LUNTRY

БЕЗОПАСНОСТЬ KUBERNETES ЧТО ВАЖНЕЕ И С ЧЕГО НАЧАТЬ

Дмитрий Евдокимов

Founder&CTO
Luntry

Обо мне

”

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 CFP DevOpsConf и HighLoad++

Спикер

VK Kubernetes
DevOpsConf
Kazhackstan

Confidence
HackInParis
HighLoad++

ZeroNights
KuberConf
OFFZONE

БеКон
BlackHat
DevOops

HITB
PHDays
SAS

Проблемы и вызовы для ИБ в Kubernetes

1. Окружение становится все сложнее

«Complexity is the worst enemy of security, and our systems are getting more complex all the time».

Bruce Schneier

«The only thing that ever yielded real security gains was controlling complexity».

Thomas Dullien, «Halvar Flake»

2. Разработка стремительно развивается

- Старые подходы к безопасности не работают
- Департаменты разработки, поддержки и безопасности должны работать вместе

3. Kubernetes – это фреймворк

- Уникальные модели нарушителя, модель угроз и поверхность атаки

4. Атакующий по-прежнему на шаг впереди

0day, unfixed 1day, backdoors, APT и т.д.

Риски контейнеризации

01

На уровне образов

- уязвимость в компонентах образа
- небезопасная конфигурация
- наличие чувствительных данных
- вредоносное ПО и ПО двойного назначения
- отсутствие подлинности образов

02

На уровне контейнеров

- недекларированные возможности
- небезопасная конфигурация
- избыточные привилегии и возможности

03

На уровне оркестратора

- неподдерживаемые системные компоненты
- уязвимость в системных компонентах
- отсутствие изоляции сред
- отсутствие сетевой сегментации
- небезопасная конфигурация
- отсутствие контроля доступа
- избыточные привилегии сущностей

Домены безопасности Kubernetes

Контроль Kubernetes-ресурсов

Контроль состояния Kubernetes-кластеров

Контроль соответствия кластера стандартам

LUNTRY

Управление безопасностью образов

Сетевая безопасность

Анализ прав доступа

Защита Runtime

С какого домена начать?

Зависит от множества моментов:

1. Назначение кластера

Коммунальный, выделенный, служебный, ML-кластер, внутренний, внешний, в публичном облаке, …

2. Структура компании

DevOps, DevSecOps, AppSec, Platform Team, Cloud Security Team, SOC, …

3. Процессы компании

Внутренняя/внешняя разработка, внутренний/внешний SOC, ИБ создает или контролирует политики, …

4. Модель нарушителя

Внутренний, внешний, скомпрометированный разработчик/devops/…

5. Модель угроз

LUNTRY

Будут представлены
Первые 3 шага!

Шагов много.

База - инвентаризация

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

IDENTIFY (ID) — *The organization's current cybersecurity risks are understood.* Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

CIS Controls

NIST Cybersecurity Framework (CSF)

Контроль состояния Kubernetes-кластеров

01 Проверить актуальность версий

- Только поддерживаемые версии Kubernetes получают обновления, улучшения и исправления безопасности

02 Проверить наличие уязвимостей системных компонентов

- Неисправленные уязвимости системных компонент могут привести к компрометации кластера и его данных

03 Обеспечить мультитенантность

- Разграничение окружений между командами, проектами, продуктами для уменьшения радиуса нанесения ущерба

Контроль соответствия кластера стандартам

01 Проверить на соответствие CIS Kubernetes Benchmark критичных пунктов

- Закрыть самые критичные проверки

02 Проверить на соответствие CIS Kubernetes Benchmark значимых пунктов

- Последовательно закрываем менее критичные проверки

03 Проверка оставшихся пунктов стандарта

- Закрыв все, достигается минимальный уровень безопасности

Контроль Kubernetes-ресурсов

01 Проверить приложение на соответствие Pod Security Standard и контролировать образы

- Привилегированный Pod
- Только подписанные образы с внутренних image registry

02 Использовать библиотеки правил для других Kubernetes ресурсов

- Контроль Ingress, Namespaces, NetworkPolicy, subresources (pods/exec и т.д.), Role, ClusterRole, …

03 Перейти от режима аудита к режиму блокировки

- Начинаем блокировать все, что не соответствует требованиям

Анализ прав доступа

01 Проверить актуальность User, Group, SA, а также наличие полных доступов «*»

- Инвентаризация учетных записей
- Определение высокопривилегированных учетных записей

02 Проверить доступ к критичным ресурсам

- Определение учетных записей способных нанести тот или иной вред в инфраструктуре

03 Установить собственные правила

- Определение учетных записей с критичными правами с учетом специфики собственной инфраструктуры

Сетевая безопасность

01 Проверить, какие приложения или сервисы доступны извне кластера и какие обращаются за пределы кластера

- Инвентаризация сетевой доступности сервисов для уменьшений поверхности атаки и исключения утечки информации

02 Изолировать Namespaces друг от друга с помощью NetworkPolicy

- Грубая изоляция для микросервисов в разных Namespaces

03 Ограничить взаи-модействие между приложениями с помощью NetworkPolicy

- Микросегментация – реализация ZeroTrust для микросервисов

Управление безопасностью образов

01 Устранить уязви-мости с патчами с учетом приоритизации

- Закрываем с учетом: CVSS, Severity, Type(RCE/DoS), наличие Exploit, KEV, EPSS, использования в Runtime

02 Проверить dockerfile на соответствие лучшим практикам

- Безопасные инструкции
- Отсутствие эксплоитов

03 Проверить образы на наличие вредоносного ПО и ПО двойного назначения

- Известный вредоносный код
- Код двойного назначения - GTFOBins: shell, curl, wget, …

Безопасность Runtime

01 Контролировать нежелательные события

- Запуск исполняемых файлов отсутствующих в исходном образе
- Обращение по сети к системным службам (SSH 22, Nodes 30000-32767, kubelet 10250, 10255)
- Обращение к критичным директориям/файлам Linux

02 Отслеживать процессные аномалии

- Запуск исполняемых файлов, не характерных для данного микросервиса

03 Отслеживать сетевые аномалии

- Сетевая активность, не характерная для данного микросервиса

Итог

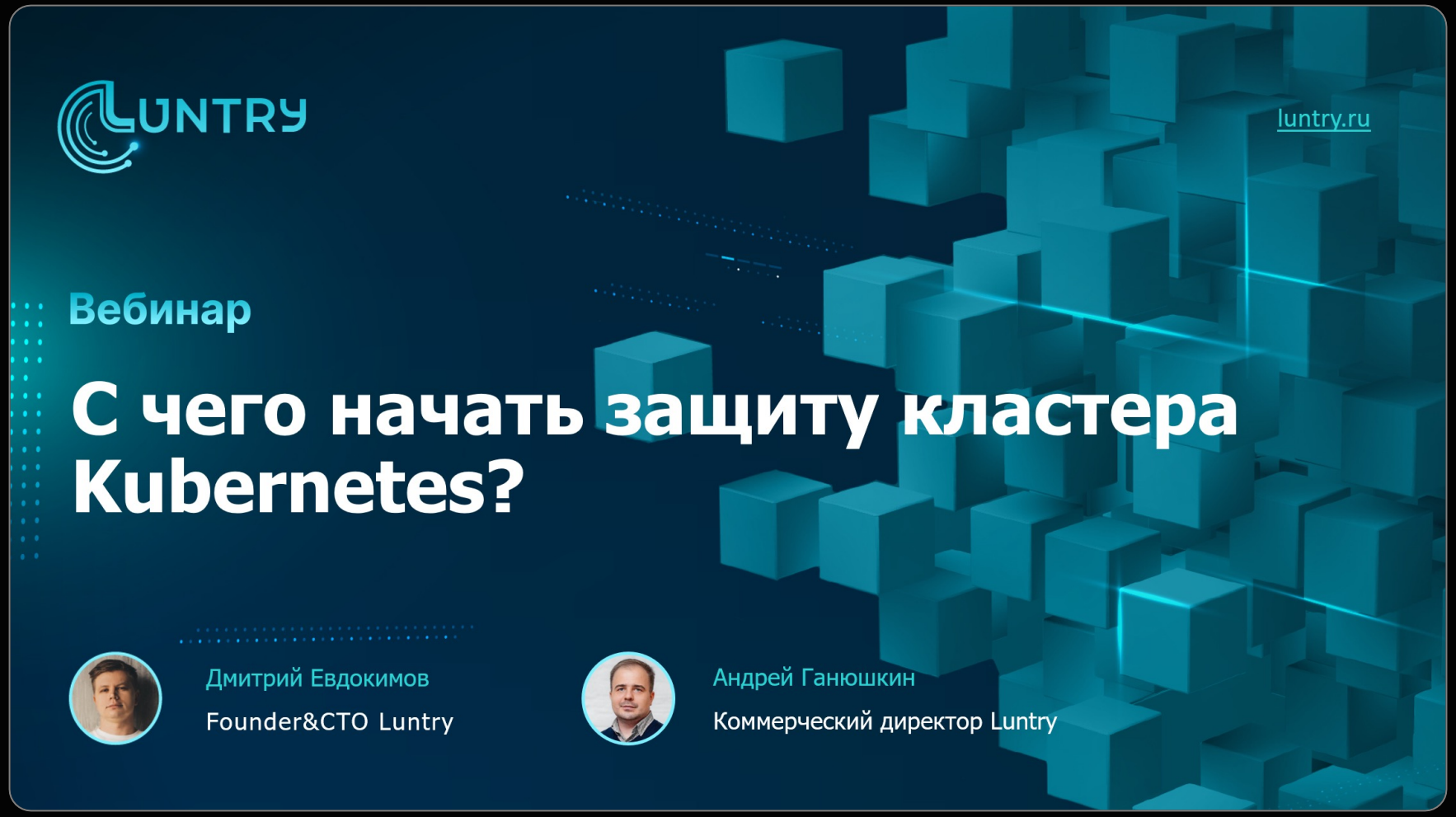
01 ПОНИМАЙТЕ СВОЕ ОКРУЖЕНИЕ – ПОЛНАЯ ИНВЕРНТАРИЗАЦИЯ

02 ИСПОЛЬЗУЙТЕ КОМПЛЕКСНЫЙ ПОДХОД

03 ПРИОРИТИЗИРУЙТЕ С УЧЕТОМ ВАШЕЙ МОДЕЛИ УГРОЗ, ПОВЕРХНОСТИ АТАКИ И МОДЕЛЕЙ НАРУШИТЕЛЯ

Более подробно

Материалы вебинара «С чего начать защиту кластера Kubernetes?»



LUNTRY

СПАСИБО ЗА ВНИМАНИЕ

ДМИТРИЙ ЕВДОКИМОВ
Founder & CTO Luntry

info@luntry.ru
@luntry_official

luntry.ru