ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

CONTAINER SECURITY: КОМПЛЕКСНЫЙ ПОДХОД К БЕЗОПАСНОСТИ K8S

2024

sec.ussc.ru

WHOAMI

- Руководитель направления «Безопасная разработка» в Центре кибербезопасности УЦСБ
- Помогаем нашим Заказчикам создавать безопасные приложения
- Обеспечиваем безопасность облаков и микросервисов
- Запустил собственную платформу анализа защищенности
- Участвую в создании профильных мероприятий

Agenda

Расскажем:

- Какие угрозы и риски ИБ существуют для контейнерных инфраструктур
- Что такое Container Security и почему об этом все говорят
- Какие концепции безопасности контейнерных сред используются в рамках подхода DevSecOps

Продемонстрируем:

- Что такое Nova Container Platform и какие инструменты находятся под капотом платформы
- Какие собственные возможности и интеграции со сторонними решениями для Container Security предлагает Nova Container Platform

Актуальность безопасности Kubernetes

Реальные примеры атак на Kubernetes

2018

Кто: злоумышленник, получивший доступ к консоли администрирования

Что: украл данные для доступа к корзине S3, запустил майнинг криптовалюты

Почему: отсутствие управления доступом, хранение конфиденциальной информации в открытом виде

Последствия: кража конфиденциальной информации, нецелевое использование ресурсов

Уязвимости

CVE: CVE-2023-3676, CVE-2023-3893 и CVE-2023-3955

Уязвимые компоненты: Kubelet

Для чего используются: для удаленного выполнения уязвимого кода на нодах Windows

Необходимые права: привилегии на apply

CVE: CVE-2024-21626, CVE-2024-23651, CVE-2024-23652, CVE-2024-23653

Уязвимые компоненты: Runc

Для чего используются: побег из контейнера

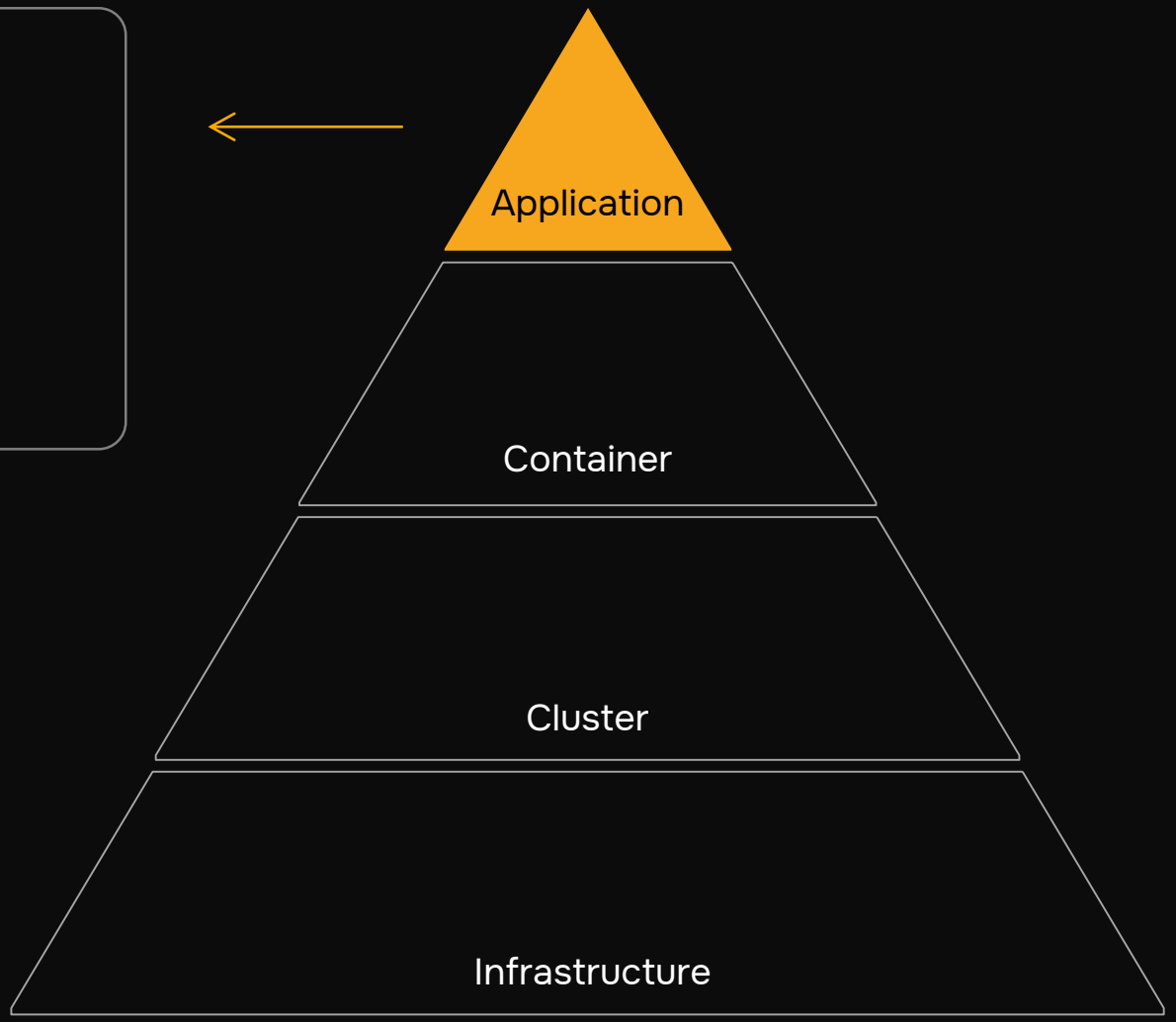
Необходимые права: иметь доступ в контейнер

Уровни безопасности

Уровни обеспечения безопасности

Безопасность приложения

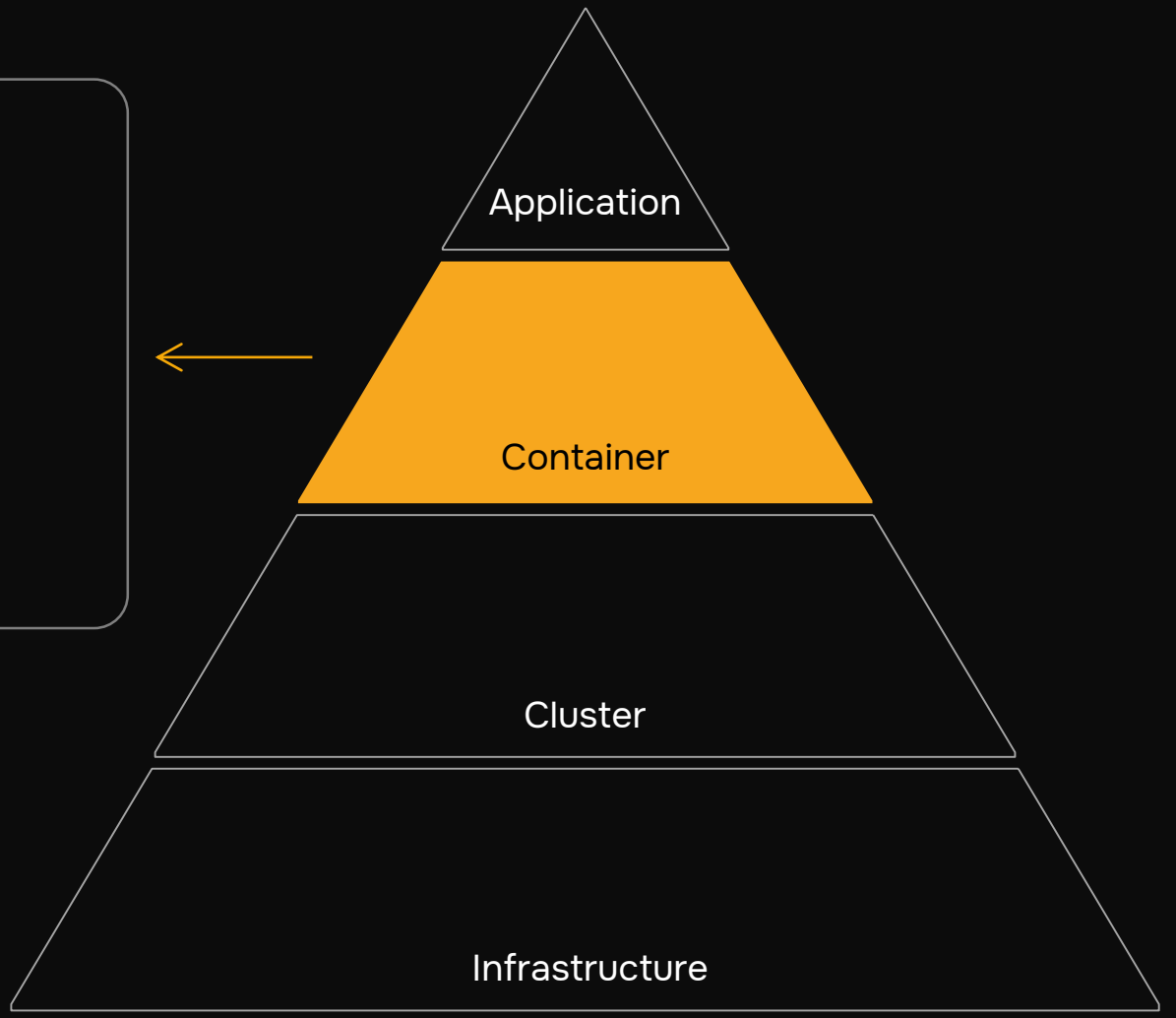
- Процессы разработки
- OSS
- Контур разработки
- Мониторинг и аудит
- Запущенное приложение



Уровни обеспечения безопасности

Безопасность контейнера

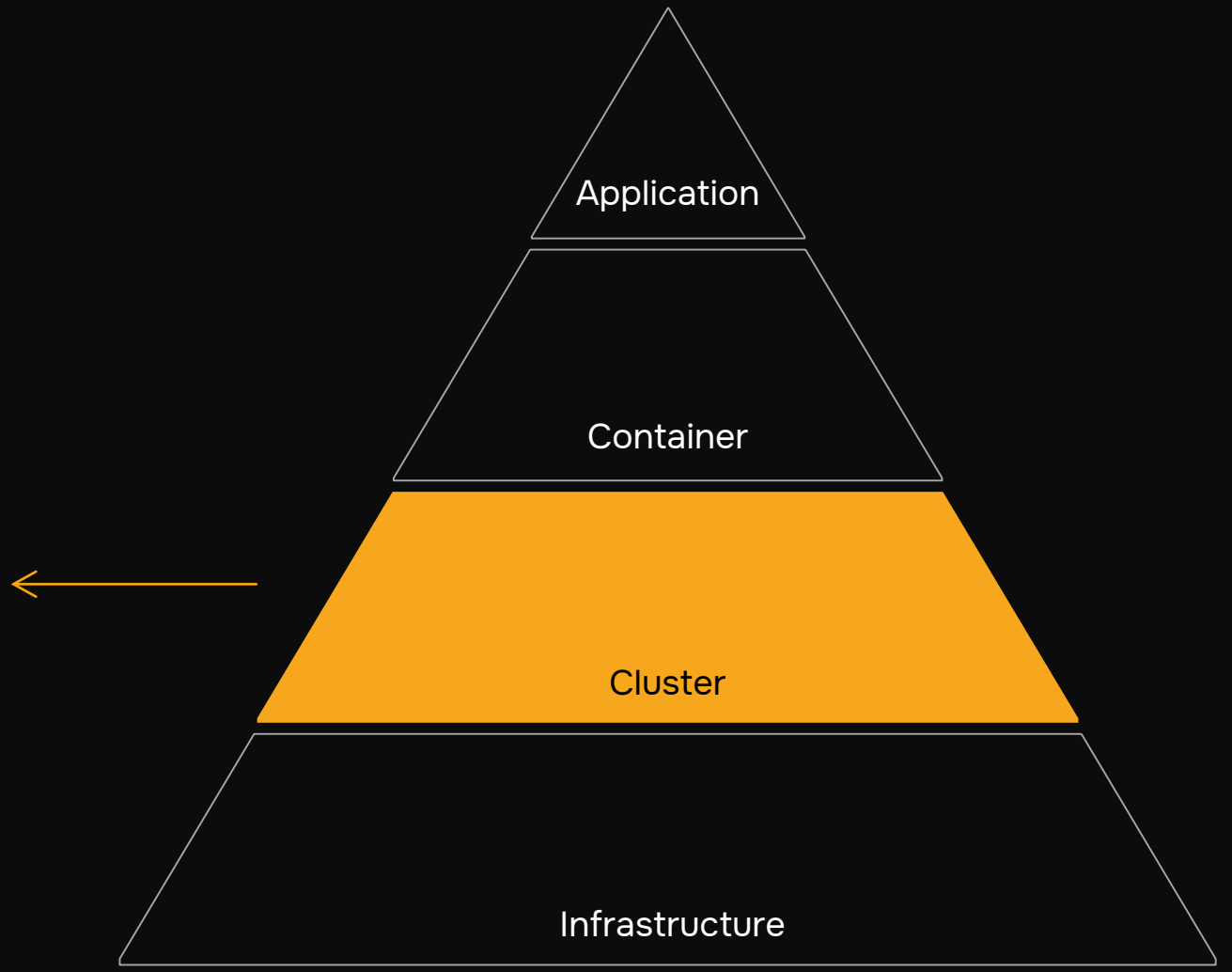
- Управление уязвимостями
- Безопасность цепочек поставок
- Защита реестра образов
- Подтверждение подлинности
- Соответствие требованиям
- Runtime анализ



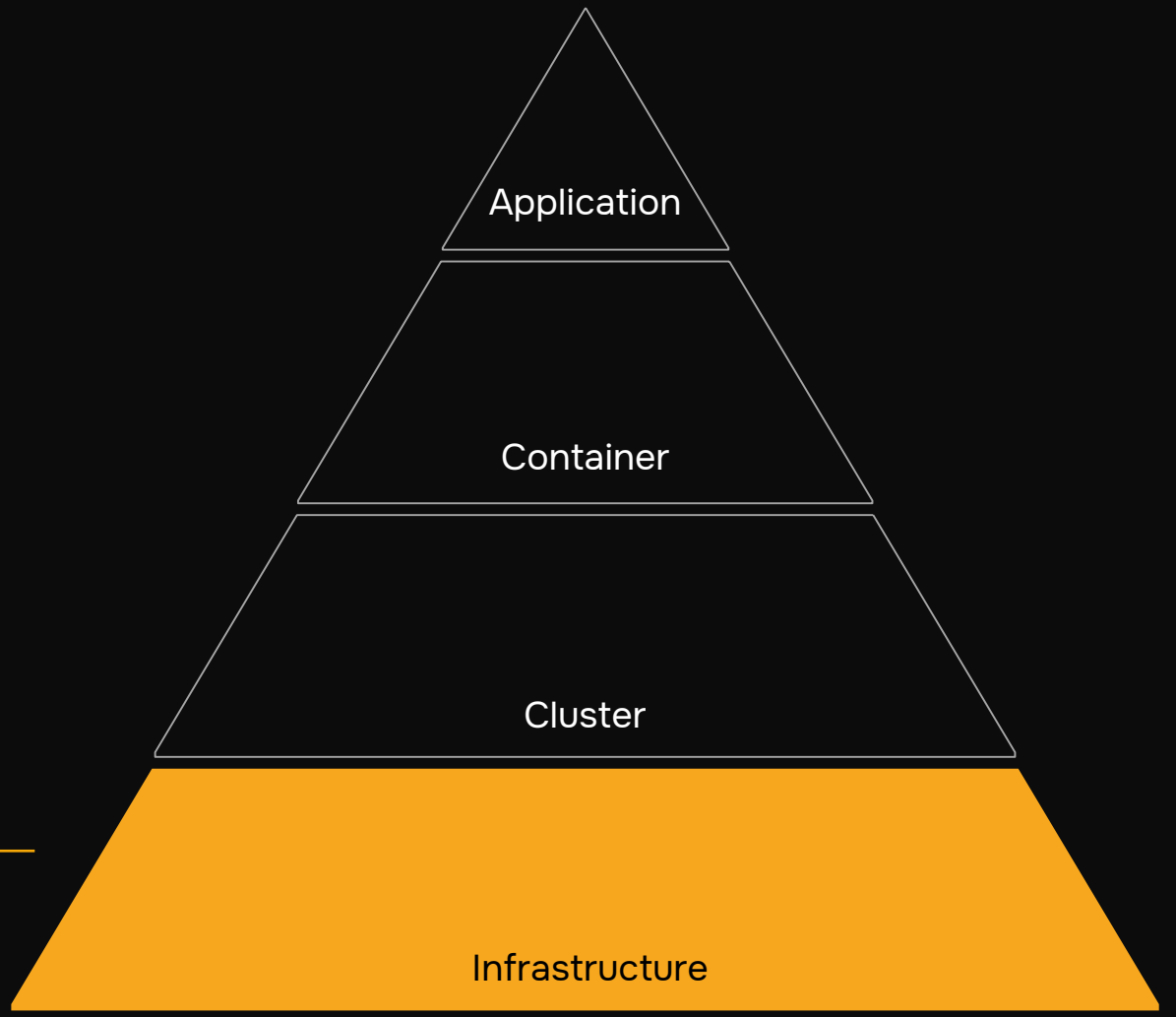
Уровни обеспечения безопасности

Безопасность среды исполнения

- Управление уязвимостями
- Соответствие стандартам
- Аутентификация и авторизация
- Мониторинг и аудит



Уровни обеспечения безопасности



Безопасность инфраструктуры

- Управление уязвимостями
- Контроль сетевых политик
- Соответствие стандартам
- Мониторинг и аудит

Обеспечение безопасности

Обеспечение безопасности

01.

Image

- Сканирование образов в CI
- Сканирование реестров образов
- Использование доверенных образов
- SBOM

Обеспечение безопасности

01.

Image

- Сканирование образов в CI
- Сканирование реестров образов
- Использование доверенных образов
- SBOM

02.

Runtime

- Мониторинг активности в контейнерах
- Поиск аномалий
- Визуализация
- Сканирование запущенных контейнеров

Обеспечение безопасности

01.

Image

- Сканирование образов в CI
- Сканирование реестров образов
- Использование доверенных образов
- SBOM

02.

Runtime

- Мониторинг активности в контейнерах
- Поиск аномалий
- Визуализация
- Сканирование запущенных контейнеров

03.

Cluster

- Защита от несанкционированных изменений
- Анализ ролевой модели
- Сетевые политики
- Контроль конфигурации запущенных ресурсов
- Соответствие стандартам

Обеспечение безопасности

01.

Image

- Сканирование образов в CI
- Сканирование реестров образов
- Использование доверенных образов
- SBOM

02.

Runtime

- Мониторинг активности в контейнерах
- Поиск аномалий
- Визуализация
- Сканирование запущенных контейнеров

03.

Cluster

- Защита от несанкционированных изменений
- Анализ ролевой модели
- Сетевые политики
- Контроль конфигурации запущенных ресурсов
- Соответствие стандартам

04.

Integration

- В процессы безопасной разработки
- В системы мониторинга и реагирования

Каким командам может быть полезно?

Бизнес

- Контроль нецелевого использования ресурсов
- Эффективное взаимодействие между командам

SOC

- Источники данных для SOC о Kubernetes и контейнерах в нем
- Помощь в расследовании инцидентов
- Обнаружение атак в реальном времени

Разработка

- Понимание целевого окружения с его структурой и политикой
- Прозрачное взаимодействие с требованиями ИБ

Security

- Все перечисленное, а также встраивание в процессы разработки
- Повышение компетенций
- Планирование обновлений и исправления безопасности

DevOps

- Осведомленность о политиках безопасности в Kubernetes
- Повышение видимости изменений и текущих нагрузок

На что ориентироваться при обеспечении безопасности

NIST 800-190 Руководство по безопасности контейнеризованных приложений

Описаны угрозы ИБ при использовании технологий контейнеризации приложений и приводятся рекомендации по способам их нейтрализации

PCI SSC Руководство по контейнерам и инструментам оркестрации контейнеров

Описаны угрозы ИБ при использовании контейнеризации и практики обеспечения безопасности с привидением примеров

CIS Benchmark for Kubernetes

Указаны конкретные рекомендации по привидению к необходимому уровню зрелости и риски, которые могут быть реализованы в случае отказа от реализации конкретной рекомендации

Приказ ФСТЭК №118 «Об утверждении требований по безопасности информации к средствам контейнеризации»

Сформированы требования к средствам контейнеризации

ОБЗОР НА НАШЕМ САЙТЕ

OWASP Kubernetes Top 10

Сформированы риски и угрозы, возникающие при использовании Kubernetes, представлены рекомендации по митигации угроз

Российский рынок

Российские продукты

Positive Technologies

Container Security

Kaspersky

Container Security

MTS RED

Clound and Container Security

Luntry

Container Security

Nova – российский продукт контейнеризации

Комплексная платформа на базе k8s

Соответствие CIS

Контроль трафика

Observability

Встроены OSS для обеспечения ИБ

Программа вебинаров

23.04 Container Security: комплексный подход к безопасности k8s. Совместно с Orion soft

14.05 Лайфхаки для защиты Kubernetes. Совместно с Лабораторией Касперского

Вебинар совместно с Luntry

Вебинар совместно с Positive Technologies

Автоматизация процессов защиты Kubernetes

- Демонстрация решений
- Атаки на Kubernetes и защита кластера
- Обнаружение атак, реагирование и блокирование действий злоумышленника
- Автоматизированное реагирование на инциденты в среде Kubernetes с использованием SOAR

ПОДПИСЫВАЙТЕСЬ НА НАШ КАНАЛ В ТЕЛЕГРАМЕ

- Практические кейсы по безопасной разработке
- Экспертные статьи о DevSecOps
- Анонсы тематических вебинаров

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

sec.ussc.ru

cybersec@ussc.ru

Евгений Тодышев

etodishev@ussc.ru +7 (950) 555-68-90 @mr.appsec