DATA-CENTRIC SECURITY: ЗАЩИТА ДАННЫХ КАК АЛЬТЕРНАТИВНЫЙ ЭШЕЛОН ЗАЩИТЫ ПЕРИМЕТРА

Старченко Кирилл
Архитектор ИБ ПАО МТС

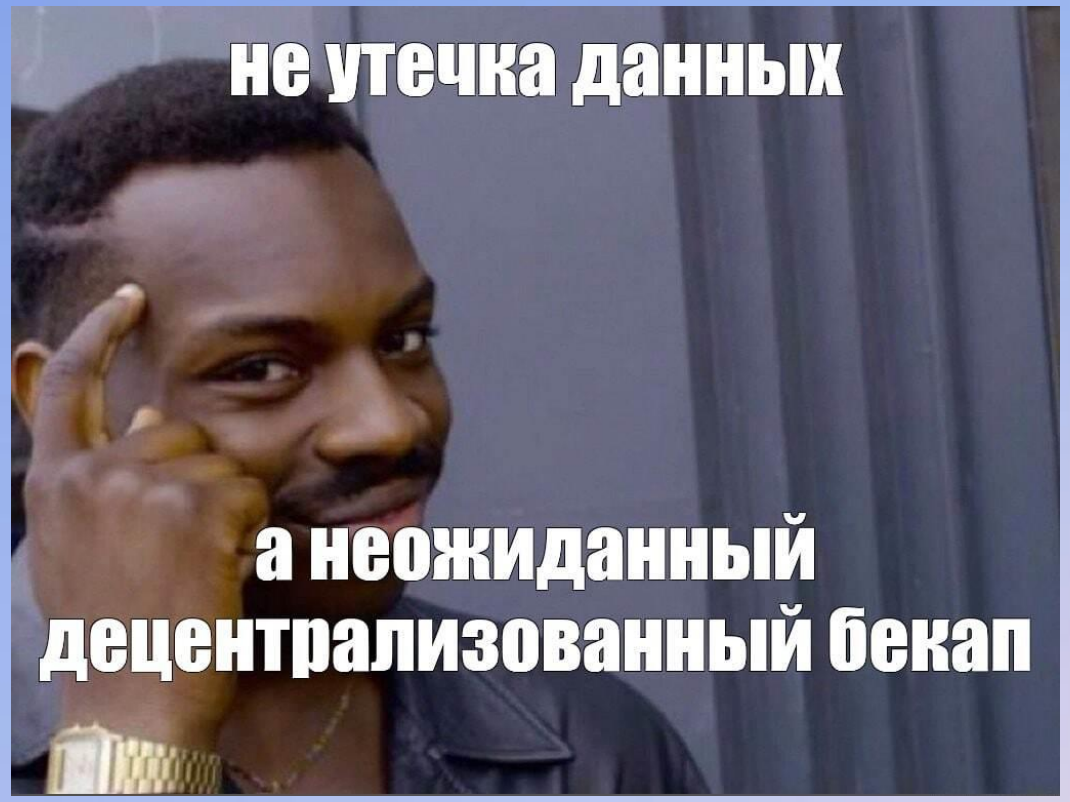
МТС : архитектура ИБ

Старченко Кирилл

Проблема крепости

Мы строим крепость. Мы защищаем место, где лежит наше золото. У нас есть уверенность в том, что наши сокровища в безопасности – однако, это не так.

Где сейчас ваши данные?



- Облака (AWS, Azure, Google Cloud)
- Удалённые устройства сотрудников
- Мессенджеры, личная почта
- Партнеры и подрядчики

Что такое Data-Centric?

Стратегия, в которой политики и средства защиты привязаны к самим данным, а не к инфраструктуре.*

Защита "Места"

Фокус на "Где"

(Периметр, сеть, устройства)

Защита "Данных"

Фокус на "Что" и "Как"

(Классификация, шифрование, DRM)

*** Важно! Такой подход не является исключающим для периметрового, а наоборот, помогает дополнить незатронутые векторы защиты.**

Три кита Data-Centric архитектуры

Любая data-centric архитектура строится на этих трёх опорах.

1. Знай свои данные

Инвентаризация и классификация.

2. Встрой защиту

Шифрование, DRM, ABAC.

3. Контролируй

UEBA, DLP, SIEM/SOAR/DAM.

Три кита Data-Centric архитектуры

Любая data-centric архитектура строится на этих трёх опорах.

1. Знай свои данные

Инвентаризация и классификация.

2. Встрой защиту

Шифрование, DRM, ABAC.

3. Контролируй

UEBA, DLP, SIEM/SOAR/DAM.

Кит 1 : знай свои данные

Невозможно защитить актив, который не виден.

- **Инструменты:** Data Discovery & Classification сканируют хранилища и автоматически ставят метки.
- **Результат:** Единый каталог данных с атрибутами чувствительности и владельцем.
- **Примеры меток:** «Общедоступные», «Внутренние», «Конфиденциальные».

Три кита Data-Centric архитектуры

Любая data-centric архитектура строится на этих трёх опорах.

1. Знай свои данные

Инвентаризация и классификация.

2. Встрой защиту

Шифрование, DRM, ABAC.

3. Контролируй

UEBA, DLP, SIEM/SOAR/DAM.

Кит 2 : встрой защиту в данные

Защита должна жить внутри данных и процессов

Шифрование
В покое, в движении, в использовании. Управление ключами (KMS/HSM).

Маскирование и токенизация
Для сред разработки и тестирования.

DRM (IRM)
«Охранная грамота» для файла. Запрет на копирование, печать.

ABAC
Контроль доступа на основе атрибутов (Кто, Где, На чем).

Кит 2 : встрой защиту в данные

Защита должна жить внутри данных и процессов

Шифрование
В покое, в движении, в использовании. Управление ключами (KMS/HSM).

Маскирование и токенизация
Для сред разработки и тестирования.

DRM (IRM)
«Охранная грамота» для файла. Запрет на копирование, печать.

ABAC
Контроль доступа на основе атрибутов (Кто, Где, На чем).

Кит 2 : встрой защиту в данные

Защита должна жить внутри данных и процессов

Шифрование
В покое, в движении, в использовании. Управление ключами (KMS/HSM).

Маскирование и токенизация
Для сред разработки и тестирования.

DRM (IRM)
«Охранная грамота» для файла. Запрет на копирование, печать.

ABAC
Контроль доступа на основе атрибутов (Кто, Где, На чем).

Кит 2 : встрой защиту в данные

Защита должна жить внутри данных и процессов

Шифрование
В покое, в движении, в использовании. Управление ключами (KMS/HSM).

Маскирование и токенизация
Для сред разработки и тестирования.

DRM (IRM)
«Охранная грамота» для файла. Запрет на копирование, печать.

ABAC
Контроль доступа на основе атрибутов (Кто, Где, На чем).

Три кита Data-Centric архитектуры

Любая data-centric архитектура строится на этих трёх опорах.

1. Знай свои данные

Инвентаризация и классификация.

2. Встрой защиту

Шифрование, DRM, ABAC.

3. Контролируй

UEBA, DLP, SIEM/SOAR/DAM.

Кит 3 : контролируй и реагируй

Мониторинг и аудит для обнаружения и реагирования на инциденты.

UEBA

Анализ поведения для обнаружения аномалий.

DLP

Исполнительный механизм для политик.

SIEM/SOAR/DAM

Центр управления и автоматизации.

Кит 3 : контролируй и реагируй

Мониторинг и аудит для обнаружения и реагирования на инциденты.

UEBA

Анализ поведения для обнаружения аномалий.

DLP

Исполнительный механизм для политик.

SIEM/SOAR/DAM

Центр управления и автоматизации.

Кит 3 : контролируй и реагируй

Мониторинг и аудит для обнаружения и реагирования на инциденты.

UEBA

Анализ поведения для обнаружения аномалий.

DLP

Исполнительный механизм для политик.

SIEM/SOAR/DAM

Центр управления и автоматизации.

Кит 3 : контролируй и реагируй

Мониторинг и аудит для обнаружения и реагирования на инциденты.

UEBA

Анализ поведения для обнаружения аномалий.

DLP

Исполнительный механизм для политик.

SIEM/SOAR/DAM

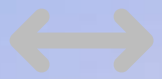
Центр управления и автоматизации.

Организационный аспект : Кто отвечает?

Data Owner

(Владелец данных)

Бизнес-пользователь. Определяет ценность и политики.
"Что защищать и зачем?"



Разделение ответственности

Data Custodian

(Хранитель данных)

IT/ИБ-специалисты. Помогают категорировать данные, выстраивать политики и технически их реализуют.
"Как защищать?"

Data-Cetnric – это не технология, а стратегия

Успех измеряется не количеством фаерволов, а снижением риска утечки. Это комплексное изменение:

Процессы + Люди + Технологии.

Процессы

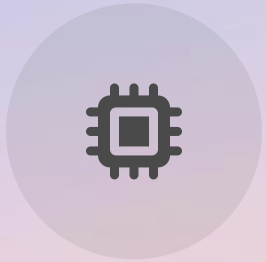
Начните с инвентаризации и классификации.

\+

Люди

Определите Владельцев данных в бизнесе.

\+



Технологии

Выбирайте решения, защищающие сами данные.

DATA-CENTRIC SECURITY: ЗАЩИТА ДАННЫХ КАК АЛЬТЕРНАТИВНЫЙ ЭШЕЛОН ЗАЩИТЫ ПЕРИМЕТРА

Старченко Кирилл
Архитектор ИБ ПАО МТС

TG : @Who_was_that