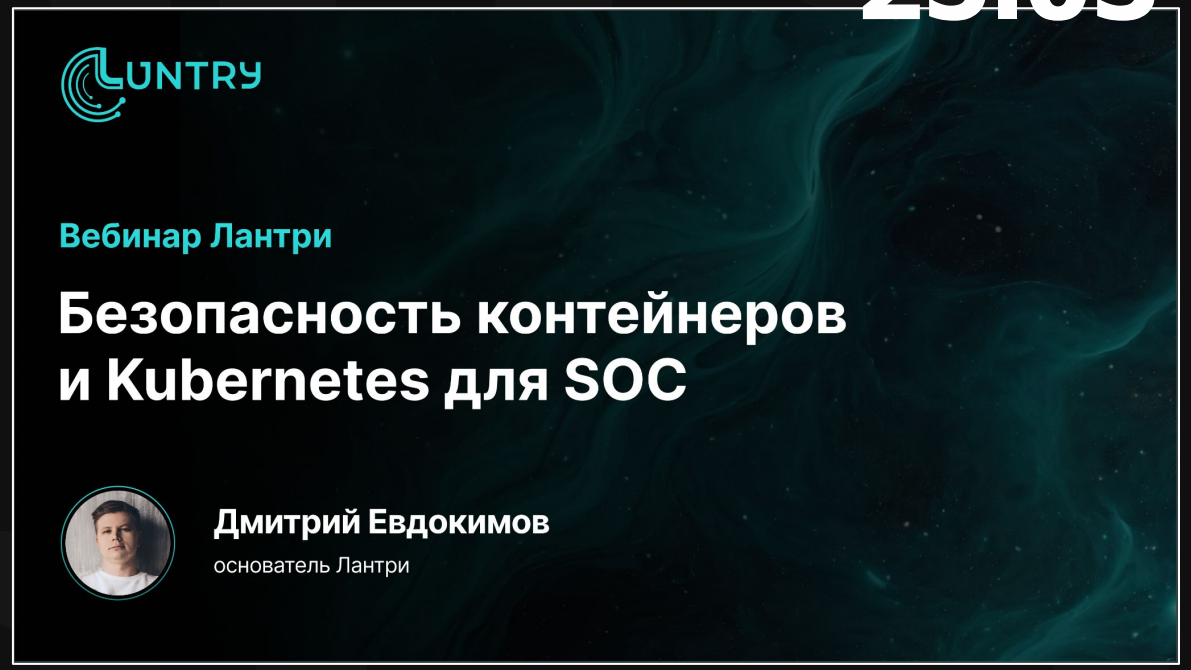
АНОНСЫ

25.03



03.06

LUNTRY

luntry.ru

Вебинар

Безопасность контейнеров и Kubernetes для CISO

Дмитрий Евдокимов

Founder & CTO Luntry

План вебинара

- Контейнеры и Kubernetes
- Зачем заниматься безопасностью?
- Безопасность через призму фреймворка PPT
  Люди (People)
  Процессы (Process)
  Технологии (Technology)

В рамках вебинара ответим на вопросы

- Что такое контейнеры и Kubernetes?
- Как и почему контейнеризация завоевывает инфраструктуры?
- Почему необходимо защищать контейнеры и Kubernetes?
- А реальные инциденты есть?
- Когда начинать заниматься безопасностью?
- Как смотреть на защиту контейнерных сред?
- Как совместно с ИТ это все использовать на благо, а не во вред?
- Почему защита Kubernetes это не то же самое,
  что защита Windows/Linux/Mac сред?
- Что приоритетнее SAST/DAST или Container security?
- Какие подводные камни есть при защите контейнерных сред?
- Где искать специалистов?
- …

whoami

- Основатель и технический директор Luntry
- Опыт в ИБ более 15 лет
- Специализация безопасность контейнеров и Kubernetes
- Программный комитет DevOpsConf, HighLoad++
- Бывший автор статей и редактор рубрик в журнале “ХАКЕР”
- Автор Telegram-канала «k8s (in)security»
- Автор курса “Cloud Native безопасность в Kubernetes”
- Не верит, что систему можно сделать надежной и безопасной, не понимая ее
- Организатор конференции по безопасности контейнеров - БеКон
- Докладчик: BlackHat, HITB, ZeroNights, HackInParis, Confidence, SAS, OFFZONE, PHDays, Kazhackstan, DevOpsConf, DevOops, KuberConf, VK Kubernetes Conference, HighLoad++, БЕКОН и др.

LUNTRY
luntry.ru

LUNTRY

luntry.ru

- Luntry – это Комплексная Защита на всем жизненном цикле контейнерных приложений и средств оркестрации на базе Kubernetes

- Продукт в реестре Минцифры
  https://reestr.digital.gov.ru/reestr/1057835/

- В процессе получения сертификата ФСТЭК

  Ориентировочно 1-2 квартал 2025

Функциональность Luntry

Введение

Специфика

Новые абстракции

- Образы, k8s ресурсы (YAML), неймспейсы, ноды, …

Разработка стремительно развивается

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

Каждый контейнер/микросервис это маленький уникальный мир

- Свое окружение и поведение
- Малый срок жизни (эфемерность)
- Очень динамичная среда
- Высокие нагрузки

Kubernetes – это фреймворк

- Build, коммунальные, ML кластера, Dev окружения, Internet faced, …
- Уникальные модели нарушителя, модель угроз и поверхность атаки

Контейнеризация это добро или зло для ИБ?

Смотря как подойти к их безопасности =)

1. Можно не учитывать специфику

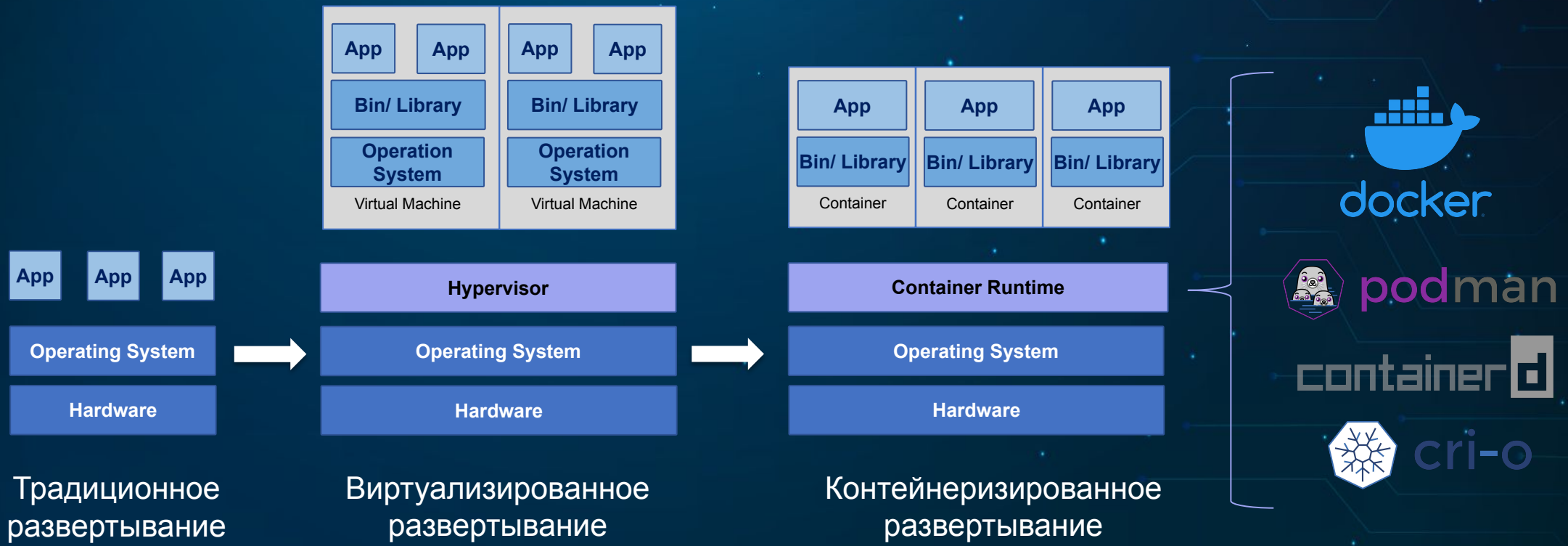
   Продолжать тушить пожары, в еще большем количестве

2. Можно использовать специфику

   Закрывать аспекты, которые сложно или невозможно закрыть в классической инфраструктуре

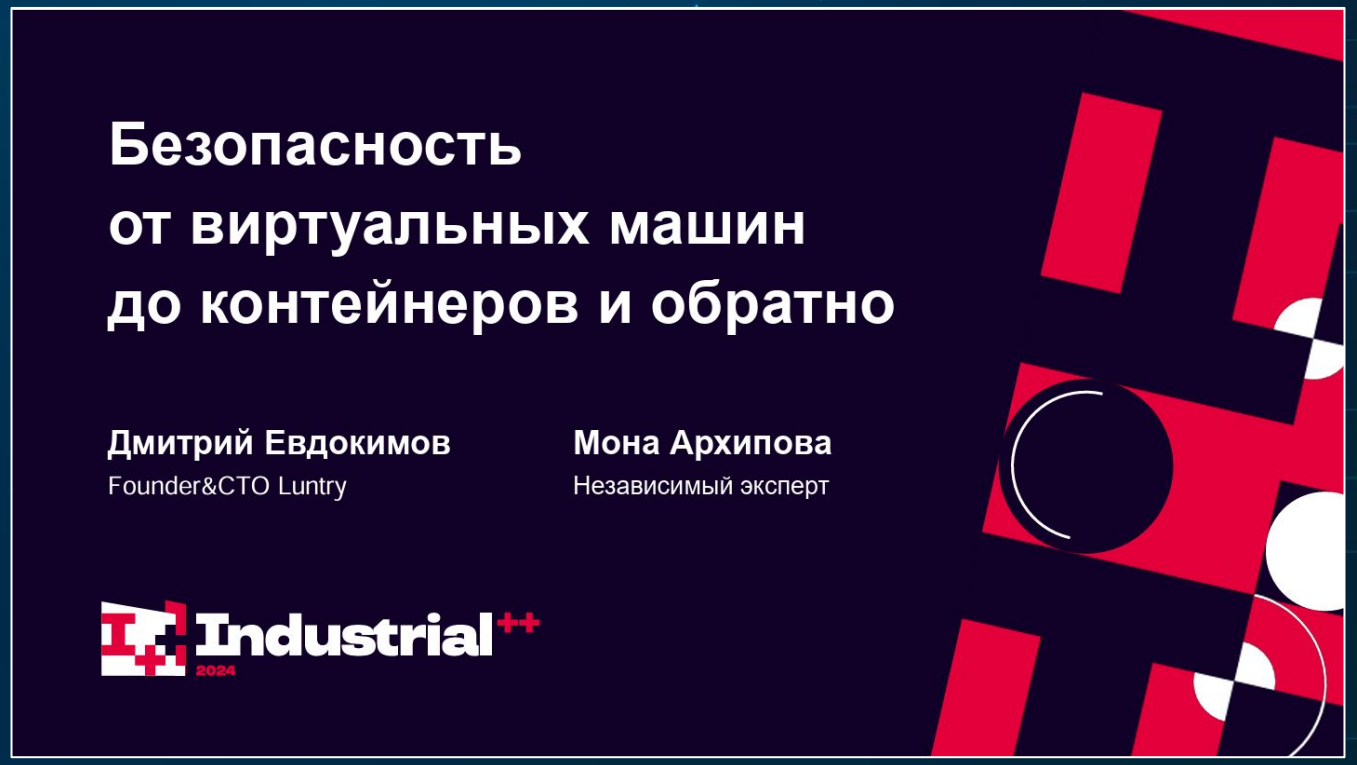
Контейниризация и оркестрация

Эволюция к контейнерам



Безопасность виртуальных сред и контейнерных сред

Для тех, кому проще и понятнее тема виртуализации
и кто хочет зайти в тему безопасности контейнеров на ассоциациях



Что такое контейнер? Он безопасен?

Container – это Linux process с определёнными свойствами/ограничениями

Что можно увидеть: namespaces (pid, user, uts, ipc, net, mnt), pivot_root (+ image)

Что можно делать: Capabilities, seccomp, LSMs

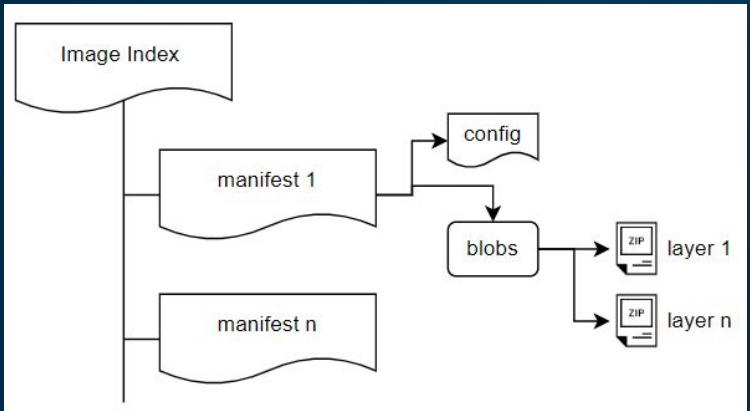
Что можно использовать: Control group (процессор, память, устройства, …

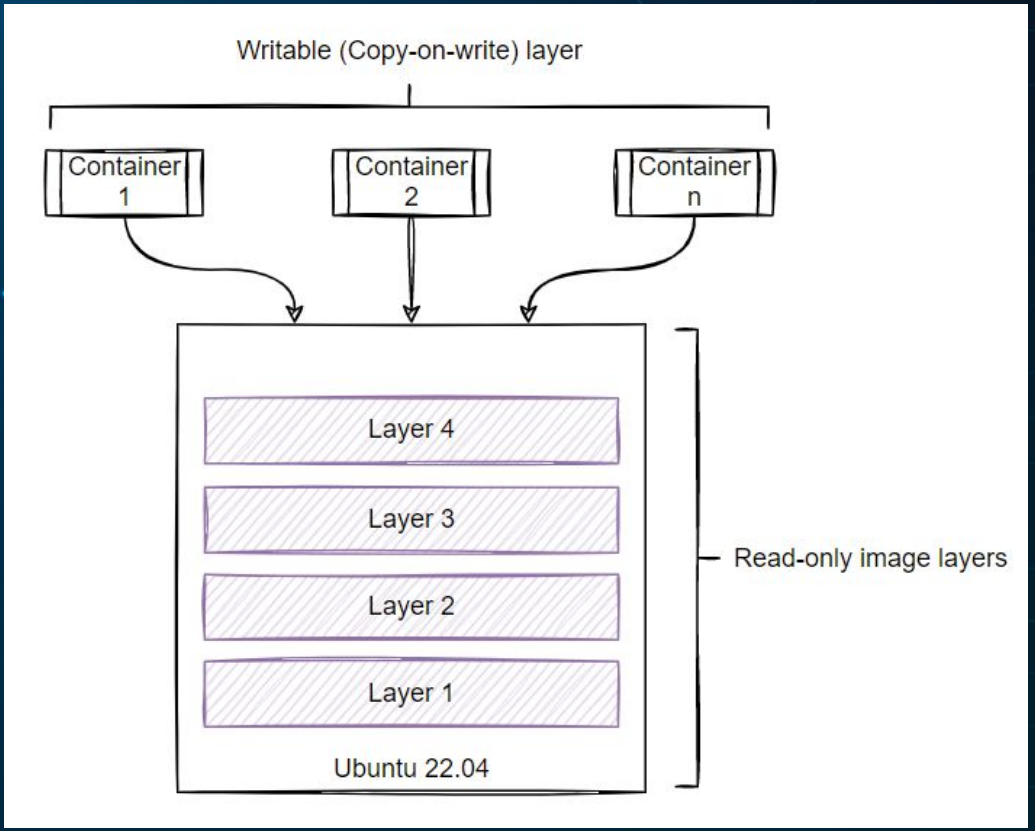
```
root     2966156  0.0  0.0 110128  5932 ?        Sl   Nov19   0:11  \_ containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1
root     2966174  0.0  0.0   1020     4 ?        Ss   Nov19   0:00  |   \_ /pause
root     2966375  0.0  0.0 108720  6356 ?        Sl   Nov19   0:11  \_ containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1
sadm     2966394  0.0  0.0 827512 19728 ?        Ssl  Nov19   0:00  |   \_ node /usr/bin/nodemon /src/index.js
sadm     2966421  0.0  0.0   4460    80 ?        S    Nov19   0:00  |       \_ sh -c node /src/index.js
sadm     2966422  0.0  0.0 967396 16596 ?        Sl   Nov19   0:00  |           \_ node /src/index.js
root     2988902  0.0  0.0 108720  5408 ?        Sl   Nov19   0:11  \_ containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1
root     2988922  0.0  0.0   1020     4 ?        Ss   Nov19   0:00  |   \_ /pause
root     2989066  0.0  0.0 108720  5408 ?        Sl   Nov19   0:26  \_ containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1
root     2989099  0.0  0.0  31000 23956 ?        Ss   Nov19   0:42  |   \_ /usr/local/bin/python /usr/local/bin/gunicorn -b :8080 --workers 1 --threads 1 --
root     2989116  0.3  0.1 142092 48964 ?        Sl   Nov19  16:50  |       \_ /usr/local/bin/python /usr/local/bin/gunicorn -b :8080 --workers 1 --threads
root     2989333  0.0  0.0 110128  5404 ?        Sl   Nov19   0:11  \_ containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1
root     2989352  0.0  0.0   1020     4 ?        Ss   Nov19   0:00  |   \_ /pause
root      596808  0.0  0.0 110128  6316 ?        Sl   Nov20   0:06  \_ containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1
root      596827  0.0  0.0   1020     4 ?        Ss   Nov20   0:00  |   \_ /pause
root      598309  0.0  0.0 110128  6224 ?        Sl   Nov20   0:07  \_ containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1
root      598334  1.4  5.5 7236340 1832196 pts/0 Ssl+ Nov20  39:39      \_ /docker-java-home/bin/java -Djava.util.logging.config.file=/opt/atlassian/conflue
root      599854  1.0  1.3 7007820 427956 pts/0  Sl+  Nov20  28:11      |   \_ /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java -classpath /opt/atlassian/conf
root      701694  0.0  0.0   4288   764 ?        Ss+  Nov20   0:00      \_ /bin/sh
```

Что такое образ?

Container Image это неизменяемый пакет файлов операционной системы, кода приложения и любых зависимостей приложения

- Union File System
  - OverlayFS как реализация
- OCI image спецификация





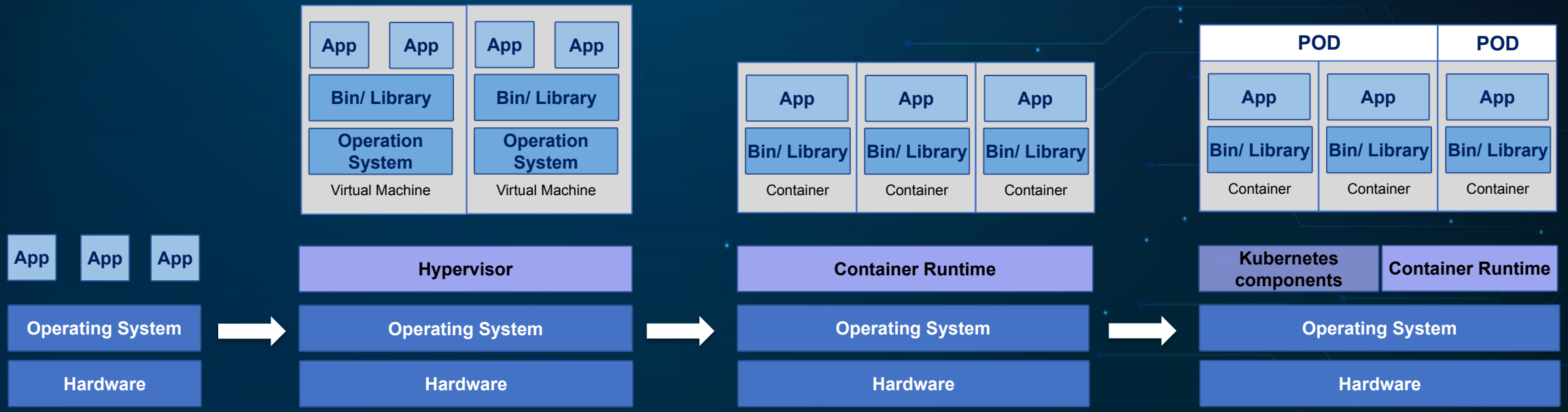
Эволюция от контейнеров к оркестраторам контейнеров

Оркестраторы:

kubernetes

HashiCorp Nomad

docker SWARM



Традиционное развертывание

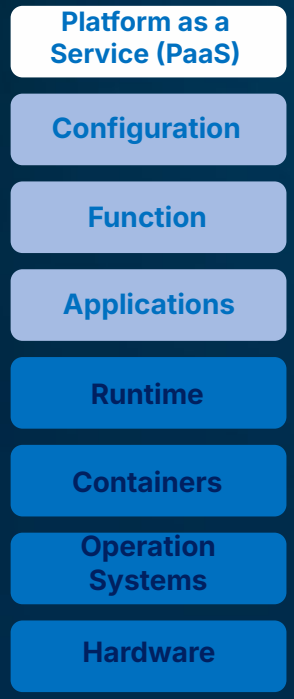
Виртуализированное развертывание

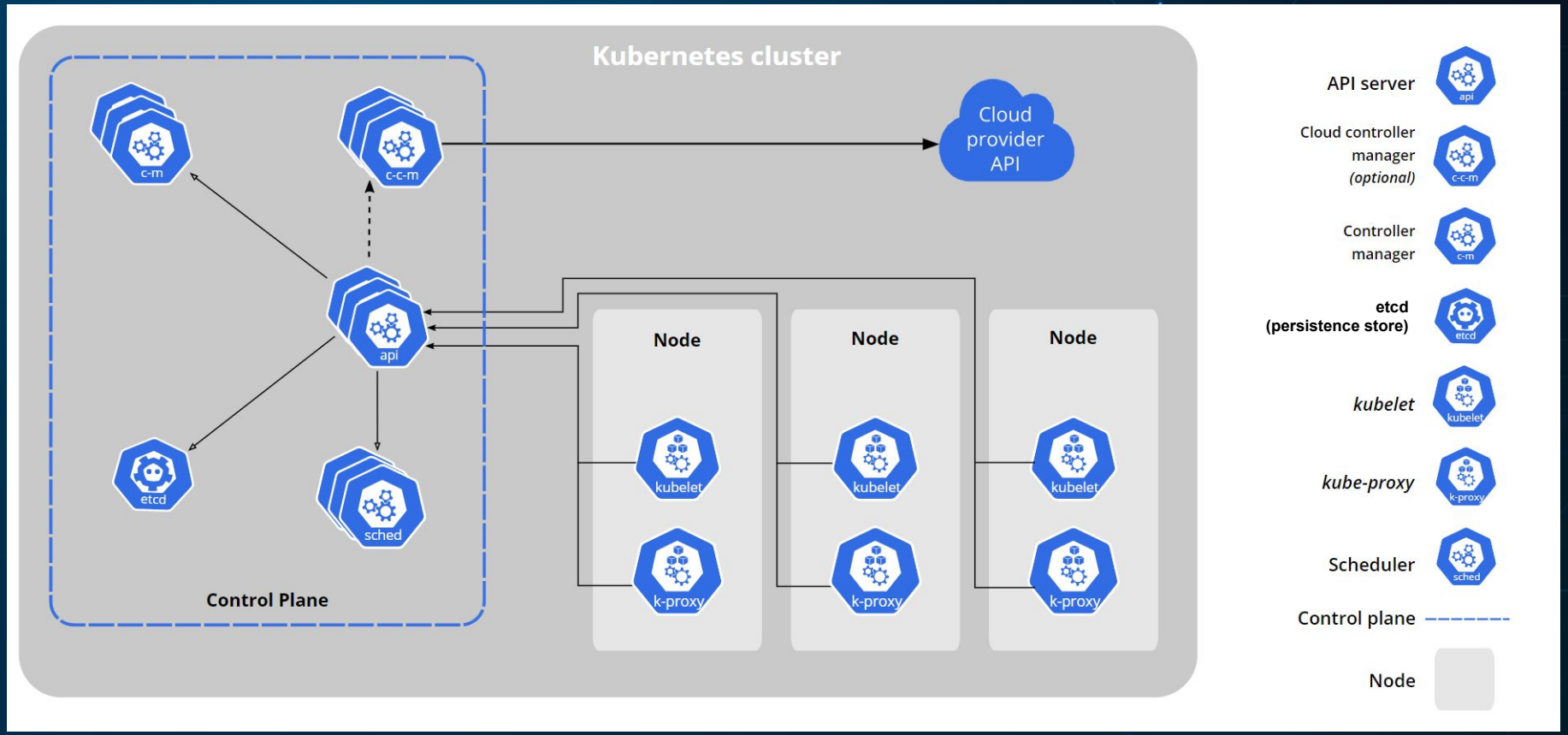
Контейнеризированное развертывание

Kubernetes развертывание

Что такое Kubernetes? Он безопасен?

- Kubernetes (K8s) — это открытое программное обеспечение для автоматизации развёртывания, масштабирования и управления контейнеризированными приложениями.
- 5 бинарей





Дистрибутивы Kubernetes

- Это фреймворк
  - OnPrem и Managed Kubernetes
  - Это ядро Linux 21 века
  - На базе Kubernetes делают свои дистрибутив

Развитие контейнерных сред

- «State of Kubernetes 2024»
- «2024 State of Production Kubernetes report»
- «Kubernetes Market Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030)»

> **Over 60% of enterprises** have adopted Kubernetes, and this number is projected to surge past **90% by 2027** [Kubernetes Market Trends].
>
> The global Kubernetes market is poised to reach a staggering **USD 10.7 billion by 2031**, highlighting its immense commercial significance [Kubernetes Adoption Statistics].

> For those that use it, Kubernetes has become a central pillar of IT, and it's not going away any time soon. 75% of users are strategically committed to Kubernetes, and 73% believe it'll still be around a decade from now.

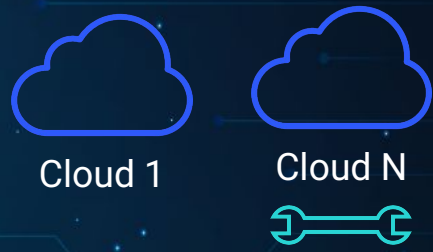
Постоянные, сложные и быстрые изменения

Разработчики

DEV-кластеры

Системные аналитики

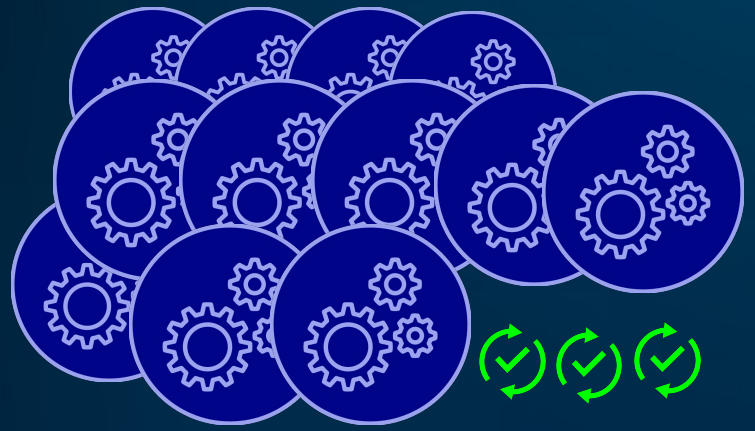
STAGE-кластеры



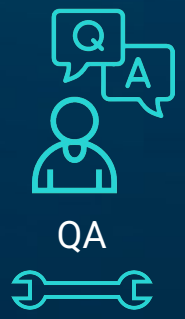
Cloud 1 Cloud N

Администраторы

Мониторинг



Собственные микросервисы



QA

Инфраструктурные микросервисы

Безопасность

Системные микросервисы

SRE

TEST-кластеры

PROD-кластеры

SOC

Зачем заниматься безопасностью?

Инциденты с/в контейнерах и Kubernetes ?

Публичных историй с привязкой к Kubernetes мало

- В основном указывается, что связано с контейнером. Сам K8s это окружение
- Никто не делится деталями – только кулуары
- Сборник Cloud Threat Landscape

В основном публичные истории касаются облачных провайдеров

- Исследования компаний по безопасности, bug bounty
- Наш опыт пентестов показывает успешность в компрометации кластеров в 90% случаях
- С 2021 года: финтех, банки, маркетплейсы, нефтегаз

Модели нарушителя

Внешний атакующий

→ Даже не подозревает, что за сервисом стоит контейнер с K8s

Внутренний атакующий

→ Находится в одной подсети с машинами кластера

Скомпрометированный разработчик

→ Влияет на содержимое образов

Скомпрометированная цепочка поставки

→ Вредоносные зависимости

Привилегированный пользователь кластера

→ Администраторы, DevOps, …

Матрица угроз для Kubernetes от Microsoft *

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access Kubernetes API server	Access cloud resources	Images from a private registry	Data destruction
Compromised image In registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Collecting data from pod	Resource hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Container service account	Network mapping	Cluster internal networking		Denial of service
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from proxy server	Application credentials in configuration files	Exposed sensitive interfaces	Application credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container	Container service account			Access managed identity credentials	Instance Metadata API	Writable hostPath mount		
	Sidecar injection	Static pods			Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

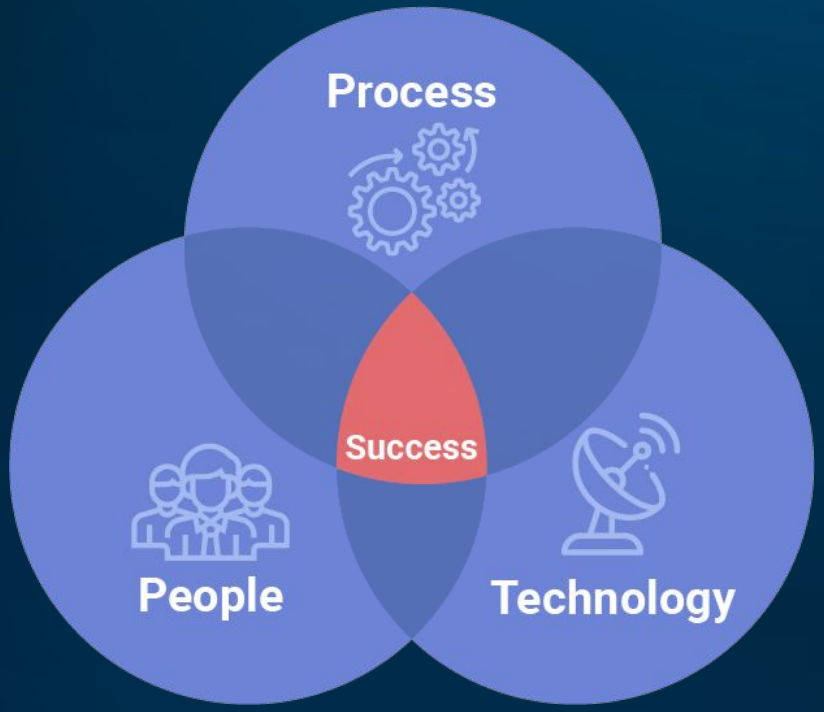
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/

* она неполная и постоянно расширяется

Картину ухудшают

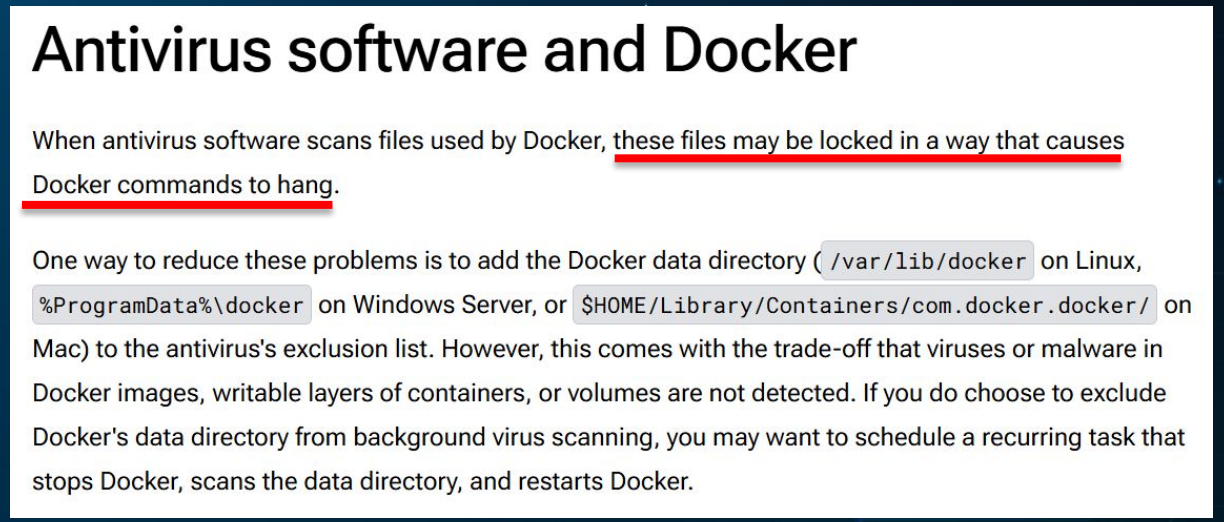
- Нехватка ИБ кадров
- Неквалифицированные кадры
- Текучка кадров
- Сторонняя разработка
- Сроки
- Процессная волокита
- Регламенты
- Сертификаты
- ...

PPT: Технологии



К чему все привыкли?

- Firewall
- IPS/IDS
- WAF
- SIEM
- DLP
- Key Management
- IAM
- PAM
- SoD
- Patch Management
- Deception Platform
- Vulnerability Assessment
- Antivirus
- FIM
- DCAP
- EDR
- SOAR
- NGFW
- …



Antivirus software and Docker

When antivirus software scans files used by Docker, these files may be locked in a way that causes Docker commands to hang.

One way to reduce these problems is to add the Docker data directory (`/var/lib/docker` on Linux, `%ProgramData%\docker` on Windows Server, or `$HOME/Library/Containers/com.docker.docker/` on Mac) to the antivirus's exclusion list. However, this comes with the trade-off that viruses or malware in Docker images, writable layers of containers, or volumes are not detected. If you do choose to exclude Docker's data directory from background virus scanning, you may want to schedule a recurring task that stops Docker, scans the data directory, and restarts Docker.

1. Половину можно смело выкинуть
2. И добавить специализированных механизмов, контролей и решений

Эшелонированная оборона

Threat modeling

Code	Images	k8s resources	Authentication Webhook	Authorization Webhook	Admission controllers	Audit Log	Container/Sandbox/VM	Observability
SAST	Distroless images	Labels, annotations	PAM	RBAC	LimitRanger	Audit Policy	NetworkPolicy	Asset management
DAST	Rootless containers	IaC	IAM		ResourceQuota		SecutityContext	Security monitoring
SCA	SBOM	Security as Code			Validating/MutatingAdmissionWebhook		Segregation of duties (Secrets, ServiceAccounts token)	Application monitoring
…	Security scan	Compliance as Code			KubeletInUserNamespace			Anomaly detection
	Secret scan	Configuration check			UserNamespacesSupport			Event resource
	Sign				PolicyEngines/PSA/PSP/ValidatingAdmissionPolicy			
	Registry staging				Kubernetes operators			

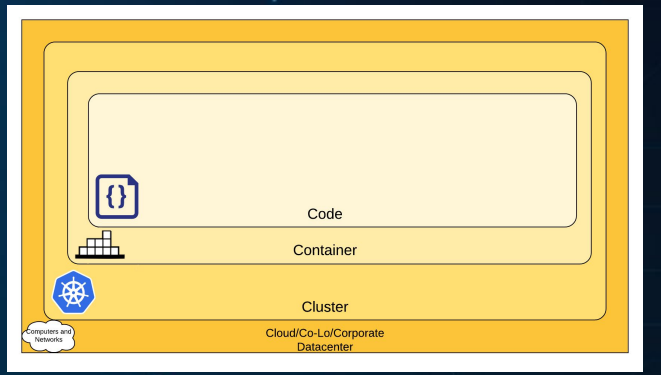
+ Multi-tenancy

Как подходить к безопасности?

- Develop
- Distribute
- Deploy
- Runtime

"CNCF Cloud Native Security Whitepaper"

- Cloud/Co-Lo/ Corporate Datacenter
- Cluster
- Container
- Code

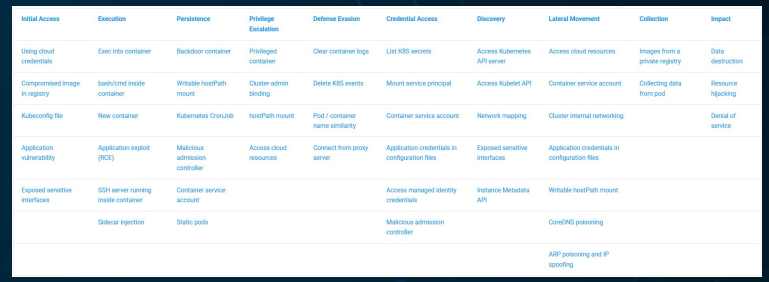


"The 4C's of Cloud Native security"

- Identify
- Protect
- Detect
- Respond
- Recover
- Deception*

"NIST CYBERSECURITY FRAMEWORK"

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Impact



"Threat Matrix for Kubernetes"

Стандарты безопасности для контейнерных сред

- CIS Kubernetes Benchmark
  https://www.cisecurity.org/benchmark/kubernetes/
- NSA/CISA Kubernetes Hardening Guide
  https://www.cisa.gov/news-events/alerts/2022/03/15/updated-kubernetes-hardening-guide
- Kubernetes Security Technical Implementation Guide (STIG)
  https://ncp.nist.gov/checklist/996
- PCI Security Standards Council: Guidance for Containers and Container Orchestration Tools

https://blog.pcisecuritystandards.org/new-information-supplement-guidance-for-containers-and-container-orchestration-tools

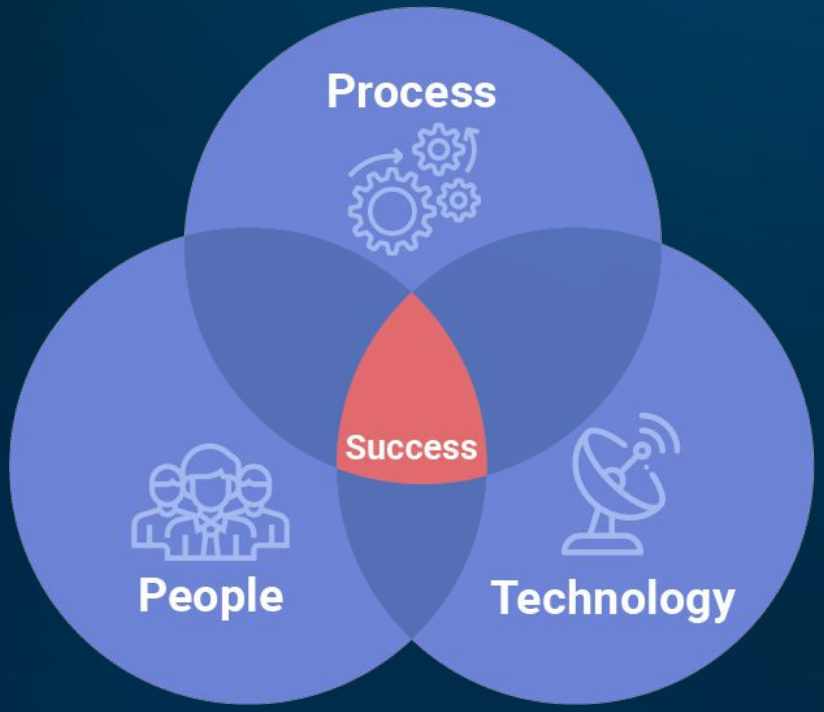
- NIST Special Publication 800-190 "Application Container Security Guide"
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf
- Приказ ФСТЭК России №118. Требования по безопасности информации к средствам контейнеризации
  https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-4-iyulya-2022-g-n-118
- ...

Что приоритетнее из решений?

SAST? DAST? IAST? Container security?

Серебряной пули нет

PPT: Процессы



Анализ рисков Kubernetes кластеров

Risk8s Business

https://tldrsec.com/p/guides-kubernetes

On this page: A zero-to-hero guide for assessing the security risk of your Kubernetes cluster and hardening it.

Table of Content

DevSecOps эра

За безопасность отвечают все департаменты, участвующие в жизненном цикле приложения и инфраструктуры

- Dev
- Ops
- Sec

Как стартовать?

0. Инвентаризация

1. Все остальное

Когда нужно начинать заниматься безопасностью?

1. Чем раньше, тем лучше (проектирования)
   - Можно продумать Secure-by-Design
   - Можно подготовить команды и процессы
2. На стадии выбора платформы
3. До начала заезда продуктовых микросервисов

Проактивный и реактивный подход к безопасности

Культура киберустойчивости (Cyber-resilient culture): «При построении культуры киберустойчивости роль безопасности заключается не в том, чтобы остановить все инциденты. Она заключается в том, чтобы не допустить влияния инцидента безопасности на бизнес».

Уязвимости != Уязвимый

Какой маркетинг вам ближе ?

- DevSecOps, SecDevOps, DevOpsSec, SecDevSecOpsSec, ...
- Shift Left Security
- Shift Right Security
- Shift Everywhere Security

blog.sqreen.com › secdevops ▾ Перевести эту страницу

What is SecDevOps and why should you care? - Sqreen Blog

19 июл. 2017 г. — What is **SecDevOps**? **SecDevOps** (also known as DevSecOps and DevOpsSec) is the process of integrating secure development best practices ...

www.altexsoft.com › blog › w... ▾ Перевести эту страницу

What is SecDevOps and Why is It So Important? | AltexSoft

right into the development

resources.whitesourcesoftware.com › ... ▾ Перевести эту страницу

DevSecOps VS SecDevOps: What Are The Differences?

21 мая 2020 г. — **SecDevOps** Puts Security First, Literally. For those wh difference between DevSecOps and **SecDevOps**, it is about putting ...

www.capgemini.com › secdev... ▾ Перевести эту страницу

SecDevOps: Cybersecurity Innovation - Capgemini

11 нояб. 2019 г. — I'm delighted today to be joined by Capgemini cybersecurity expert Luis Delabarre. This topic is known as **SecDevOps**. It's the process of ...

www.acunetix.com › blog › d... ▾ Перевести эту страницу

DevSecOps vs. SecDevOps | Acunetix

24 сент. 2019 г. — It is an extension of DevOps (Development + Operati security. The order of component terms in the DevSecOps name, howeve

blog.newrelic.com › technology ▾ Перевести эту страницу

SecDevOps: Injecting Security Into DevOps Processes

16 июл. 2018 г. — Think of **SecDevOps**—practitioners are sometimes called "Security DevOps Engineers"—as a set of best practices designed to help organizations ...

www.csoonline.com › article ▾ Перевести эту страницу

DevOpsSec, SecDevOps, DevSecOps: What's in a Name ...

18 окт. 2016 г. — The world is awash in DevOps, but what does that really mean? Although DevOps can mean several things to different individuals and ...

blog.ariacybersecurity.com › ... ▾ Перевести эту страницу

DevSecOps vs. SecDevOps vs. DevOpsSec: Is there really a ...

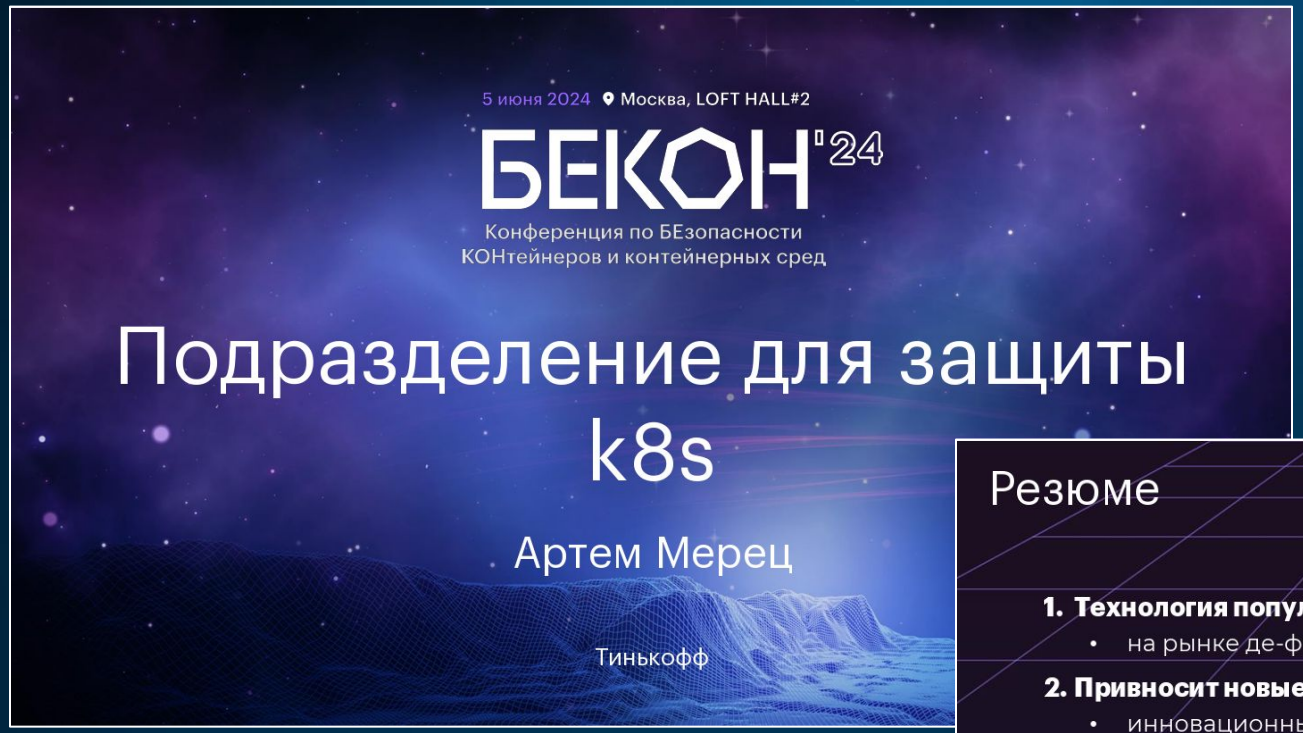
14 июн. 2018 г. — **SecDevOps**: To borrow from "Goldilocks and the Three Bears," this approach is just right! According to this insightful article on CSO.com, ...

"Shift Left" is becoming "Shift Everywhere."

- Although shift left has been promoted as doing some security testing during development, that is a large simplification of what we meant. More accurately today, some secure software development lifecycles (SSDLs) seek to conduct an activity as quickly as possible with the highest fidelity as soon as the artifacts on which that activity depend are made available. Sometimes, that's to the left of where you're doing things today, but often times, it's to the right. In addition, technology trends naturally require shifting right to produce rapid and accurate telemetry from modern languages, frameworks, and software orchestration.

PPT: Люди

Обоснование команды



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)

Конференция по БЕзопасности КОНтейнеров и контейнерных сред 14

Кадры

- Хороших специалистов по ИБ мало
- Специалистов по ИБ контейнерных сред еще меньше
- Стоимость высокая
- Опыт показывает, что проще делать специалиста по безопасности контейнерных сред из DevOps, чем из классического специалиста безопасности
- Главное не количество, а качество

Подготовка кадров

- Наш 3-дневный тренинг «Cloud Native безопасность в Kubernetes»
- Лаборатория квест по обеспечению безопасности в Kubernetes вместе с Luntry от наших партнеров
- Кураторство и помощь в научно-исследовательской деятельности от Luntry
  - https://luntry.ru/initiatives/curation
- База знаний по контейнерной безопасности от Luntry на русском языке
  - https://luntry.ru/research
- Конференция БЕКОН от команды Luntry
  - https://bekon.luntry.ru/

Если все учесть

- People: Совместная работа всех департаментов
- Process: Обеспечение безопасности в рамках всего жизненного цикла приложений и инфраструктуры
- Technology: Высокий уровень безопасности без вреда для скорости доставки нового value

Итог

1. Обеспечение безопасности контейнеров и оркестратора неминуемый новый вызов для ИБ
2. Новые технологии это не только новые вызовы, но и новые возможности
3. Старые подходы не работают
4. Стройте безопасность, понимая свое окружение

Спасибо
за внимание!

Дмитрий Евдокимов
Founder&CTO


Email: de@luntry.ru


Twitter: @evdokimovds

@Qu3b3c


Channel: @k8security


Site: www.luntry.ru

k8security luntrysolution