



ASOC как инструмент реагирования на
информацию об уязвимостях

Докладывает: Дмитрий Частухин

О компании Hexway

Высококвалифицированная команда разработчиков с более чем 15-летним опытом в сфере информационной безопасности. Компания состоит в реестре аккредитованных ИТ-компаний Минцифры.



Hexway Vampy ASPM включен в реестр
отечественного ПО Минцифры РФ

Клиенты

Банки, крупные промышленные и сырьевые компании, ИТ-разработчики

Миссия

Предоставлять клиентам комплексные решения для упрощения и автоматизации процессов безопасной разработки, помогая компаниям выпускать безопасные продукты.

Hexway Vampy ASOC

Российская DevSecOps
платформа для
управления безопасной
разработкой



Реагирования на уязвимости – отдельный процесс

- Уязвимости обнаруживаются постоянно: внутренние сканеры, подрядчики, исследователи
- Без формализованного процесса информация теряется или обрабатывается хаотично
- ГОСТ требует управляемый и воспроизводимый процесс реагирования
- Важно не только найти уязвимость, но и принять обоснованное решение

ГОСТ не про инструменты, а про процесс.

Даже лучшая находка бесполезна, если дальше ничего не происходит



Процесс реагирования на уязвимости

1. Получение информации

- Определить и зафиксировать источники информации об уязвимостях (сканер, подрядчик, фид и т.д.)

2. Регистрация и классификация

- Источник, описание, затронутый продукт, дата, FP или нет, дубликат или нет

3. Анализ и оценка

- Эксплуатируемая? Условия эксплуатации? Какой ущерб? Риски? Срочность реакции?

4. Принятие решения

- Что нужно делать? Принять риск? Исправлять? Назначить ответственного и сроки

5. Исправление и контроль

- Исправляем, контролируем SLA, перепроверяем

6. Фиксация и аудит

- Документируем что сделано, кем, когда и с каким результатом

7. Улучшение процесса



Обнаружение и учет

- Все источники уязвимостей должны попадать в единый контур учёта
- Любая информация фиксируется, даже неподтверждённая
- Привязка к продукту, версии и источнику

Что проверить:

- Есть ли единый реестр уязвимостей
- Можно ли восстановить историю появления проблемы



Анализ и принятие решений

- Анализ применимости и влияния на безопасность
- Оценка критичности и риска
- Для каждой уязвимости фиксируется решение:
 - исправлять
 - принять риск
 - компенсировать
 - отклонить

«Ничего не делать» это тоже ок, если есть аргументы



Исполнение, контроль и аудит

- Назначается ответственный и срок
 - Контролируется выполнение (SLA)
 - Результат фиксируется: что, когда и кем сделано
-
- Процесс должен быть проверяемым
 - Данные должны сохраняться для аудита



Реагируешь - улучшаешься

- Анализ повторяющихся уязвимостей
- Корректировка требований безопасности
- Улучшение проверок и процессов разработки

Реагирование на уязвимости - это механизм постоянного повышения зрелости РБПО

Hexway Vampy ASOC

ASOC как инструмент реагирования на
информацию об уязвимостях



Меньше рисков и быстрый go-to-market

ASOC система – стратегический ход, который напрямую влияет на ключевые цели DevSecOps и CISO

Решение позволяет выявлять уязвимости на ранних этапах разработки, минимизируя риски компрометации и сокращая время на исправление ошибок.

Не только ускоряет выход продукта на рынок, но и снижает вероятность дорогостоящих инцидентов после релиза.

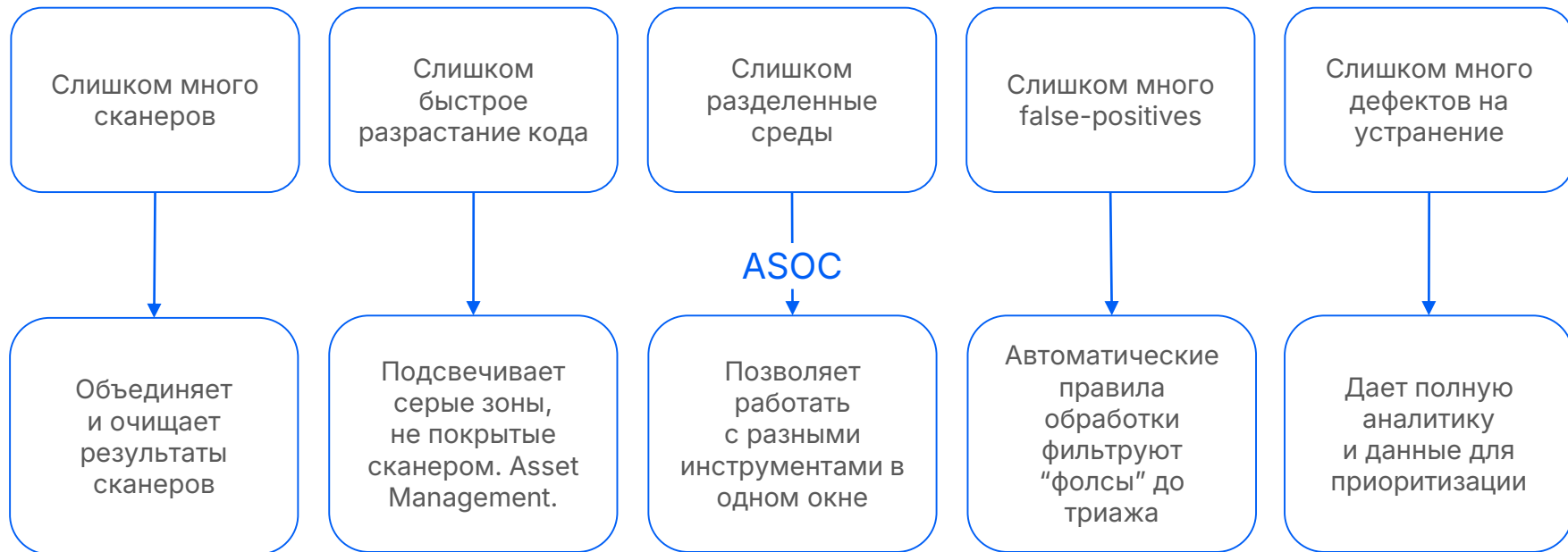
AVC	
ASTO	
ASOC	
ASPM	
AppSec platform	

[Пробуем окно в DevSecOps,внедряя ASPM](#)



Как Hexway Vampr ASOC помогает в работе

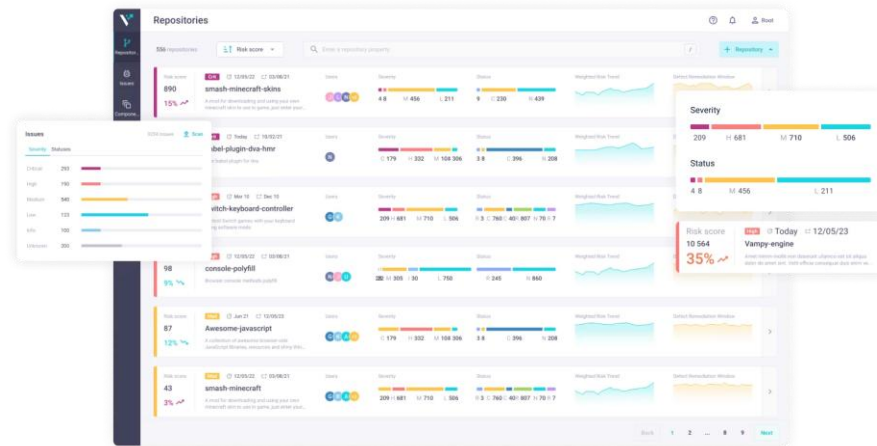
Проблемы DevSecOps





Hexway Vampy ASOC

Hexway Vampy ASOC — это комплексная платформа для управления безопасностью приложений. Она предоставляет инструменты анализа, мониторинга и устранения уязвимостей.



Управление безопасностью

Обнаружение

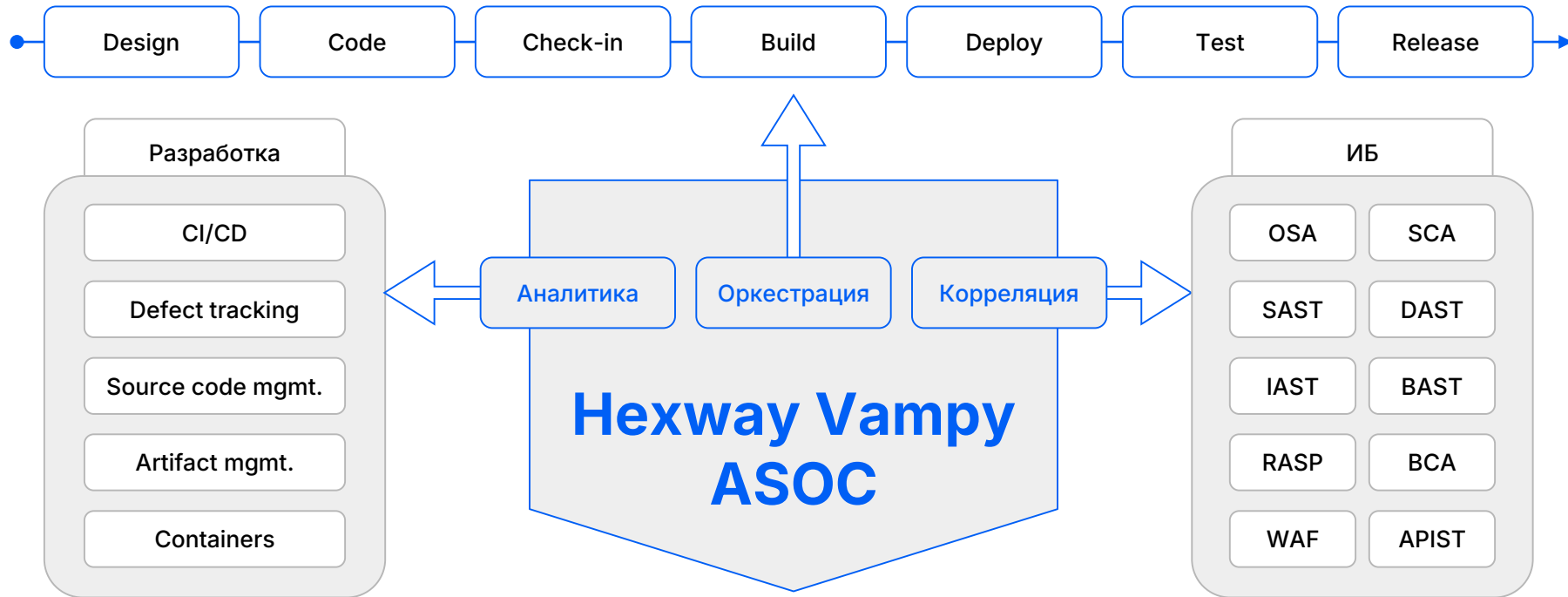
Анализ

Мониторинг

Устранение



Hexway Vampy ASOC – сердце DevSecOps





Единая платформа для всех сканеров

Мгновенно агрегируйте результаты сканирования уязвимостей SAST, DAST, SCA в одном окне. Haxway Vampry ASOC поддерживает интеграцию из коробки с опенсорс и коммерческими сканерами, в том числе российскими, а также таск-трекерами.

The interface displays the overall status of a task as **In progress** (blue lightning bolt icon). The profile is set to **Default**. Below this, there are buttons for **Semgrep** and **Trivy: FileSystem**, with a **Start** button (green play icon) to the right. Above the main interface, there are floating labels for **Done** (green checkmark), **Trufflehog**, **Gitleaks**, and **Error** (red X).

Status	Task ID
> In progress	1525efd5-3efd-4295-b395-7090977d3989
> Error	1525efd5-3efd-4295-b395-7090977d3989
> Done	1525efd5-3efd-4295-b395-7090977d3989
> Done	1525efd5-3efd-4295-b395-7090977d3989

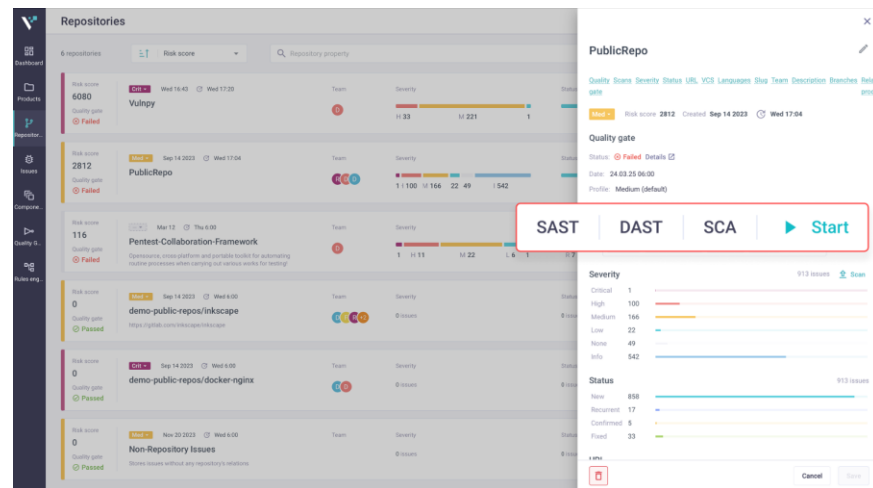


Сканируйте... даже если нет сканеров

SAST и SCA сканеры доступны из коробки.

Установите Hexway Vampy ASOC, и уже через 10 минут можно сканировать репозитории и контейнеры – даже если у вас нет своих сканеров.

Hexway Vampy ASOC имеет все нужное в комплекте поставки и умеет управлять как известными опенсорс сканерами, так и российскими коммерческими продуктами.





Все для качественного триажа

Hexway Vampr ASOC автоматически упорядочивает данные от сканеров, устраняя повторяющиеся уязвимости и игнорирует ложные срабатывания.

Платформа подскажет, какие из обнаруженных уязвимостей требуют немедленной реакции, а какие можно отправить в бэклог.

<input type="checkbox"/>	Title	Status	Sev... 1 2 3 4 5	CVE
<input type="checkbox"/>	Service 'postgres' is running with a writabl...	Recurrent	Crit	
<input type="checkbox"/>	CVE-2021-20270 in Pygments:2.3.1	New	Crit	CVE-2021-20270
<input type="checkbox"/>	Detected possible formatted SQL query	New	Crit	
<input type="checkbox"/>	Unnecessary semicolon.	Reopened	Crit	
<input type="checkbox"/>	libxpat: Integer Overflow or Wraparound	New	Crit	CVE-2024-45491
<input type="checkbox"/>	CVE-2021-20270 in Pygments:2.3.1	New	Crit	CVE-2021-20270
<input type="checkbox"/>	CVE-2020-11022	New	Crit	CVE-2020-11022
<input type="checkbox"/>	zlib: integer overflow and resultant heap-b...	Recurrent	Crit	CVE-2023-45853

Crit

High

Med

Low

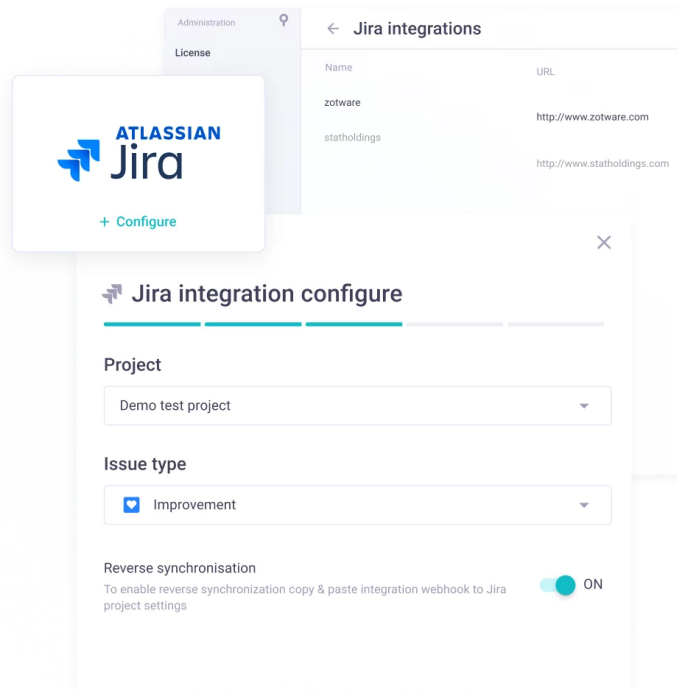
Info



Полный контроль над исправлением

Hexway Vampy ASOC **имеет двустороннюю интеграцию с task трекерами**, такими как Jira и Kaiten, что позволяет автоматически обновлять статусы задач и переоткрывать/закрывать уязвимости при повторных сканированиях.

Устраняйте уязвимости на ранних этапах, повышайте безопасность приложений и ускоряйте исправление ошибок.

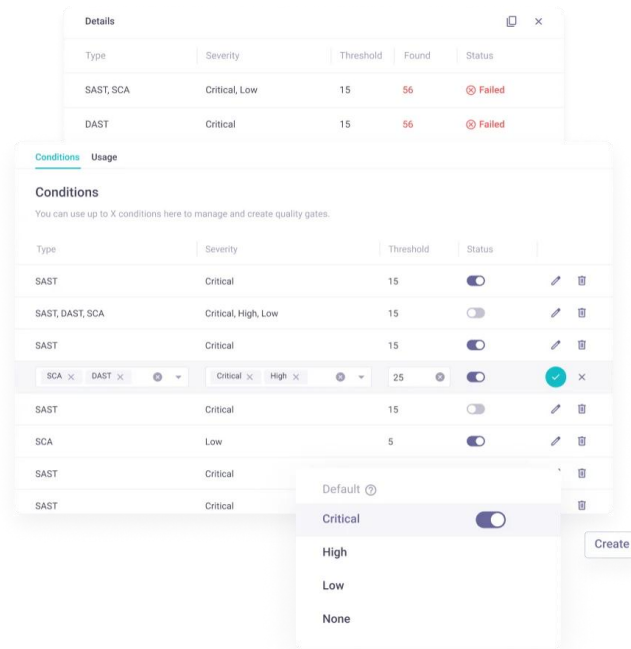




Контроль безопасности с Quality Gates

Гибкая система Security Quality Gates позволяет **настроить критерии прохождения сканирований**, на основе которых можно принимать решения о продолжении сборки продукта или остановки CI/CD пайплайнов.

Больше никаких критов в продакшене!

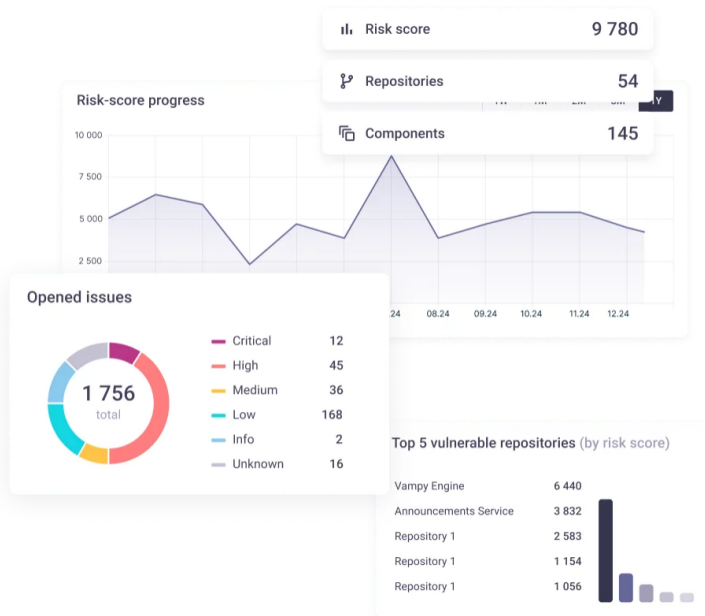




Анализ на основе метрик

Получите полное представление о состоянии безопасности продуктов. Становятся ли продукты безопаснее? Кто из разработчиков чаще всего пишет уязвимый код? Долго триажат или долго фиксируют? Какие репозитории не покрыты SASTами?

Ответы вы найдете в наглядных дашбордах и отчетах Hexway Vampy ASOC.





Готово к большим нагрузкам

Платформа выдерживает большие нагрузки, работая с десятками тысяч репозиторий и сотнями сканеров одновременно.

Скорость чтения и обработки данных Nexway Vamru ASOCкратно превышает эти показатели open-source решений из коробки.

Title	Status	Severity	CVE	CVSS	File Path	Line No	Lib Name	Lib Version	Repository
BlueKeep vulnerability is not patched (CVE-2019-0708)	New	Crit	CVE-2022-30284	9,5	/libquery-1.8.0.min.js	44	senry-sdk	1.13.0	Repository
Weak passwords to SSH accounts	Retest required	Crit	CVE-2022-30284	9,1	/libquery-1.8.0.min.js	1	senry-sdk	1.13.0	Repository
Python libmap 0.7.2 adds unittest	New	High	CVE-2022-30284	8,9	/libquery-1.8.0.min.js	4567	senry-sdk	1.13.0	Repository
MS17-010 security update missing	Fix not confirmed	High	CVE-2022-30284	8,3	/libquery-1.8.0.min.js	4567	senry-sdk	1.13.0	Repository
BlueKeep vulnerability is not patched (CVE-2019-0708)	New	High	CVE-2022-30284	7,2	/libquery-1.8.0.min.js	44	senry-sdk	1.13.0	Repository
MS17-010 security update missing	Verified	Med	CVE-2022-30284	6,9	/libquery-1.8.0.min.js	34	senry-sdk	1.13.0	Repository
MS17-010 security update missing	New	Med	CVE-2022-30284	5,4	/libquery-1.8.0.min.js	1	senry-sdk	1.13.0	Repository
BlueKeep vulnerability is not patched (CVE-2019-0708)	New	Med	CVE-2022-30284	5,1	/libquery-1.8.0.min.js	44	senry-sdk	1.13.0	Repository
BlueKeep vulnerability is not patched (CVE-2019-0708)	Risk accepted	Med	CVE-2022-30284	5,0	/libquery-1.8.0.min.js	4567	senry-sdk	1.13.0	Repository
BlueKeep vulnerability is not patched (CVE-2019-0708)	New	Med	CVE-2022-30284	4,5	/libquery-1.8.0.min.js	567	senry-sdk	1.13.0	Repository
BlueKeep vulnerability is not patched (CVE-2019-0708)	New	Med	CVE-2022-30284	4,1	/libquery-1.8.0.min.js	34	senry-sdk	1.13.0	Repository
BlueKeep vulnerability is not patched (CVE-2019-0708)	Assigned	Low	CVE-2022-30284	3,2	/libquery-1.8.0.min.js	4567	senry-sdk	1.13.0	Repository

Демонстрация





СПА-СИ-БО!



hexway.ru