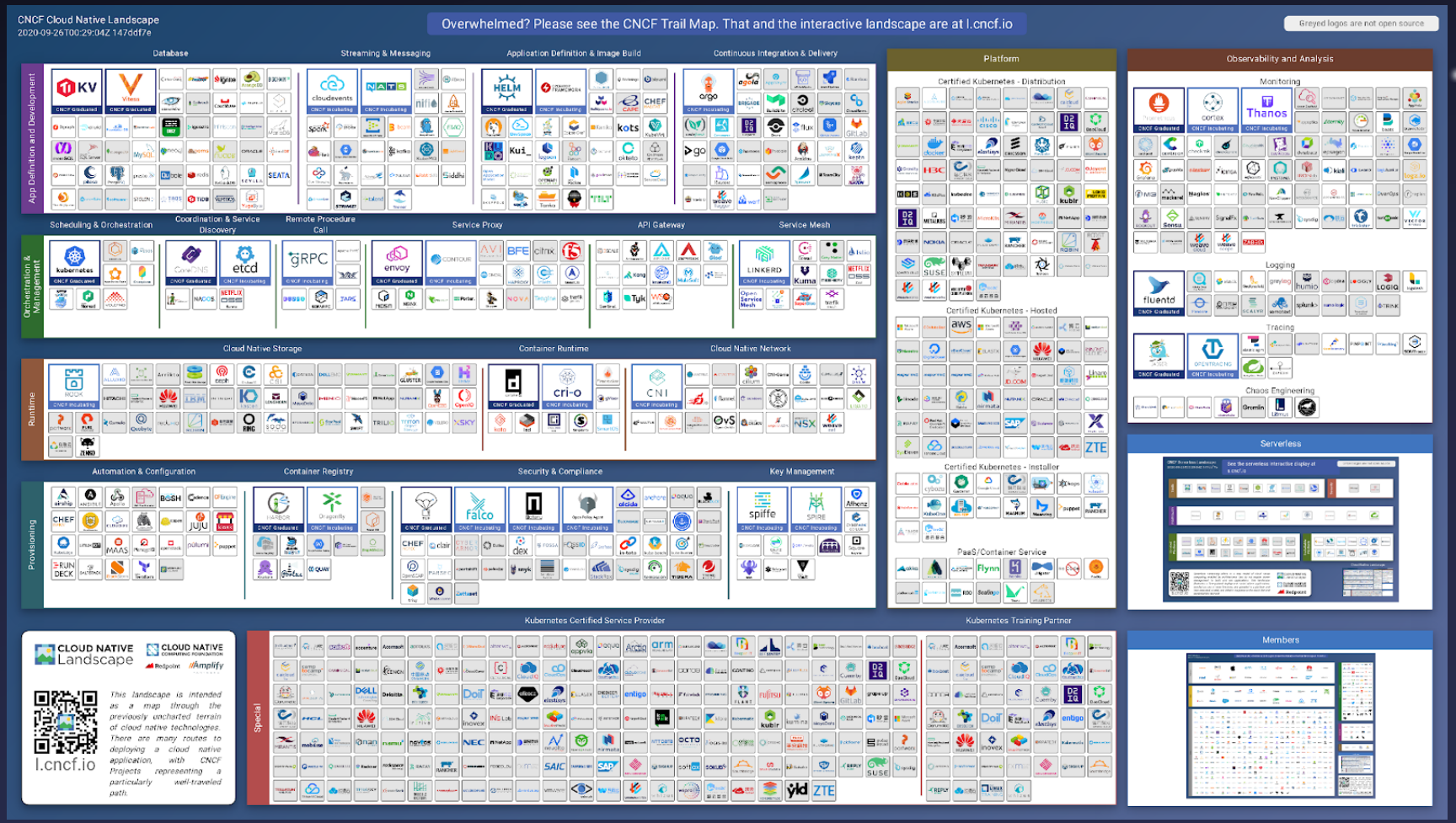
Kubernetes:
Незнание своей системы — злейший враг

Дмитрий Евдокимов,
Технический директор Luntry

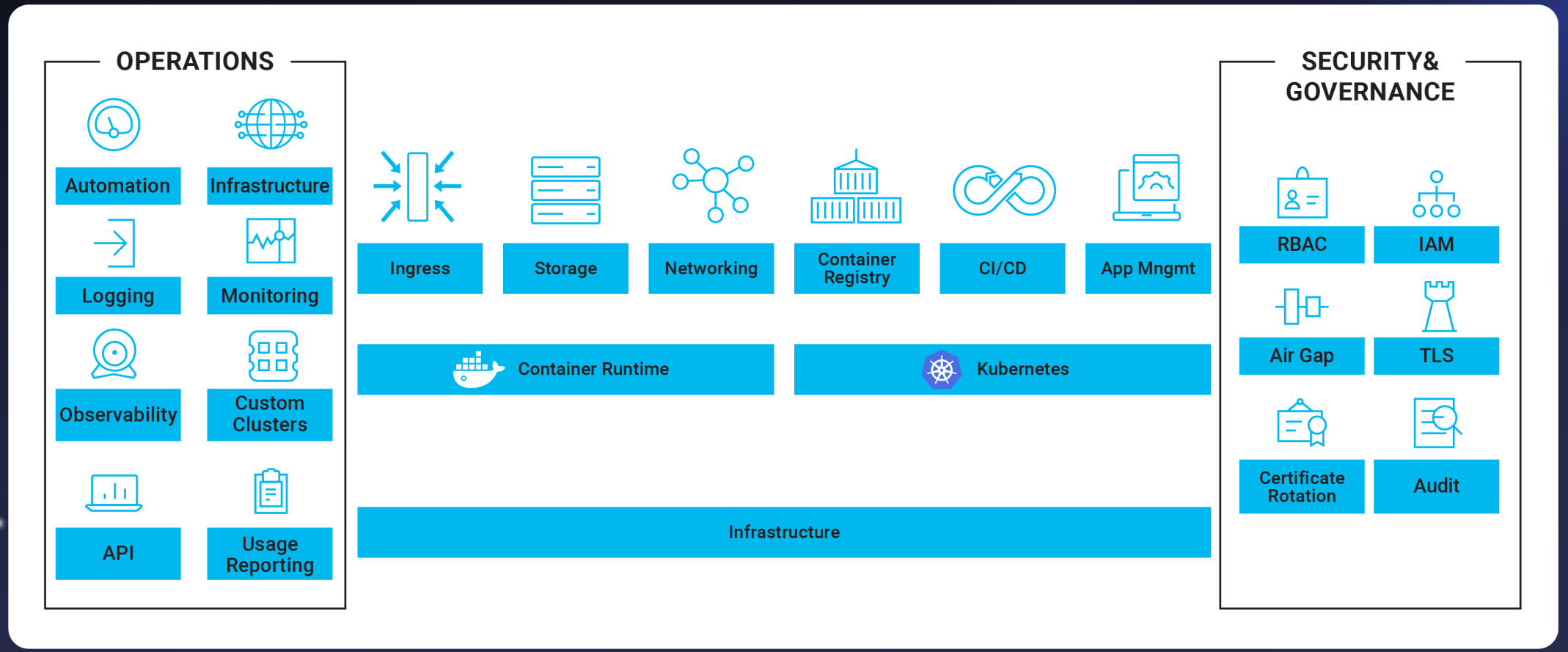
Обо мне

- CTO, исследователь безопасности
- Соорганизатор конференций ZeroNights, DEFCON Russia (#7812)
- Бывший редактор рубрик в журнале "ХАКЕР"
- Создатель проекта "Python Arsenal for Reverse Engineering"
- Автор telegram-канала "k8s (in)security“
- Автор тренинга “Безопасность Cloud Native приложений в Kubernetes-based инфраструктурах”
- Докладчик: BlackHat, HITB, ZeroNights, HackInParis, Confidence, SAS, PHDays, ...

Облачный подход захватывает мир



Kubernetes


OPERATIONS
Automation
Infrastructure
Logging
Monitoring
Observability
Custom Clusters
API
Usage Reporting
Ingress
Storage
Networking
Container Registry
CI/CD
App Mngmt
Container Runtime
Kubernetes
Infrastructure
SECURITY& GOVERNANCE
RBAC
IAM
Air Gap
TLS
Certificate Rotation
Audit

Зона ответственности

Рабочая нагрузка:

- Системные сервисы
  - Сервисы ОС
  - Сервисы Kubernetes
- Собственные сервисы
  - Ваши приложения, выполняющие бизнес-логику
- Сторонние сервисы
  - CI\CD, хранилища исходного кода, хранилища образов контейнеров, системы мониторинга и логирования и т.д.

Проблемы

- 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”
- Разработка стремительно развивается
  - Старые подходы к безопасности не работают
    - Департаменты разработки, поддержки и безопасности должны работать вместе
- Уникальные модели нарушителя, модель угроз и поверхность атаки
  - Атакующий по-прежнему на шаг впереди
    - 0-days, backdoors, APTs и т.д.

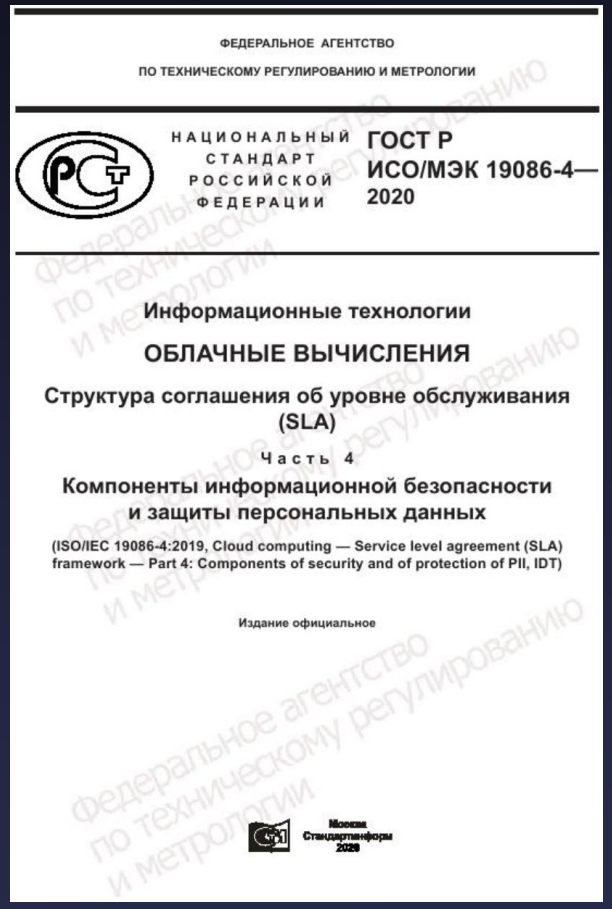
Управление угрозами

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Assess Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

NIST Cyber Security Framework

ГОСТ по облачным вычислениям



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 19086-4— 2020

Информационные технологии

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Структура соглашения об уровне обслуживания (SLA)

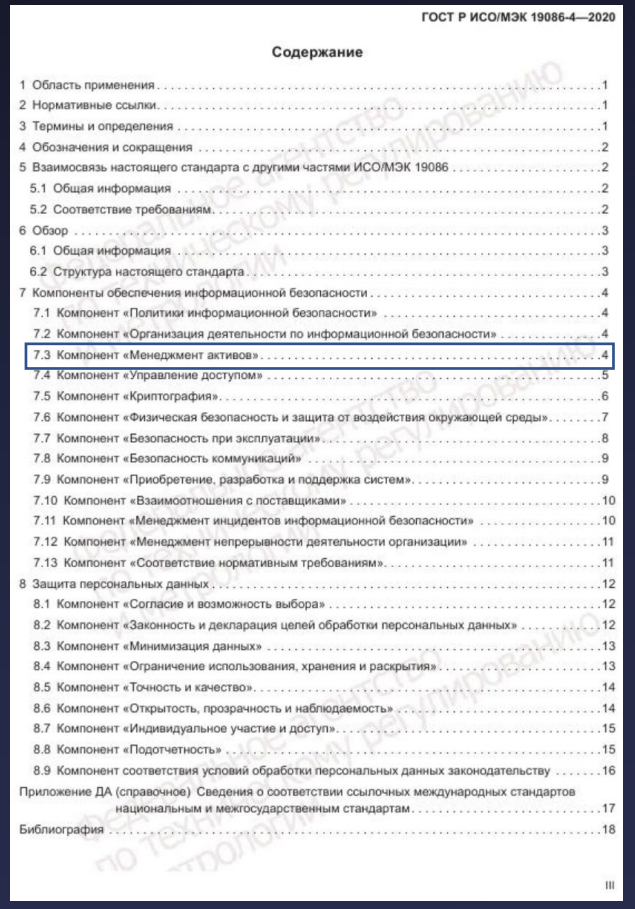
Часть 4

Компоненты информационной безопасности и защиты персональных данных

(ISO/IEC 19086-4:2019, Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII, IDT)

Издание официальное

Москва
Стандартинформ
2020



ГОСТ Р ИСО/МЭК 19086-4—2020

Содержание

III

Вступает в силу 01.06.2021 года

Что такое хорошо и что такое плохо?

- **Атакующий на шаг впереди, потому что:**
  - Для достижения цели он может глубоко изучить систему в поисках даже 1 недостатка
  - Строит план атаки на знаниях, которыми не владеет защищающийся
  - Часто защита строится на текущих знаниях об атакующем, а не на возможных
- **Для симметричного ответа необходимо:**
  - Всегда знать и понимать свой периметр
    - Инвентаризация активов/ресурсов
  - Отсутствие слепых зон в окружении
  - Детектировать аномальное поведение
    - Никаких правил, сигнатур и т.д.
    - Полезно как для безопасности, так и для надежности системы

На примере атаки на SolarWinds

В контексте Kubernetes, злоумышленник может внедриться в:

- Код компании
- OpenSource-код
- Образы контейнеров
- Ресурсы Kubernetes YAML
- Helm-чарты

Kubernetes и контейнеры предоставляют:

- Возможность высокой наблюдаемости (observability) и наглядность (visibility) происходящего
- Подход ZeroTrust
- Подход ShiftLeft security
- Подход Infrastructure-as-Code/Policy-as-Code/Security-as-Code

Заключение

Понимайте технологии, с которыми работаете

- Окружение без слепых зон
- You Can’t Secure What You Can’t See

Понимайте процессы, с которыми работаете

- Встраивание в процесс разработки

Понимайте людей, с которыми работаете

- Работа рука об руку с разработкой и поддержкой
- Единый взгляд на систему и процессы

LUNTRY

Как с нами связаться:
+7 (495) 223-07-86

www.luntry.ru