

# Новая эра безопасности

—  
Andrii Kuzmenko  
IBM Security

Мы живём со  
скоростью облака



40 kg/ha

80 kg/ha

80%

Нагрузки бюджет  
перенесено в  
облако

75%

Организаций с  
несколькими  
«облаками» в 2020-  
м

Безопасность тоже  
должна  
ускориться...

# Такие у нас правила

Блокировка

Использование  
ПО и железа

Политики по  
IP и хостам

Блокировать  
все аномалии

Сегментация

Агенты везде

Регулярные  
проверки

Ручное  
устранение и  
реагирование

# Время менять правила



1981

2019



F1

[facebook.com/Formula1](https://www.facebook.com/Formula1)

Мы должны принимать

Культуру Контроли Хаос

Культура начинается с  
разговора

# Наш простой язык безопасности

Threat Landscape

Advanced Malware

Cyber Kill Chain

Zero Day Vulnerability

User Behavior Analytics

False Positives

Indicators of Compromise

Zero Trust Model

Vulnerability Assessment

# Пора говорить на языке бизнеса

Риски

Лояльность

Бренд

Инновации

Продуктивность

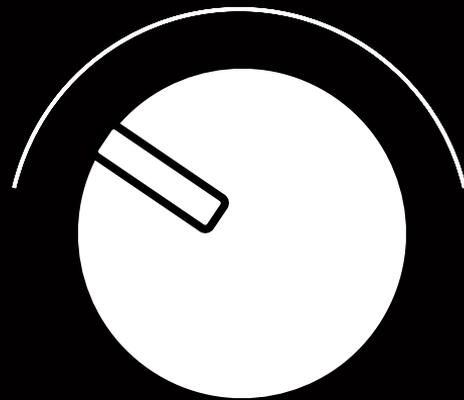
Лидерство

ОРЕХ

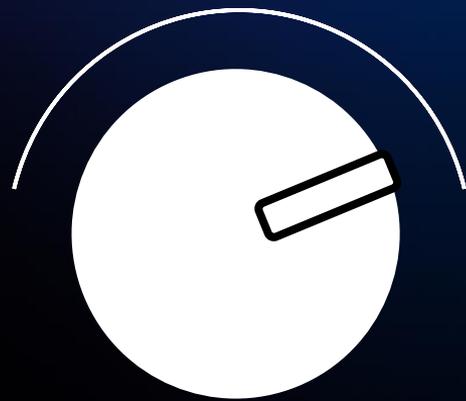
Стратегия

**Маркетинг**

Разговор  
требуется усиления



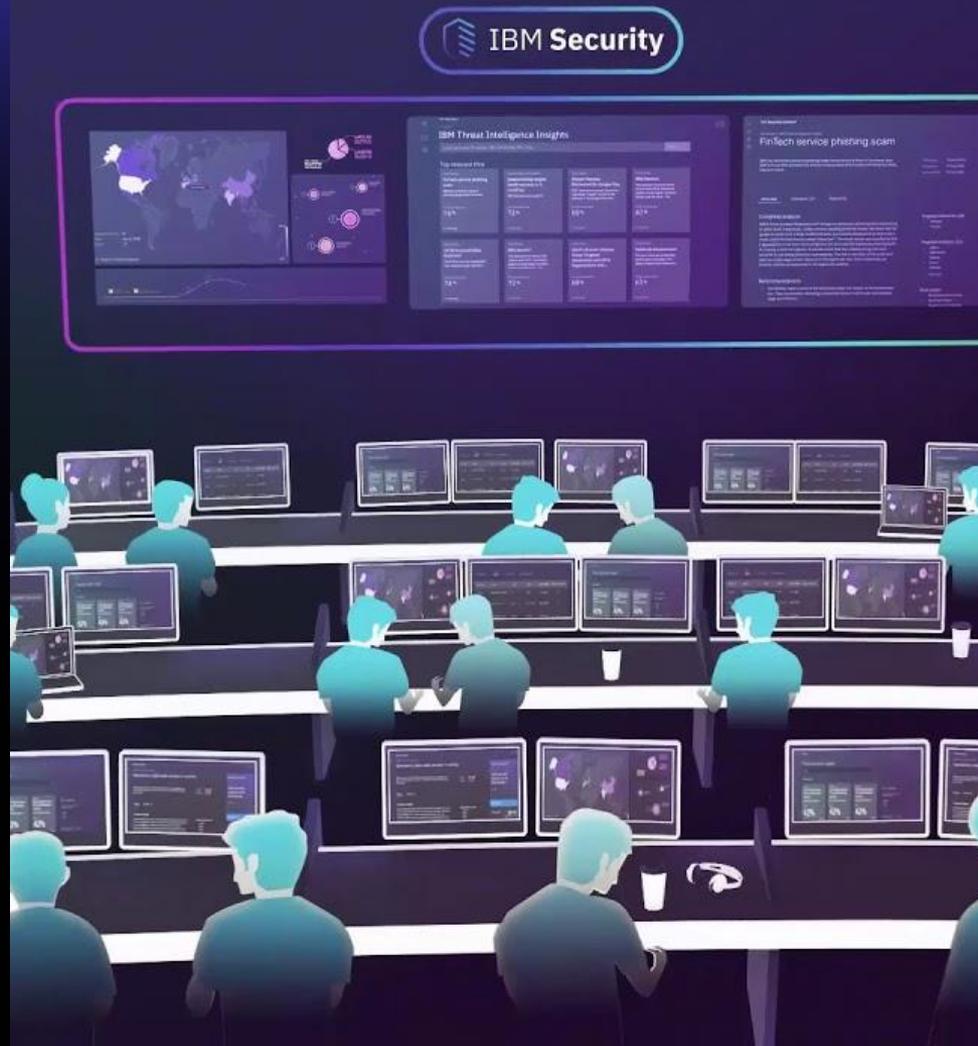
Разговор  
требует усиления  
через действия



# Привлечение внимания

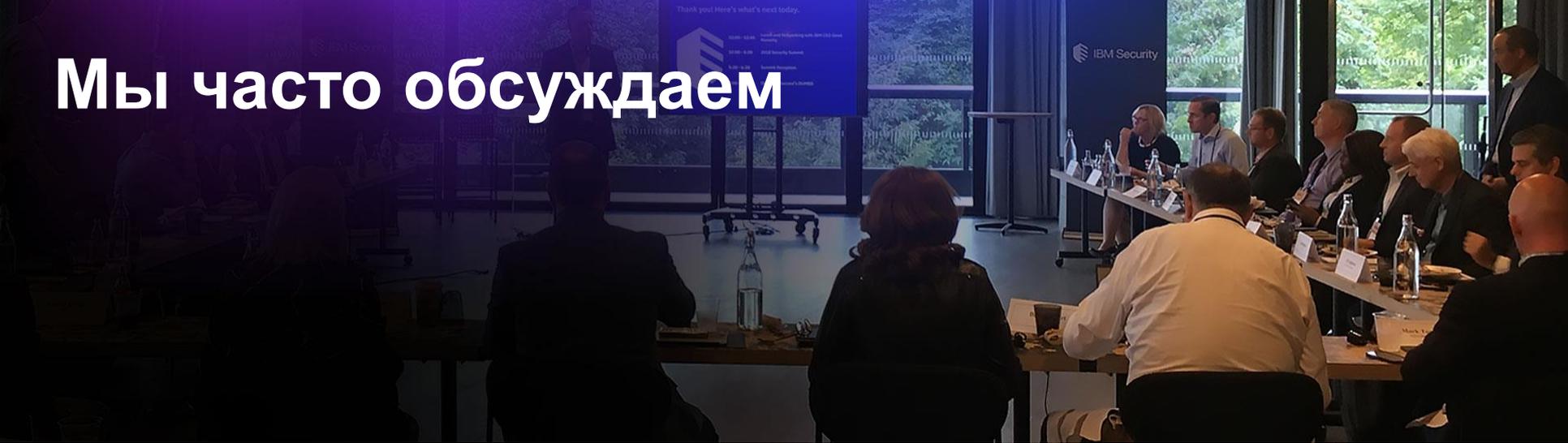


# Взаимодействие



КОНТРОЛИ

# Мы часто обсуждаем



**Нам нужны  
новые  
контроли**

**Нам не  
хватает  
сотрудников**

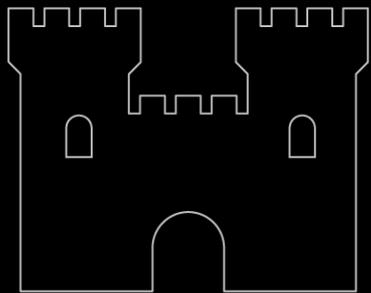
**Как нам  
защищать  
IoT?**

**Мы уходим в  
облако**

**Что делать с  
регулятором?**

# Будущее и настоящее.

До 2013

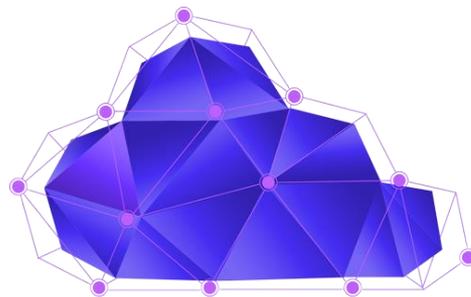


2013-2018

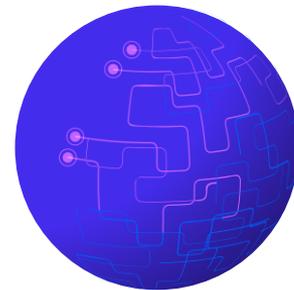


2019+

Connected security



AI, ML



Меньше  
блоков

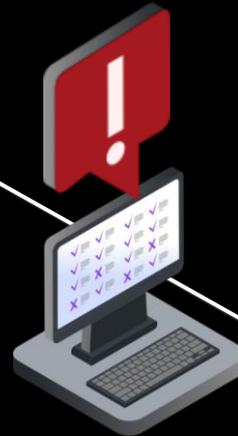


Больше  
направ-  
лений



Скорость  
облака

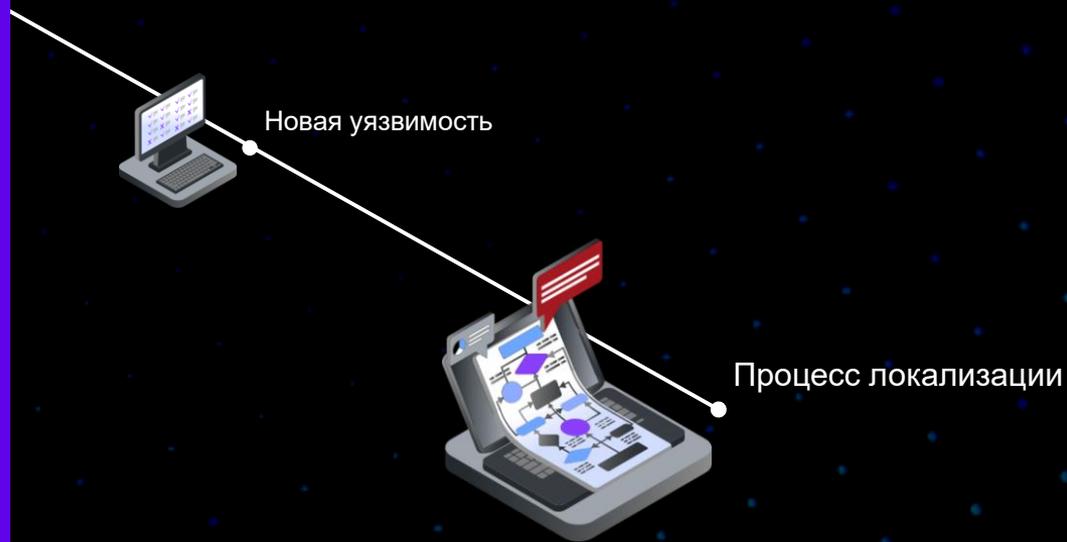
Доброе утро



Новая уязвимость

# Скорость облака

Ставим кофе



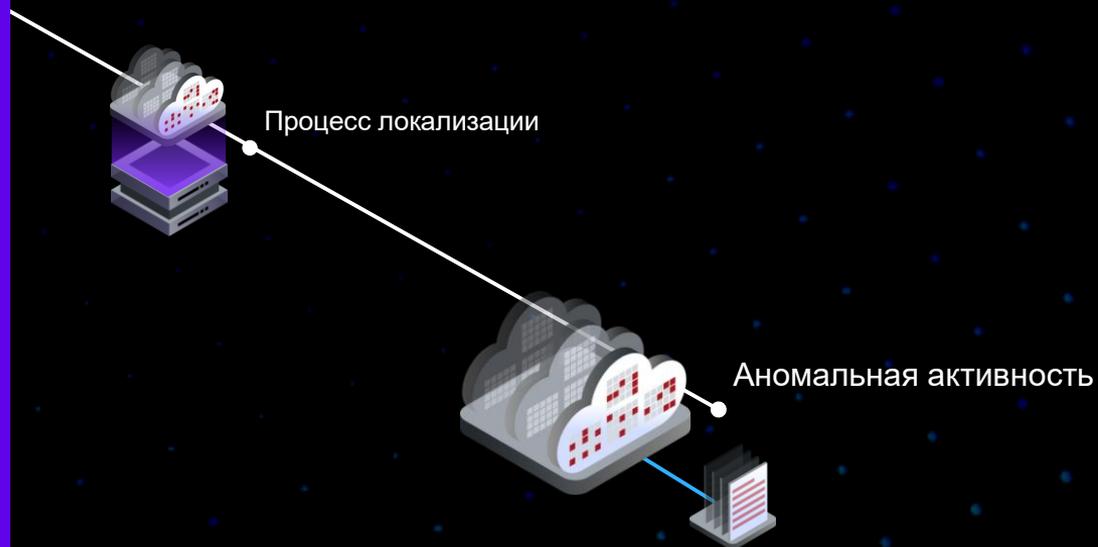
# Скорость облака

Кофе закипает



# Скорость облака

Наливаем кофе в чашку



# Скорость облака

## Первый глоток



# Скорость облака

Пока кофе не остыл



# Скорость облака

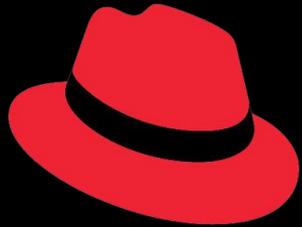
Успели до обеда



# Скорость облака

Успели до обеда...





**Red Hat**

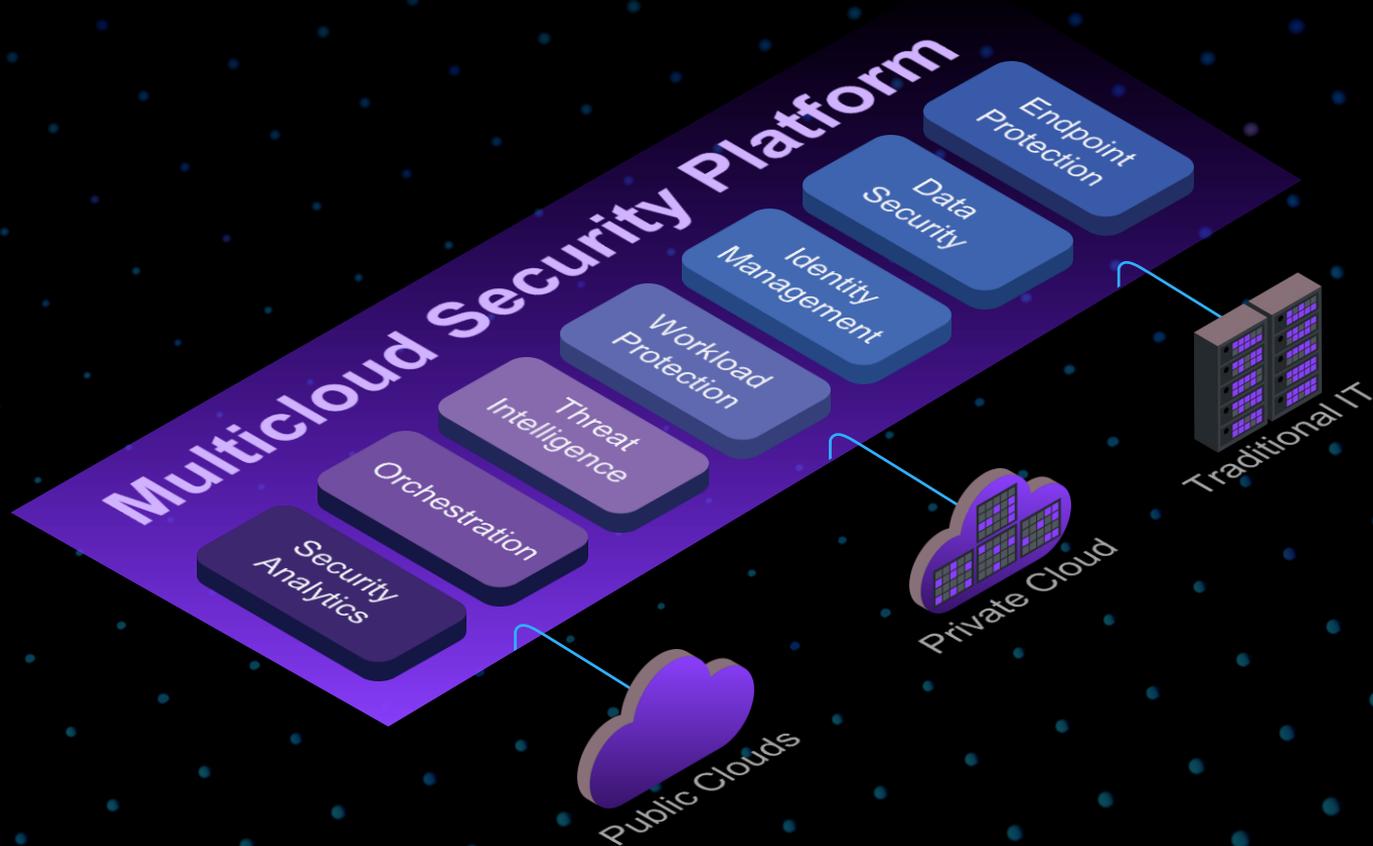


Xaoc

# Хаос в инструментах и инфраструктуре



# Наше видение и настоящее



# IBM Security



Обнаружить



Среагировать

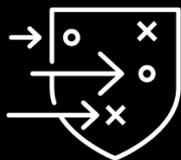


Понять суть



**IBM  
Qradar**

**IBM  
Guardium**



**Журналы<sup>Unlim\*</sup>**

**Сеть**

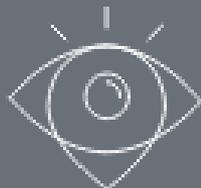
**Уязвимости**

**Топология**

**Активы**

**Пользователи**

**Базы**



**IBM Watson**

**Qradar UBA**

**DNS Analyzer**

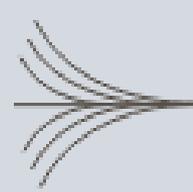
**OpenVas**

**Qlean**

**Assistant**



**IBM  
Resilient  
IBM i2**



# Открытая платформа для упрощения работы на каждом этапе

## IBM Security App Exchange

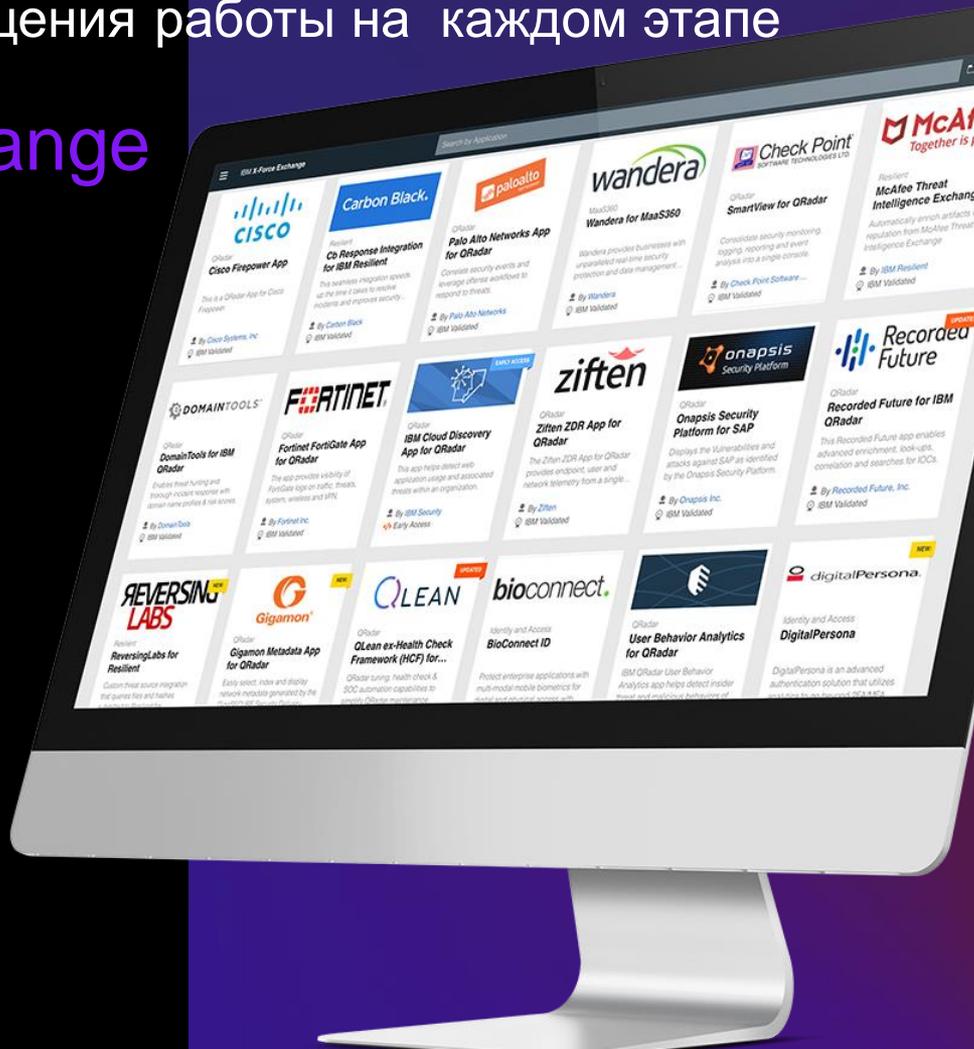


Приложения | Контент | Услуги

Производители

Консультанты

Клиенты



Живём со  
скоростью облака

Защита со  
скоростью облака

