

PT Container Security

Решение для комплексной
защиты инфраструктуры
гибридного облака

Технологии контейнеризации упростили построение отказоустойчивых систем, автоматически масштабируемых под имеющуюся нагрузку, но вместе с тем создали сложности для классических средств защиты информации.

Контейнеризация создает уникальные вызовы для безопасности: короткое время жизни, механизмы изоляции контейнеров и дополнительные уровни абстракции инфраструктуры затрудняют эффективную сегментацию сети и мониторинг инцидентов.

Подобные проблемы решают технологии, обеспечивающие доступ к внутреннему устройству платформ контейнеризации и дополняющие классические средства защиты специфическими функциями.

Именно такие технологии мы реализовали в **PT Container Security** — решении для обеспечения безопасности контейнеров на всех этапах их жизненного цикла.

Ошибки в контейнерных образах, конфигурациях и настройках Kubernetes быстро масштабируются на все среды — dev, test и prod. Одна уязвимость в базовом образе или конфигурации может затронуть сразу десятки сервисов.



Помогает автоматизировать управление уязвимостями и дефектами в конфигурациях образов и контейнеров



Позволяет контролировать операции над кластером Kubernetes



Решает задачи мониторинга и реагирования на инциденты ИБ в рантайме контейнеров



Контейнерная безопасность становится обязательной частью процессов DevSecOps и защиты гибридной инфраструктуры.

65%

компаний активно используют контейнеры для развертывания приложений

92%

из них не имеют ресурсов для выявления серьезных инцидентов ИБ в контейнерах

*По данным исследования Positive Technologies и «K2 Кибербезопасность»

Ключевые преимущества



Мультикластерность

Централизованное управление несколькими кластерами Kubernetes вне зависимости от их расположения и масштаба экономит время специалистов по ИБ. Решение легко устанавливается и позволяет настроить потребление ресурсов в зависимости от обрабатываемого потока событий



Прозрачность системы

Метрики, аудит и показатели работы самого продукта, инвентаризация и мониторинг событий в наблюдаемом кластере

Благодаря визуализированной карте кластера с отображением нод, пространств имен, подов, мониторингу рантайма, поддержки prometheus, loki, grafana



Security as code

Практическая реализация подхода, который позволяет описывать политики безопасности на языках программирования высокого уровня с использованием технологии WebAssembly, дает возможность создавать и кастомизировать конфигурации под нужды клиента



Создание политик

Поддержка языков программирования для разработки политик предоставляет неограниченные возможности для реализации логики реагирования на инциденты ИБ, возникающие при работе приложений



Движок выявления инцидентов

Собственный производительный движок для контроля соблюдения политик и поиска аномалий в рантайме контейнеров позволяет гибко настраивать мониторинг событий и выявляет угрозы сразу «из коробки»



Покрытие всего цикла использования приложений

Безопасность обеспечивается на всех этапах — от расширенного анализа образов инструментов для сборки кода до контроля обращений к API кластера и событий, возникающих в ходе работы

Расширенный анализ образов: послойное сканирование, проверка на наличие вредоносного ПО и контроль подписи образов при развертывании



Быстрый старт

Сотни правил для контроля API и манифестов Kubernetes позволяют защитить кластер сразу после установки продукта



Интеграция с экосистемой PT:
PT SIEM, PT Sandbox + IAM/SSO



Запишитесь на «пилот» и протестируйте PT Container Security для защиты контейнерных сред



Исследование



Подробнее о продукте

