5 июня 2024 Москва, LOFT HALL#2

БЕКОН'24

Конференция по БЕзопасности
КОНтейнеров и контейнерных сред

Подразделение для защиты k8s

Артем Мерец

Тинькофф

Дисклэймер

БЕКОН

- Говорим про отрасль в целом, есть более и менее зрелые компании
- Достигать целей и решать проблемы можно по разному, обсуждаем один из вариантов
- Релевантность к своим компаниям предлагается определить самостоятельно

План

БЕКОН

- Предпосылки (почему именно сейчас)
- Аналогии с защитой классической инфраструктуры
- Специфичные новые угрозы, от которых раньше не защищались
- Итоги и выводы

Предпоссылки

БЕКОН

Рост атак на приложения

Тренд на приложения вместо инфраструктуры

- Компании научились защищать свой периметр
- Тренд на атаки приложений

Охота за кадрами (разработчиками)

- Современные технологии - лучшие кадры

Изменения в runtime platform

- Спрост на time2market
- Это приводит к миграции на более современные технологии доставки ценностей и инфру (в т.ч. k8s)
- Традиционно слабая позиция безопасности относительно внедрения новых технологий (догоняющие)

Предпоссылки

БЕКОН

Рост атак на приложения

Тренд на приложения вместо инфраструктуры

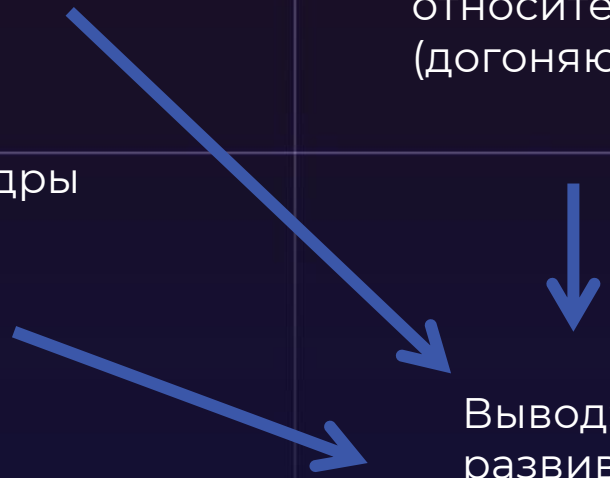
- Компании научились защищать свой периметр
- Тренд на атаки приложений

Охота за кадрами (разработчиками)

- Современные технологии - лучшие кадры

Изменения в runtime platform

- Спрост на time2market
- Это приводит к миграции на более современные технологии доставки ценностей и инфру (в т.ч. k8s)
- Традиционно слабая позиция безопасности относительно внедрения новых технологий (догоняющие)



Вывод: k8s и подобные технологии развиваются, де-факто являются стандартом, технология от «бункеров» в компаниях становится основой, безопасность защищает старую инфраструктуру

Предпоссылки

БЕКОН

Появление k8s и попытки его защитить

Сценарий 1 - «бункер»

- Внедрение - проблемы ИТ
- ИБ почти не участвуют

Сценарий 2 - AppSec

- Триггер к появлению k8s - разработка
- Значит защита k8s переходит к AppSec

Сценарий 3 - InfraSec

- Развертыванием куба занимается инфраструктурная команда
- За харденингом приходят к коллегам из инфраструктурной безопасности

Предпоссылки

БЕКОН

Появление k8s и попытки его защитить

Сценарий 1 - «бункер»

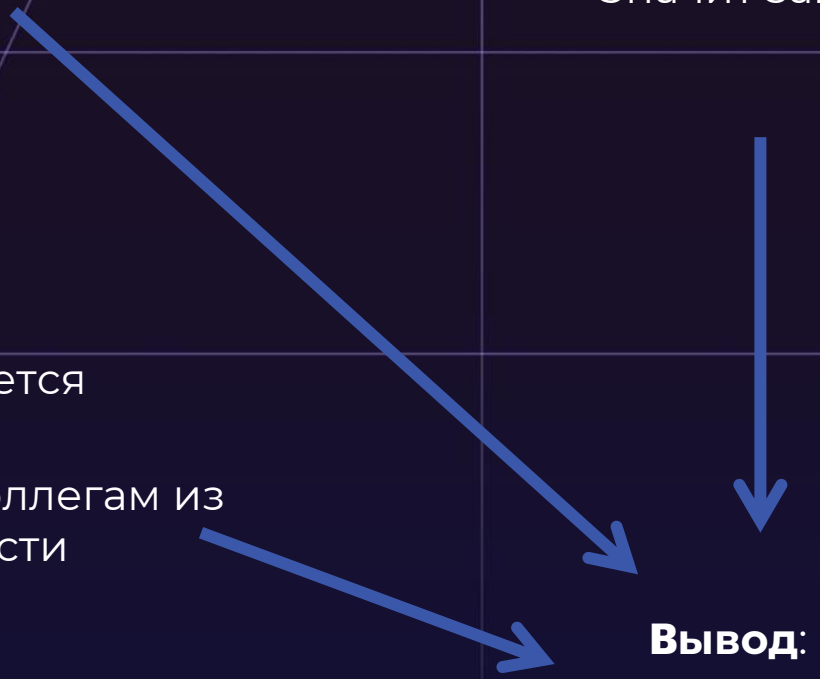
- Внедрение - проблемы ИТ
- ИБ почти не участвуют

Сценарий 2 - AppSec

- Триггер к появлению k8s - разработка
- Значит защита k8s переходит к AppSec

Сценарий 3 - InfraSec

- Развертыванием куба занимается инфраструктурная команда
- За харденингом приходят к коллегам из инфраструктурной безопасности



Вывод: на безопасность k8s не смотрят, либо смотрят как на приложение, либо смотрят как на набор хостов

Защита классической инфраструктуры (1/3)

БЕКОН

и защита k8s

Атаки на центр администрирования и конфигурирования	
Domain Controllers	kubeapi
AWX	

Атаки на привелигерованных пользователей и credentials	
Active Directory (GPO)	k8s IAM
NTDS.dit / NTLM / SAM	kubeconfig

Атаки на сеть	
Firewall / HBFW	CNI (Cilium / Calico /...)

Реагирования на инциденты	
понимание классической инфраструктуры	понимание инфраструктуры k8s

Защита классической инфраструктуры (2/3)

БЕКОН

и защита k8s

Атаки на локальные и сервисные УЗ	
Windows/Linux Accounts	k8s Service Accounts

Встраивание защиты от атак	
EDR / AV / IDS / …	Admission Controller
	DaemonSet
	CronJob
	Sidecar

Сбор событий и телеметрия	
eventlog windows	kube audit
auditd	node exporter

Атаки на хранение конфигурации и секреты	
vault/CMDB	vault/etcd
	secrets

Защита классической инфраструктуры (3/3)

БЕКОН

и защита k8s

Атаки на отказ в обслуживании	
nginx/ ha-proxy	ingress
	scheduler
	kubeapi
	affinity

Методы закрепления	
user autorun dir	cronjob
.bashrc	daemonset
daemon	sidecar
...	...

Итоги сравнения с классической инфрой

БЕКОН

1. Растягивать классические контроли на инфраструктуру k8s - недостаточно
2. Нужно строить новый слой контролей, решающих те же самые проблемы, но уже в k8s
3. K8s - это отдельная инфраструктура (технологический стек, процессы, пр), а не просто точка деплоя приложений

Дополнительные угрозы

БЕКОН

1. Управление секретами. Децентрализованный набор секретов в классической схеме и единый рантайм, внутри которого доступны все секреты компании в случае с k8s
2. Управление доступами и протоколами конфигурирования. Разделение SSH/RDP/WMI протоколов от прикладных в одном случае и единый HTTP интерфейс в другом
3. Управление сетью. Отдельное железо и нотация конфигурирования сменяется на SDN и описание в коде.
4. Организация мультитенантности. Раньше вопрос решался отделением командных серверов в сетевых сегментах, теперь чаще решается набором иных мер (RBAC + CNI) внутри единого кластера.
5. Стандарты конфигурирования. Хорошо известные и обкатанные CIS бенчмарки в противовес новым стандартам по инфраструктуре, которая внутри ИБ незнакома. «Безопасное конфигурирование» хостов в кластере вообще не гарантирует практически ничего в k8s
6. Широкие возможности кастомизации. Например, admission controller’ы, где один дополнительный компонент может кардинально поменять уровень защищенности кластера (как в лучшую, так и вхудшу/ сторону)

- https://microsoft.github.io/Threat-Matrix-for-Kubernetes/
- https://kubernetes-threat-matrix.redguard.ch
- https://attack.mitre.org/matrices/enterprise/containers/

Вы контролируете защищенность?

БЕКОН

Вопросы-маркеры

1. Можно ли получить сетевой доступ от pod до node?
2. У вас в production окружении версии k8s без критичных уязвимостей?
3. Как выглядит процесс обновления версий k8s?
4. При обновлении k8s обновляется ли операционная система?
5. Как вы контролируете root в контейнерах?
6. Как выглядит процедура проверки для подключения новых Admission Controllers?
7. Какой identity providers используется для доступа к кластеру?
8. Как хранятся секреты в runtime?
9. Кто и при каких условиях имеет техничскую возможность зайти на node'ы от Control Plane?
10. Где хранится перечень Mutating Admission Controllers от вашего k8s?
11. **Уверены ли вы на 90% в полученных ответах?**

Резюме

БЕКОН

1. **Технология популярная**
   - на рынке де-факто стандарт, в атаках набирает тренд
2. **Привносит новые угрозы**
   - инновационные подходы, о которых надо знать и контролировать
3. **Представляет собой целую альтернативную инфраструктуру**
   - может быть неплохо интегрирована в классическую
   - а может ее расширять или заменять в зависимости от реализации
4. **Неизбежно меняет модель угроз**
5. **Требует защиты**
   - поддерживаем целые подразделения для закрытия этих угроз в одном виде инфраструктуры
   - почти игнорируем все эти же угрозы в другом виде инфраструктуры (более популярном)

Linkedin: artem-merets

Tg: @infobez

Company: Tinkoff