

РИСКИ КОНТЕЙНЕРИЗАЦИИ

НА УРОВНЕ ОБРАЗОВ

- Уязвимости в компонентах образа
- небезопасная конфигурация
- Наличие чувствительной информации
- Вредоносное ПО и ПО двойного назначения
- Отсутствие подлинности образов

НА УРОВНЕ КОНТЕЙНЕРОВ

- Недекларированные возможности
- небезопасная конфигурация

НА УРОВНЕ ОРКЕСТРАТОРА

- неподдерживаемые системные компоненты
- Уязвимости в системных компонентах
- Отсутствие изоляции сред
- Отсутствие сетевой сегментации
- небезопасная конфигурация
- Отсутствие контроля доступа
- Избыточные привилегии и возможности

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

ВЫСТРАИВАНИЕ DEVSECOPS ПРОЦЕССОВ

Поддержка высокого уровня защищенности в рамках быстрого цикла разработки

ПОМОЩЬ для SOC

Источник данных для SOC о Kubernetes и контейнерах, работающих в нем

УСИЛЕНИЕ ЗАЩИТЫ KUBERNETES

Комплексный анализ и контроль на всех уровнях и аспектах контейнерной инфраструктуры

РЕАЛИЗАЦИЯ ZERO TRUST

Генерирование превентивных политик

ОСНОВНОЙ ФУНКЦИОНАЛ для ЗАЩИТЫ KUBERNETES

ОБЩИЕ СВОЙСТВА СИСТЕМЫ

- Мультикластерность
- Многопользовательность
- SSO
- Наличие API
- Уведомления (40+ систем)
- Отчеты в форматах PDF, HTML, XML, JSON, CSV
- Работа в закрытом контуре

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ОБРАЗОВ

- Инвентаризация использования
- Компонентный анализ (SBOM)
- Сканирование на уязвимости
- Приоритизация уязвимостей
- Поддержка отечественных ОС и БДУ ФСТЭК
- Интеграция с ASOC
- Поиск секретов
- Контроль соответствия лучшим практикам
- Анализ на вредоносный код и код двойного назначения
- Поддержка внешних и собственных IoC
- Встроенная библиотека уникальных проверок
- Security Gates в CI/CD, Registry, Runtime
- Высокая скорость и парализация сканирований

КОНТРОЛЬ СОСТОЯНИЯ KUBERNETES-КЛАСТЕРОВ

- Контроль актуальности используемых версий
- Проверка системных компонент на уязвимости

КОНТРОЛЬ KUBERNETES-РЕСУРСОВ

- Контроль изменений любых ресурсов
- Анализ Kubernetes Audit Log
- Проверка любых ресурсов на лучшие практики и внутренние стандарты
- Интеграция с Policy Engine: Kyverno, OPA Gatekeeper
- Встроенная библиотека политик и правил
- Создание собственных политик и правил

АНАЛИЗ ПРАВ ДОСТУПА

- Отображение прав доступа с их связями
- Поиск субъектов с опасными правами доступа
- Встроенная библиотека правил
- Создание собственных правил

КОНТРОЛЬ СООТВЕТСТВИЯ КЛАСТЕРА СТАНДАРТАМ

- 99% автоматизации стандарта CIS Kubernetes Benchmark
- Приоритизация пунктов стандарта
- Создание собственных стандартов
- Отслеживание прогресса/регресса
- Отсутствие дополнительной нагрузки на API Server

ЗАЩИТА RUNTIME

- Построение модели поведения микросервисов
- Гибридное обнаружение атак по аномалиям и правилам
- Встроенная библиотека правил/детектов
- File Integrity Monitoring (FIM) для процессов
- Генерирование политик предотвращения
- Реагирование на инциденты
- Сбор данных для расследования инцидентов
- Интеграция с SIEM и другими внешними системами

СЕТЕВАЯ БЕЗОПАСНОСТЬ

- Построение сетевой карты
- Представление любых данных на сетевой карте
- Автоматическое генерирование Network Policy
- Контроль использования Network Policy

[ОСТАВИТЬ ЗАЯВКУ НА ДЕМО](#)[luntry_official](#)[luntrysolution](#)[luntrysolution](#)sales@luntry.ru