LUNTRY

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

БЕЗОПАСНОСТЬ КОНТЕЙНЕРОВ И KUBERNETES: НЕ ПРОБЛЕМА, А РЕШЕНИЕ

Дмитрий Евдокимов

Основатель и технический директор 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»
- Член программного комитета CFP DevOpsConf и HighLoad++

Спикер

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

LUNTRY

Содержимое ответа
Длинное тире (—) — знак

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 во втором квартале 2026 года.

LUNTRY.RU

Функциональность Luntry

Контроль всех Kubernetes-ресурсов

Контроль состояния Kubernetes-кластеров

Контроль соответствия кластера стандартам

LUNTRY

Управление уязвимостями образов и best practice

Сетевая безопасность

Анализ прав доступа

Защита Runtime

Функциональность Luntry

Контроль всех Kubernetes-ресурсов

Контроль состояния Kubernetes-кластеров

Контроль соответствия кластера стандартам

LUNTRY

Управление уязвимостями образов и best practice

Сетевая безопасность

Анализ прав доступа

Защита Runtime

Жизненный путь образа

LUNTRY

CI\CD Pipeline
- Сборка образа
- Анализ образа
- Security/Quality gates
  - Возможна блокировка
- Подпись образа

Image registry
- Хранение
- Очистка/ротация
- Анализ образов
- Security/Quality gates

Runtime
- Запуск
- Анализ образов
- Security/Quality gates

Shift Left Security ← Shift Everywhere Security → Shift Right Security

↓

Shift Down Security

Жизненный путь образа

LUNTRY

CI\CD Pipeline
- Сборка образа
- Анализ образа
- Security/Quality gates
  - Возможна блокировка
- Подпись образа

Image registry
- Хранение
- Очистка/ротация
- Анализ образов
- Security/Quality gates

Runtime
- Запуск
- Анализ образов
- Security/Quality gates

Shift Left Security ← Shift Everywhere Security → Shift Right Security

↓

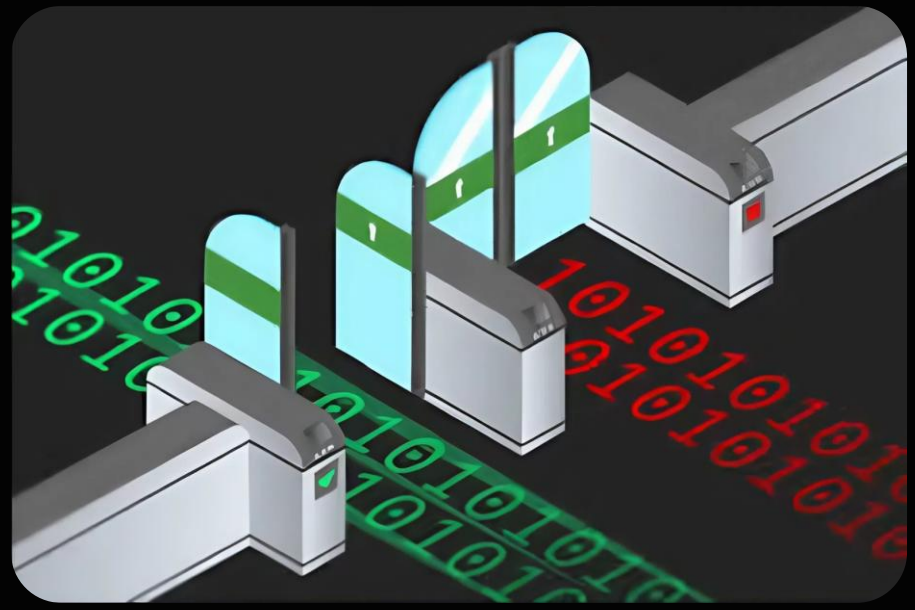
Shift Down Security

Security/Quality Gates – ворота качества

CI
- Уведомление
- Блокировка

Image registry
- Уведомление

Runtime
- Уведомление



Блокировка на Deploy, Runtime – опасная и плохая практика!

«Безопасность Kubernetes кластеров: вредные советы», DevOpsConf 2024

Домены безопасности образов

LUNTRY

5 ДОМЕНОВ:

Анализ Dockerfile
на лучшие практики

Поиск чувствительной информации

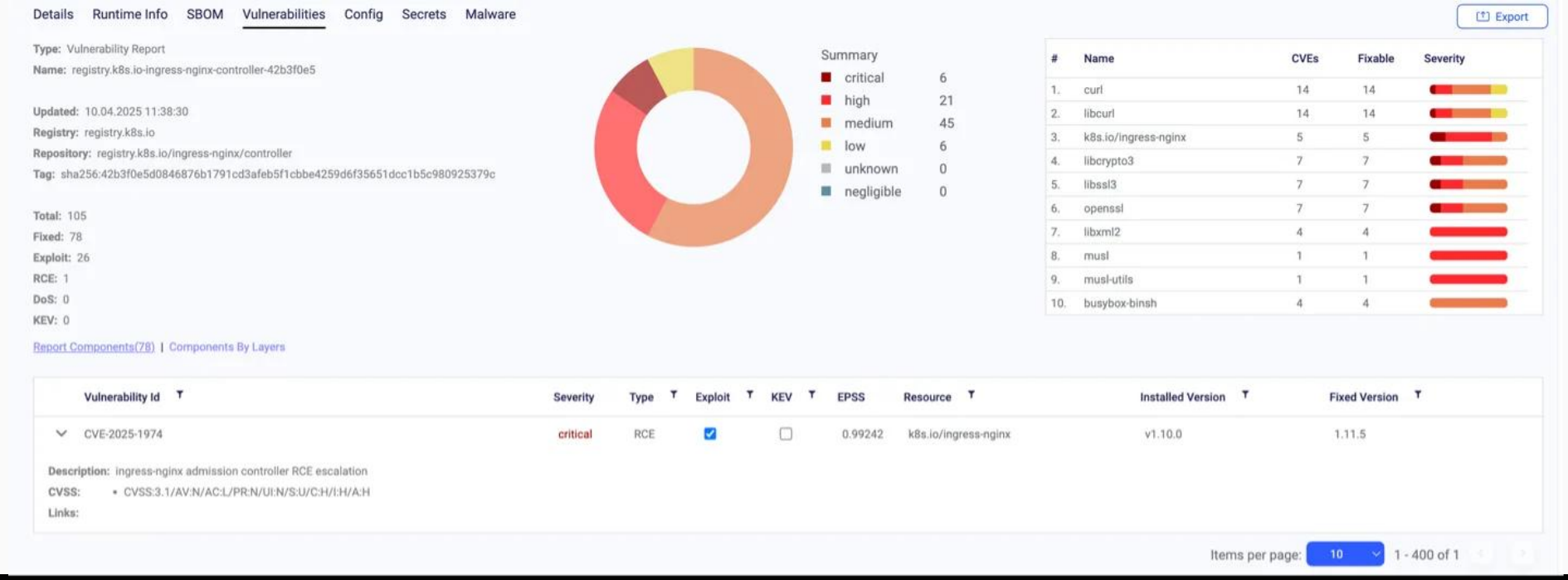
Анализ на известные
уязвимости

Анализ на вредоносный код
и код двойного назначения

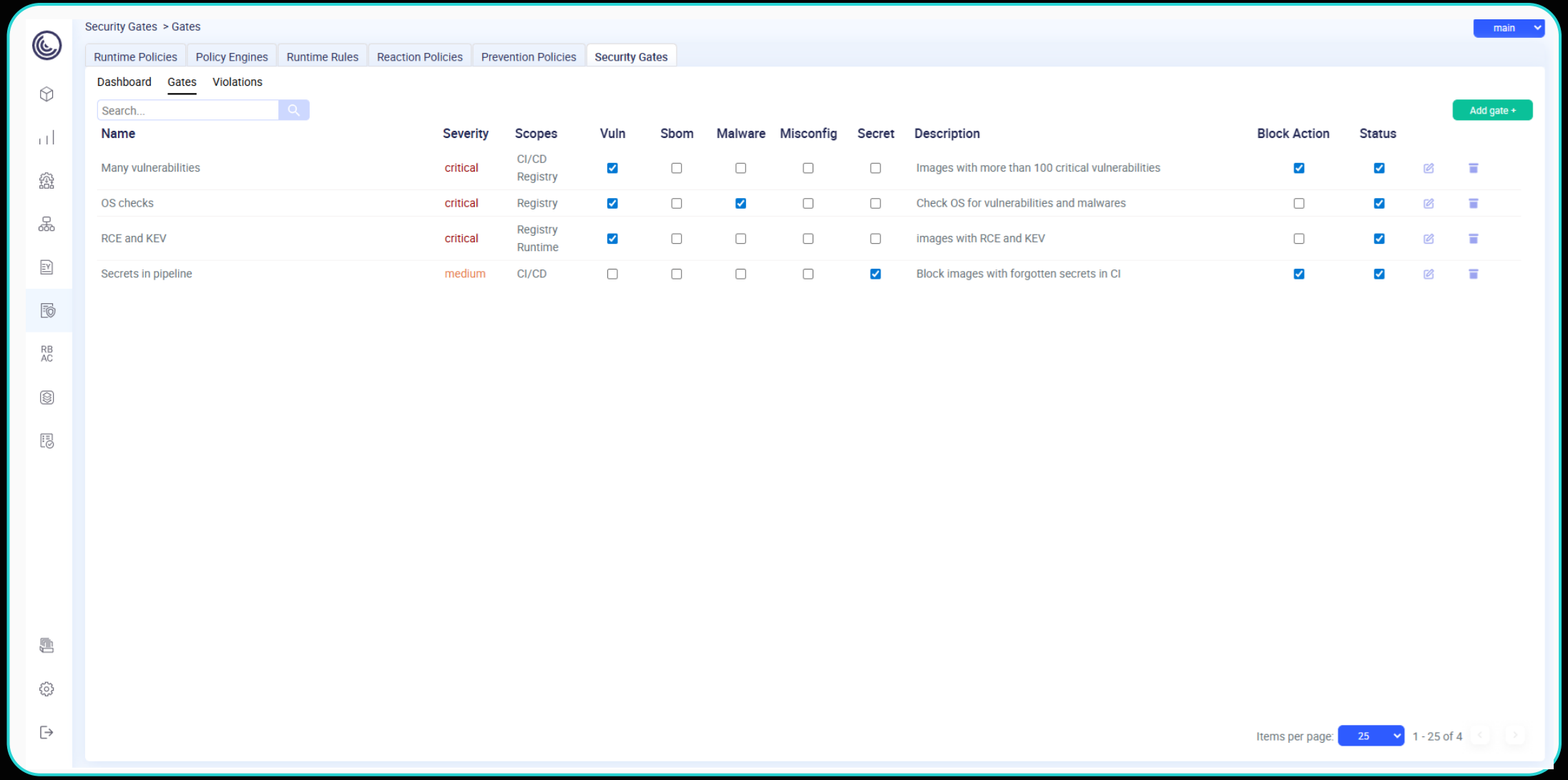
Компонентный анализ

Анализ образов в Luntry

- Встраивание в CI\CD, Registry, Runtime
- Инвентаризация использования образов
- Компонентный анализ (SBOM)
- Сканирование на известные уязвимости
- Поддержка отечественных ОС и БДУ ФСТЭК
- Приоритизация уязвимостей CVSS, Severity, Type(RCE/DoS), Exploit, KEV, EPSS, Runtime
- Контроль соответствия лучшим практикам
- Поиск секретов
- Анализ на вредоносный код и код двойного назначения
- Поддержка внешних и собственных IoC
- Встроенная библиотека уникальных проверок
- Скорость и парализация сканирований
- Security Gates в CI\CD, Registry, Runtime



Security Gates в CI\CD, Registry, Runtime



Пример 1: В CI

Максимум экономии

на «самом дешёвом» этапе:

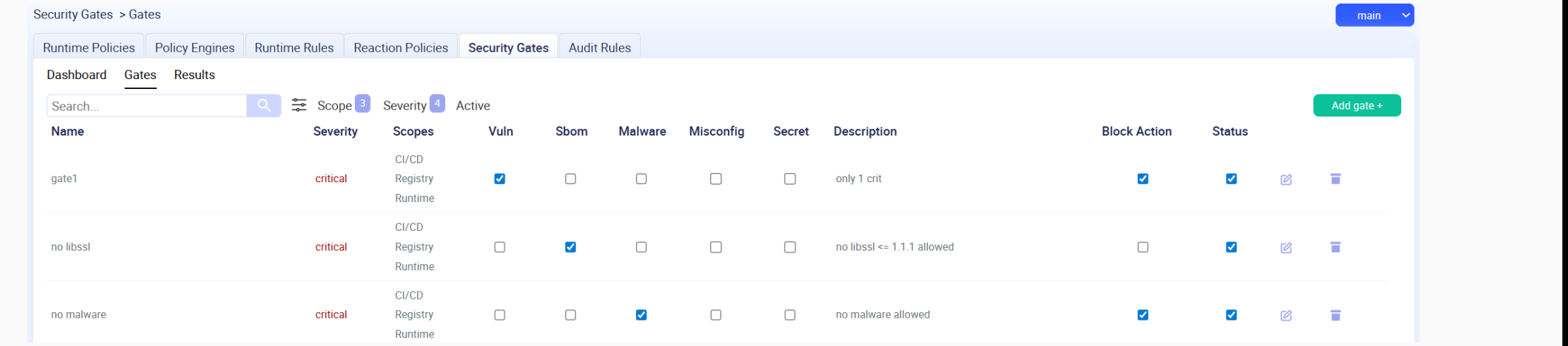
- Раннее обнаружение дефектов

Экономика:

- Исправление проблемы на этапе CI дешевле, чем на последующих этапах

Эффект на команду:

- Снижается нагрузка на QA/DevOps/SRE



Пример 2: В Image Registry

LUNTRY

Снижение риска и затрат на масштабирование ошибок:

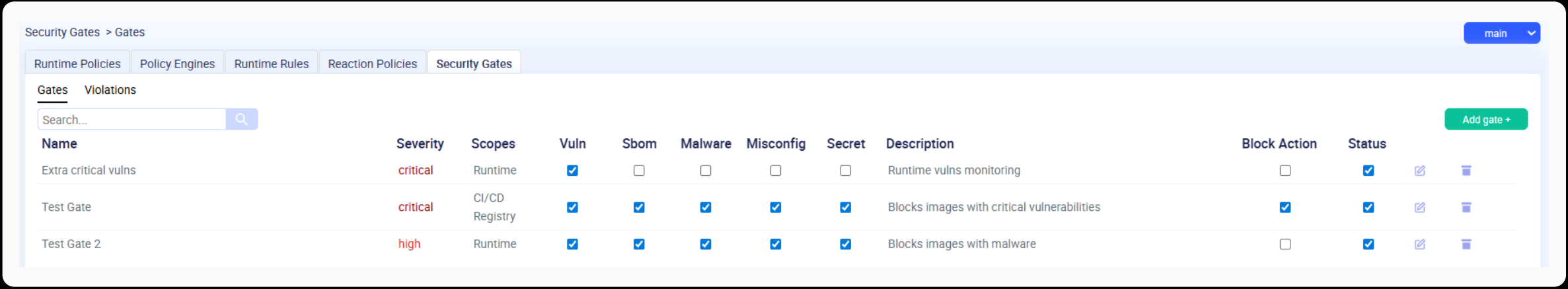
- Единая точка контроля

Экономика:

- Снижает стоимость аудита / соответствия — упрощает проверки и перепроверки, сокращает ручной труд

Эффект на команду:

- Снижение FTE на команду безопасности



Пример 3: В Runtime

LUNTRY

Фокусирование на действительно опасном и важном в текущий момент:

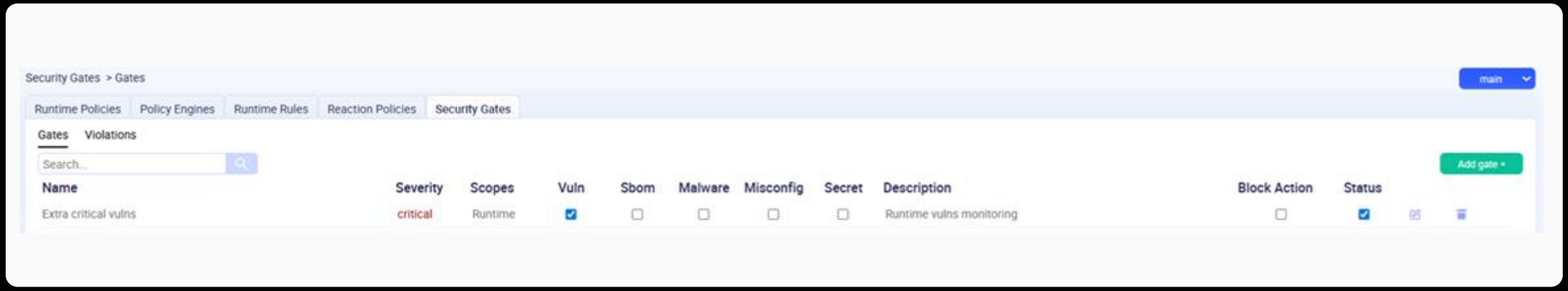
- Контроль самого актуального

Экономика:

- Экономия на инцидентах и простоях

Эффект на команду:

- Простота работы и понижения порога входа за счет приоритезации задач



Польза Security Gates

LUNTRY

DEFENSE IN DEPTH:

- CI: «дешево исправить»
- Registry: «не дать распространиться»
- Runtime: «не дать навредить (или минимизировать ущерб)»

Ключевые бизнес-метрики, которые обычно улучшаются

- Lead time / time-to-release: меньше откатов и «красных» релизов.
- Change failure rate: снижается за счёт отсева дефектов и небезопасных изменений.
- MTTR (время восстановления): ниже, потому что меньше инцидентов и выше прозрачность.
- Стоимость владения (TCO) платформы: меньше ручных процессов, меньше «пожарных» часов, меньше потерь от downtime.

LUNTRY

кВартирник по безопасной разработке

СПАСИБО ЗА ВНИМАНИЕ!

luntry_official
luntrysolution
luntrysolution

luntry.ru
info@luntry.ru

de@luntry.ru
Qu3b3c
k8security

Дмитрий Евдокимов

Основатель и технический директор Luntry