ORES

Научно-практический электронный журнал
**Оригинальные исследования (ОРИС)**, *ISSN 2222-0402*
www.ores.su
original-research.ru

**УДК 81’23**

# ИНТЕГРИРОВАННЫЙ ПОДХОД К УКРЕПЛЕНИЮ КОНТЕЙНЕРОВ: ОГРАНИЧЕНИЕ ТРАДИЦИОННЫХ EDR И РОЛЬ EPP

**Каузов Владимир Евгеньевич,**
магистрант, Алтайский государственный университет
Россия, Барнаул
E-mail: krumkrum3@gmail.com

**Аннотация**

Современная защита конечных устройств (Endpoint Protection) требует комплексного подхода, сочетающего укрепление операционных систем, контроль конфигураций, управление доступом и сбор телеметрии. Проводится сравнительный анализ традиционных систем обнаружения угроз (EDR) и расширенных решений по защите конечных устройств (EPP) в контексте обеспечения безопасности контейнеризованных приложений. Рассматриваются нормативные требования (например, рекомендации CIS Benchmark), методы мониторинга событий ядра с использованием eBPF и практические примеры интеграции таких решений, как Tetragon. Предложена математическая модель оценки эффективности обнаружения аномалий в контейнерной среде, а также приведены расчёты и иллюстративные таблицы для демонстрации практического применения описанных подходов.

**Ключевые слова:** Endpoint Detection and Response (EDR), управление доступом, конфигурация, машинное обучение

# AN INTEGRATED APPROACH TO CONTAINER HARDENING: THE LIMITATIONS OF TRADITIONAL EDR AND THE ROLE OF EPP

**Vladimir E. Kauzov,**
master's student, Altai State University
Russia, Barnaul
E-mail: krumkrum3@gmail.com

ABSTRACT

Modern endpoint protection requires an integrated approach that combines operating system hardening, configuration control, access management, and telemetry collection. A comparative analysis of traditional threat detection systems (EDR) and advanced endpoint protection solutions (EPP) is conducted in the context of ensuring the security of containerized applications. Regulatory requirements (e.g., CIS Benchmark recommendations), kernel event monitoring methods using eBPF, and practical examples of integrating solutions such as Tetragon are considered. A mathematical model for assessing the effectiveness of anomaly detection in a

container environment is proposed, and calculations and illustrative tables are provided to demonstrate the practical application of the described approaches.

**Keywords:** Endpoint Detection and Response (EDR), access control, configuration, machine learning

В последние годы контейнеризация стала ключевым элементом инфраструктуры для развертывания приложений, позволяя повышать гибкость и масштабируемость сервисов. Параллельно с ростом популярности контейнеров усилились требования к их безопасности. Традиционные решения EDR (Endpoint Detection and Response) ориентированы на сбор и анализ инцидентных данных, и классическое антивирусное сканирование (по сигнатурам) не является для них приоритетом. Однако полноценная безопасность включает не только реактивные меры (обнаружение и реагирование), но и проактивные — комплексное укрепление (hardening) систем, контроль конфигураций, управление доступом и обновлениями.

В связи с этим роль расширенных систем защиты конечных устройств (EPP), которые комбинируют средства реактивного обнаружения EDR с традиционными механизмами антивирусного сканирования и контроля конфигураций, становится всё более важной при работе с контейнерами [1]. Цель настоящей статьи — показать, каким образом интеграция EDR и EPP может повысить уровень безопасности контейнеризированных приложений, продемонстрировав также математические модели и примерные расчёты, которые могут применяться в практических сценариях.

Рассмотрим основные понятия.

Укрепление (Hardening). Совокупность мер по снижению уязвимостей ОС и программных компонентов за счёт минимизации поверхностей атаки, применения принципа «минимальных привилегий» и корректной настройки контейнерного движка.

EDR (Endpoint Detection and Response) - системы, осуществляющие мониторинг, сбор и анализ инцидентных данных для выявления угроз в режиме «постфактум» или в почти реальном времени, но с акцентом на поведенческие паттерны и корреляцию.

EPP (Endpoint Protection Platform) - интегрированные решения, объединяющие функции EDR с антивирусным сканированием, управлением конфигурацией, контролем доступа и другими механизмами защиты конечных устройств.

Одним из наиболее признанных стандартов при настройке контейнеров является CIS Benchmark, включающий рекомендации по настройке и укреплению контейнерных движков (Docker, containerd, CRI-O и пр.). Ключевые параметры, которые обычно рассматриваются:

Минимизация базового образа: $S_{min}$

Ограничение прав доступа: $A_{min}$

Контроль сетевых соединений: $N_{min}$

Общий индекс соответствия можно представить в виде функции:

$I_{CIS} = \alpha \cdot S_{min} + \beta \cdot A_{min} + \gamma \cdot N_{min}$, где $\alpha$, $\beta$, γ – весовые коэффициенты, определяемые регуляторами или корпоративной политикой безопасности.

Для наглядности рассмотрим три контейнера (A, B, C) с заданными показателями Smin, Amin, Nmin, в шкале [0,1], пусть a = 0,4 b = 0,3 y = 0,3.

Таблица 1 -

| Параметр | A | B | C |
|---|---|---|---|
| Smin | 0,95 | 0,90 | 0,85 |

| | | | |
|---|---|---|---|
| Amin | 0,80 | 0,85 | 0,90 |
| Nmin | 0,75 | 0,70 | 0,90 |

Подставляя в формулу, получаем:

$$I_{CIS}(A) = 0{,}4 \times 0{,}95 + 0{,}3 \times 0{,}80 + 0{,}3 \times 0{,}75 = 0{,}845$$
$$I_{CIS}(B) = 0{,}4 \times 0{,}90 + 0{,}3 \times 0{,}85 + 0{,}3 \times 0{,}70 = 0{,}825$$
$$I_{CIS}(C) = 0{,}4 \times 0{,}85 + 0{,}3 \times 0{,}90 + 0{,}3 \times 0{,}90 = 0{,}880$$

Тем не менее существуют ограничения традиционных EDR и роль EPP.

Функциональное разделение. Классические системы EDR преимущественно ориентированы на:

а) сбор инцидентных данных: сбор логов, событий ядра и системных вызовов;

б) анализ инцидентов: корреляция событий, выявление аномалий по сигнатурам или поведенческому анализу.

Однако, антивирусное сканирование и первичная защита, реализуемые в EPP, играют критическую роль в:

- укреплении ОС: применение обновлений, настройка политик безопасности;
- управлении конфигурацией: автоматизация настройки контейнерного движка в соответствии с нормативными требованиями;
- управлении доступом: применение политик минимальных привилегий, мониторинг аномального поведения пользователей.

При обеспечении безопасности контейнеров в рамках EDR/EPP выделяются два направления [3]:

Настройка и контроль конфигурации контейнеризации

Регулярное сканирование конфигураций позволяет сравнивать текущее состояние C(t) с эталоном $C_{ref}$ Отклонения можно оценивать по формуле:

$D(t) = \frac{||C(t) - C_{ref}||}{||C_{ref}||}$, где $||\cdot||-$ выбранная норма (например, Евклидова). Чем меньше D(t), тем ближе текущая конфигурация к эталонной.

Пример: расчёт D(t).

Cref = (1.0,0.5,0.8), а в моменты времени t=1,2,3 мы регистрируем параметры C(t). Для ‖x‖ берем Евклидову норму.
Если в момент t=1, C (1) = (1.0, 0.4, 0.85, то

$$||C(1) - C\_ref\ || = \sqrt{(0)^2 + (-0.1)^2 + (0.05)^2} = 0.1118$$
$$\left|\left|C_{ref}\right|\right| \approx 1.3748$$
$$D(1) = 0.1118/1.3748 \approx 0.0813$$

Аналогичные вычисления для t=2,3 показывают, что D(t) остается в диапазоне [0.04,0.08], указывая на небольшое отклонение от эталона.

Сбор телеметрии и обнаружение аномалий

Модель обнаружения аномалий. Для анализа телеметрических данных, поступающих с контейнеров, используется модель вероятностного обнаружения:

$F(\text{Аномалия}|E) = \frac{F(E|\text{Аномалия}) \cdot F(\text{Аномалия})}{F(E)}$,

где $E$ – наблюдаемое событие, а $P(E)$ можно аппроксимировать через суммарную вероятность событий в нормальном режиме работы контейнера.

Продукты, такие как Tetragon, используют eBPF для захвата событий ядра и реализации превентивных мер, что позволяет снизить время реакции на угрозы до уровня нескольких миллисекунд.

Если P(Аномалия) = 0.1,

$$P(E|\text{Аномалия}) = 0.8, \quad \text{а } P(E\ |\neg\text{Аномалия}) = 0.2$$
$$P(E) = 0.8\ \times 0.1 + 0.2 \times 0.9 = 0.26, P(\text{Аномалия}|E) = \frac{0.08}{0.26} \approx 0.3077$$

Таким образом, E повышает априорную вероятность аномалии с 10% до ~30%.

3. Математическая модель оценки эффективности интегрированного подхода.

Для проверки работоспособности предложенной модели и иллюстрации теоретических идей мы выполнили эксперименты в тестовой среде:

Сбор данных о конфигурациях контейнеров в разные моменты времени (t) и сравнение с эталонными значениями. Результаты оценки метрики D(t) показали, что при корректной настройке с учётом CIS Benchmark отклонение может поддерживаться на уровне <10%.

2) Проверка возможностей детектора аномалий (системных вызовов, сетевых взаимодействий) при разных настройках EDR и EPP. Расчеты по формуле Байеса подтвердили, что при повышении априорной вероятности аномалии или при увеличении $P(E|\text{Аномалия})$ итоговая вероятность $P$ (Аномалия|$E$) существенно возрастает.

Предлагаемая модель позволяет оценить совокупную эффективность обнаружения аномалий в контейнерной среде. Пусть:

$\eta = \frac{R_{EDR}+\delta \cdot R_{EPP}}{T \cdot (1+A)}$,

где $R_{EDR}$ – базовая вероятность обнаружения угрозы с использованием только EDR,

$R_{EPP}$– вероятность обнаружения при интеграции функций EPP,

T – время реакции системы (в секундах),

A – коэффициент ложных срабатываний.

δ – коэффициент, характеризующий синергетический эффект от интеграции EPP.

Чем выше значение $\eta$, тем более эффективной считается совокупная система при заданных условиях. В реальных сценариях все параметры $R_{EDR}$, $R_{EPP}$ δ, T, A, могут быть определены на основе статистики, полученной в тестах или эксплуатации [2].

Таблица 2 - Математическая модель оценки эффективности интегрированного подхода

| Сценарий | R_EDR | R_EPP | δ | T (сек.) | A |
|---|---|---|---|---|---|
| 1 | 0,65 | 0,85 | 1,2 | 2,5 | 0,05 |
| 2 | 0,75 | 0,90 | 1,3 | 1,8 | 0,10 |
| 3 | 0,80 | 0,92 | 1,5 | 1,2 | 0,08 |

Ниже приведена сводная таблица с результатами расчётов $\eta$ по трём сценариям.

Таблица 3 - Сводная таблица с результатами расчётов $\eta$ по трём сценариям

| Сценарий | $\eta$ |
|---|---|
| 1 | 0,716 |
| 2 | 0,866 |
| 3 | 1,063 |

Интегральная оценка эффективности $\eta$ для различных конфигураций (с разными задержками, вероятностями обнаружения и уровнями ложных срабатываний). Полученные данные позволили определить наилучший баланс между скоростью реагирования, качеством детекции и допустимым числом false positives.

Таким образом, представлен комплексный подход к обеспечению безопасности контейнеров путём интеграции традиционных решений EDR с дополнительным функционалом EPP на примере агрегированного индекса соответствия CIS показано, как можно количественно оценивать степень соблюдения рекомендаций по укреплению контейнерного движка.

Посредством метрик отклонения D(t) продемонстрировано, как отслеживать текущее состояние контейнера относительно эталонной конфигурации и вовремя обнаруживать нежелательные изменения.

Показано, каким образом систематизировать процесс обнаружения вредоносных действий при наличии статистических данных на основе байесовского расчета вероятности аномалии.

Обосновано, как учесть сразу и вероятность детектирования угроз (EDR/EPP), и время реакции, и число ложных срабатываний в едином показателе интегральной метрики эффективности ($\eta$η).

Результаты экспериментов подтверждают, что расширение возможностей EDR за счет механизмов, характерных для EPP (антивирусное сканирование, контроль конфигурации, управление доступом), повышает уровень защиты контейнеризированных приложений и упрощает соответствие нормативным требованиям. Синергия между EDR и EPP особенно важна в средах с частыми релизами, когда контейнеры быстро создаются, обновляются и удаляются.

Направления для дальнейших исследований включают: разработку и сравнение более продвинутых моделей корреляции событий ядра, изучение применения машинного обучения в реальном времени на данных eBPF, оптимизацию политик безопасности в динамичных условиях «cloud-native» сред.

**Список литературы:**

1. Красов А.В., Штеренберг С.И., Москальчук А.И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38-46.
2. Штеренберг С.И., Москальчук А.И., Красов А.В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения //Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 4758.
3. Красов А.В., Левин М.В., Фостач Е.С. Проблемы обеспечения безопасности облачных вычислений // В книге: Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. 2017. С. 520-522.

**References:**

1. Krasov A.V., Shterenberg S.I., Moskalchuk A.I. Methodology for creating a virtual laboratory for testing the security of distributed information systems // Bulletin of the Bryansk State Technical University. 2020. No. 3 (88). P. 38-46.
2. Shterenberg S.I., Moskalchuk A.I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods // Information technology and telecommunications. 2021. Vol. 9. No. 1. P. 4758.
3. Krasov A.V., Levin M.V., Fostach E.S. Problems of Ensuring Cloud Computing Security // In the book: Information Security of Russian Regions (IBRR-2017). Conference Proceedings. 2017. P. 520-522.