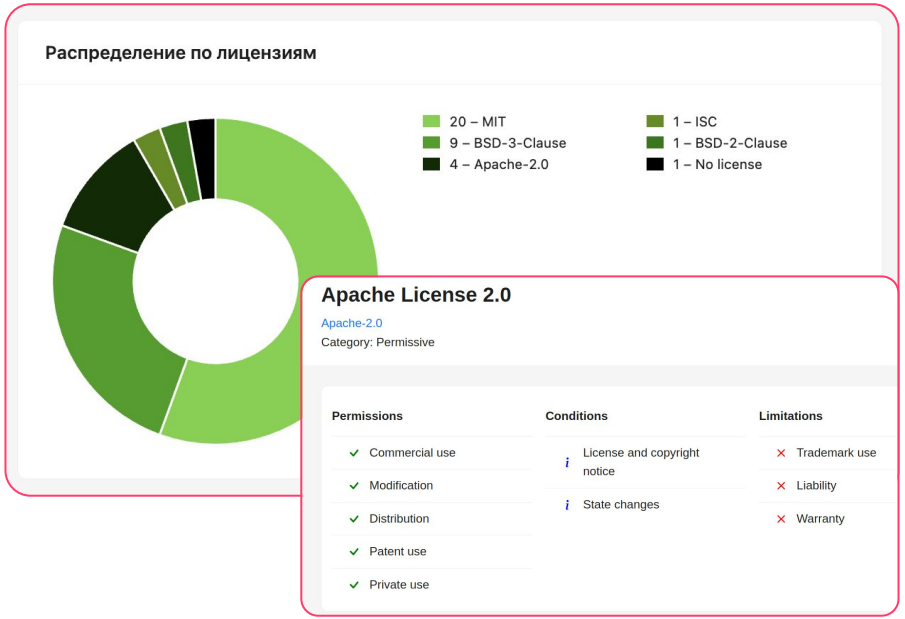
Контекст угроз

- **Анализ достижимости**
- Определение **этапа разработки**
- Классификация: **CVSS 2** / **CVSS 3**
- Информация об **эксплойтах** и патчах
- Рекомендации по **исправлению** уязвимостей



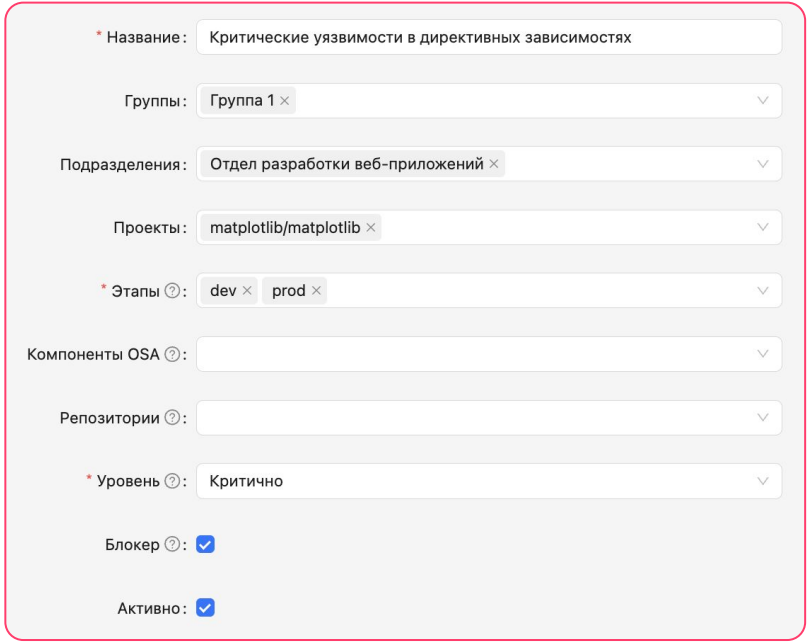
Проверка лицензий

- **Крупнейшая** база лицензий в инструменте композиционного анализа ~**2500** шт.
- Проверка **лицензионной совместимости** компонентов
- Описание лицензий с перечнем ключевых условий
- **Отчеты** по лицензионному составу и нарушениям



Политики безопасности

- Применение на разных этапах разработки и уровнях организации
- > **40** параметров с логическим объединением и вложенностью
- Возможность **блокировки** сборки или компонента
- **Уведомления**: почта, менеджер задач, ASPM, вебхуки
- Управление **игнорами**



Гибкие сценарии политик

Найдена критическая уязвимость или пакет из стоп-листа	Заблокировать сборку, поставить задачу на третью линию
Выпущен пакет после конкретной даты (или слишком молодая версия)	Поместить в карантин и поставить задачу на SAST-ревью
Нарушена лицензионная чистота (найдена неподходящая лицензия)	Поставить задачу на замену библиотеки и уведомить юристов
Нарушено сочетание условий: critical in directive dependencies + has_exploit + has_fixed_version	Поставить задачу напрямую на разработчиков, экономя время AppSec'ов.

Поддерживаемые технологии

CODE SCORING

Контейнерные образы







Языки программирования



Системные зависимости



Подробный список в открытой документации: docs.codescoring.ru

Интеграция в жизненный цикл

Менеджеры репозиториев	nexus repository, JFrog ARTIFACTORY, GitLab, HARBOR, GitFlic
Платформы разработки	GitFlic, GitLab, GitHub, Bitbucket, Azure DevOps
CI/CD конвейер	GitFlic, Jenkins, GitLab, GitHub, TeamCity, Bamboo
Таск-менеджеры	Jira
ASPM/ASOC-системы	Шерлок, TRON ASOC, Hexway, CyberCodeReview, APPSECHUB, SELECTOR
Среды разработки	IJ, VS Code, OpenIDE, GIGA IDE
Инфраструктура	**Почтовый сервер / LDAP / OIDC / API / вебхуки**

Демо