LUNTRY

LUNTRY 4.6
НОВЫЕ ВОЗМОЖНОСТИ ДЛЯ ЗАЩИТЫ КОНТЕЙНЕРНЫХ И ОБЛАЧНЫХ СРЕД

Дмитрий Евдокимов

Founder&CTO Luntry

Обо мне

> Я не верю в то, что систему можно сделать надежной и безопасной, не понимая того, как она устроена.

Основатель и технический директор Luntry

Более 15 лет опыта в ИБ

Специализация — безопасность контейнеров и Kubernetes

Автор ТГ-канала k8s(in)security

Эксперт в сфере безопасности контейнерных сред

- Организатор конференции «БеКон» по БЕзопасности КОНтейнеров
- Бывший редактор рубрик в журнале «ХАКЕР», автор серии статей
- Автор курса «Cloud Native безопасность в Kubernetes»
- Создатель канала k8s (in)security
- Член программного комитета CFP DevOpsConf и KUBER CONF

Спикер

VK Kubernetes	Confidence	ZeroNights	БеКон	HITB
DevOpsConf	HackInParis	KuberConf	BlackHat	PHDays
Kazhackstan	HighLoad++	OFFZONE	DevOops	SAS

LUNTRY

О компании Luntry

Luntry — это Комплексная Защита
на всем жизненном цикле
контейнерных приложений
и средств оркестрации на базе Kubernetes

Продукт в реестре Минцифры
https://reestr.digital.gov.ru/reestr/1057835/

Получение сертификата ФСТЭК планируется в сентябре 2026 года.

LUNTRY.RU

Регуляторика по контейнеризации и Luntry

LUNTRY

ПРИМЕНИМОСТЬ LUNTRY

Защита ГИС и гос. ИС:

- Приказ ФСТЭК № 117 и методический документ от 12.04.26

Защита КИИ:

- 187-ФЗ
- Приказ ФСТЭК № 239 (Приложение)

Защита ИСПДн:

- ФСТЭК № 21 (п.8.11, Приложение)

ОБЯЗАТЕЛЬНОСТЬ

- ГИС: К1, К2, К3
- ИСПДн: У31, У32
- КИИ: да

118 приказ ФСТЭК

Это требование к средам контейнеризации, Luntry это навесное средство защиты и под данный приказ не попадает. НО реализует ряд требований из данного приказа.

117 приказ ФСТЭК и его методический документ

Luntry закрывает пункты про защиту технологий контейнерных сред и их оркестрации (ЗКО) и общие процессы и меры

Информационное сообщение ФСТЭК России 240/24/38

О повышении безопасности средств защиты информации, в состав которых разработчики включают средства контейнеризации или образы контейнеров

Банк данных угроз безопасности информации от ФСТЭК

Luntry закрывает все 5 УБИ посвященные контейнерам

Функциональность Luntry

Контроль Kubernetes-ресурсов

Контроль состояния Kubernetes-кластеров

Контроль соответствия кластера стандартам

Управление безопасностью образов

Сетевая безопасность

Анализ прав доступа

Защита Runtime

Обновления в Luntry 4.6

Контроль Kubernetes-ресурсов

Контроль состояния Kubernetes-кластеров

Контроль соответствия кластера стандартам

Управление безопасностью образов

Сетевая безопасность

Анализ прав доступа

Защита Runtime

LUNTRY 4.6

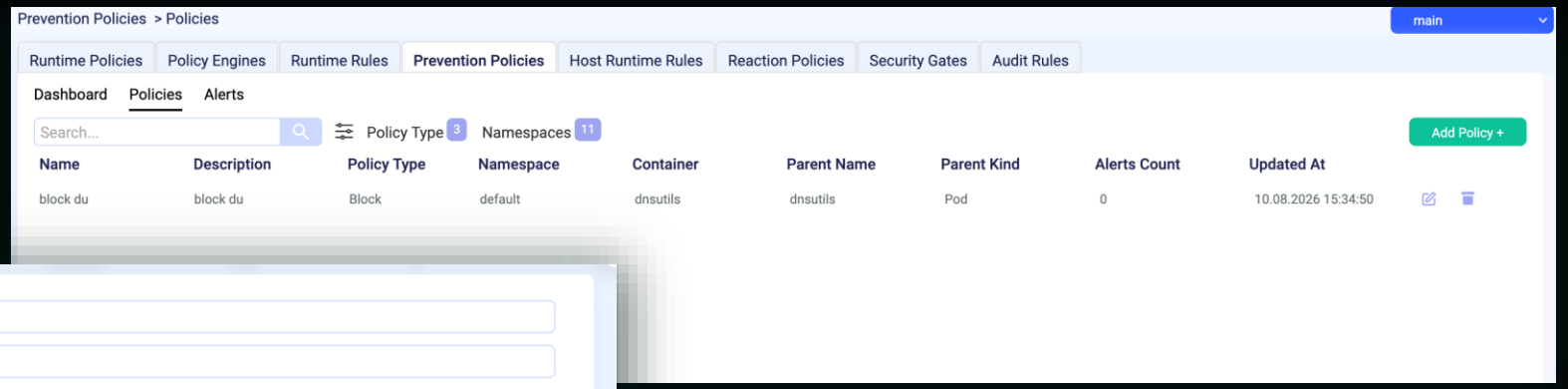
LUNTRY

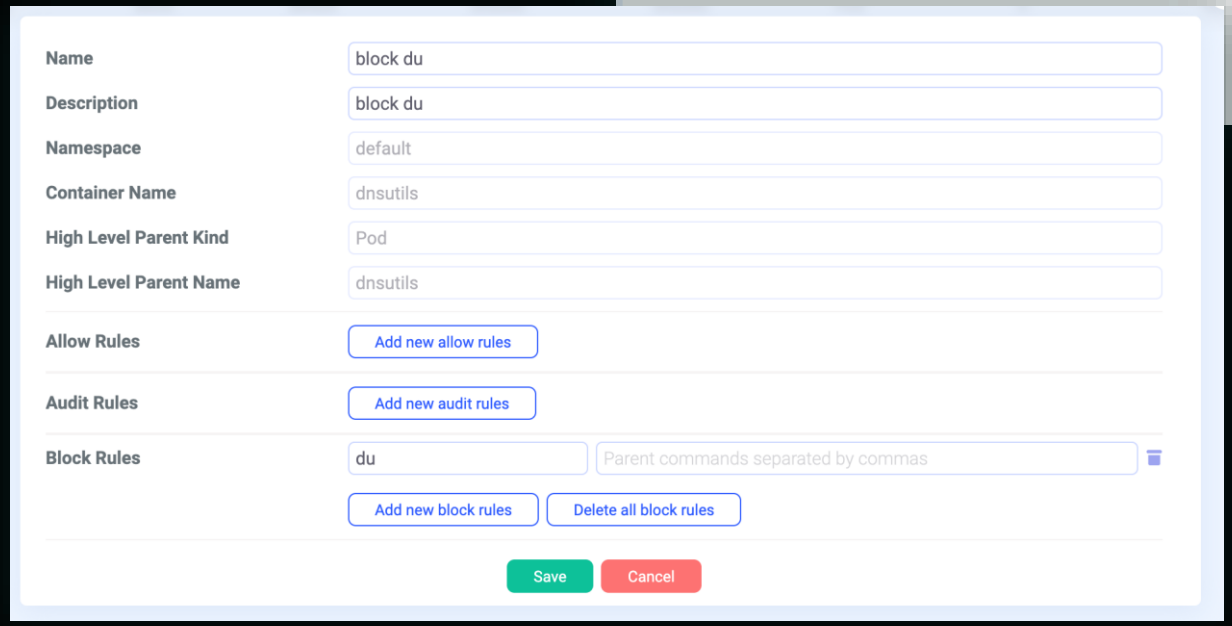
	LUNTRY 4.6
Модуль Runtime защиты	• Добавление Host Runtime Rules • Добавление Prevention Policies • Добавление поддержки не оркестриуемых окружений Docker Rules
Модуль сетевой безопасности	• Генерация DNS политик для CNI Cilium
Модуль безопасности образов	• Новые виды отчетов • Продвинутая приоритезация найденных уязвимостей с учетом различных факторов • Добавление поддержки Threat Intelligence (TI) от Solar 4Rays

PREVENTION POLICIES

Задача для runtime

- Исключить запуск нежелательных исполняемых файлов внутри контейнера
  - Подход через whitelist и blacklist

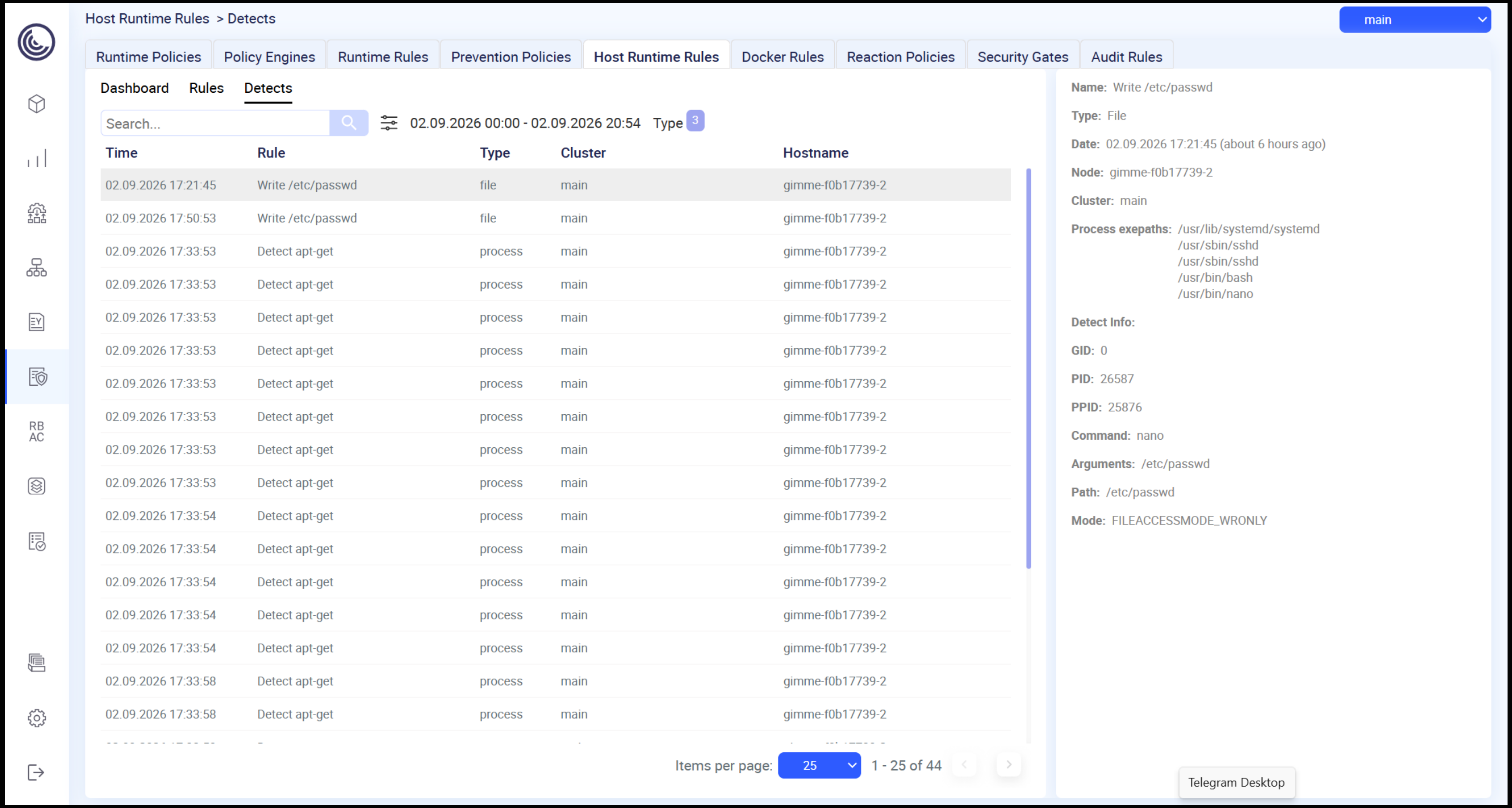




HOST RUNTIME RULES

Задача для runtime

- Обнаружить вредоносную, нежелательную активность за пределами контейнера на контейнером хосте
    - Атакующий сбежал из контейнера, атакующий получил доступ к Node кластера Kubernetes

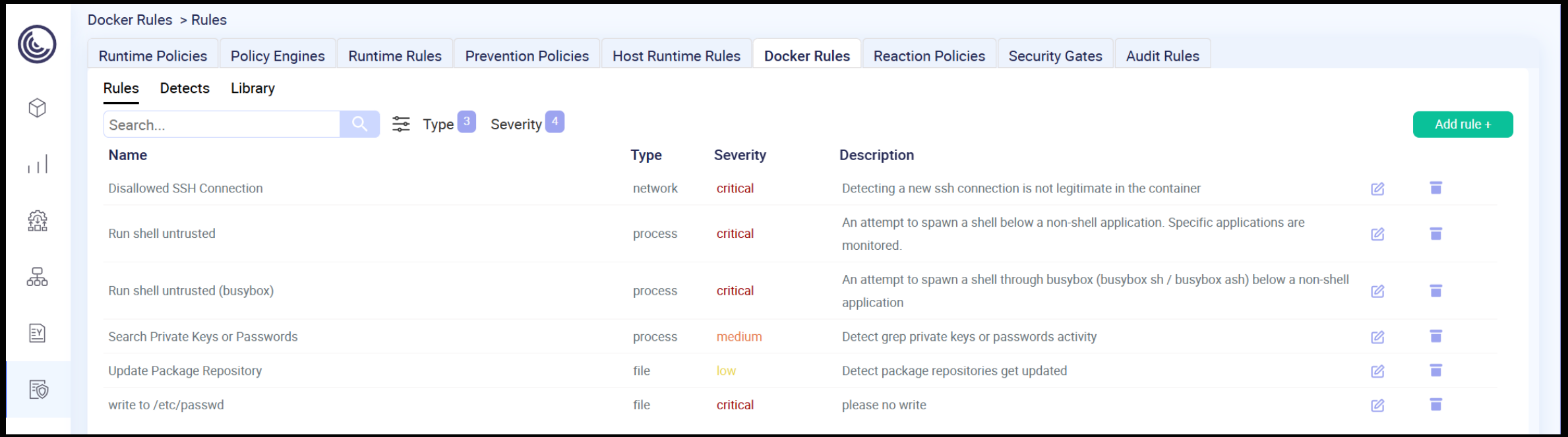


DOCKER RULES

НЕОРКЕСТРИРУЕМЫЕ ОКРУЖЕНИЯ

Задача для runtime

- Обнаружить вредоносную, нежелательную активность в контейнере в не оркестрируемом окружении
  - Аналог Runtime Rules, но для Docker, Podman
  - Атакующий внутри Docker контейнера



ГЕНЕРАЦИЯ DNS ПОЛИТИК ДЛЯ CNI CILIUM

Задача сетевой безопасности

- Гранулированной сетевой контроль исходящего трафика из кластера
- Решение проблемы динамических IP
- Микросегментация для внешних зависимостей

```yaml
apiVersion: cilium.io/v2
kind: CiliumNetworkPolicy
metadata:
  creationTimestamp: null
  name: luntry-np-pod-default-curl-loop-5
  namespace: default
spec:
  egress:
  - toCIDR:
    - 156.137.3.32/32
    toPorts:
    - ports:
      - port: "443"
        protocol: TCP
  - toFQDNs:
    - matchName: dhl.com.
    - matchName: fedex.com.
    - matchName: www.dhl.com.
    - matchName: express.dhl.ru.
    - matchName: www.fedex.com.
    - matchName: www.logistics.dhl.ru.
```

LUNTRY

LUNTRY

НОВАЯ THREAT INTELLIGENCE (TI) ИНФОРМАЦИЯ

Задача анализа образов

- Анализ ОС базового слоя образа
  - Контроль в Security Gates
- Анализ EOL (End Of Live) программных продуктов и пакетов
  - Новый тип отчета
  - Контроль в Security Gates
- Анализ на вредоносные пакеты (Malicious packages)
  - Новый тип отчета
  - Контроль в Security Gates
- Поддержка YARA-правил от Solar 4Rays для обнаружения malware
  - Уникальная экспертиза и детекты

LUNTRY

4RAYS by SOLAR

LUNTRY

CTEM

ПРОДВИНУТАЯ ПРИОРИТЕЗАЦИЯ НАЙДЕННЫХ УЯЗВИМОСТЕЙ

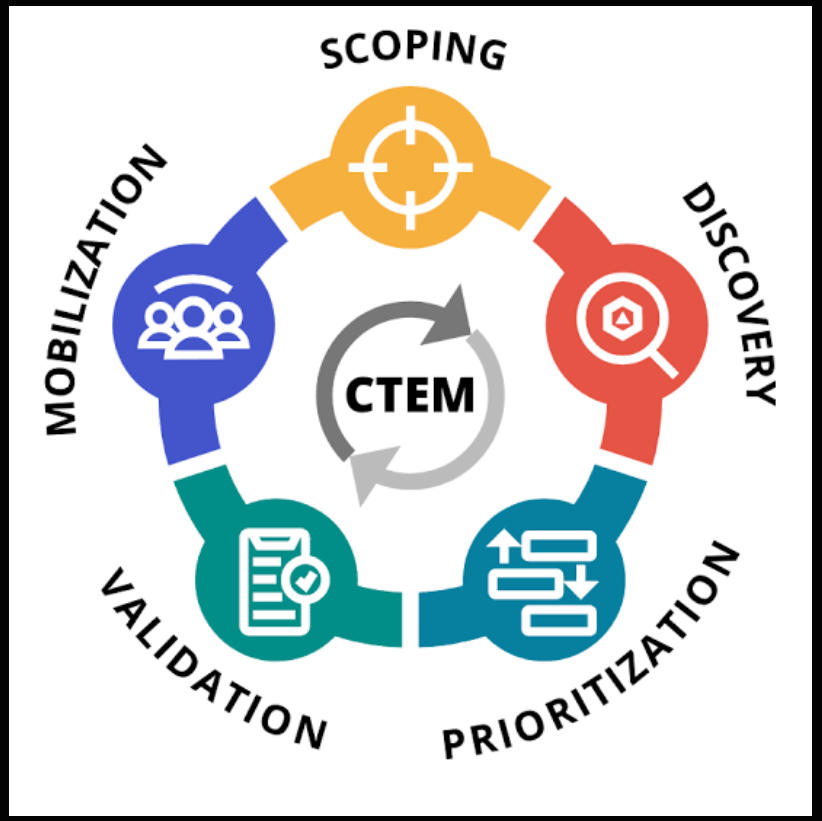
Задача по работе с уязвимостями

- Уязвимостей много
  - Даже с уровнем критичности Critical и High
  - Невозможно окружение без уязвимостей вообще
- Уязвимости постоянного появляются
  - Время играет против нас
  - Преимущество на стороне атакующего
- Исправления требует вовлечение/отвлечение специалистов
  - Страдает развитие продукта
  - Специалистов не хватает

LUNTRY

Что такое CTEM?

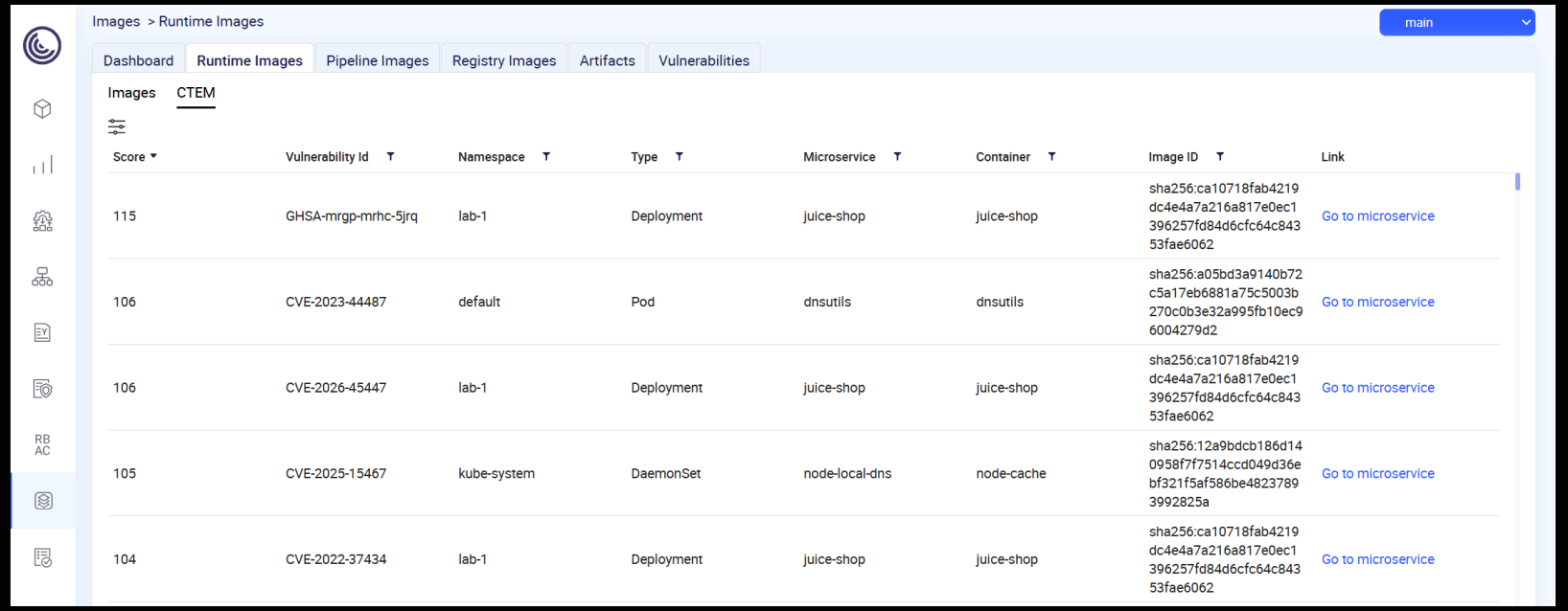
- CTEM (Continuous Threat Exposure Management) в информационной безопасности — это проактивная методология непрерывного выявления, оценки, приоритизации и устранения киберугроз и уязвимостей в цифровых активах компании.



CTEM в LUNTRY

Для приоритезации уязвимостей в образах контейнеров учитывается информация о:

- Уязвимости
- Эксплоитах и атаках
- Свойства контейнера
- Сетевом расположении и доступности
- Примененных мер безопасности к микросервису



LUNTRY

ROADMAP LUNTRY

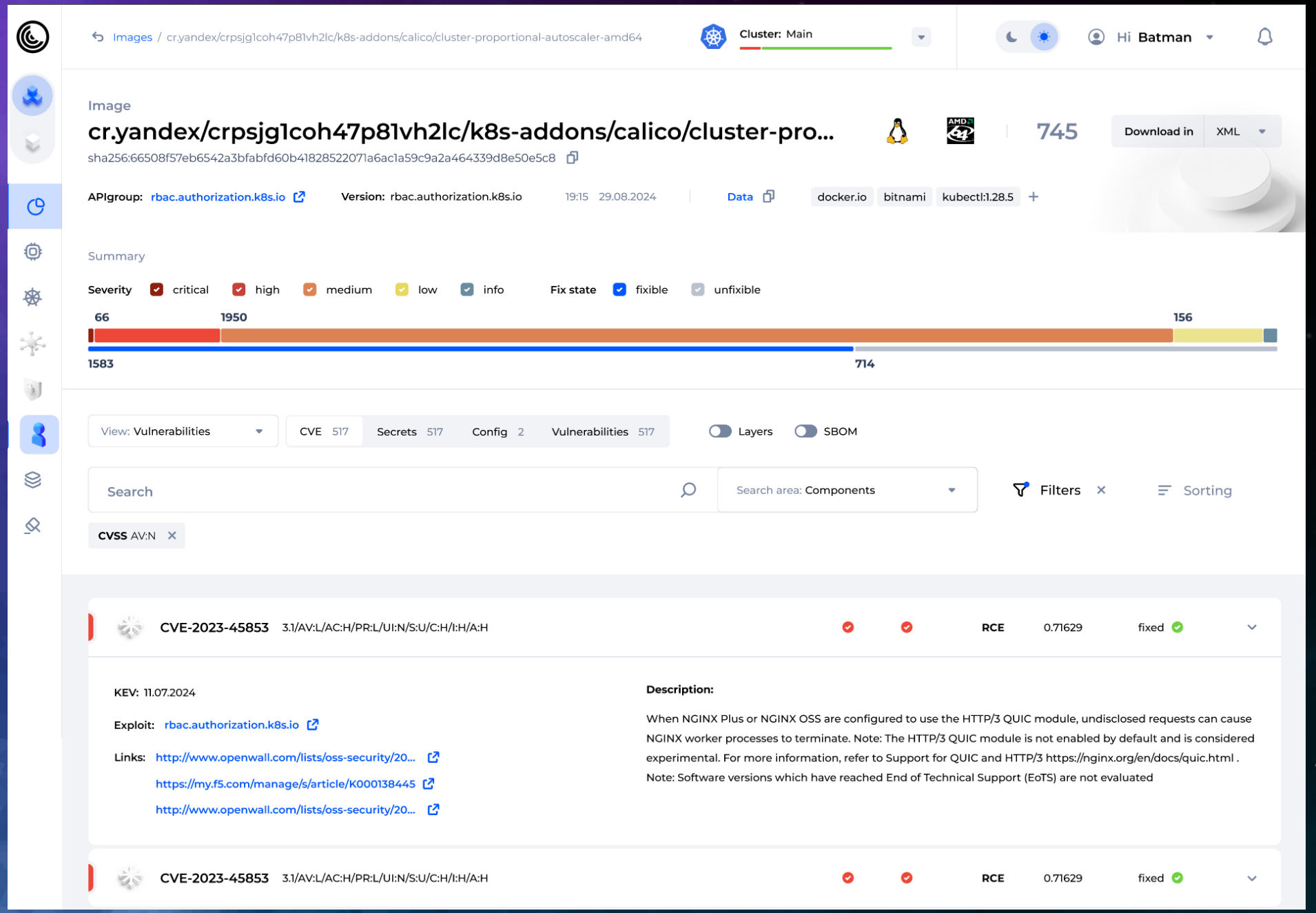
RoadMap Luntry

	Luntry 5.0
Модуль Runtime защиты	• Реализация функциональности SOAR
Модуль сетевой безопасности	• Конструктор NetworkPolicy
Модуль безопасности образов	• Пользовательские правила на YARA
Модуль контроля Kubernetes-ресурсов	• Обновление библиотеки детектов для Kubernetes Audit Log • Обновление библиотеки политик для PolicyEngines (VAP)
Модуль состояния Kubernetes-кластеров	• Анализ безопасности хостовой ОС
Общее	• Выпуск обновленного UI/UX • Продвинутое предоставление прав доступа и области видимости пользователей • Обработка 1M EPS

LUNTRY

5.0

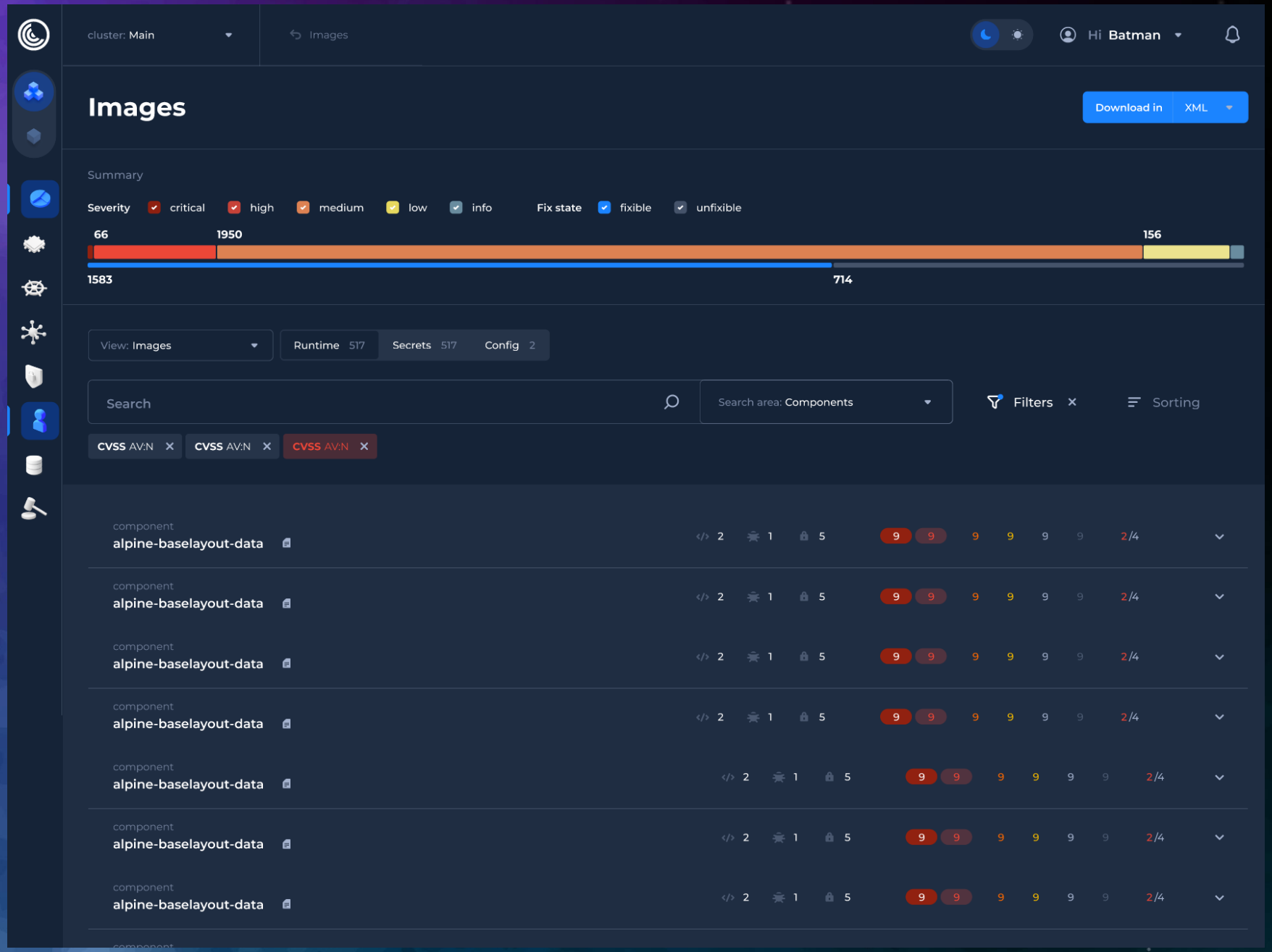
UX/UI



LUNTRY

5.0

UX/UI



LUNTRY

LUNTRY

luntry_official
luntrysolution
luntrysolution
luntry.ru
info@luntry.ru

ДМИТРИЙ ЕВДОКИМОВ
Founder & CTO Luntry

de@luntry.ru
Qu3b3c
k8security

СПАСИБО ЗА ВНИМАНИЕ!