cyber camp '25

LUNTRY

1000 и 1 способ избавиться от уязвимостей в контейнерных приложениях

Дмитрий Евдокимов

Founder&CTO Luntry

Обо мне

LUNTRY

> 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 конференций DevOpsConf и KUBER CONF

Спикер

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

План доклада

LUNTRY

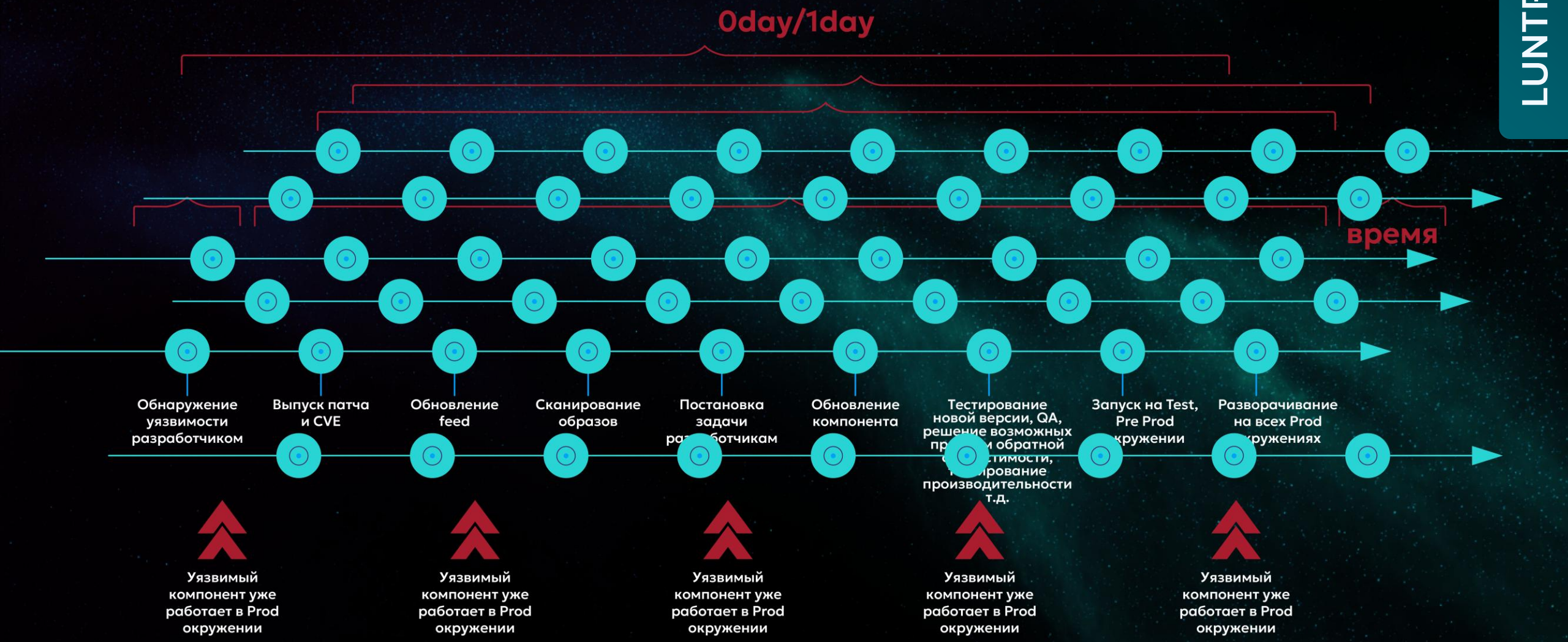
01	Введение / Проблематика
02	Способы противодействия уязвимостям в образах контейнеров
03	Выводы

LUNTRY

Проблематика

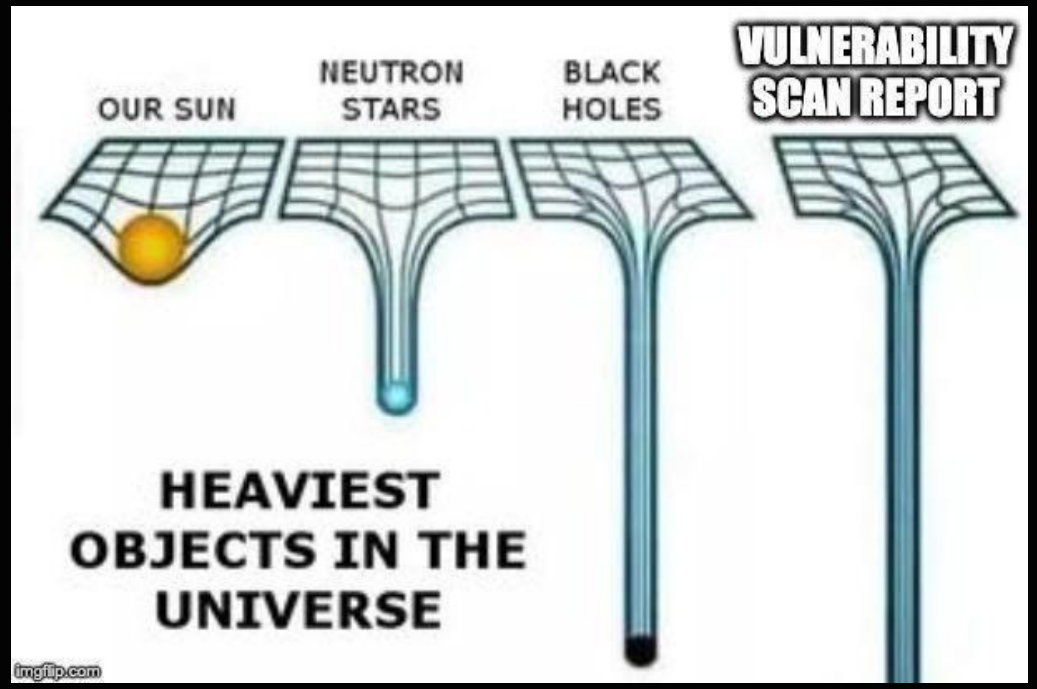
Скорость патчинга низкая

Работа с уязвимостями по факту



LUNTRY

Большое количество уязвимостей



Вот приблизительные данные по годам на основе доступных статистик из надежных источников (например, CVE.org, CVE Details и других):

- 1999: около 300 (начало программы CVE). cve.org
- 2000–2016: постепенный рост от сотен до тысяч в год, с пиком в 2016 году около 6,500. До 2017 года ежегодное количество не превышало 10,000. researchgate.net
- 2017: около 14,700 (первый год свыше 10,000).
- 2018: около 16,500.
- 2019: 17,300. cve.mitre.org
- 2020: 18,400. cve.mitre.org
- 2021: 20,200. cvedetails.com
- 2022: 25,100. cvedetails.com
- 2023: 29,100. cvedetails.com
- 2024: 40,300. cvedetails.com
- 2025: около 30,800 (на август 2025 года, частичные данные). cvedetails.com

Тренд показывает ускорение роста: с 2020 года ежегодное увеличение составляет 15–40%. В 2024 году зафиксирован рекордный скачок н 38% по сравнению с 2023 годом. yeswehack.com

Скорость появления 1day эксплоитов высокая

- Time-to-Exploit, TTE
- По данным: Mandiant Time-to-Exploit Trends 2023 ,
  Rapid7 Vulnerability Intelligence Report, VulnCheck Q1 2025 Report

Год	Показатель	Значение
2018-2019	Среднее TTE	63 дня
2020-2021	Среднее TTE	44 дня
2021-2022	Среднее TTE	32 дня
2022	Среднее TTE	7 дней
2023	Среднее TTE	5 дней
Q1 2025	Среднее TTE (28,3% - 45 уязвимостей)	1 день

Учащение использования 0day эксплоитов

- 2014: около 24 (начало систематического отслеживания Project Zero).
- 2015: 54. en.wikipedia.org
- 2016: 38.
- 2017: 28.
- 2018: 23.
- 2019: 22 (стабилизация на низком уровне). blog.google
- 2020: 25. mandiant.com
- 2021: 106 (резкий рост, в основном за счет шпионского ПО и государственных актеров). cloud.google.com
- 2022: 62 (спад по сравнению с 2021, но все равно выше предыдущих лет; фокус на вариантах известных уязвимостей). cloud.google.com
- 2023: 97 (рост на ~56% от 2022; рекордное число, с преобладанием атак на браузеры, ОС и enterprise-продукты; 50% случаев связаны со spyware-вендорами). cloud.google.com cloud.google.com

- 2024: 75 (небольшой спад, но сдвиг к enterprise-технологиям, таким как VPN и системы безопасности; меньше фокуса на consumer-устройствах). cloud.google.com darkreading.com
- 2025: частичные данные (на август 2025): в первой половине года зафиксирован рост на 46% по сравнению с аналогичным периодом 2024 (около 55 случаев); год на траектории рекорда (>100 по прогнозам), с акцентом на zero-day в SharePoint, Chrome и других. nwajtech.com todyl.com csoonline.com

Общий тренд: с 2015 по 2020 наблюдался относительный спад после пика 2015 года, но с 2021 начался резкий рост, достигший пика в 2021 и 2023. В 2022 и 2024 был небольшой откат, но 2025 показывает ускорение.

LUNTRY

Процесс исправления уязвимостей

- Ходьба на месте …
- Мало обнаружить уязвимость, нужно еще исправить и выкатить в прод
- У Vulnerability Management (VM) есть много проблем
- На мой взгляд VM теряет свою значимость от года к году
  - Но это тема другого выступления ;)

Способы противодействия уязвимостям в образах контейнеров

Параметры рассмотрения и сравнения

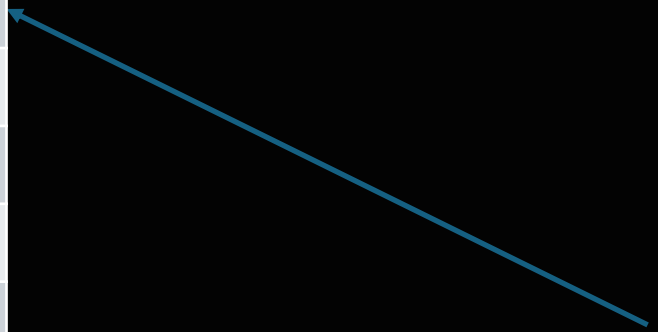
Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

Что есть что и для чего

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

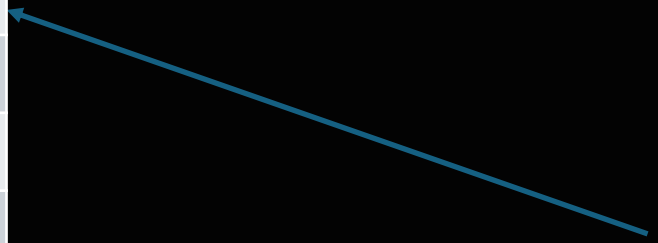


Остается ли по факту уязвимость в коде после проведенных манипуляций

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий



Влияет ли
на уязвимости
базового слоя

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

Влияет ли
на уязвимости
компонентов в слоях
отличных от базового

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

Требует ли подход наличия артефактов необходимых для воспроизведения сборки

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

Остается ли
у атакующего
возможность успешно
проэксплуатировать
уязвимость в коде
после проведенных
манипуляций

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

Происходит ли модификация приложения после проведенных манипуляций

LUNTRY

Параметры рассмотрения и сравнения

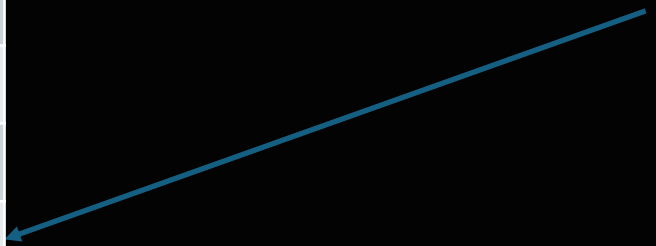
Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

Возможна ли защита от еще неизвестных уязвимостей (0day) в коде после проведенных манипуляций

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

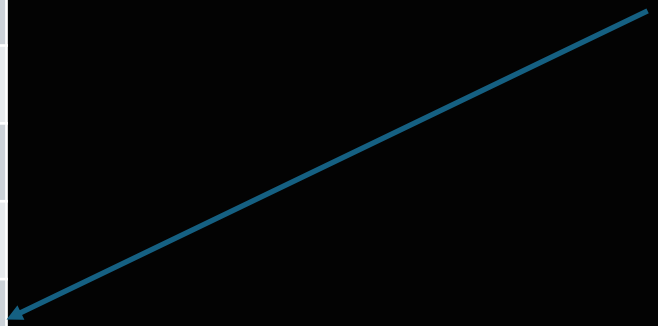


Насколько сложно
реализовать / применить
это внутри компании

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

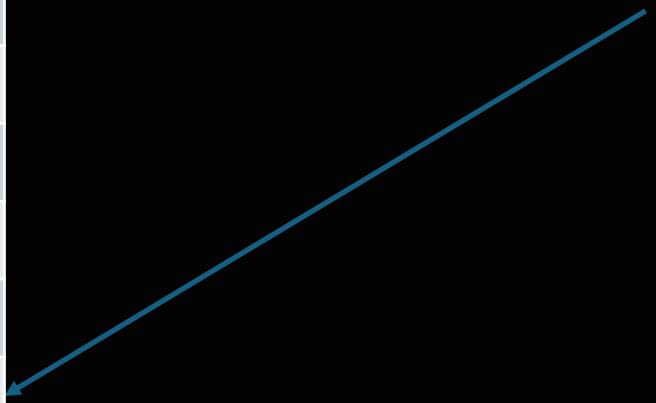


Насколько данный подход позволяет разбираться со множеством уязвимостей за раз

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

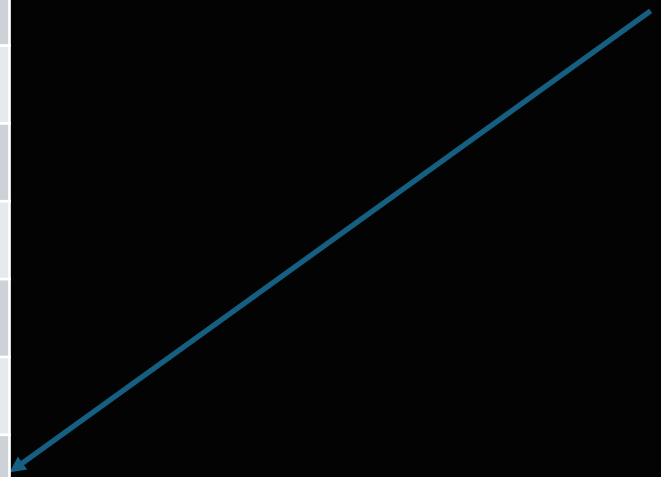


Насколько данный подход быстро отрабатывает / внедряется

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий

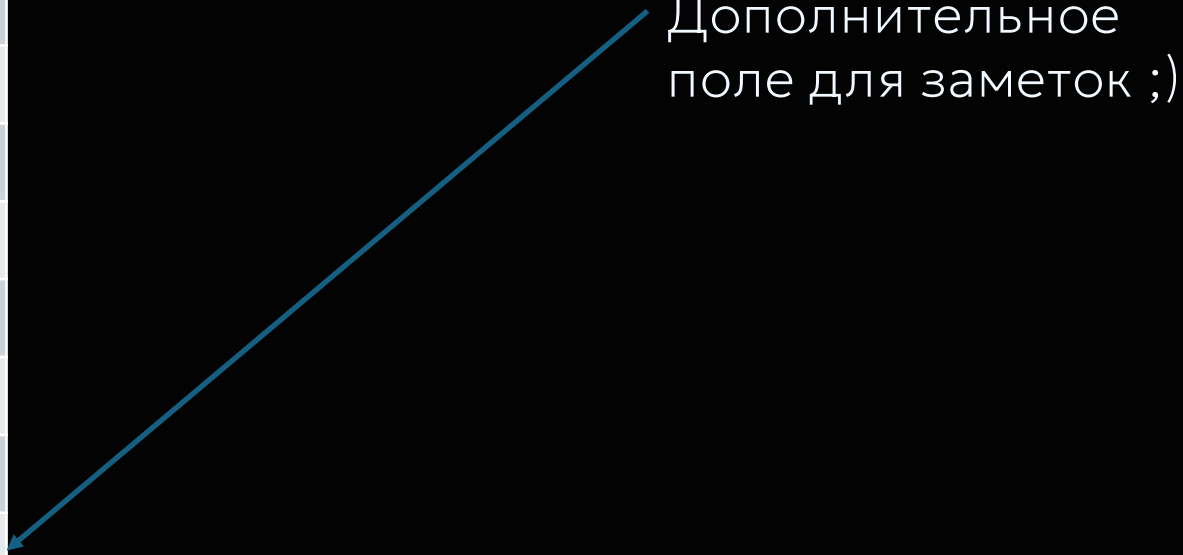


Насколько код
будет вести себя
корректно / работоспособно
после проведенных
манипуляций и вмешательств

LUNTRY

Параметры рассмотрения и сравнения

Пункт
CVE исчезает или нет
Уязвимости базового слоя
Уязвимости других слоев
Исходные артефакты
Эксплуатация баги
Модификация
Защита от 0day
Сложность
Покрытие
Скорость
Надежность
Комментарий



LUNTRY

Способ 1:
Честный патчинг ручками

Честный патчинг ручками

- Классика со всеми своими преимуществами и недостатками
- Возможна небольшая автоматизация с помощью Dependabot и Renovate
- Не имеет никакой контейнерной специфики и не позволяет использовать ее преимущества
- Используем как отправную точку, нулевой срез

LUNTRY

Характеристика

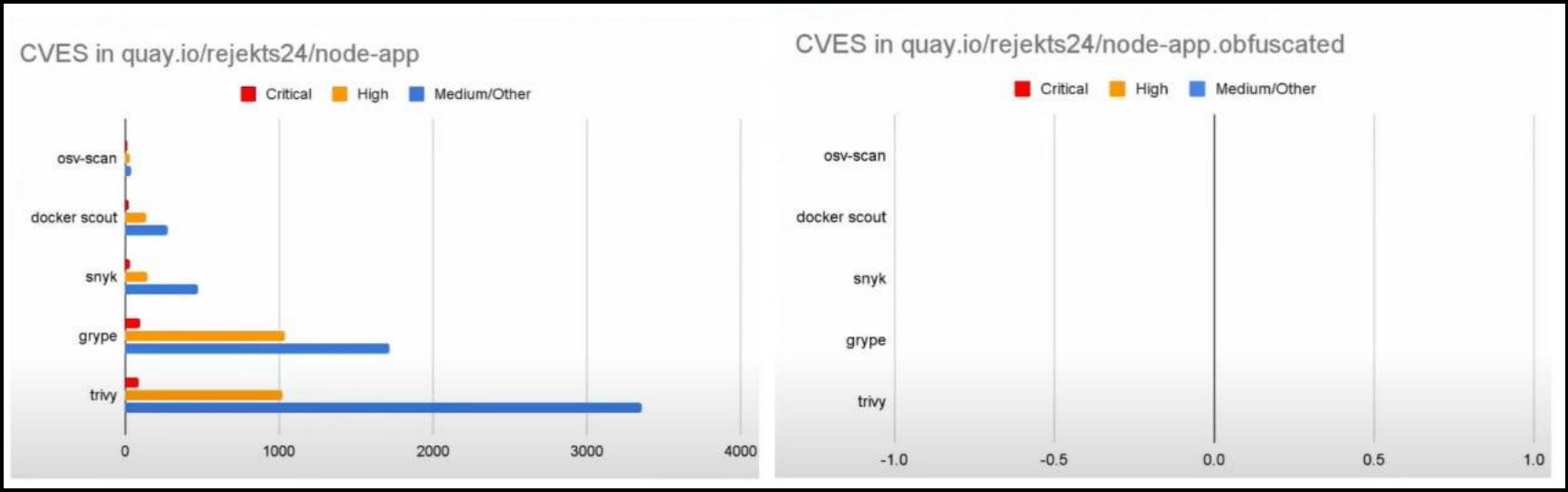
Пункт	Значение
CVE исчезает или нет	Да
Уязвимости базового слоя	Нет*
Уязвимости других слоев	Да
Исходные артефакты	Да
Эксплуатация баги	Нет
Модификация	Да
Защита от 0day	Нет
Сложность	Средняя
Покрытие	Низкое
Скорость	Низкая
Надежность	Высокая
Комментарий	Все сильно зависит от людей и процессов

** - Да, если только самостоятельно готовите базовые образы*

LUNTRY

Способ 2:
Обфускация

Обфускация



- Доклад “Malicious Compliance Automated: When You Have 4000 Vulnerabilities and only 24 Hours Before Release” с Cloud Native Rejekts 2024
- Инструмент mint с флагами
  - --obfuscate-metadata
  - --obfuscate-app-package-names
- Все подходы на базе статического анализа позволяют защититься только лишь от легитимного пользователя, но не являются никакой помехой для вредоносного!

Серебряной пули нет!

Характеристика

Пункт	Значение
CVE исчезает или нет	Нет
Уязвимости базового слоя	-
Уязвимости других слоев	-
Исходные артефакты	Нет
Эксплуатация баги	Да
Модификация	Нет
Защита от 0day	Нет
Сложность	Низкая
Покрытие	Высокое
Скорость	Высокая
Надежность	-
Комментарий	Это про обман/обход, которым могут пользоваться на Security/Quality gates

LUNTRY

LUNTRY

Способ 3: Автоматизация с помощью AI

AI-ассистент

- Доклад «Контроль зависимостей на автопилоте: AI-ассистент на страже Dockerfile» с PHDays 2025
  - Вдохновлено “SWE-agent: Agent-Computer Interfaces Enable Automated Software Engineering”
  - С помощью LLM-агента анализируются команды Dockerfile на наличие устанавливаемых компонент и отчет об уязвимостях от классических сканеров уязвимостей
  - Исправление компонент с перепроверкой
  - Создание MR с рекомендациями для разработчика

LUNTRY

Характеристика

Пункт	Значение
CVE исчезает или нет	Да
Уязвимости базового слоя	Нет*
Уязвимости других слоев	Да
Исходные артефакты	Да
Эксплуатация баги	Нет
Модификация	Да
Защита от 0day	Нет
Сложность	Высокая
Покрытие	Высокое
Скорость	Низкая
Надежность	Средняя
Комментарий	Частичная оптимизация ручного патчинга, также возможны галлюцинации!

** - Да, если только самостоятельно готовите базовые образы*

LUNTRY

LUNTRY

Способ 4:
Золотой образ

Golden image

- Образ, который включает все необходимые операционные системы, библиотеки и зависимости
- Создается для каждого из сообществ внутри компании (Go, Java, PHP, ML и т.д.)
- Упрощение работы с уязвимостями за счёт централизации, стандартизации и автоматизации
- Изменение в одном месте сразу затрагивает всех
- Снижается configuration drift

LUNTRY

Характеристика

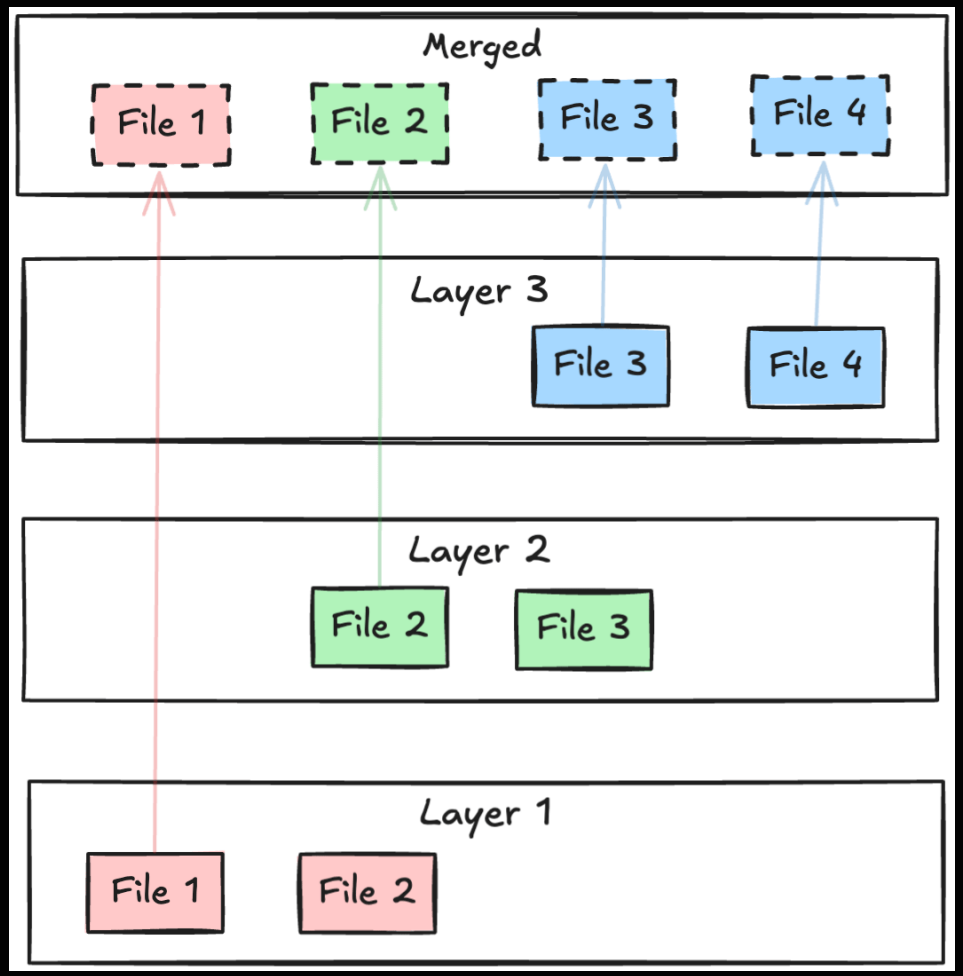
Пункт	Значение
CVE исчезает или нет	Да
Уязвимости базового слоя	Да
Уязвимости других слоев	Нет
Исходные артефакты	Да
Эксплуатация баги	Нет
Модификация	Да
Защита от 0day	Нет
Сложность	Средняя
Покрытие	Высокое
Скорость	Средняя
Надежность	Высокая
Комментарий	Можно использовать тонкие образы, что усложнят развитие атаки

LUNTRY

Способ 5: Дополнительный слой образа

Новый слой

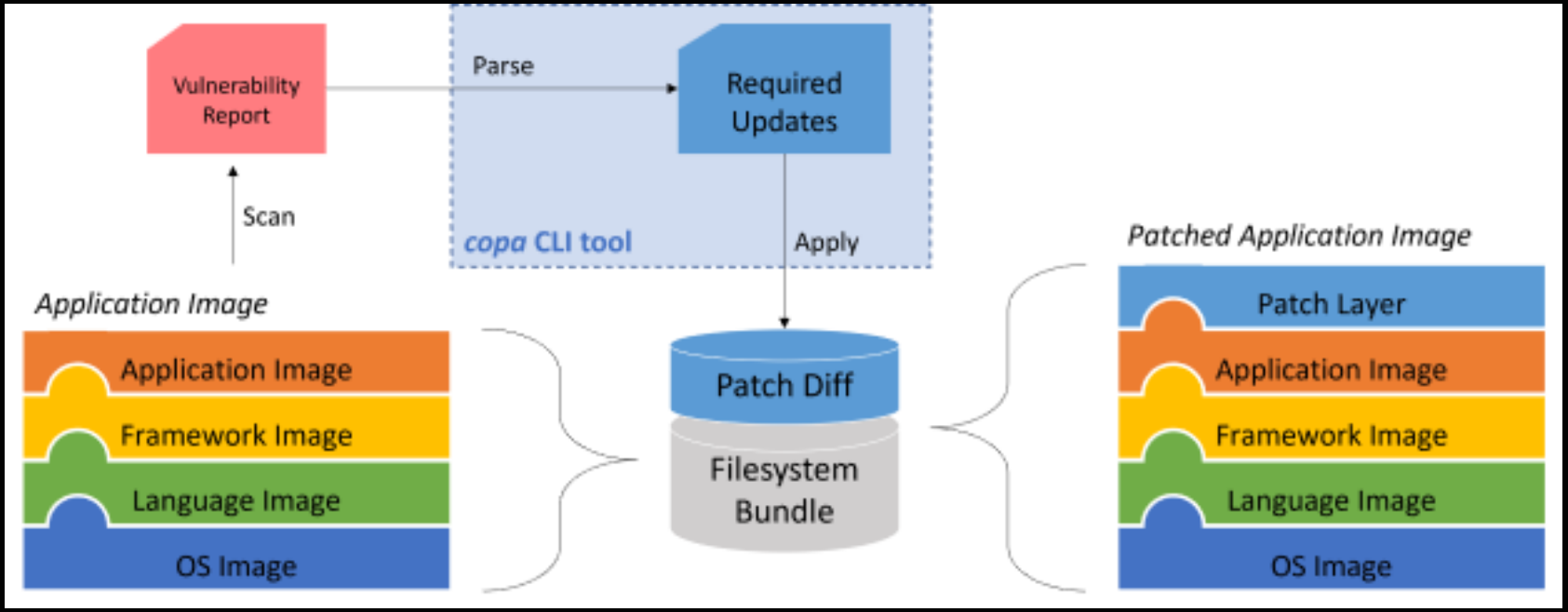
- Играем на специфике Union File System (например, OverlayFS) в контейнерах
- Если файл существует в двух слоях, то, тот что в верхнем слое, имеет приоритет над тем, что в нижнем
- Можно перезаписать старую библиотеку новой с исправлением



LUNTRY

Автоматический подход

- Project Copacetic — это инструмент для прямого исправления уязвимостей в образах контейнеров без полной пересборки. Работает на базе Trivy (можно и другие сканеры) и BuildKit
- Используется в Azure Container Registry (ACR) Continuous, Kubescape, Devtron, Helmper



Ручной подход

- crane — инструмент, который позволяет извлекать файловую систему образа, манипулировать ею и экспортировать обратно. Его можно использовать для создания диффа между двумя версиями образа и ручного применения исправлений
- Команда crane mutate для модификации

DESCRIPTION

The **crane mutate** command, part of the *go-containerregistry (crane)* utility, allows for efficient modification of container image metadata and content directly within a container registry without requiring a full image pull or a local Docker daemon. It enables users to alter various aspects of an image, such as environment variables, labels, entrypoints, working directories, or even add/delete layers. This capability is particularly valuable in CI/CD pipelines for post-processing images, re-tagging, or applying patches without incurring the overhead of rebuilding or transferring large image blobs locally. It manipulates the image manifest and configuration, then pushes the updated manifest back to the registry, often resulting in a new image digest.

Характеристика

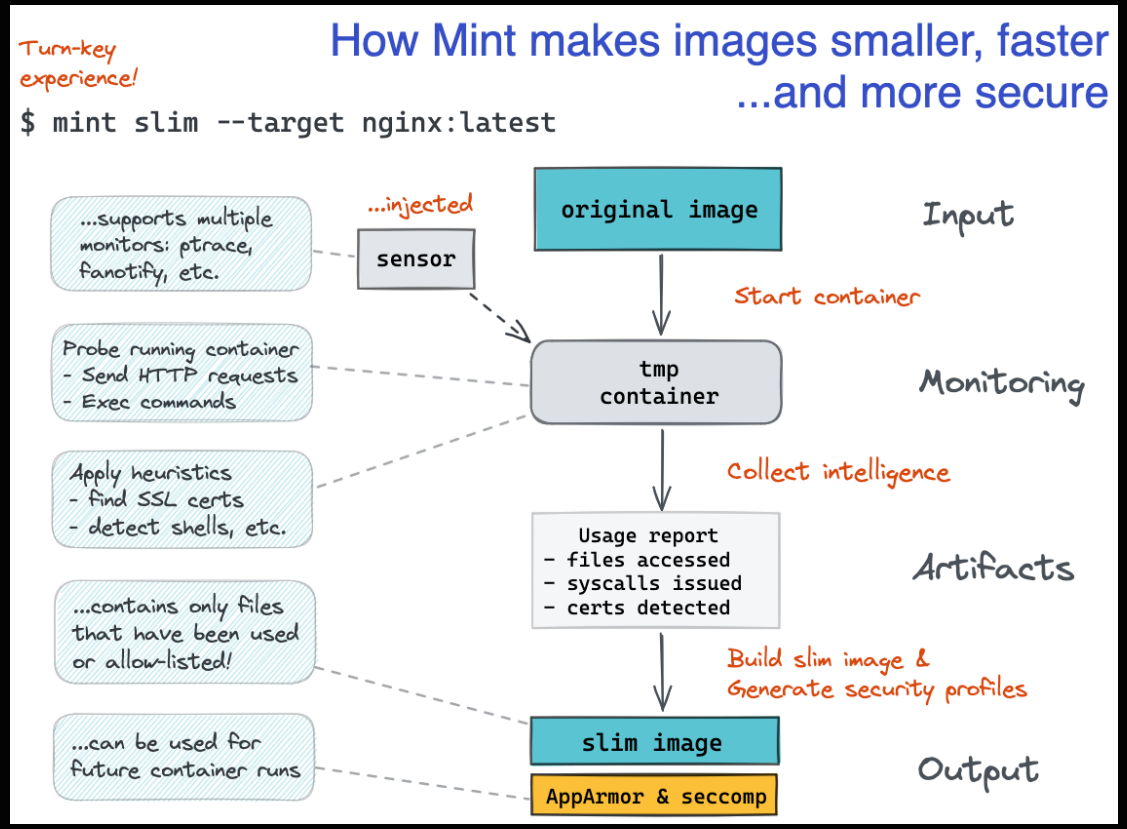
Пункт	Значение
CVE исчезает или нет	Да
Уязвимости базового слоя	Да
Уязвимости других слоев	Да
Исходные артефакты	Нет
Эксплуатация баги	Нет
Модификация	Да
Защита от 0day	Нет
Сложность	Низкая
Покрытие	Высокое
Скорость	Высокая
Надежность	Низкая
Комментарий	Простое использование более старшей/новой версии библиотеки может сломать проект – требуется хорошее тестирование

LUNTRY

Способ 6: Минификация

Минимизируем поверхность атаки

- Минификация — исключения из образа не используемых файлов. В новый образ попадает только то, что необходимо для работы
- Для профилирования нужно иметь хорошие, полноценные unit tests / integration tests. Иначе профилирование будет не точное и новый образ не рабочим
- Инструменты:
  - Mint
  - BLAFS



Характеристика

Пункт	Значение
CVE исчезает или нет	Частично
Уязвимости базового слоя	Да
Уязвимости других слоев	Да
Исходные артефакты	Нет
Эксплуатация баги	Нет
Модификация	Да
Защита от 0day	Возможна*
Сложность	Высокая
Покрытие	Среднее
Скорость	Низкая
Надежность	Средняя
Комментарий	Нужно хорошее покрытие тестами, сильно усложняет развитие атаки

** - зависит от типа уязвимости*

LUNTRY

Способ 7: Перегенерация / транспайлинг кода

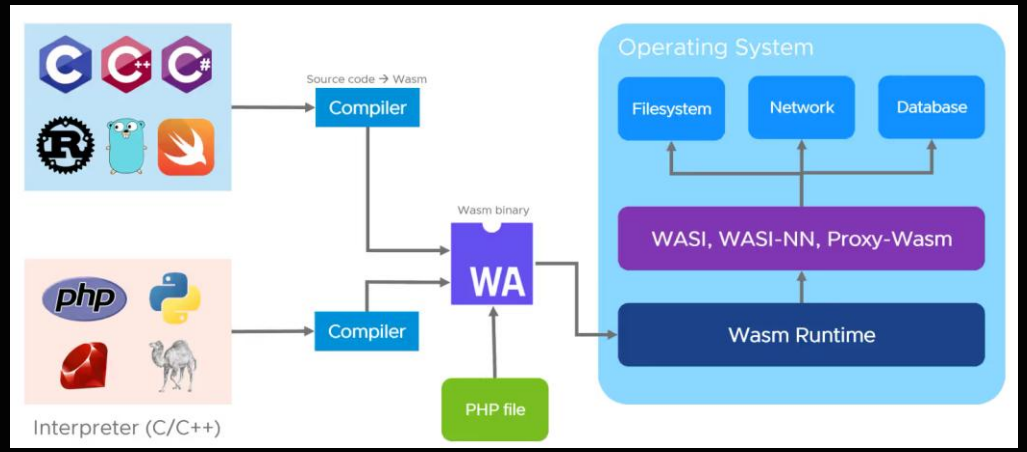
WASM код и контейнер

Транспайлеры / конверторы / трансляторы:

- У каждого ЯП может быть свой инструмент
- Container2wasm — конвертор контейнера в WebAssembly
- Elfconv — AOT бинарный транслятор Linux/ELF в WebAssembly

Среда выполнения:

- WASM runtime в виде:
  - Отдельный образ
  - Отдельный RuntimeClass в Kubernetes
- Много зависит от выбранного runtime и ситуации с WASI
  - WASI еще очень сырой



Характеристика

Пункт	Значение
CVE исчезает или нет	Частично
Уязвимости базового слоя	Да
Уязвимости других слоев	Да
Исходные артефакты	Да/Нет**
Эксплуатация баги	Нет
Модификация	Да
Защита от 0day	Возможна*
Сложность	Высокая
Покрытие	Высокое
Скорость	Высокая
Надежность	Низкая
Комментарий	Возможны новые уязвимости, сильно усложняет развитие атаки, проблемы WASI, просадка производительности

** - зависит от типа уязвимости*

*** - зависит от способа и инструмента*

LUNTRY

LUNTRY

Способ 8: Превентивный / проактивный подход

Проактивный и реактивный подход к безопасности

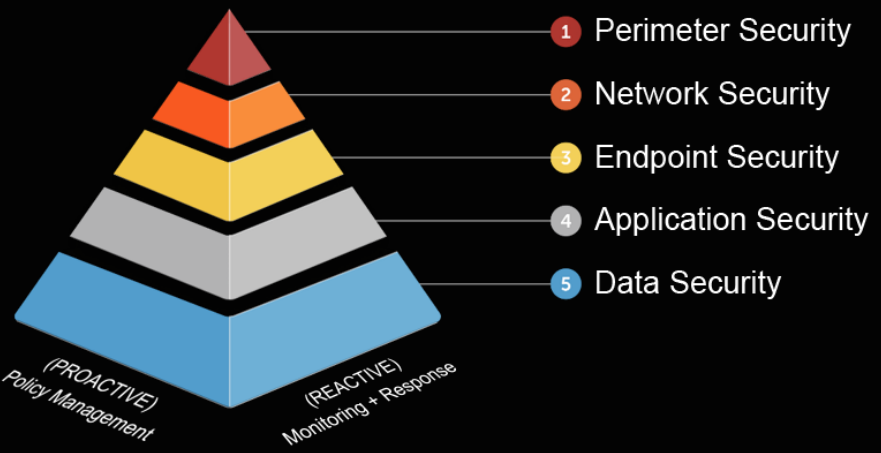
Cyber-resilient culture: “In building a cyber-resilient culture, the role of security is not to stop all incidents. It is to prevent a security incident from impacting the business.”

Vulnerabilities != vulnerable

Пример проактивной защиты

Микросервис:

- На базе минимального образа
  - Distroless, Chainguard, …
- С файловой системой доступной только для чтения
  - SecurityContext.readOnlyRootFilesystem.true
- Без лишних возможностей
  - SecurityContext.capabilities.drop.all
- Со строго определённым набором исполняемых файлов
  - AppArmor profile
- С ограниченной активностью по сети
  - NetworkPolicy
- …



Рекомендация: «Сочетание несочетаемого в Kubernetes: удобство, производительность, безопасность»

Характеристика

Пункт	Значение
CVE исчезает или нет	Нет
Уязвимости базового слоя	-
Уязвимости других слоев	-
Исходные артефакты	Нет
Эксплуатация баги	Нет
Модификация	Нет
Защита от 0day	Возможна*
Сложность	Средняя
Покрытие	Высокое
Скорость	Средняя**
Надежность	Высокая
Комментарий	Не только сторонний код, но и собстввенные уникальные уязвимости, дает дополнительное время на спокойный ручной патчинг

** - зависит от типа уязвимости*

*** - нужны усилия на старте, дальше переиспользуется*

LUNTRY

Итоговое сравнение

Пункт	1	2	3	4	5	6	7	8
CVE исчезает или нет	Да	Нет	Да	Да	Да	Частично	Частично	Нет
Уязвимости базового слоя	Нет	-	Нет	Да	Да	Да	Да	-
Уязвимости других слоев	Да	-	Да	Нет	Да	Да	Да	-
Исходные артефакты	Да	Нет	Да	Да	Нет	Нет	Да/Нет	Нет
Эксплуатация баги	Нет	Да	Нет	Нет	Нет	Нет	Нет	Нет
Модификация	Да	Нет	Да	Да	Да	Да	Да	Нет
Защита от 0day	Нет	Нет	Нет	Нет	Нет	Возможна	Возможна	Возможна
Сложность	Средняя	Низкая	Высокая	Средняя	Низкая	Высокая	Высокая	Средняя
Покрытие	Низкое	Высокое	Высокое	Высокое	Высокое	Среднее	Высокое	Высокое
Скорость	Низкая	Высокая	Низкая	Средняя	Высокая	Низкая	Высокая	Средняя
Надежность	Высокая	-	Средняя	Высокая	Низкая	Средняя	Низкая	Высокая

LUNTRY

Итоговое сравнение

Пункт	Руками	Обман	AI	Golden	Новый слой	Мини.	Переген.	Proactive
CVE исчезает или нет	Да	Нет	Да	Да	Да	Частично	Частично	Нет
Уязвимости базового слоя	Нет	-	Нет	Да	Да	Да	Да	-
Уязвимости других слоев	Да	-	Да	Нет	Да	Да	Да	-
Исходные артефакты	Да	Нет	Да	Да	Нет	Нет	Да/Нет	Нет
Эксплуатация баги	Нет	Да	Нет	Нет	Нет	Нет	Нет	Нет
Модификация	Да	Нет	Да	Да	Да	Да	Да	Нет
Защита от 0day	Нет	Нет	Нет	Нет	Нет	Возможна	Возможна	Возможна
Сложность	Средняя	Низкая	Высокая	Средняя	Низкая	Высокая	Высокая	Средняя
Покрытие	Низкое	Высокое	Высокое	Высокое	Высокое	Среднее	Высокое	Высокое
Скорость	Низкая	Высокая	Низкая	Средняя	Высокая	Низкая	Высокая	Средняя
Надежность	Высокая	-	Средняя	Высокая	Низкая	Средняя	Низкая	Высокая

LUNTRY

Выводы

Выводы

LUNTRY

01 Контейнеры открывают новые возможности

02 Идеального решения работы с уязвимостями нет,
но есть вариант на любой случай

03 Помните, что задача не закрыть все уязвимости,
а не дать нанести ущерб

04 Риск-ориентированный подход наше все

Полезные материалы

- Вебинар «Patch management не поможет, фиксики не спасут»
- Доклад «Управление уязвимостями в микросервисах и контейнерных средах», Территория Безопасности 2024
- Вебинар «Безопасность контейнеров и Kubernetes для DevSecOps специалистов»
- Доклад «Латаем огрехи в образах приложений с помощью Kubernetes», БеКон 2024
- Статья «Контейнеры уязвимы. И что теперь?»
- Статья «Разбираемся с Docker: как создаются образы»
- Доклад «Кубик Runtime в конструкторе Kubernetes для безопасности», PHDays 2
- Доклад «SCAзка о SCAнерах», Positive Hack Days 12

LUNTRY

cyber camp '25

Дмитрий Евдокимов

Founder & CTO Luntry

НА СВЯЗИ

de@luntry.ru

@Qu3b3c

@k8security

@luntry_official