ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Программное обеспечение для мониторинга и проверки контейнерных сред

АТОМИК

Описание функциональных характеристик

На 23 листах

Москва
2024

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Содержание

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Список таблиц

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Список рисунков

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

1 Введение

Настоящее описание содержит информацию об основных функциональных характеристиках продукта АТОМИК (далее по тексту - Продукт).

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

2 Общие сведения

АТОМИК - программное обеспечение для сканирования контейнерных информационных систем и приложений в них с целью обнаружения уязвимостей в процессах разработки и эксплуатации.

АТОМИК интегрируется в контейнерную среду для получения данных о ее структуре и приложениях.

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

3 Функциональные характеристики

3.1 Пользовательский интерфейс

АТОМИК реализует собственный Web-интерфейс управления с поддержкой Web-браузеров: Yandex Browser, Google Chrome, Edge, Mozilla Firefox. Для получения доступа к функциям управления Web-интерфейса требуется ввести данные учетной записи пользователя.

3.2 Панель мониторинга

Поддерживается отображение статистических метрик результатов работы Продукта в текстовом и графическом отображении.

Поддерживается возможность добавлять, редактировать отображение и размещение метрик в удобном порядке.

Наглядное отображение статистики анализа уязвимостей представлено ниже.

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

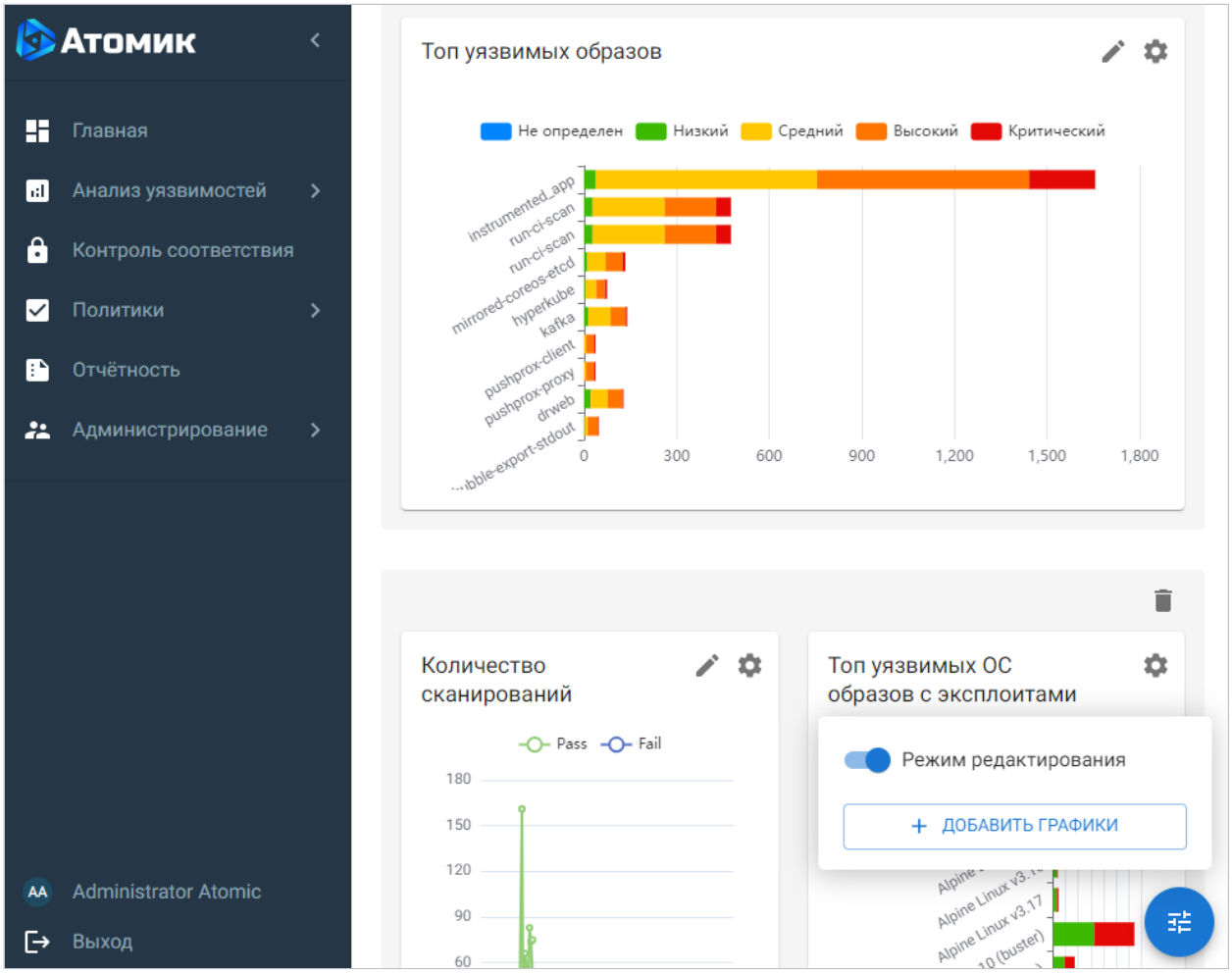

Рисунок 1 – Форма «Панель мониторинга»

3.3 Анализ уязвимостей

Поддерживается проведения сканирования следующими методами:

- встраивание кода сканирования в pipeline;
- интеграция агента сканирования в runtime среде;
- выборочное сканирование Docker-образов.

Используя перечисленные методы поддерживается анализ сканируемых приложений, включает в себя следующие функциональные особенности:

- обнаружение уязвимостей с эксплойтами;
- обнаружение возможности исправления уязвимостей;
- обнаружение секретов в образах и исходном коде приложений;
- обнаружение вирусов в образах и исходном коде приложений;

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

– представление подробной информации о контейнерной среде, включает в себя детализацию по принадлежности к кластеру, по namespace, по образу, по приложению;
– предоставление подробной информации о каждом просканированном образе: ОС, архитектура, тип образа, список установленного ПО, размер;
– анализ контейнерной среды об уязвимостях в виде: общего количества и списка уязвимостей, с детализацией по критичности, в разрезе количества уязвимостей в каждом установленном программном пакете, с пометкой о наличии эксплойта и/или исправления;
– ведение истории сканирований с вердиктом успешности или неуспешности сканирования;
– детальное определение уровня опасности каждой уязвимости по оценке CVSS;
– предоставление ссылки на уязвимости в базе CVE;

Просмотр просканированных приложений:

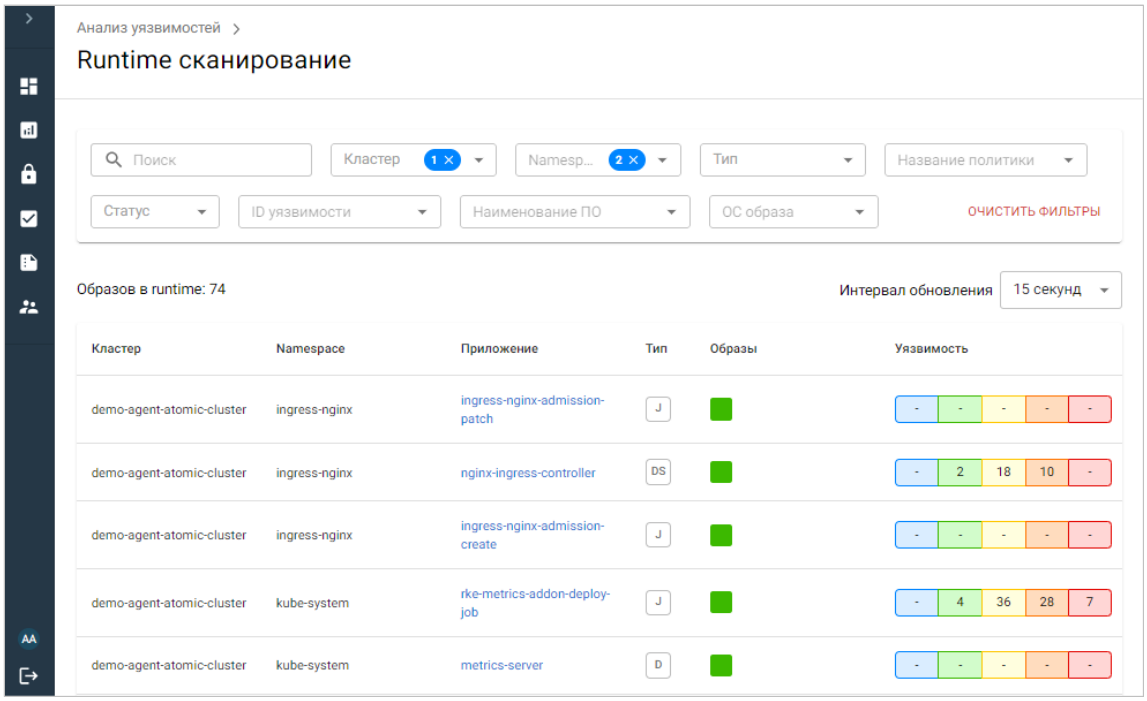

Рисунок 2 – Форма «Сканирований Runtime»

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Просмотр определенного контейнера:

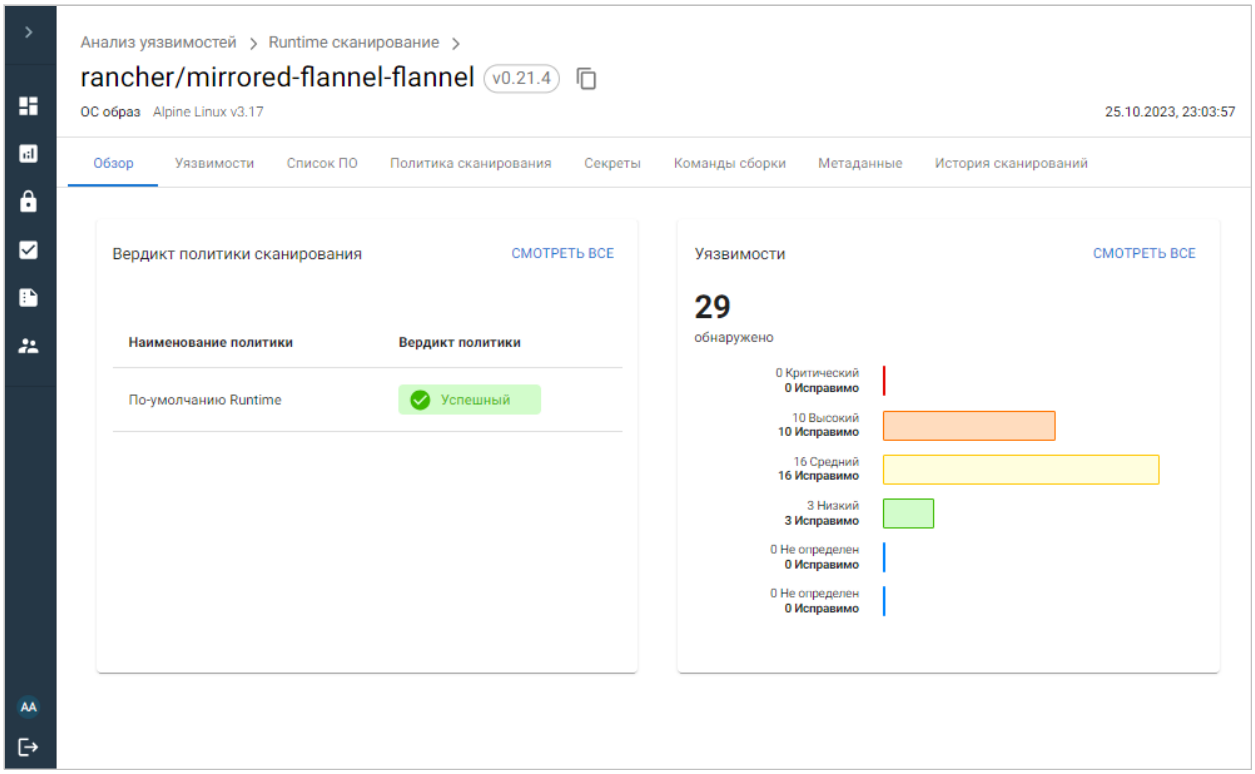

Рисунок 3 – Сканирование. Обзор

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Просмотр списка уязвимостей определенного контейнера:

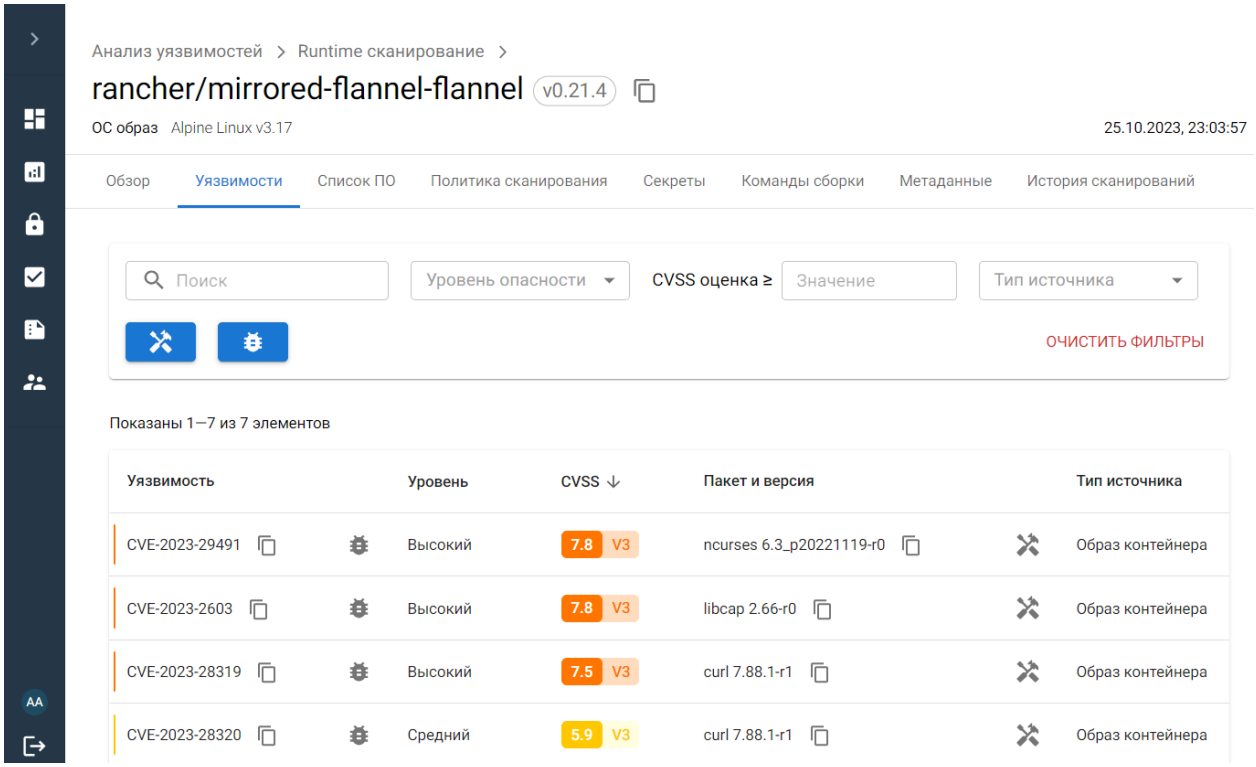

Рисунок 4 – Сканирование. Уязвимости

Просмотр определенной уязвимости:

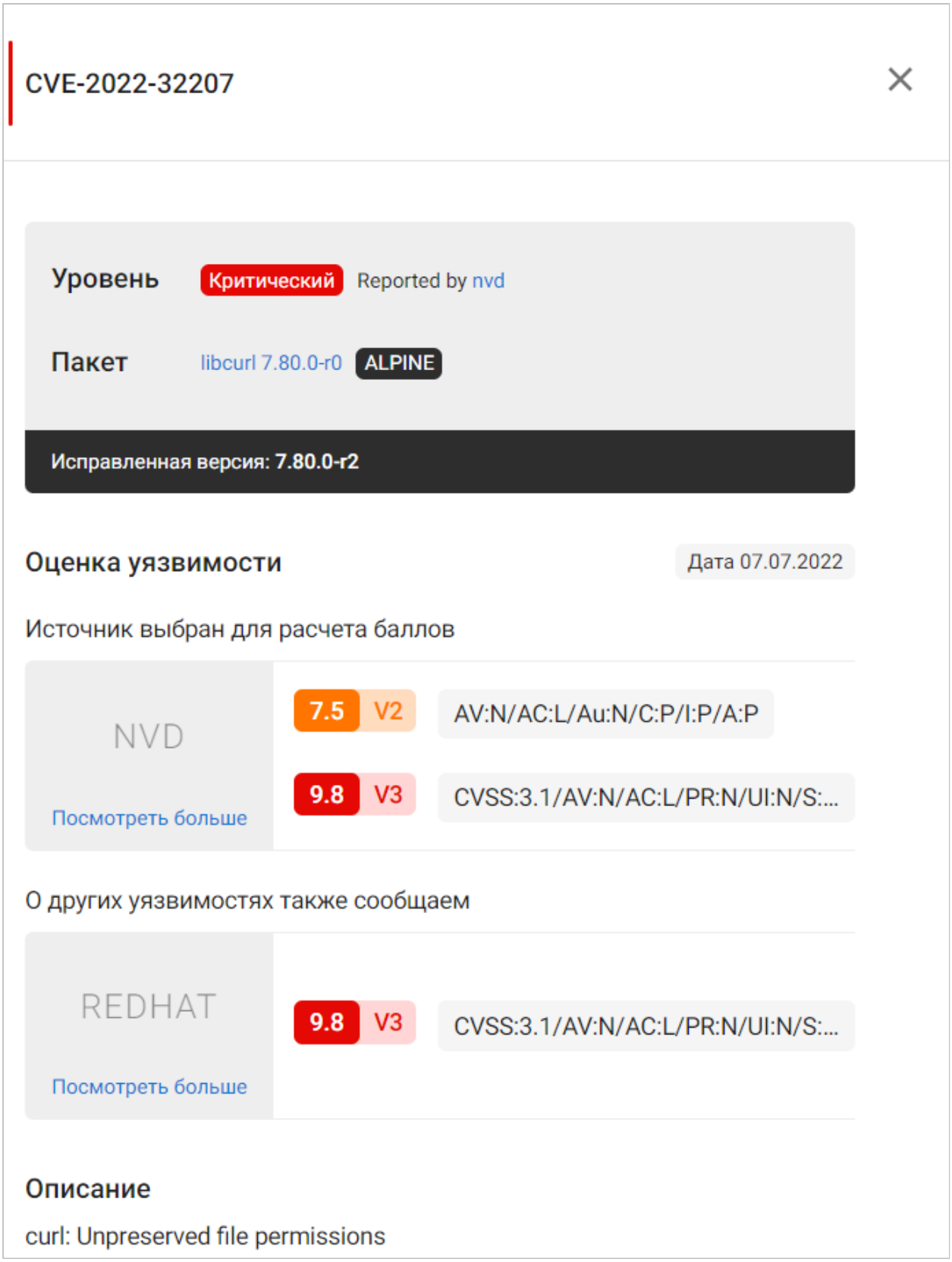

Рисунок 5 – Сканирование. Сведения об уязвимости

Просмотр списка ПО определенного контейнера:

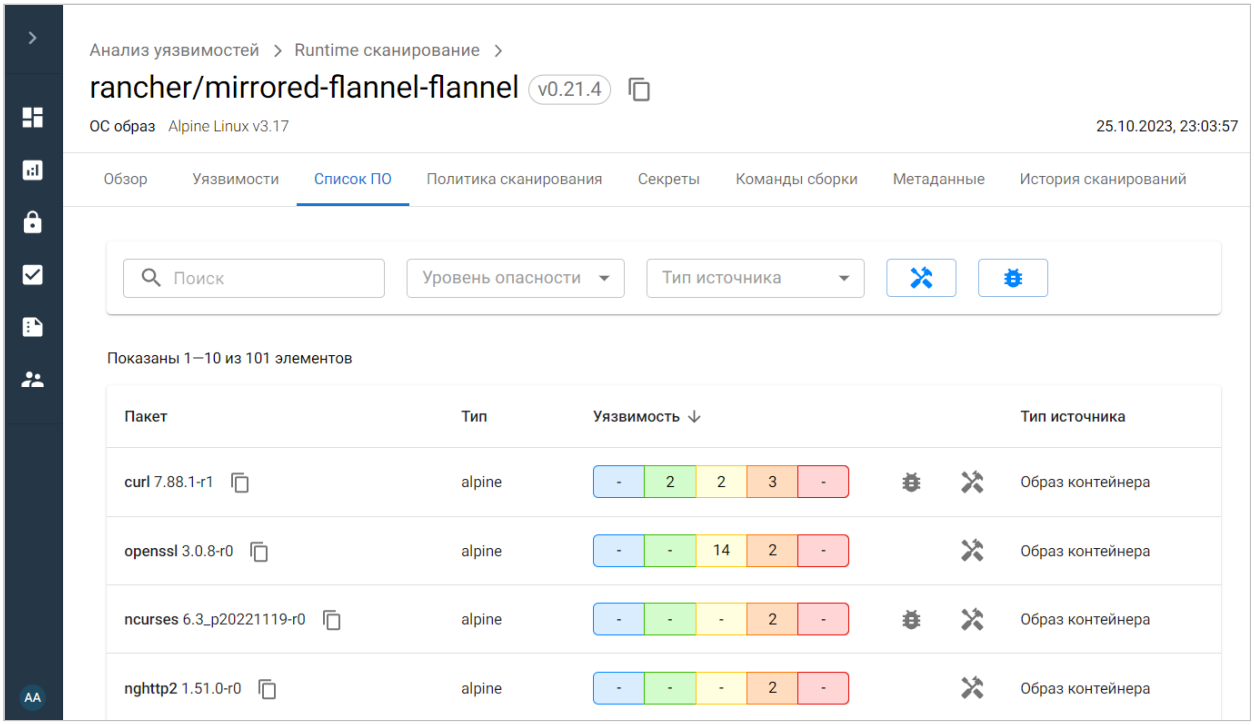

Рисунок 6 – Сканирование. Список ПО

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Просмотр уязвимостей определенного программного пакета:

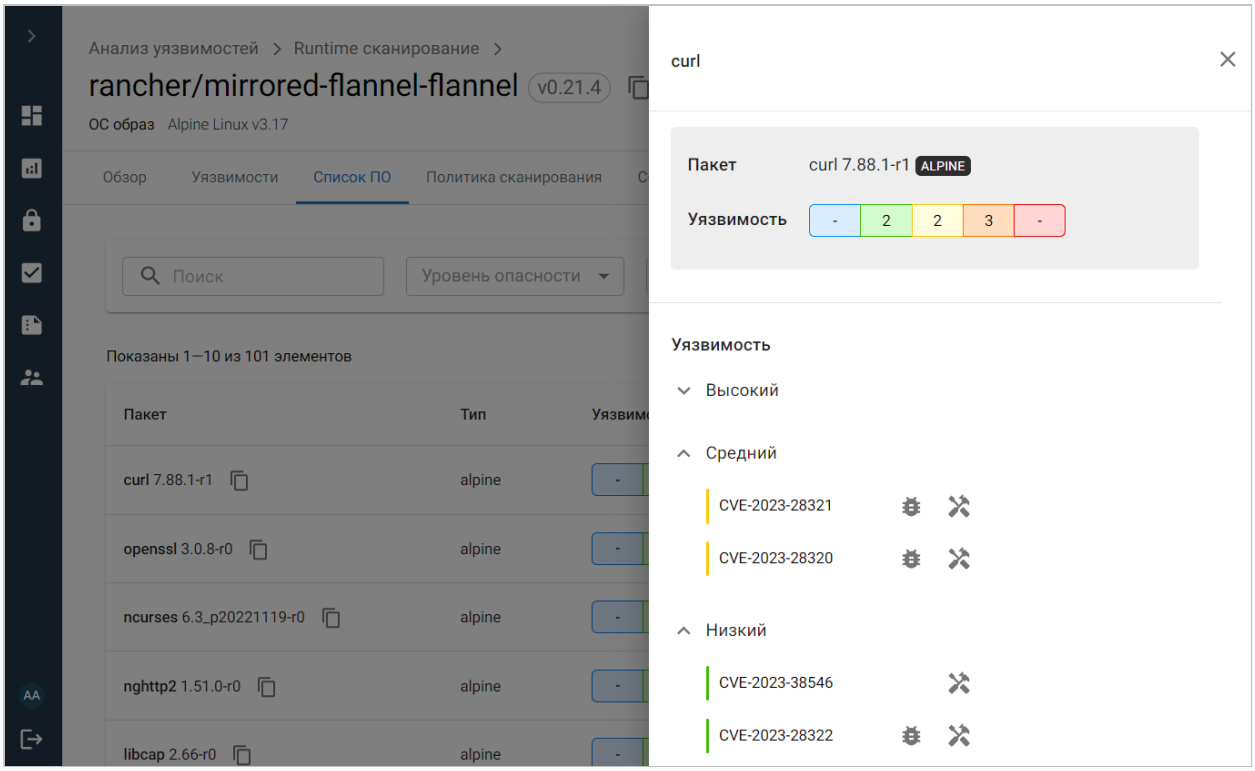

Рисунок 7 – Сканирование. Сведения о пакете ПО

3.4 Контроль соответствия

Поддерживается контроль соответствия серверов контейнерного оркестратора Kubernetes стандартам защиты от распространенных уязвимостей и неправильных конфигураций, включает в себя следующие функциональные особенности:

- создание собственных политик контроля соответствия;
- обнаружение соответствий стандартам по каждому отдельному правилу;
- подробное описание причины неуспешных результатов проверок;
- подробная детализация выполняемых действий во время проверок в неуспешных проверках;
- ведение истории проверок.

3.5 Политики безопасности

Поддерживается создание и применение политик безопасности с указанием нескольких наборов правил сканирования, имеет следующие функции:

- создание собственных политик;
- возможность блокировки сборки образа при отрицательном вердикте политики;
- возможность получения уведомлений о применении политик;
- возможность ограничения действия политик по основным тегам образа;
- применение политик к одному из типов сканирования: pipeline, runtime или registry (только одного);
- применение политик к отдельным агентам или ко всем;
- применение политик согласно выбранным наборам правил обнаружения уязвимостей;
- применение политик согласно найденным секретам;
- применение политик согласно найденным вирусам.

3.6 Наборы правил сканирования

Поддерживается создание определенных наборов правил обнаружения уязвимостей для их применения в политиках безопасности, включает в себя следующие функциональные особенности:

- создание нескольких правил проверок уязвимостей образа в одном наборе;
- проверки уязвимостей на наличие эксплойта;
- проверки уязвимостей по скорингу CVSS V2/V3;
- проверки уровня критичности уязвимостей;
- проверки даты публикации уязвимостей;
- проверки наличия исправления уязвимостей;
- проверки по конкретным id уязвимостей;
- проверки используемых команд сборки образов Docker.

Набор правил сканирования:

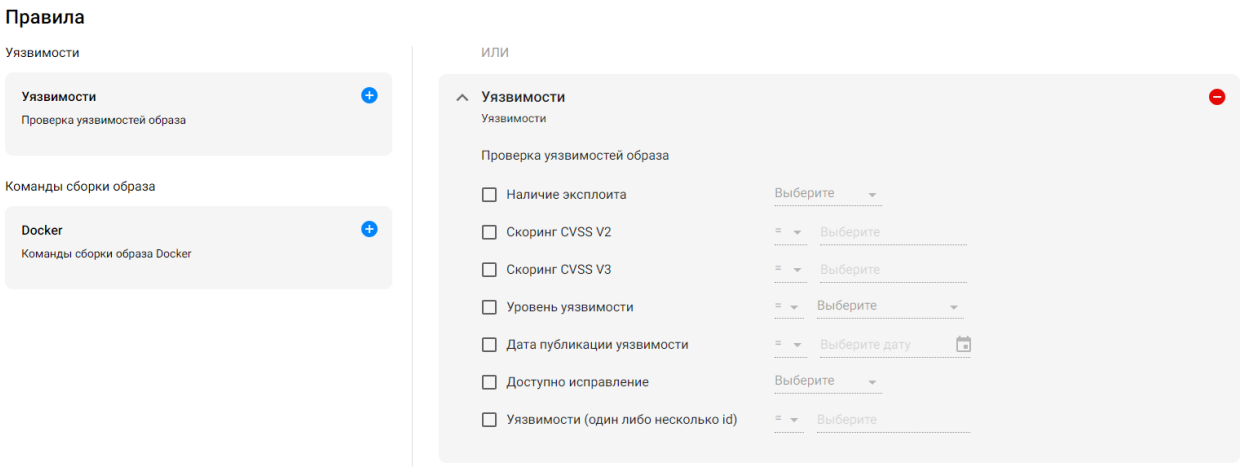

Рисунок 8 – Политики. Пакеты правил

3.7 Агенты сканирования

Поддерживается создание множественных API ключей для интеграции агента в системе контейнерной оркестрации, позволяет проводить поиск уязвимостей и применять блокирующие политики безопасности.

Поддерживается применение политики без блокировки.

Поддерживается разделение отличающихся политик путем создания нескольких агентов и применения к ним соответствующей политики.

Список агентов:

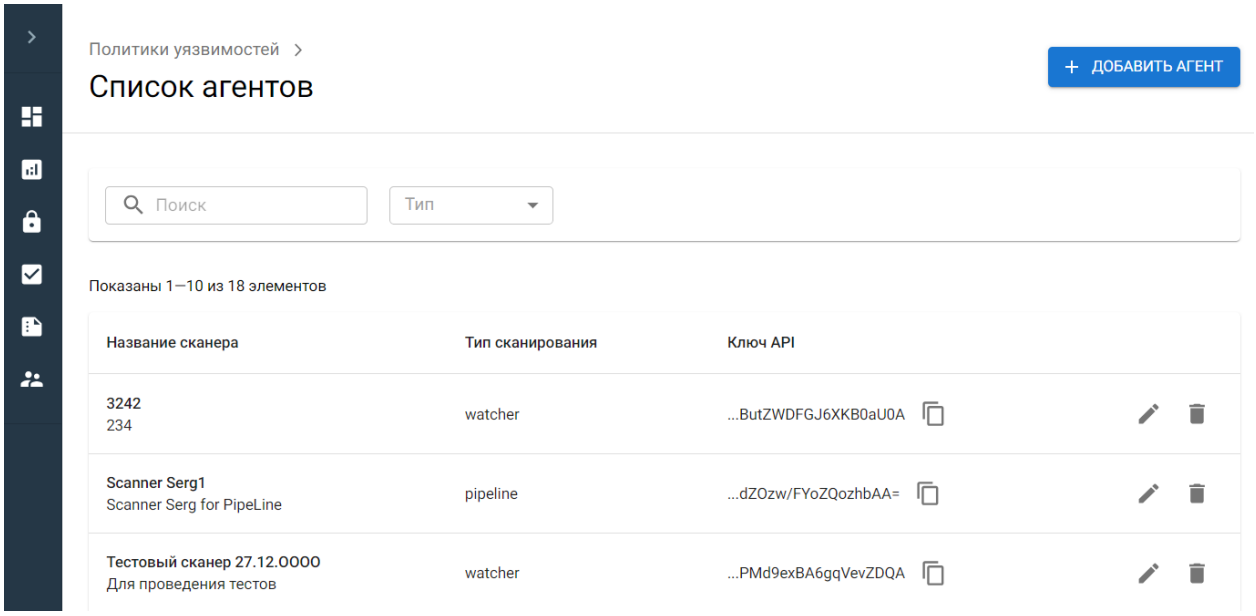

Рисунок 9 – Политики. Список агентов

3.8 Отчетность

Поддерживается выгрузка отчетов по данным об уязвимостях в формате NDJSON, поддерживается возможность выбора периода выгрузки, поддерживается отправка отчетов по расписанию.

3.9 Ролевой доступ пользователей. LDAP

Поддерживается интеграция со службами каталогов с использованием SSL шифрования.

Системой поддерживается разграничение доступа пользователей по ролям и группам доступа в соответствии с группами LDAP.

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

4 Требования к среде развертывания

Перечень основных требований к среде развертывания приведен в Табл.1

Табл. 1 – Требования к среде развертывания

Тип	Наименование
Операционная система	Поддержка eBPF: Linux Kernel 4.16+; Поддержка BTF: Linux Kernel 5.1+
Программное обеспечение для автоматизации развёртывания и управления приложениями	Docker, Kubernetes
СУБД	PostgreSQL, ClickHouse
Брокер сообщений	Apache Kafka
Балансировщик	Nginx Ingress

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

5 Системные требования

Перечень минимальных системных требований для работы остновных компонентов Продукта приведен в Табл.2

Табл. 2 – Системные требования

Количество процессоров:	4
Оперативная память:	16 Гб
Жесткий диск:	80 Гб свободного места

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

6 Перечень принятых сокращений

ИС	–	автоматизированная информационная система Заказчика
БД	–	база данных, управляемая реляционной СУБД
ПО	–	программное обеспечение
ПП	–	программная платформа
ПК	–	программный комплекс
СКЗИ	–	средство криптографической защиты информации
СУБД	–	система управления базами данных

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

7 Перечень терминов и определений

CI/CD - технология автоматизации тестирования и доставки новых модулей разрабатываемого программного обеспечения заинтересованным сторонам (разработчики, аналитики, инженеры качества, конечные пользователи и др.);

Pipeline - процесс, который ведет разработку программного обеспечения путем создания, тестирования и развертывания кода, также известного как CI / CD;

Runtime – процесс в контейнерной среде содержащий разработанное программное обеспечение с целью его использования;

Namespace – группа ресурсов в пределах одного кластера;

CVE - база данных общеизвестных уязвимостей информационной безопасности;

CVSS - открытый стандарт, используемый для расчета количественных оценок уязвимости в информационной безопасности.

Автоматизированная информационная система (ИС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор системный – лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

Администратор информационной безопасности – лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.

Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

Доступ к информации (доступ) – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступность (санкционированная доступность) информации – состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Защита информации от несанкционированного доступа (защита от НСД) **или воздействия** – деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922).

Информационная технология – приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных (ГОСТ 34.003).

Информационные сети общего пользования – вычислительные (информационно-телекоммуникационные сети) открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Локальная вычислительная сеть – вычислительная сеть, поддерживающая в пределах ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации, предоставляемых подключаемым устройствам для кратковременного монопольного использования.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обработка информации – совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

Продукт – программный комплекс **АТОМИК**, введенный в эксплуатацию в составе Информационной системы Заказчик.

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации (ГОСТ Р 50922).

Целостность информации – устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.