LUNTRY

КЕЙС ПОЛУЧЕНИЯ СЕРТИФИКАТА ФСТЭК РОССИИ ДЛЯ ЗАЩИТЫ КОНТЕЙНЕРОВ



Дмитрий Евдокимов

Основатель и технический директор Luntry



Анатолий Карпенко

Инженер автоматизации Luntry

Команда

LUNTRY

Дмитрий Евдокимов

Основатель Luntry

Специализация – безопасность контейнеров и Kubernetes

Специалисты с опытом ИБ более 15 лет

Команда базируется в Санкт-Петербурге

- Ведем тренинги по организации безопасности в Kubernetes
- Курс "Безопасность облачных технологий" в МГТУ им. Баумана на кафедре ИУ10 «Защита информации»
- Организуем уникальную конференцию по безопасности контейнеров – “БеКон”
- Занимаемся кураторством учащихся по тематике безопасности контейнеров
- Делимся с сообществом знаниями о безопасности Kubernetes в telegram канале "k8s (in)security"
- Входим в экспертный совет ассоциации профессионалов индустрии облачно-ориентированных технологий (АОТ)

Выступления на конференциях

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

В основе продукта LUNTRY заложены собственные исследования, а также опыт проведения аудитов и пентестов Kubernetes

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

Обо мне

> Мировоззрение:
> Все, что нажимается чаще двух раз, лучше автоматизировать.



Инженер автоматизации Luntry

20 лет опыта в ИТ

Специализация – безопасность контейнеров и Kubernetes

Автор ТГ-канала «Технологический Болт Генона»

Любитель митапошных форматов

SPb Reliability Meetup	SafeCode	DevOops	UDW
DEFCON'ы	ТБ Форум	ITGM	
TechTrain	БеКон	CodeFest	

Рисую несмешные мемы

:|

LUNTRY

О компании Luntry

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

Сертификат ФСТЭК России № 5116 от 30.09.2026 г.
Входит в реестр российского ПО Минцифры России № 15188

LUNTRY.RU

План вебинара

LUNTRY

01 Требования регулятора в области защиты контейнерных систем

02 Сертификация LUNTRY

03 Создание защищенной контейнерной системы вместе с LUNTRY

04 Заключение

LUNTRY

ТРЕБОВАНИЯ РЕГУЛЯТОРА В ОБЛАСТИ ЗАЩИТЫ КОНТЕЙНЕРНЫХ СИСТЕМ

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)

АКТУАЛЬНОСТЬ

- 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

Защита ГИС и гос. ИС и контейнеризация

11. Оператор (обладатель информации) должен определить цели защиты информации в зависимости от ожидаемых результатов от проведения мероприятий и принятия мер по защите информации.

Негативные последствия (события) определяются оператором (обладателем информации) на основе информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России.

Посредством выполнения оператором (обладателем информации) задач защиты информации должны быть достигнуты цели защиты информации.

23. Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечить выполнение возложенных на них обязанностей (функций) по защите информации, в том числе по выявлению угроз безопасности информации, обнаружению и предотвращению вторжений, проведению контроля уровня защищенности информации, содержащейся в информационных системах, мониторингу информационной безопасности информационных систем, выявлению уязвимостей, контролю настроек и конфигураций информационных систем, а также средства и системы, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации.

Состав программных, программно-аппаратных средств, необходимых структурному подразделению (специалистам) по защите информации для выполнения возложенных на них обязанностей (функций), определяется во внутренних стандартах и регламентах по защите информации.

62. Мероприятия по реализации в информационных системах мер по их защите и содержащейся в них информации должны включать:

1. реализацию базовых мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности, устанавливаемых оператором (обладателем информации);

2. адаптацию базовых мер защиты информационных систем и содержащейся в них информации применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям функционирования информационных систем;

3. верификацию адаптированного базовых мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

LUNTRY

Защита КИИ и контейнеризация

Меры безопасности, что могут быть полностью / частично закрыты Luntry в контейнерном окружении:

3. Ограничение программной среды (ОПС)

5. Аудит безопасности (АУД)

7. Предотвращение вторжений (компьютерных атак) (СОВ)

8. Обеспечение целостности (ОЦЛ)

10. Защита технических средств и систем (ЗТС)

11. Защиты информационной (автоматизированной) системы и ее компоненты (ЗИС)

12. Реагирование на компьютерные инциденты (ИНЦ)

13. Управление конфигурацией (УКФ)

14. Управление обновлениями программного обеспечения (ОПО)

LUNTRY

Защита ИСПДн и контейнеризация

LUNTRY

8.11. **Меры по защите среды виртуализации должны исключать** несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них,
в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным
и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Текущие документы

LUNTRY

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

Методический документ по 117 приказу

Отдельный раздел «Защита технологий контейнерных сред и их оркестрации (ЗКО)» :

- ЗКО.1 Контроль целостности в контейнерных средах
- ЗКО.2 Регистрация событий безопасности в контейнерных средах
- ЗКО.3 Управление доступом в контейнерных средах
- ЗКО.4 Резервное копирование в контейнерных средах
- ЗКО.5 Изоляция контейнеров в контейнерной среде
- ЗКО.6 Идентификация и аутентификация в контейнерной среде
- ЗКО.7 Управление контейнерами и их образами (оркестрация)
- ЗКО.8 Выявление и устранение уязвимостей в контейнерной среде

При этом на контейнерную среду дополнительно распространяются общие процессы и меры:

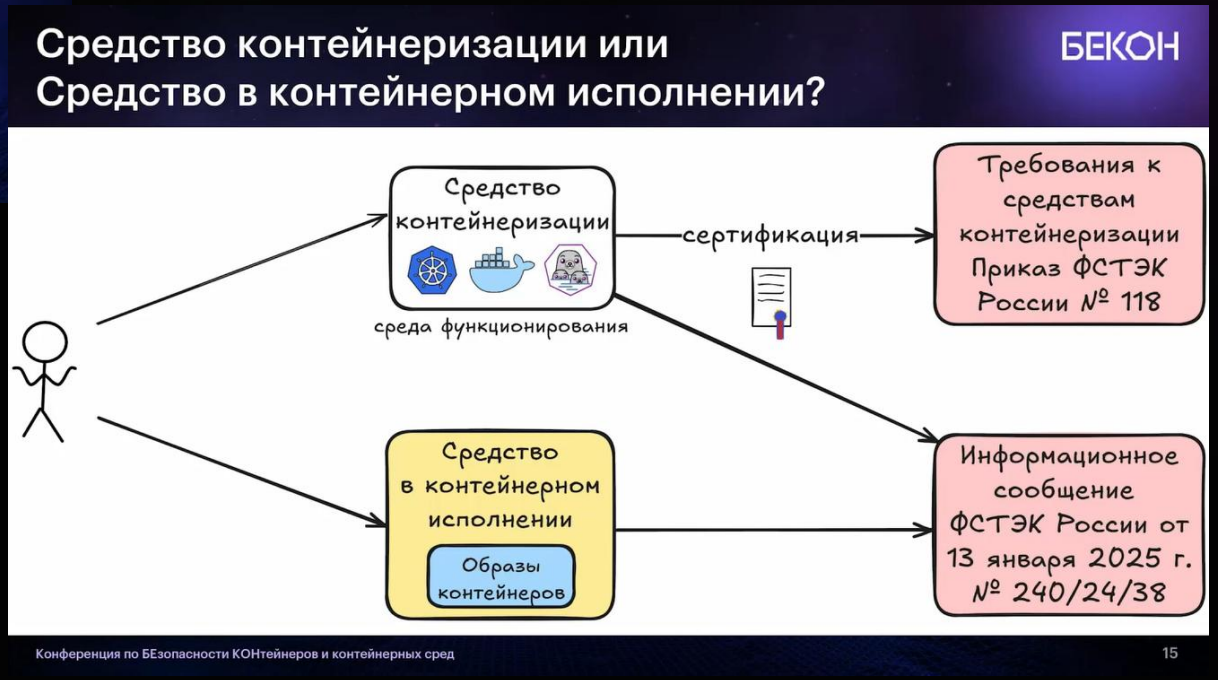
- Выявление и оценка угроз
- Контроль конфигураций
- Управление уязвимостями
- Управление обновлениями
- Мониторинг ИБ
- Управление доступом
- Регистрация событий безопасности
- Сегментация
- Защита сетевого взаимодействия
- Непрерывность функционирования
- Разработка безопасного ПО

LUNTRY

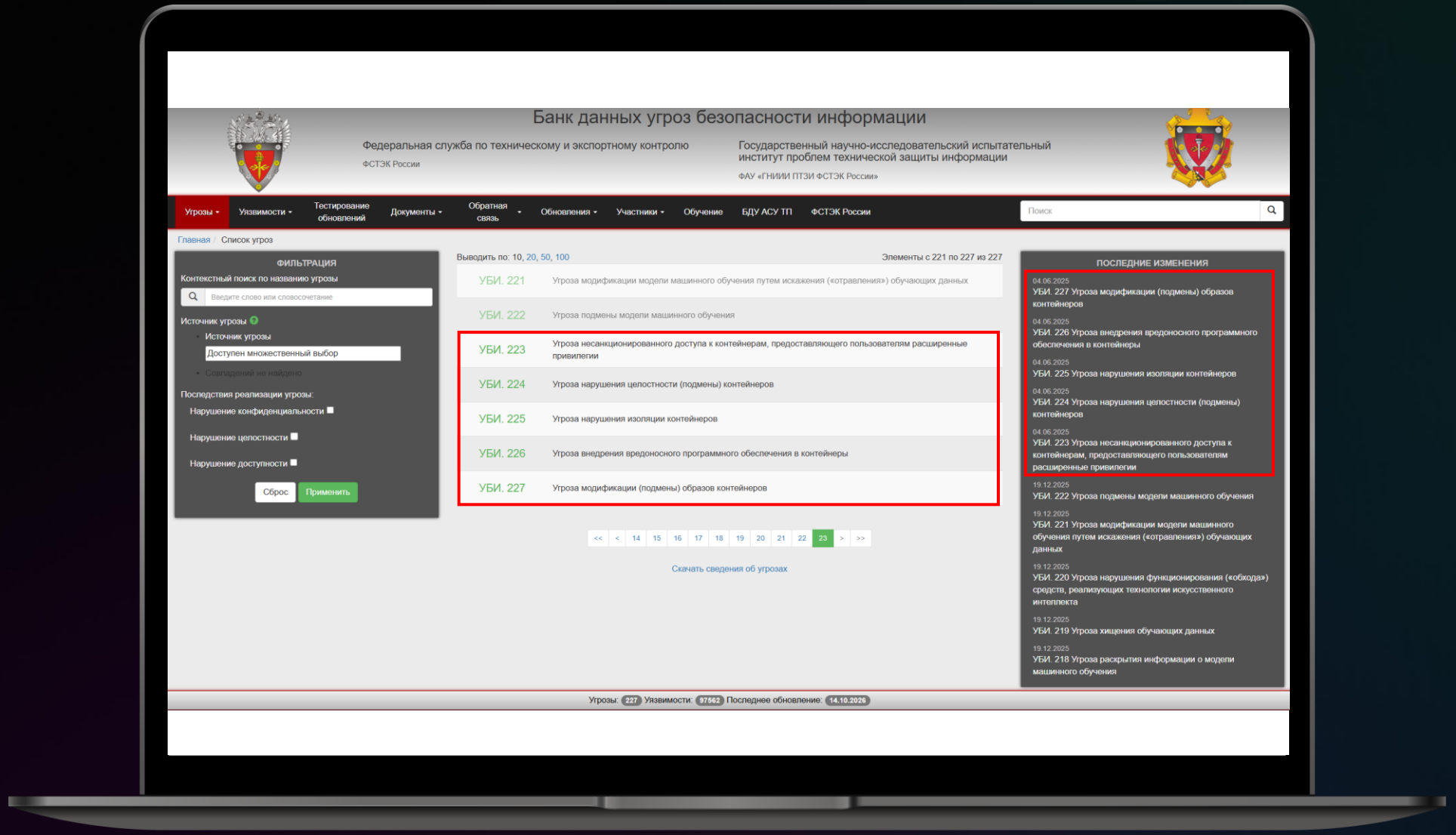
13

Информационное сообщение ФСТЭК России 240/24/38





БДУ ФСТЭК


Банк данных угроз безопасности информации
Федеральная служба по техническому и экспортному контролю
ФСТЭК России
Государственный научно-исследовательский испытательный институт проблем технической защиты информации
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
Угрозы
Уязвимости
Тестирование обновлений
Документы
Обратная связь
Обновления
Участники
Обучение
БДУ АСУ ТП
ФСТЭК России
Поиск
Главная / Список угроз
ФИЛЬТРАЦИЯ
Контекстный поиск по названию угрозы
Введите слово или словосочетание
Источник угрозы
Источник угрозы
Доступен множественный выбор
Совпадений не найдено
Последствия реализации угрозы:
Нарушение конфиденциальности
Нарушение целостности
Нарушение доступности
Сброс
Применить
Выводить по: 10, 20, 50, 100
Элементы с 221 по 227 из 227
УБИ. 221 Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных
УБИ. 222 Угроза подмены модели машинного обучения
УБИ. 223 Угроза несанкционированного доступа к контейнерам, предоставляющего пользователям расширенные привилегии
УБИ. 224 Угроза нарушения целостности (подмены) контейнеров
УБИ. 225 Угроза нарушения изоляции контейнеров
УБИ. 226 Угроза внедрения вредоносного программного обеспечения в контейнеры
УБИ. 227 Угроза модификации (подмены) образов контейнеров
<< < 14 15 16 17 18 19 20 21 22 23 > >>
Скачать сведения об угрозах
ПОСЛЕДНИЕ ИЗМЕНЕНИЯ
04.06.2025 УБИ. 227 Угроза модификации (подмены) образов контейнеров
04.06.2025 УБИ. 226 Угроза внедрения вредоносного программного обеспечения в контейнеры
04.06.2025 УБИ. 225 Угроза нарушения изоляции контейнеров
04.06.2025 УБИ. 224 Угроза нарушения целостности (подмены) контейнеров
04.06.2025 УБИ. 223 Угроза несанкционированного доступа к контейнерам, предоставляющего пользователям расширенные привилегии
19.12.2025 УБИ. 222 Угроза подмены модели машинного обучения
19.12.2025 УБИ. 221 Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных
19.12.2025 УБИ. 220 Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта
19.12.2025 УБИ. 219 Угроза хищения обучающих данных
19.12.2025 УБИ. 218 Угроза раскрытия информации о модели машинного обучения
Угрозы: 227 Уязвимости: 97562 Последнее обновление: 14.10.2026

15

LUNTRY

СЕРТИФИКАЦИЯ LUNTRY

БЕКОН'26

ФСТЭК и контейнеры: от заявки до сертификата

Андрей Слепых (Фобос-НТ)

Анатолий Карпенко (Luntry)

КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

LUNTRY

Проведенные работы

- Убрали Python
- Уменьшили поверхность атаки
- Отразили поверхность атаки
- Подготовили SBOM (ППК) по требованиям ФСТЭК России
- Закрытие уязвимостей
- Унификация версий сторонних компонентов
- Минимизация кодовой базы решения
- Отказ от nginx в пользу caddy
- Входим в группу по анализу NodeJS в рамках центра исследований безопасности системного ПО
- Доработали pipelines сборки (SAST, fuzzing, …)
- Documentation-as-a-Code (DocOps, Latex)
- …

LUNTRY

Сертифицированная версия LUNTRY

LUNTRY

Текущая сертифицируемая версии:

Luntry (Лантри) Certified 1.0c

Данная версия является ответвлением от не сертифицируемой версии:

Luntry v4.4.0

Текущая последняя версия не сертифицированная версия:

Luntry v4.5.0

19

Основная функциональность

Контроль Kubernetes-ресурсов

Контроль состояния Kubernetes-кластеров

Контроль соответствия кластера стандартам



Управление безопасностью образов

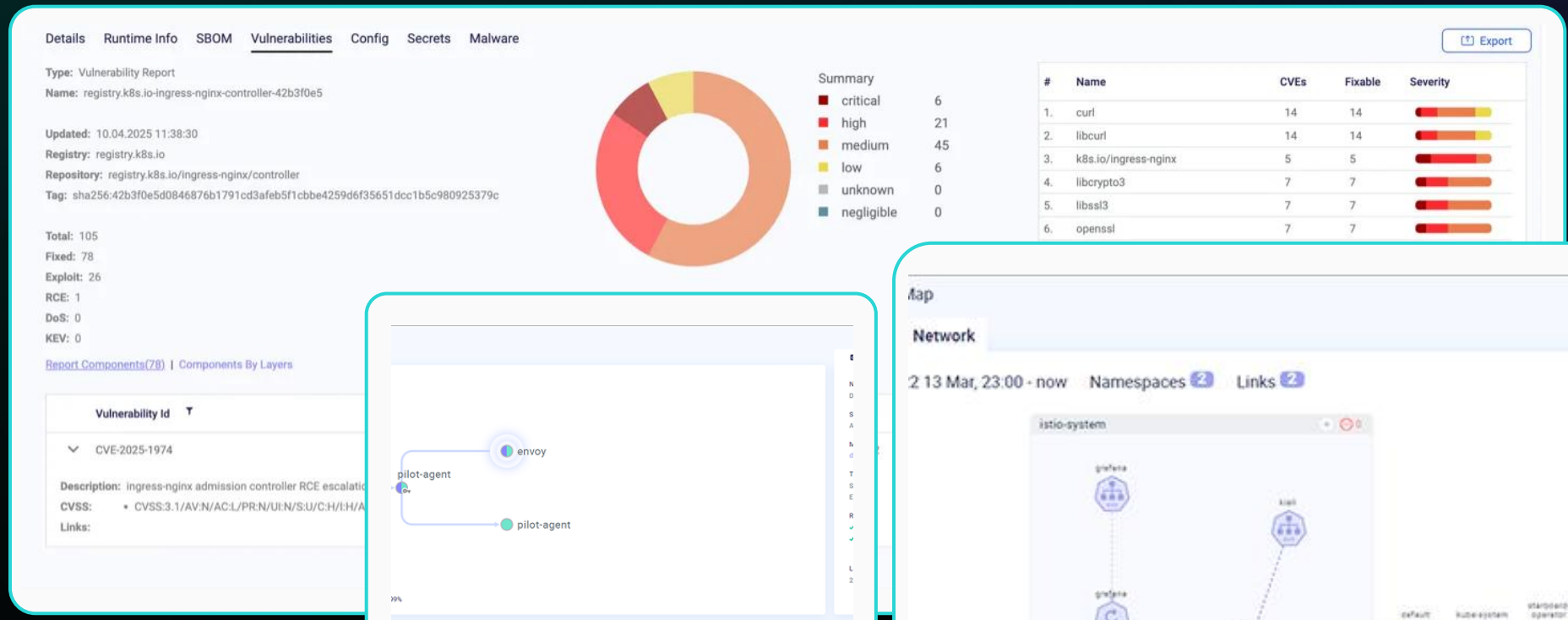
Сетевая безопасность

Анализ прав доступа

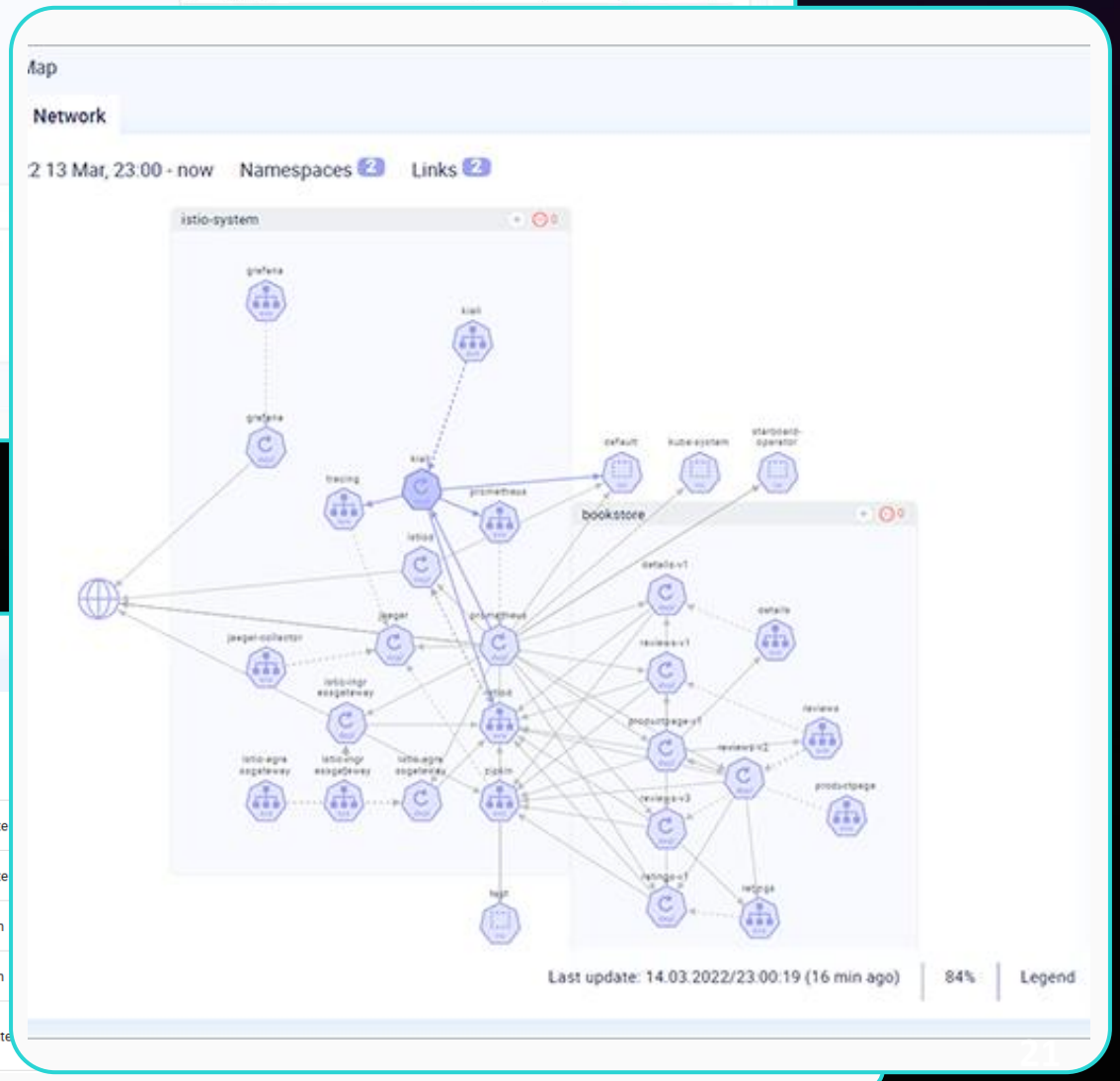
Защита Runtime

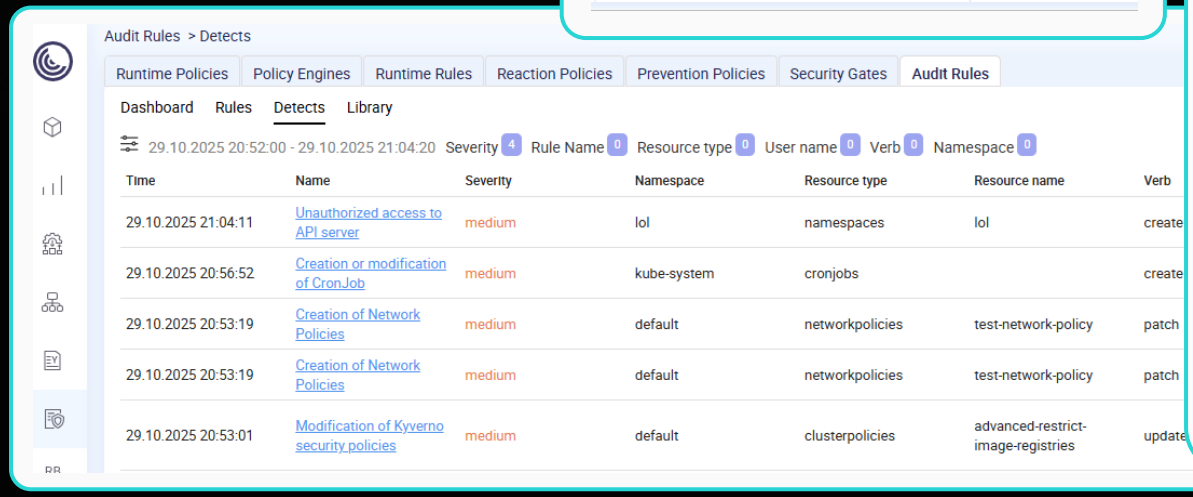
Все в одном для Container Security: VM + EDR + Firewall + Security Gate + GRC + SoD

UI


Details
Runtime Info
SBOM
Vulnerabilities
Config
Secrets
Malware
Export
Type: Vulnerability Report
Name: registry.k8s.io-ingress-nginx-controller-42b3f0e5
Updated: 10.04.2025 11:38:30
Registry: registry.k8s.io
Repository: registry.k8s.io/ingress-nginx/controller
Tag: sha256:42b3f0e5d0846876b1791cd3afeb5f1cbbe4259d6f35651dcc1b5c980925379c
Total: 105
Fixed: 78
Exploit: 26
RCE: 1
DoS: 0
KEV: 0
Report Components(78) | Components By Layers
Summary
critical 6
high 21
medium 45
low 6
unknown 0
negligible 0
Name CVEs Fixable Severity
1. curl 14 14
2. libcurl 14 14
3. k8s.io/ingress-nginx 5 5
4. libcrypto3 7 7
5. libssl3 7 7
6. openssl 7 7
Vulnerability Id
CVE-2025-1974
Description: ingress-nginx admission controller RCE escalatic
CVSS: • CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A
Links:

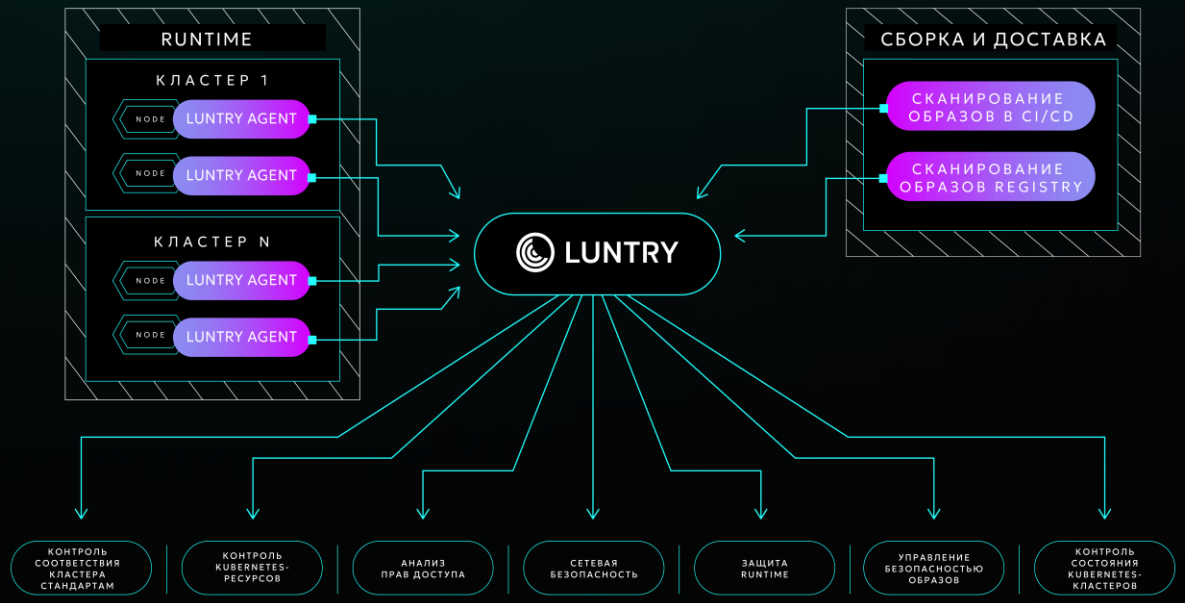
envoy
pilot-agent
pilot-agent
File structure
Permissions
Direction
Endpoint


Map
Network
13 Mar, 23:00 - now
Namespaces 2
Links 2
istio-system
bookstore
Last update: 14.03.2022/23:00:19 (16 min ago)
84%
Legend


Audit Rules > Detects
Runtime Policies
Policy Engines
Runtime Rules
Reaction Policies
Prevention Policies
Security Gates
Audit Rules
Dashboard
Rules
Detects
Library
29.10.2025 20:52:00 - 29.10.2025 21:04:20
Severity 4
Rule Name 0
Resource type 0
User name 0
Verb 0
Namespace 0
Time Name Severity Namespace Resource type Resource name Verb
29.10.2025 21:04:11 Unauthorized access to API server medium lol namespaces lol create
29.10.2025 20:56:52 Creation or modification of CronJob medium kube-system cronjobs create
29.10.2025 20:53:19 Creation of Network Policies medium default networkpolicies test-network-policy patch
29.10.2025 20:53:19 Creation of Network Policies medium default networkpolicies test-network-policy patch
29.10.2025 20:53:01 Modification of Kyverno security policies medium default clusterpolicies advanced-restrict-image-registries update

LUNTRY

Архитектура



1. Установка (20мин – Helm chart)

2. Инвентаризация
- Анализ окружения
- Поиск взаимосвязей

3. Анализ и обучение
- Поиск недостатков
- Генерация моделей поведения

4. Решение проблем
- Поиск первопричин

5. Обработка недостатков и аномалий
- Управление политиками
- Анализ оповещений

Поддержка	Версия
Kubernetes	>=1.16
Container Runtime	CRI
CNI	Любой
Kernel version	>= 4.18 >= 3.10 (rhel7)

Yandex Cloud
deckhouse
VK Cloud Solutions
Selectel
SBER CLOUD
RED HAT OPENSHIFT
NOVA BY ORION SOFT
штурвал
BASIS

LUNTRY

СОЗДАНИЕ ЗАЩИЩЕННОЙ КОНТЕЙНЕРНОЙ СИСТЕМЫ ВМЕСТЕ С LUNTRY

Целевая система

LUNTRY

СЕРТИФИЦИРОВАННОЕ СЗИ LUNTRY

СЕРТИФИЦИРОВАННАЯ ПЛАТФОРМА КОНТЕЙНЕРИЗАЦИИ

СЕРТИФИЦИРОВАННАЯ ОС

Полный стэк

Сертифицированная ОС:
- защищает хостовый уровень
- защита в рамках одного хоста, а не группы/кластера
- не понимает контейнерный контекст

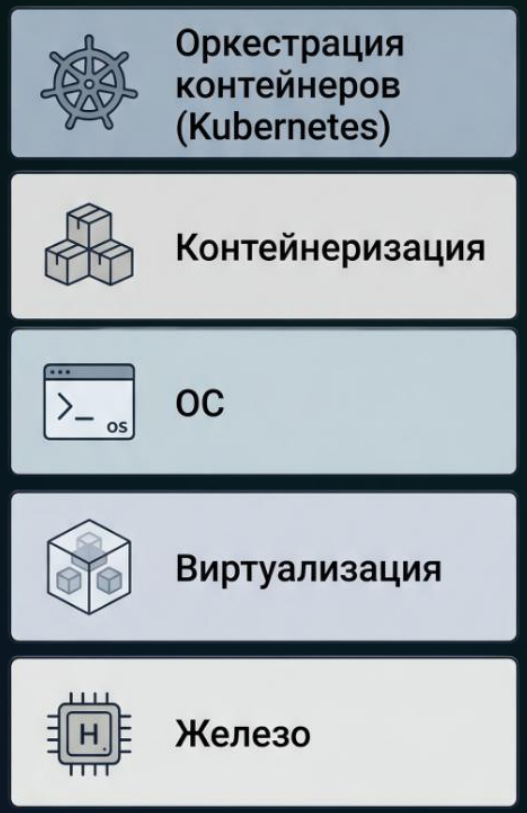
Сертифицированная платформа контейнеризации:
- обеспечивает доверенное создание, запуск, изоляцию и базовый контроль
- покрывает обязательный минимум требований

Luntry:
- обеспечивает непрерывную защиту контейнерного жизненного цикла
- контролирует образы, конфигурации, Kubernetes и runtime
- выявляет и предотвращает реальные атаки
- выступает независимым слоем контроля

ВЫВОД:

ОС + платформа = фундамент

Luntry = полноценная эксплуатационная безопасность контейнерной среды



LUNTRY

25

Что и как Luntry дополняет:

ОТСТРОЙКА 1. Не заменяет ОС и платформу, а закрывает то, что у них вне фокуса
- ОС защищает хост.
- Платформа обеспечивает функционирование контейнеров.
- Luntry защищает саму контейнерную среду как объект эксплуатации и атак.

ОТСТРОЙКА 2. Контейнерно-нативное понимание среды
- Видит не просто процессы, а pod / image / namespace / service account / deployment / registry.
- Поэтому Luntry точно обнаруживает риски и быстрее расследует инциденты.

ОТСТРОЙКА 3. Непрерывный контроль вместо базового регламентного минимума
- Контроль должен быть не раз в неделю / месяц, а постоянно.
- Это критично для динамичной контейнерной среды, которая постоянно меняется, саморегулируется

ОТСТРОЙКА 4. Защита всего жизненного цикла
- От образа и pipeline сборки до запуска в runtime и форензики.

ОТСТРОЙКА 5. Независимый слой контроля
- Проверяет не только контейнеры, но и корректность / безопасность самой контейнерной платформы.
- Единый контроль над разными ОС и разными платформами контейнеризации.
- Единая точка анализа и контроля разных сред и окружений для всех департаментов.

ОТСТРОЙКА 6. Глубокий runtime и гибридный анализ
- Выявляет реальные атаки, а не только “неправильные настройки” и базовые случаи.

ОТСТРОЙКА 7. Выстраивание полноценного процесса DevSecOps
- ОС и платформа дают механизмы, но не формируют процесс.

26

Luntry и пункты ЗКО 117 приказа

Пункт ЗКО	Выполнение	Что закрывает Luntry
Контроль целостности в контейнерных средах	+	Контроль целостности образов и конфигураций, выявление несанкционированных изменений в запущенных образах
Регистрация событий безопасности в контейнерных средах	+	Регистрация атак, изменений образов, запуска / остановки контейнеров, изменения ролевой модели
Управление доступом в контейнерных средах	+	Контроль доступа пользователей и сущностей к контейнерам и образам
Резервное копирование в контейнерных средах	-/+	Инвентаризация объектов резервирования, экспорт конфигураций
Изоляция контейнеров в контейнерной среде	+	Контроль привилегий контейнеров, изоляции и небезопасных настроек
Идентификация и аутентификация в контейнерной среде	-/+	Контроль сервисных аккаунтов и субъектов доступа
Управление контейнерами и их образами (оркестрация)	+	Инвентаризация контейнеров и образов, контроль размещения и использования
Выявление и устранение уязвимостей в контейнерной среде	+	Выявление, приоритизация, регулярный контроль уязвимостей образов

27

Luntry и смежные требования по 117 приказу

РЕШЕНИЕ LUNTRY ПОЛНОСТЬЮ ИЛИ ЧАСТИЧНО ЗАКРЫВАЕТ ПУНКТЫ ИЗ СЛЕДУЮЩИХ РАЗДЕЛОВ:

- Управление доступом (УПД)
- Регистрация событий безопасности (РСБ)
- Обнаружение вторжений в сегментах (СОВ)
- Сегментация и межсетевое экранирование (МСЭ)
- Защита каналов связи и сетевого взаимодействия (ЗКС)
- Контроль конфигураций информационных систем (КК)
- Управление уязвимостями (КУ)
- Управление обновлениями (КО)
- Разработка безопасного ПО (БР)
- Мониторинг информационной безопасности (МБ)

LUNTRY

28

УБИ 223

LUNTRY

УБИ.223: Угроза несанкционированного доступа к контейнерам, предоставляющего пользователям расширенные привилегии

Вид

Описание угрозы	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия путем получения повышенных привилегий при несанкционированном использовании docker-контейнера. Данная угроза обусловлена наличием у docker-контейнеров повышенных привилегий для работы в системе. Реализация данной угрозы возможна при условии наличия у нарушителя доступа к docker-контейнеру и привилегий, достаточных для работы с ним
Источники угрозы	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом
Объект воздействия	Docker-контейнер
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

УБИ 223

Что не закрывает сертифицированная ОС

Не видит контейнерный контекст привилегий (capabilities, RBAC, service account и т.д.)

Что не закрывает сертифицированная платформа

Нет анализа прав (RBAC), нет анализа runtime окружения.

Организационных мер недостаточно

1. Угроза обусловлена уязвимостями и слабостями — это не устраняется организационно

LUNTRY

LUNTRY ЗАКРЫВАЕТ

Обнаружение внешнего и внутреннего нарушителя, через runtime политики, правила и анализ прав RBAC. Детектирование как известных, так и не известных атак, побегов из контейнеры.

УБИ 224

LUNTRY

УБИ.224: Угроза нарушения целостности (подмены) контейнеров

Вид

Описание угрозы	Угроза заключается в возможности запуска нарушителем собственного docker-контейнера, функционирующего по уровню логического воздействия ниже компрометируемого docker-контейнера. Данная угроза обусловлена уязвимостями программного обеспечения docker-контейнера, реализующего функцию изолированной программной среды для функционирующих в ней программ, а также слабостями инструкций аппаратной поддержки контейнеризации на уровне процессора. Реализация данной угрозы приводит не только к компрометации docker-контейнера, но и запущенных в созданной им среде средств защиты
Источники угрозы	Внешний нарушитель со средним потенциалом Внутренний нарушитель со средним потенциалом
Объект воздействия	Информационная система, сетевой узел, носитель информации, объекты файловой системы, учетные данные пользователя, образ docker-контейнера
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

УБИ 224

Что не закрывает сертифицированная ОС

Не знает "нормального" состава контейнерной среды, не видит нелегитимный контейнер. Может содержать уязвимость через которую и будет реализована угроза.

Что не закрывает сертифицированная платформа

Контролирует целостность известных образов, но не обнаруживает новый посторонний контейнер. Может содержать уязвимость через которую и будет реализована угроза.

Организационных мер недостаточно:

1. Угроза обусловлена уязвимостями и слабостями — это не устраняется организационно.
2. Угроза предполагает, что нарушитель действует уже внутри системы и обошел организационные меры.

КАК LUNTRY ЗАКРЫВАЕТ

Обнаружение внешнего и внутреннего нарушителя и их попытки эксплуатации уязвимостей, через runtime политики, и обнаружение попыток побега из контейнера еще на стадии анализа dockerfile.

LUNTRY

УБИ 225

LUNTRY

УБИ.225: Угроза нарушения изоляции контейнеров	Вид
Описание угрозы	Угроза заключается в возможности нарушения целостности изолированного программного кода своего и (или) других docker-контейнеров, а также параметров его (их) настроек. Данная угроза обусловлена наличием уязвимостей программного кода службы контейнеризации, обеспечиваемого изолированность программной среды и защиты от несанкционированного доступа со стороны нарушителя. Реализация данной угрозы возможна при условии осуществления успешно реализованного несанкционированного доступа со стороны нарушителя и (или) вредоносной программы к docker-контейнеру.
Источники угрозы	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом
Объект воздействия	Сервер, рабочая станция, docker-контейнер, машинный носитель информации, метаданные
Последствия реализации угрозы	Нарушение целостности Нарушение доступности

УБИ 225

Что не закрывает сертифицированная ОС

Реализует изоляцию как механизм,
но не выявляет попытки её обхода.

Что не закрывает сертифицированная платформа

Реализует изоляцию как механизм,
но не выявляет попытки её обхода.

Организационных мер недостаточно:

1. Изоляция — это принципиально техническая функция.
2. Эксплуатация уязвимости это чисто техническая вещь.

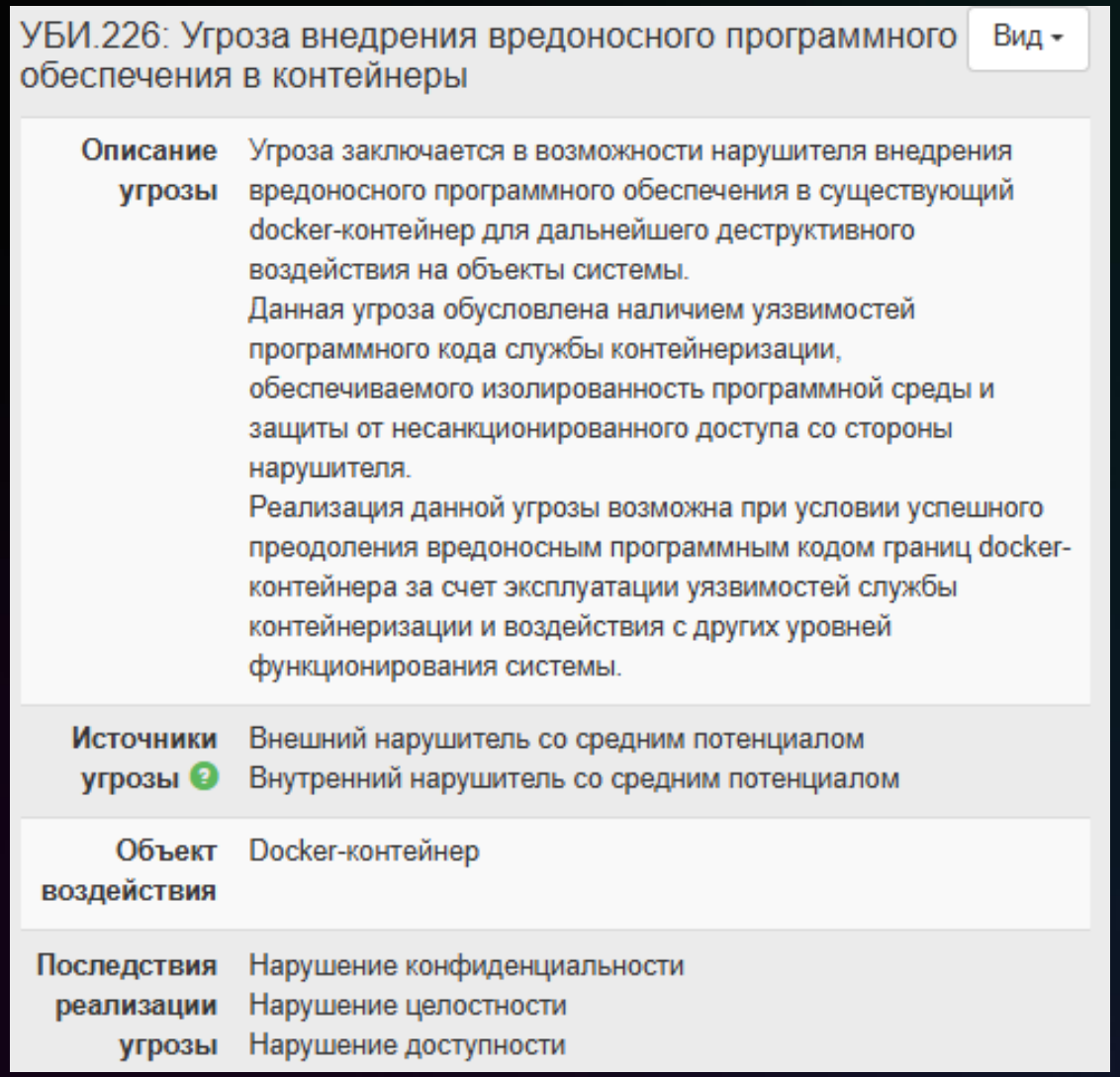
КАК LUNTRY ЗАКРЫВАЕТ

Обнаружение внешнего и внутреннего нарушителя и их попытки эксплуатации уязвимостей, через runtime политики, и обнаружение попыток побега из контейнера еще на стадии анализа dockerfile.

LUNTRY

34

УБИ 226



УБИ.226: Угроза внедрения вредоносного программного обеспечения в контейнеры

Вид

Описание угрозы	Угроза заключается в возможности нарушителя внедрения вредоносного программного обеспечения в существующий docker-контейнер для дальнейшего деструктивного воздействия на объекты системы. Данная угроза обусловлена наличием уязвимостей программного кода службы контейнеризации, обеспечиваемого изолированность программной среды и защиты от несанкционированного доступа со стороны нарушителя. Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ docker-контейнера за счет эксплуатации уязвимостей службы контейнеризации и воздействия с других уровней функционирования системы.
Источники угрозы	Внешний нарушитель со средним потенциалом Внутренний нарушитель со средним потенциалом
Объект воздействия	Docker-контейнер
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

УБИ 226

Что не закрывает сертифицированная ОС

Не анализирует образы на вредоносные объекты и вредоносную активность.

Что не закрывает сертифицированная платформа

Не анализирует образы на вредоносные объекты и вредоносную активность.

Организационных мер недостаточно:

1. Анализ / сканирование это техническая мера.
2. Эксплуатация уязвимости это чисто техническая вещь.

КАК LUNTRY ЗАКРЫВАЕТ

Анализ образа контейнера и его содержимого на всем его жизненном цикле от сборки до запуска в runtime. В runtime фиксирует вредоносную / аномальную / нелегитимную активность с помощью контроля runtime.

LUNTRY

УБИ 227

УБИ.227: Угроза модификации (подмены) образов контейнеров

Вид

Описание угрозы	Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через нее на другие системы путем осуществления несанкционированного доступа к образам docker-контейнеров. Данная угроза обусловлена слабостями мер разграничения доступа к образам docker-контейнеров, реализованных в программном обеспечении контейнеризации. Реализация данной угрозы может привести к нарушению конфиденциальности информации, целостности программного обеспечения и доступности ресурсов docker-контейнеров, а также создания ботнета путем внедрения вредоносного программного обеспечения в образы docker-контейнеров, используемых в качестве шаблонов.
Источники угрозы	Внешний нарушитель со средним потенциалом Внутренний нарушитель со средним потенциалом
Объект воздействия	Образ docker-контейнера, сетевой узел, сетевое программное обеспечение, docker-контейнер
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

LUNTRY

УБИ 227

Что не закрывает сертифицированная ОС

Не умеет отличать легитимно и нелегитимно модифицированный образ.

Что не закрывает сертифицированная платформа

Не умеет отличать легитимно и нелегитимно модифицированный образ.

Организационных мер недостаточно:

1. Атака на цепочку поставки не видна через организационные процедуры.
2. Атака может происходить с использованием уязвимостей еще на стадии сборки образа в CI/CD.

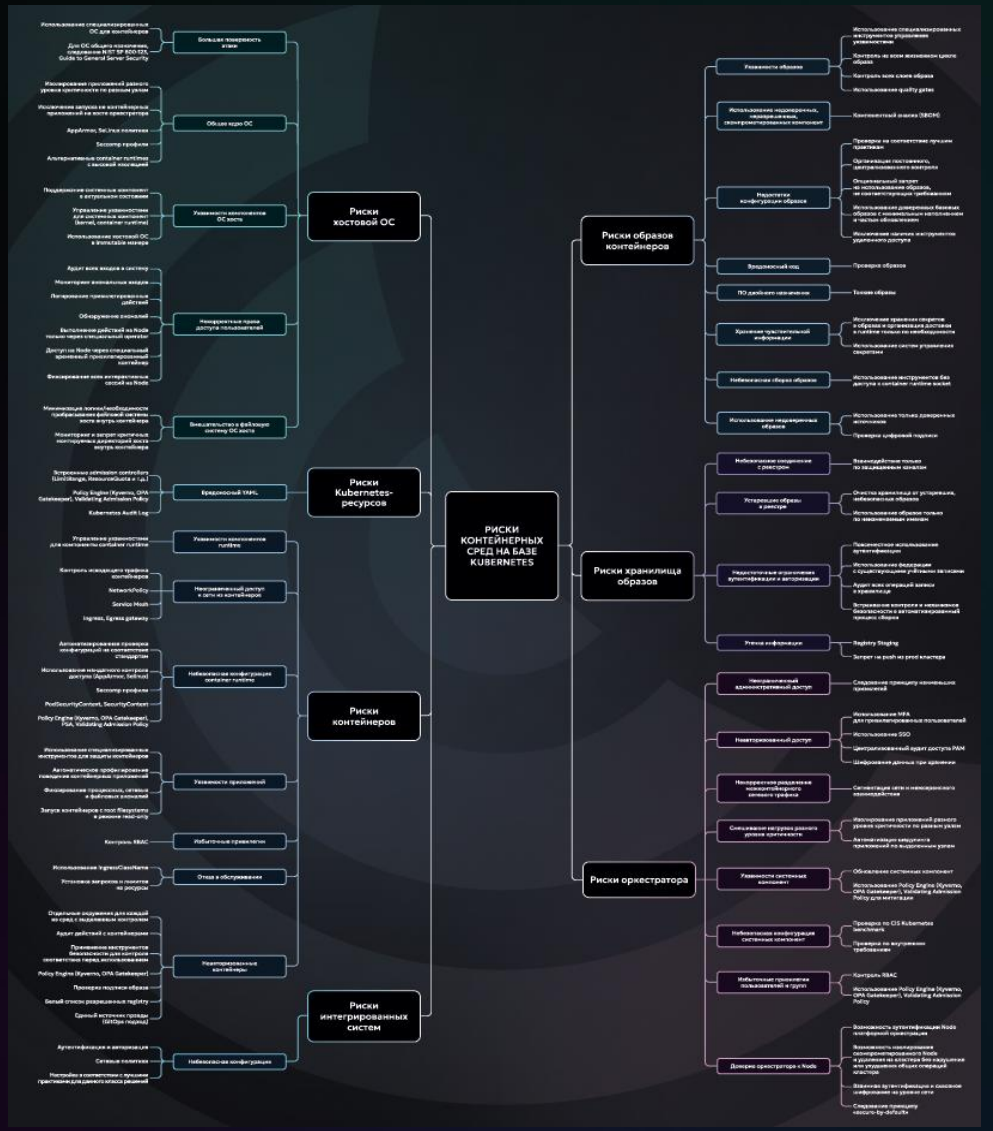
КАК LUNTRY ЗАКРЫВАЕТ

Инвентаризация распространения образа, фиксация вредоносного / аномального поведения в запущенных контейнерах.

LUNTRY

Карта безопасности для контейнерных сред

- **Версия от Luntry,**
  с учетом NIST SP 800-190
  и учетом специфики Kubernetes
  - Риски
  - Механизмы защиты



LUNTRY

LUNTRY

ВЫВОДЫ

Выводы

LUNTRY

01 Сертификация важный и нужный процесс

02 Luntry – первое сертифицированное СЗИ для контейнеров

03 С Luntry появилась возможность создавать защищенные аттестованные системы, готовые противостать любым нарушителям и угрозам

LUNTRY

luntry_official
luntrysolution
luntrysolution

luntry.ru
info@luntry.ru

ДМИТРИЙ ЕВДОКИМОВ

Основатель и технический директор Luntry

de@luntry.ru
Qu3b3c
k8security

СПАСИБО ЗА ВНИМАНИЕ!

АНАТОЛИЙ КАРПЕНКО

Инженер автоматизации Luntry

«Технологический Болт Генона»
@rusdacent