



Kubernetes:

Незнание своей системы — злейший враг

Дмитрий Евдокимов,
Технический директор Luntry

I Обо мне

- СТО, 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

CNCF Cloud Native Landscape
2020-09-26T00:29:04Z.147d4f7e

Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io

Greyed logos are not open source

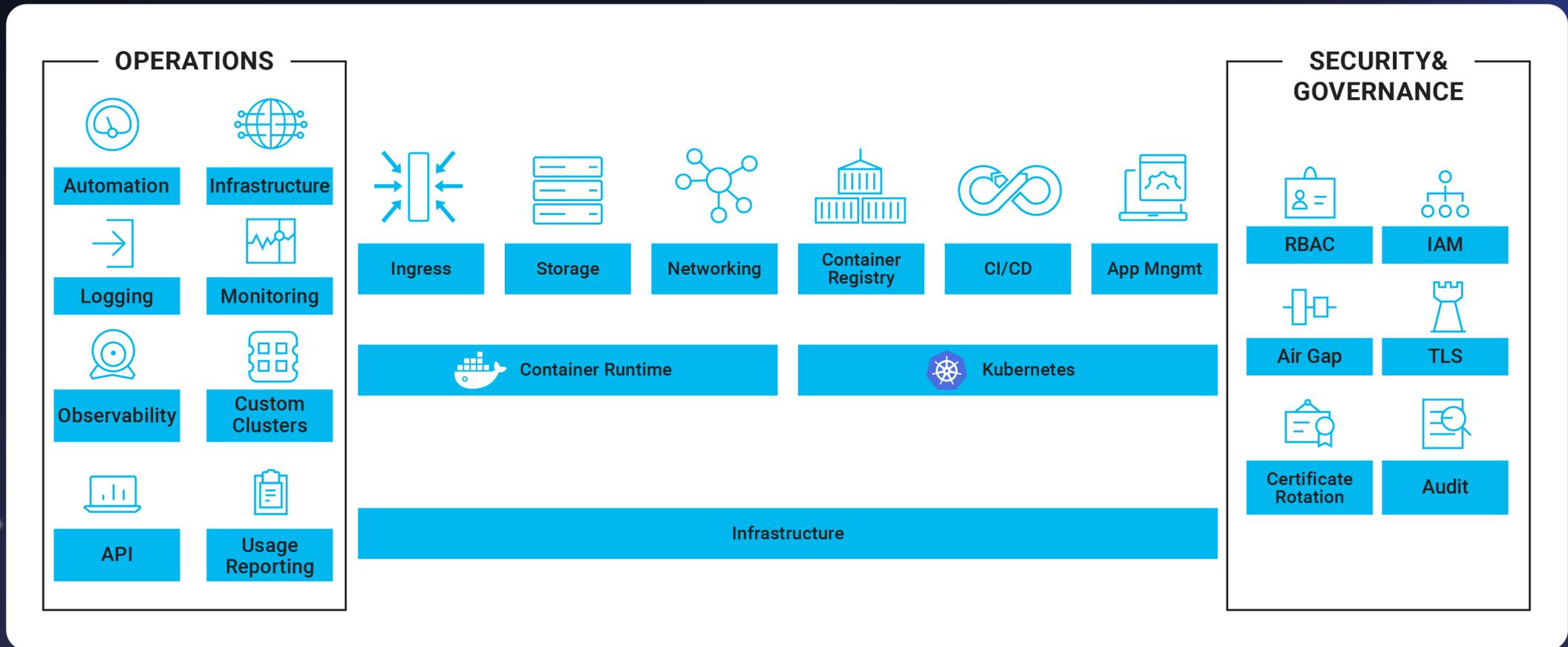
The landscape is organized into several functional categories:

- App Definition and Development:** Includes logos for KV, V, and various database and messaging services.
- Streaming & Messaging:** Includes logos for cloudevents, NATS, and other event-driven architectures.
- Application Definition & Image Build:** Includes logos for HELM, K8S, and other container management tools.
- Continuous Integration & Delivery:** Includes logos for Argo, Jenkins, and other CI/CD tools.
- Platform:** Includes logos for Certified Kubernetes - Distribution, Hosted, and Installer.
- Observability and Analysis:** Includes logos for Monitoring (Prometheus, Grafana), Logging (Elasticsearch, Fluentd), Tracing (Jaeger), and Chaos Engineering.
- Serverless:** Includes logos for various serverless computing services.
- Members:** A grid of logos representing the members of the Cloud Native Computing Foundation.

Cloud Native Landscape
This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

l.cncf.io

Kubernetes



I 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.

I 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

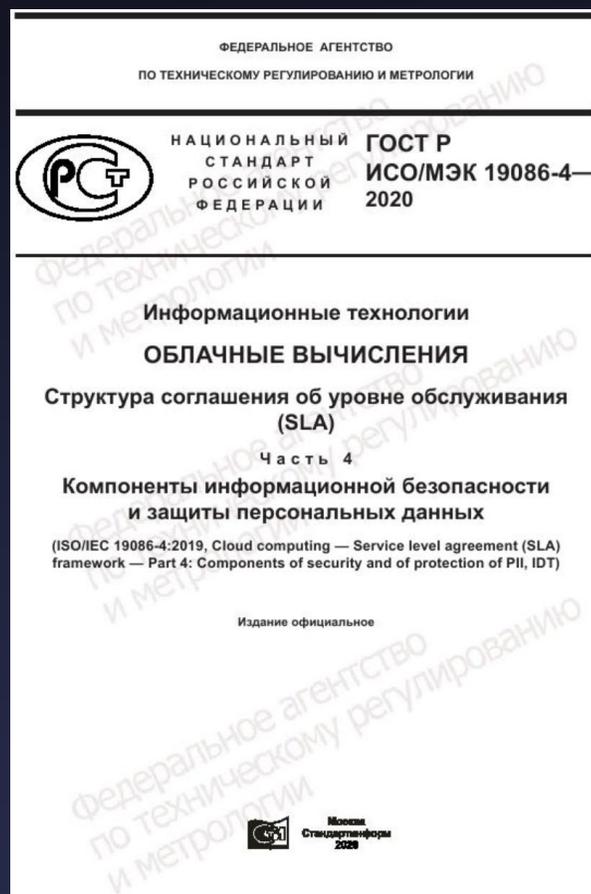


NIST Cyber Security Framework

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



ГОСТ Р ИСО/МЭК 19086-4—2020

Содержание

1 Область применения	1
2 Нормативные ссылки	1
3 Термины и определения	1
4 Обозначения и сокращения	2
5 Взаимосвязь настоящего стандарта с другими частями ИСО/МЭК 19086	2
5.1 Общая информация	2
5.2 Соответствие требованиям	2
6 Обзор	3
6.1 Общая информация	3
6.2 Структура настоящего стандарта	3
7 Компоненты обеспечения информационной безопасности	4
7.1 Компонент «Политики информационной безопасности»	4
7.2 Компонент «Организация деятельности по информационной безопасности»	4
7.3 Компонент «Менеджмент активов»	4
7.4 Компонент «Управление доступом»	5
7.5 Компонент «Криптография»	6
7.6 Компонент «Физическая безопасность и защита от воздействия окружающей среды»	7
7.7 Компонент «Безопасность при эксплуатации»	8
7.8 Компонент «Безопасность коммуникаций»	9
7.9 Компонент «Приобретение, разработка и поддержка систем»	9
7.10 Компонент «Взаимоотношения с поставщиками»	10
7.11 Компонент «Менеджмент инцидентов информационной безопасности»	10
7.12 Компонент «Менеджмент непрерывности деятельности организации»	11
7.13 Компонент «Соответствие нормативным требованиям»	11
8 Защита персональных данных	12
8.1 Компонент «Согласие и возможность выбора»	12
8.2 Компонент «Законность и декларация целей обработки персональных данных»	12
8.3 Компонент «Минимизация данных»	13
8.4 Компонент «Ограничение использования, хранения и раскрытия»	13
8.5 Компонент «Точность и качество»	14
8.6 Компонент «Открытость, прозрачность и наблюдаемость»	14
8.7 Компонент «Индивидуальное участие и доступ»	15
8.8 Компонент «Подотчетность»	15
8.9 Компонент соответствия условий обработки персональных данных законодательству	16
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам	17
Библиография	18

III

I 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

I 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



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

www.luntry.ru