



ТИНЬКОФФ

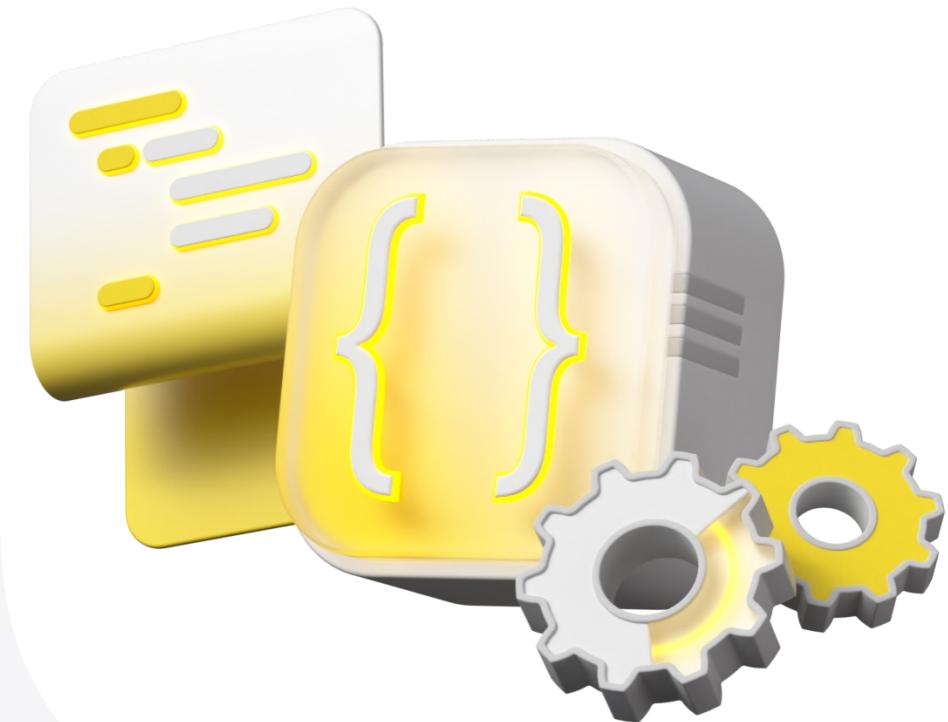
Анализ проекта с точки зрения ИБ



#Whoami

Ермаков Александр

- Security analytics team
- Ex. Telecom attack researcher in MNO
- MVNO & Insurance Security BP





ТИНЬКОФФ

Термины

Термины

Угроза

Уязвимость

Риск

Воздействие

Термины

Угроза

Потенциальная опасность для информации/ процесса/системы

Уязвимость

Риск

Воздействие

Термины

Угроза

Потенциальная опасность для информации/ процесса/системы

Уязвимость

Риск

Вероятность реализации угрозы

Х

Стоимость последствий

Сочетание вероятности события и его последствий

Воздействие

Термины

Угроза

Потенциальная опасность для информации/ процесса/системы

Уязвимость

Свойство актива из-за которого становится возможна реализация угрозы

Риск

Вероятность реализации угрозы

Х

Стоимость последствий

Сочетание вероятности события и его последствий

Воздействие

Термины

Угроза

Потенциальная опасность для информации/ процесса/системы

Уязвимость

Свойство актива из-за которого становится возможна реализация угрозы

Риск

Вероятность реализации угрозы

Х

Стоимость последствий

Сочетание вероятности события и его последствий

Воздействие

Что-то, приводящие
К эксплуатации уязвимости=>

Реализации угрозы => Реализации риска

Термины

Угроза

Потенциальная опасность для информации/ процесса/системы

Риск

Вероятность реализации угрозы

Х

Стоимость последствий

Сочетание вероятности события и его последствий

Термины

Угроза

Потенциальная опасность для информации/ процесса/системы

Риск

Вероятность реализации угрозы

Х

Стоимость последствий

Сочетание вероятности события и его последствий

Критичность /
Оценка эффективности

Термины

Угроза

Потенциальная опасность для информации/ процесса/системы

Риск

Вероятность реализации угрозы

Х

Стоимость последствий

Сочетание вероятности события и его последствий

Критичность /

Оценка эффективности

- Наличие данных/процессов
- Недоступность, изменение, кража, которых приведет к потерям для бизнеса

Термины

Угроза

Потенциальная опасность для информации/ процесса/системы

Риск

Вероятность реализации угрозы

Х

Стоимость последствий

Сочетание вероятности события и его последствий

Критичность /

Оценка эффективности

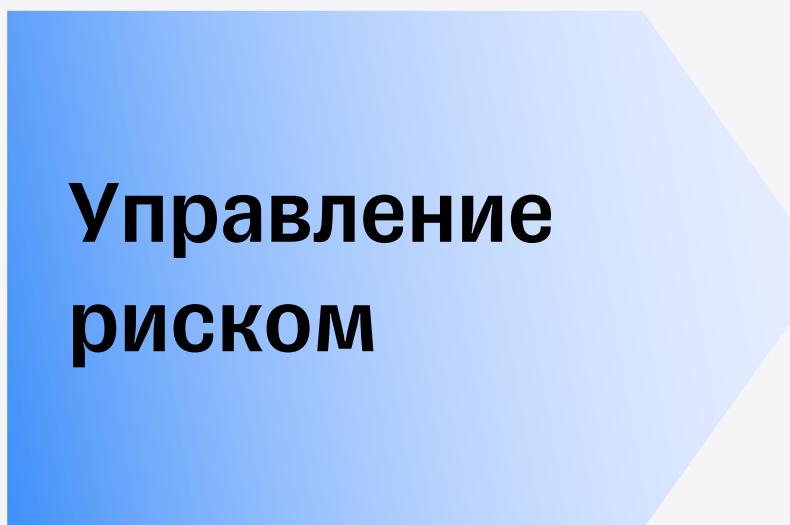
- Наличие данных/процессов
- Недоступность, изменение, кража, которых приведет к потерям для бизнеса
- Или наличие данных/процессов, через которые можно повлиять на другие критичные активы



ТИНЬКОФФ

Соответствие стандартам vs Управление риском

Соответствие стандартам vs Управление риском



Для Аналитика ИБ

- Процесс анализа типизирован
- Часто затянут
- Повышенный риск пропустить специфичный риск

Для Бизнеса

- Непонятные последствия нарушения
- Низкая скорость анализа
- Высокая стоимость р-и требований

- Повышенные требования к экспертизе сотрудника
- Риск упустить типовую проблему
- Учет специфики бизнеса

- Понятные риски
- Возможность принимать решения

01

Оценка соответствия

Получен список требований ИБ

02

Нагрузка

Большой список требований,
высокие затраты на реализацию

03

Мотивация

ИТ, Аналитки, РМ не понимают
необходимости требований

04

Конфликт

Снижение приоритета,
эскалация на бизнес

Оценка соответствия стандартам ИБ наихудший сценарий



ТИНЬКОФФ

Этапы анализа

Проекта, сервиса, фичи

Анализ проекта

Определение
критичности

Сбор
информации

Подключение
команд ИБ

Применимые
угрозы

Требования
и контроли

Остаточные
риски



ТИНЬКОФФ

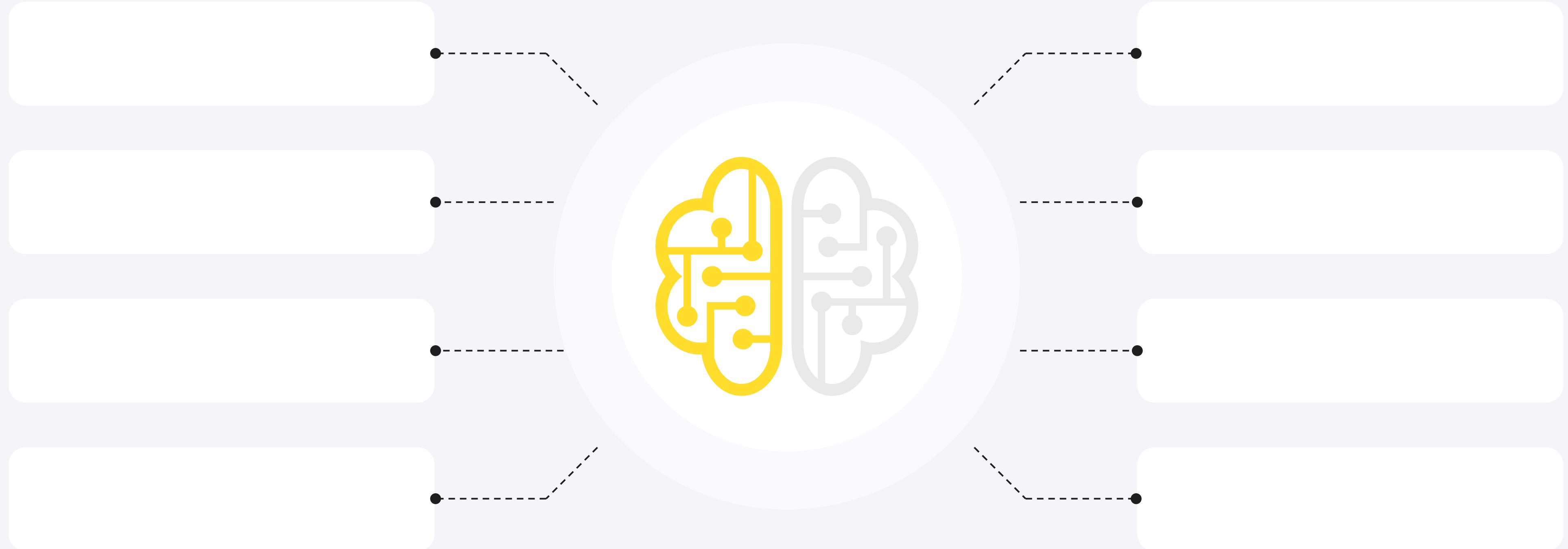
Критичность

Ключевые категории

Что делает проект* критичным?

*Сервис, метод, фичу, платформу

Критичность



MITRE ATT&CK



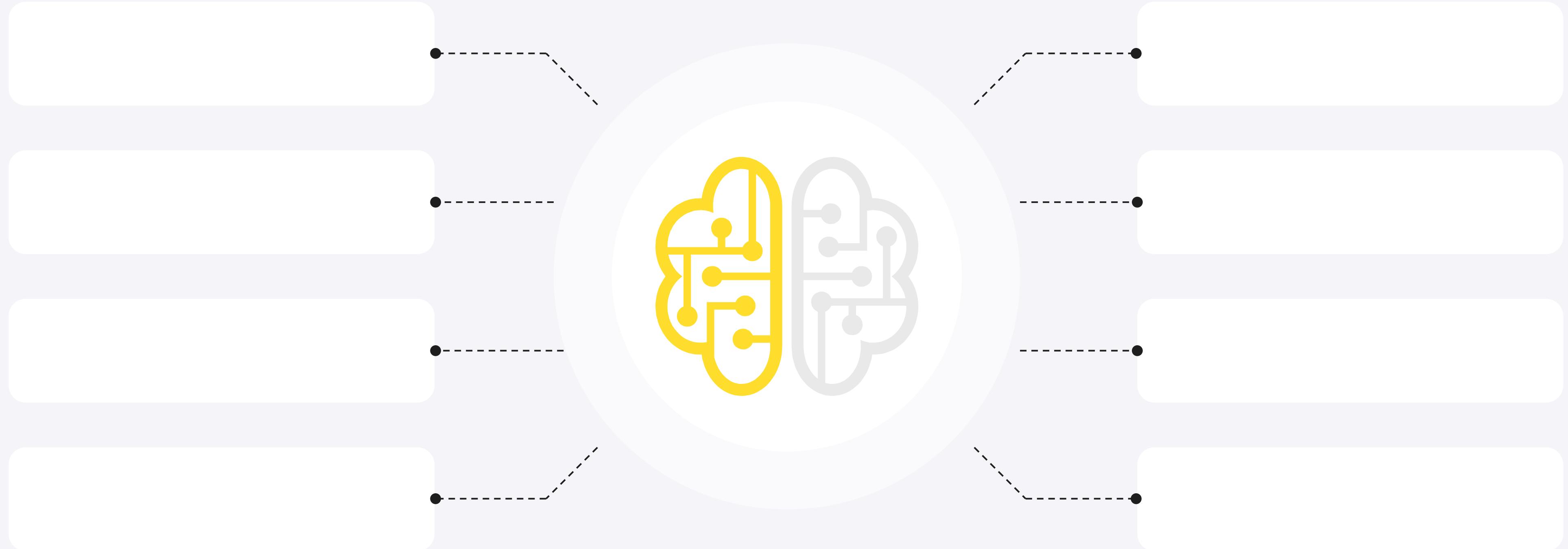
MITRE ATT&CK



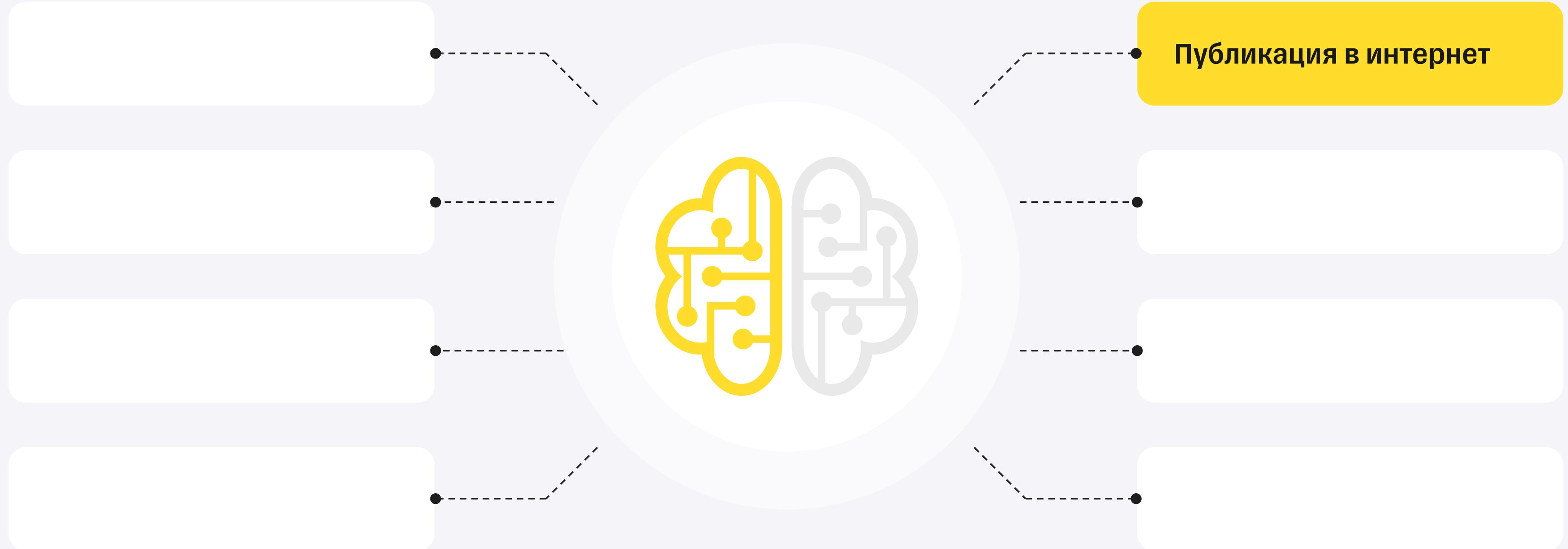
Malicious actors commonly use the following techniques to gain initial access to victim networks. [\[TA0001\]](#)

- Exploit Public-Facing Application [\[T1190\]](#)
- External Remote Services [\[T1133\]](#)
- Phishing [\[T1566\]](#)
-
- Valid Accounts [\[T1078\]](#)

Критичность



Критичность



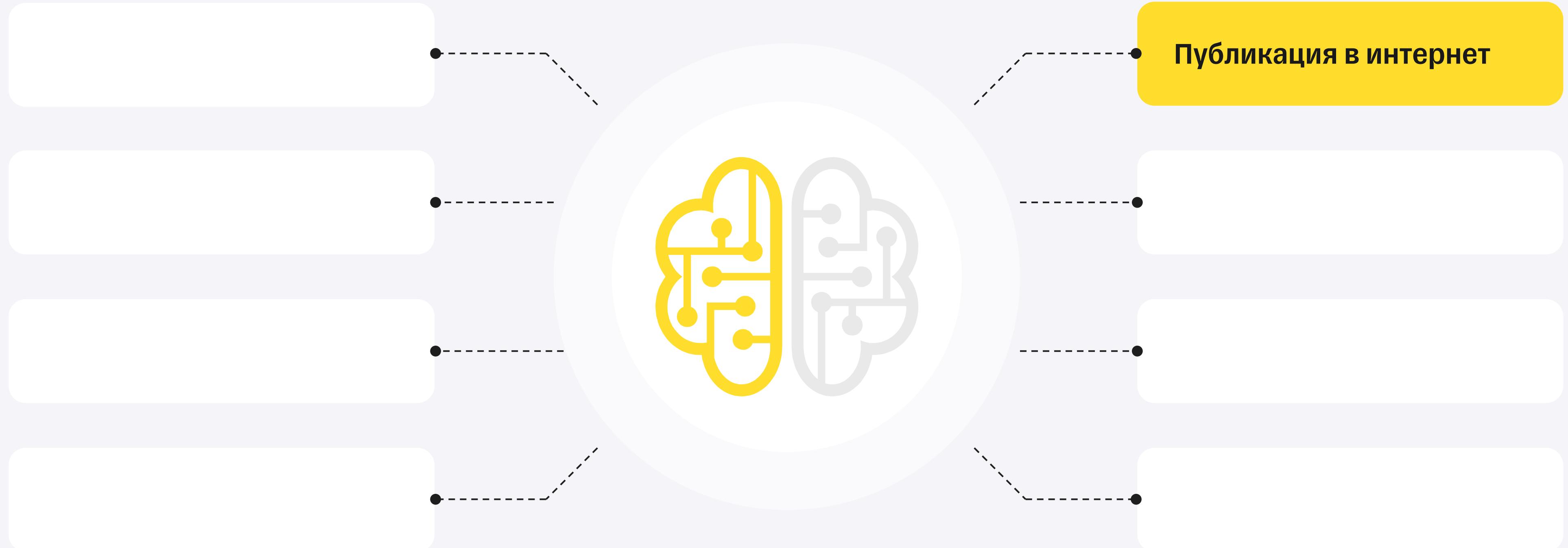
Malicious actors commonly use the following techniques to gain initial access to victim networks. [\[TA0001\]](#)

- Exploit Public-Facing Application [\[T1190\]](#)
- External Remote Services [\[T1133\]](#)
- Phishing [\[T1566\]](#)
-
- Valid Accounts [\[T1078\]](#)

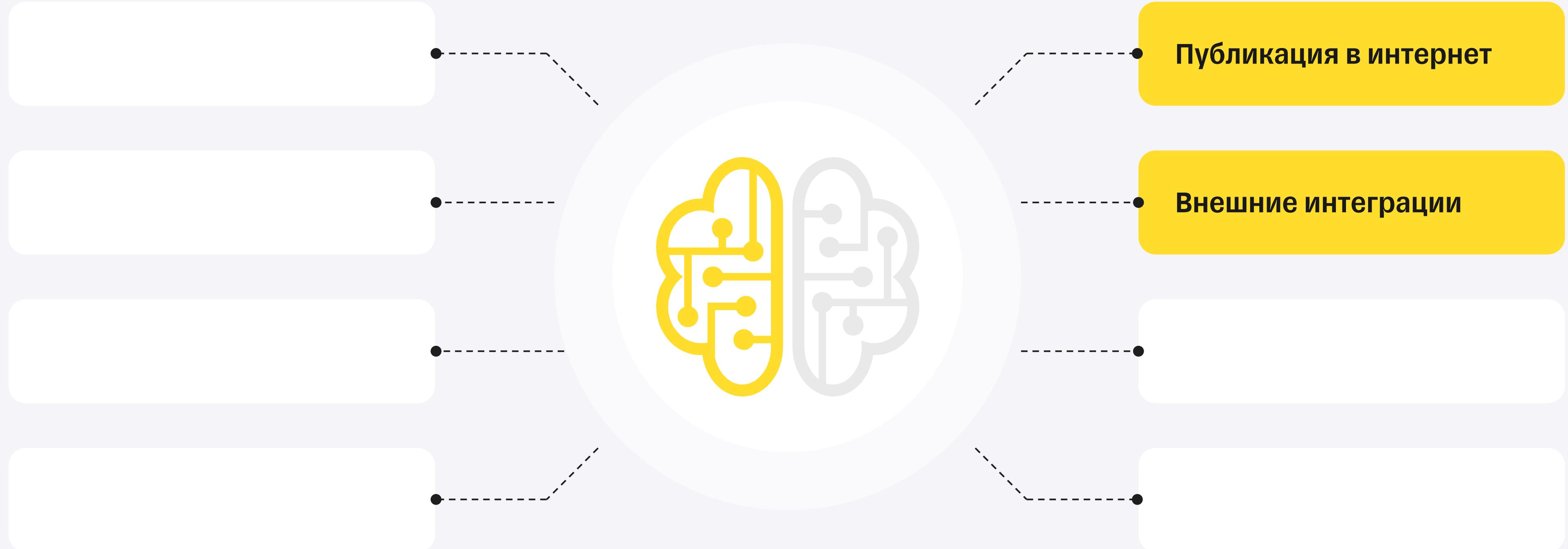
Malicious actors commonly use the following techniques to gain initial access to victim networks. [\[TA0001\]](#)

- Exploit Public-Facing Application [\[T1190\]](#)
- External Remote Services [\[T1133\]](#)
- Phishing [\[T1566\]](#)
- Trusted Relationship [\[T1199\]](#)
- Valid Accounts [\[T1078\]](#)

Критичность



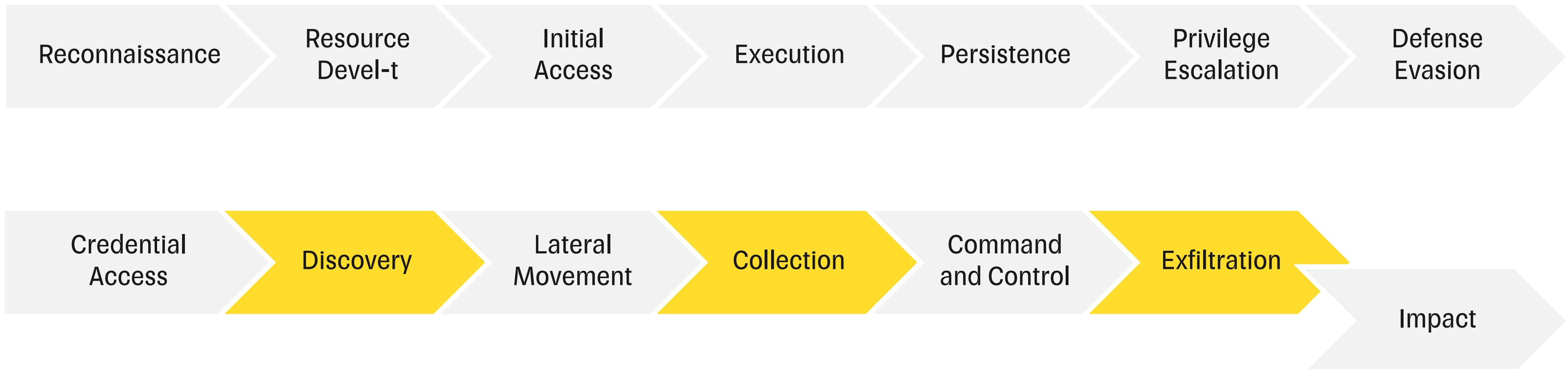
Критичность



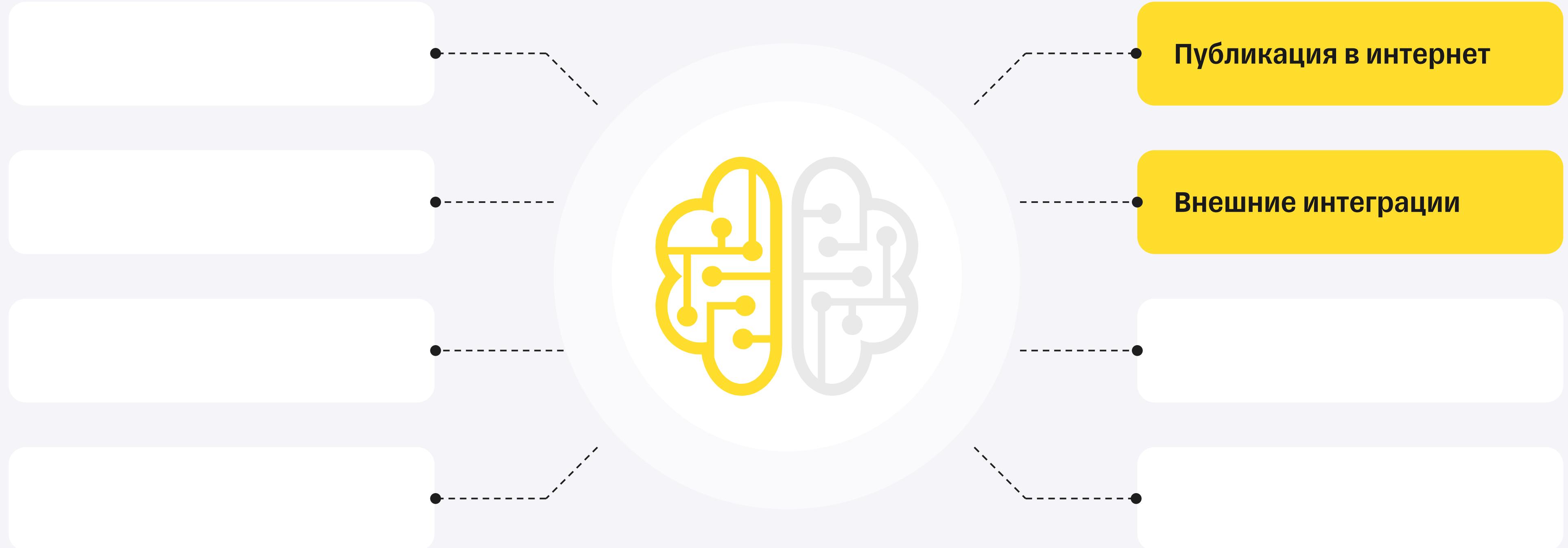
MITRE ATT&CK



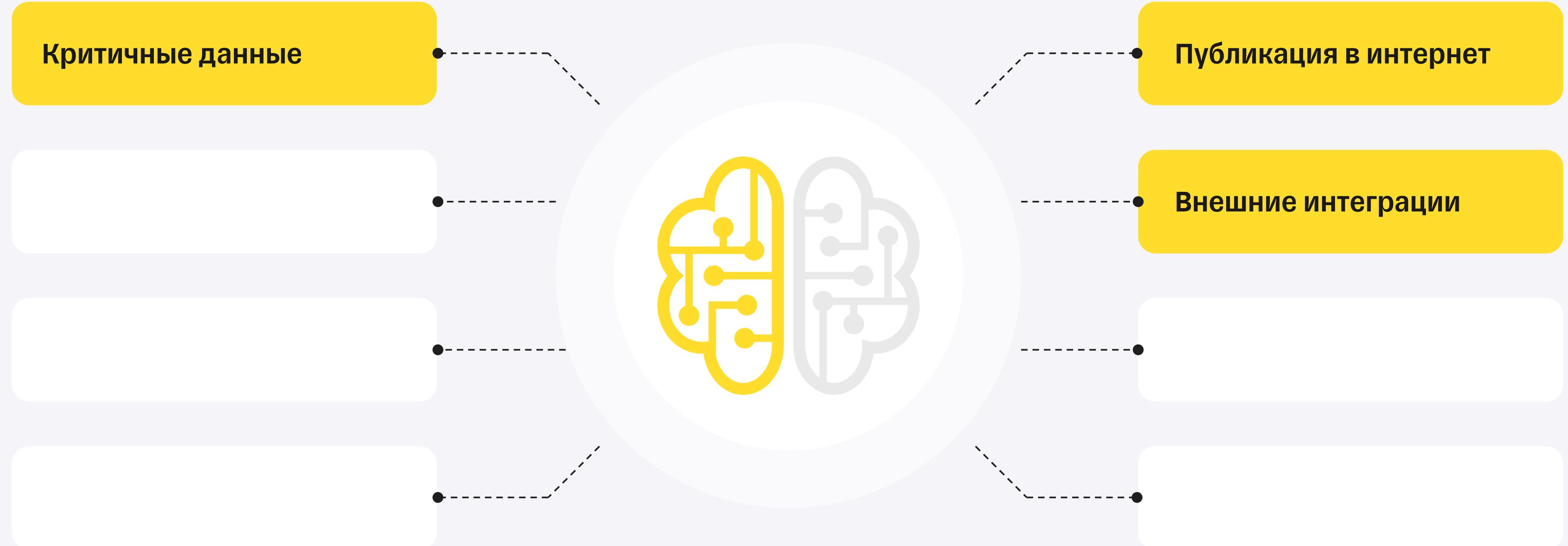
MITRE ATT&CK



Критичность



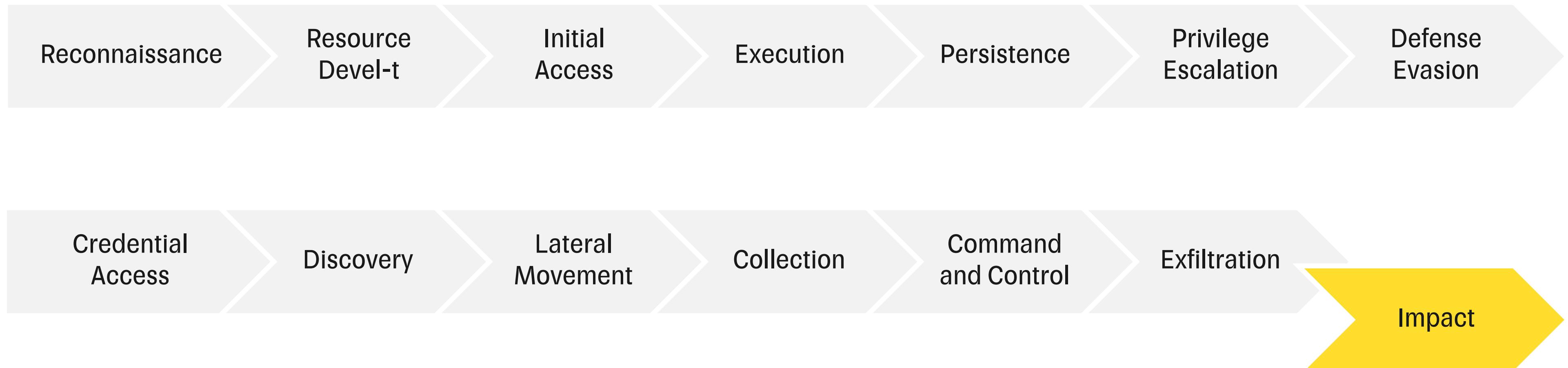
Критичность



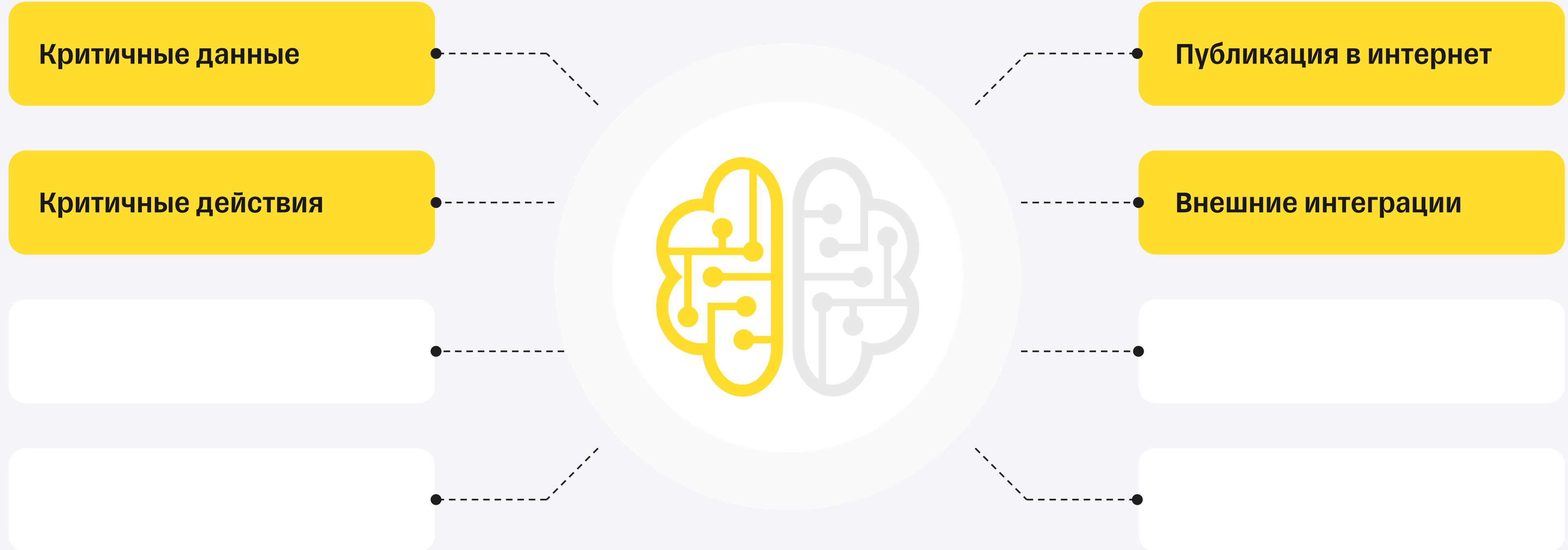
MITRE ATT&CK



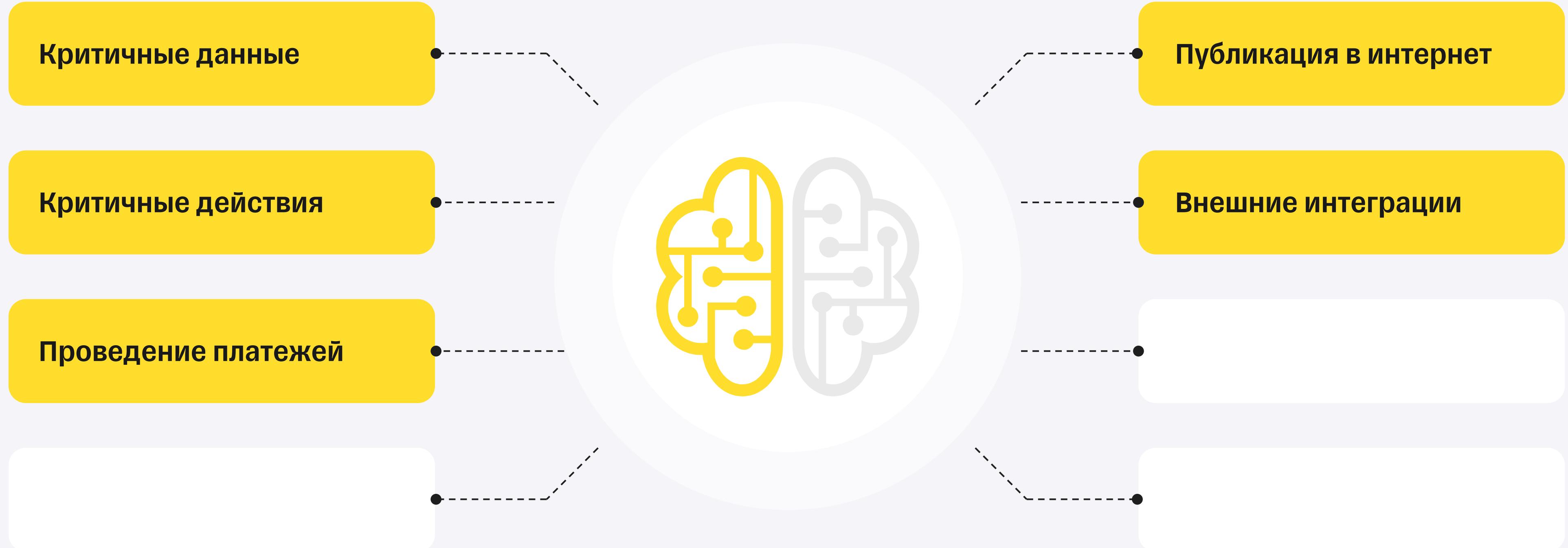
MITRE ATT&CK



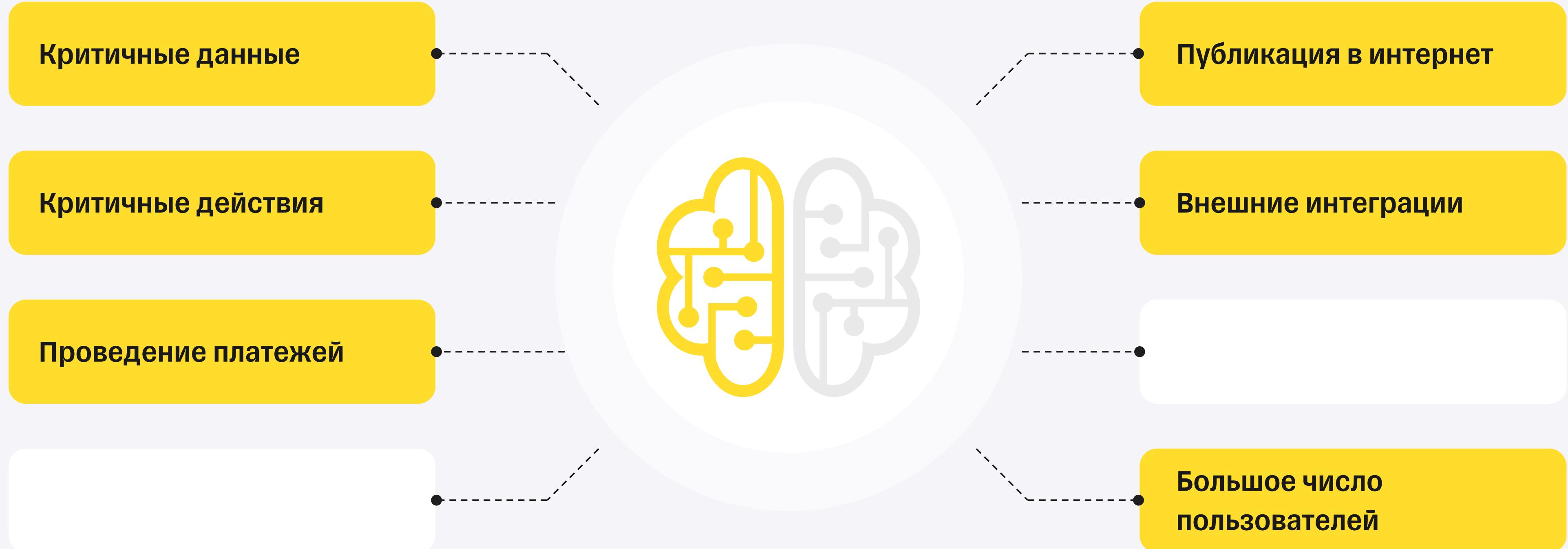
Критичность



Критичность



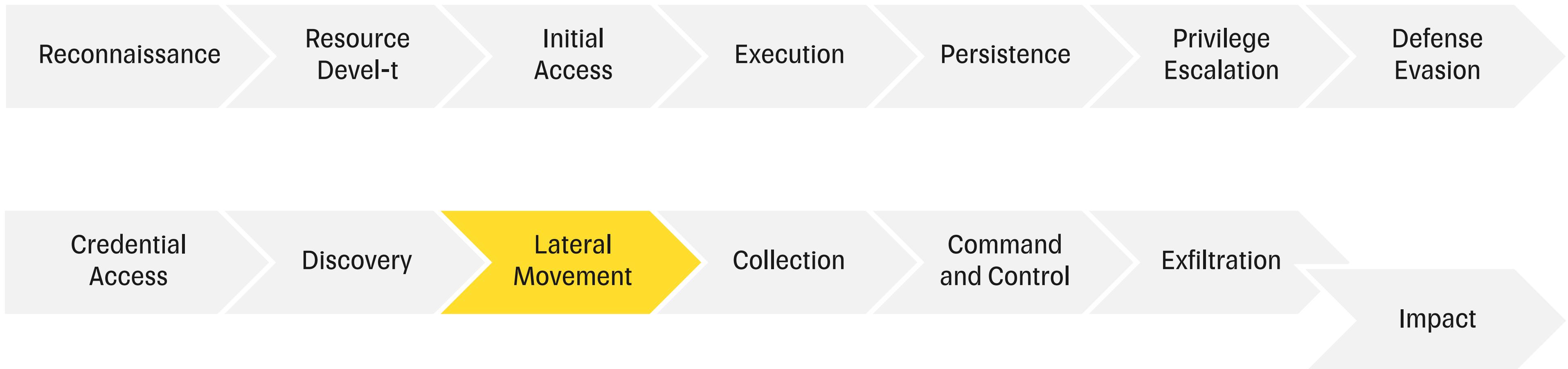
Критичность



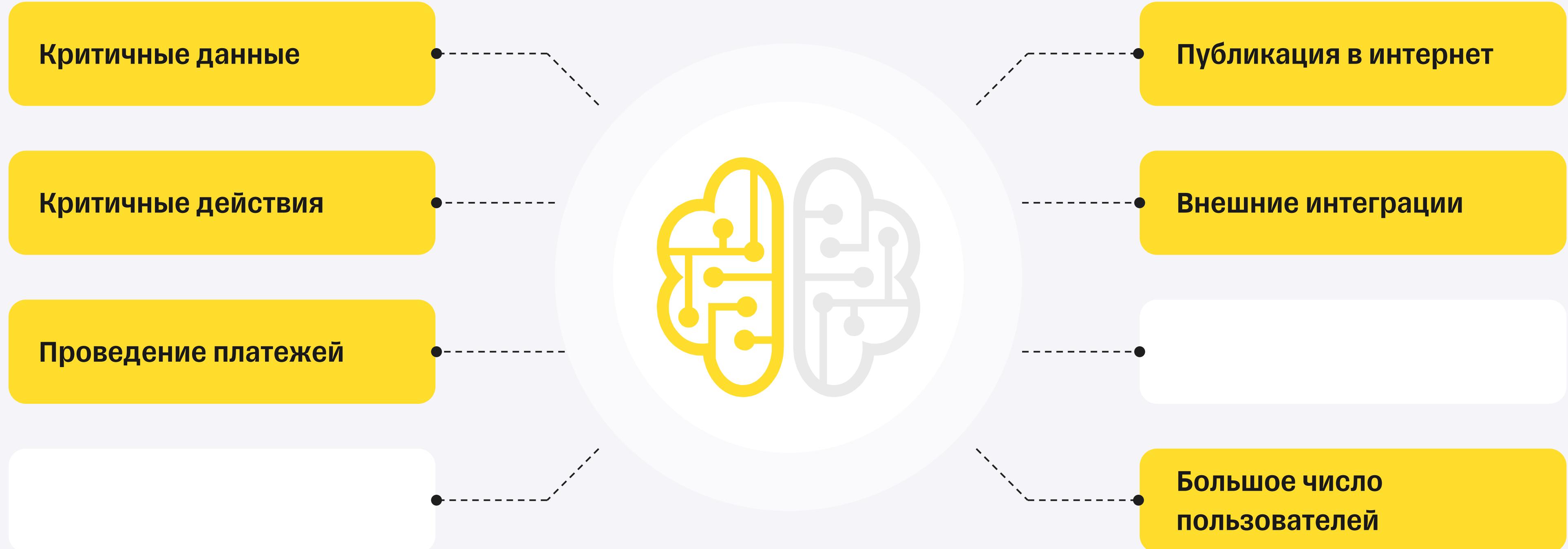
MITRE ATT&CK



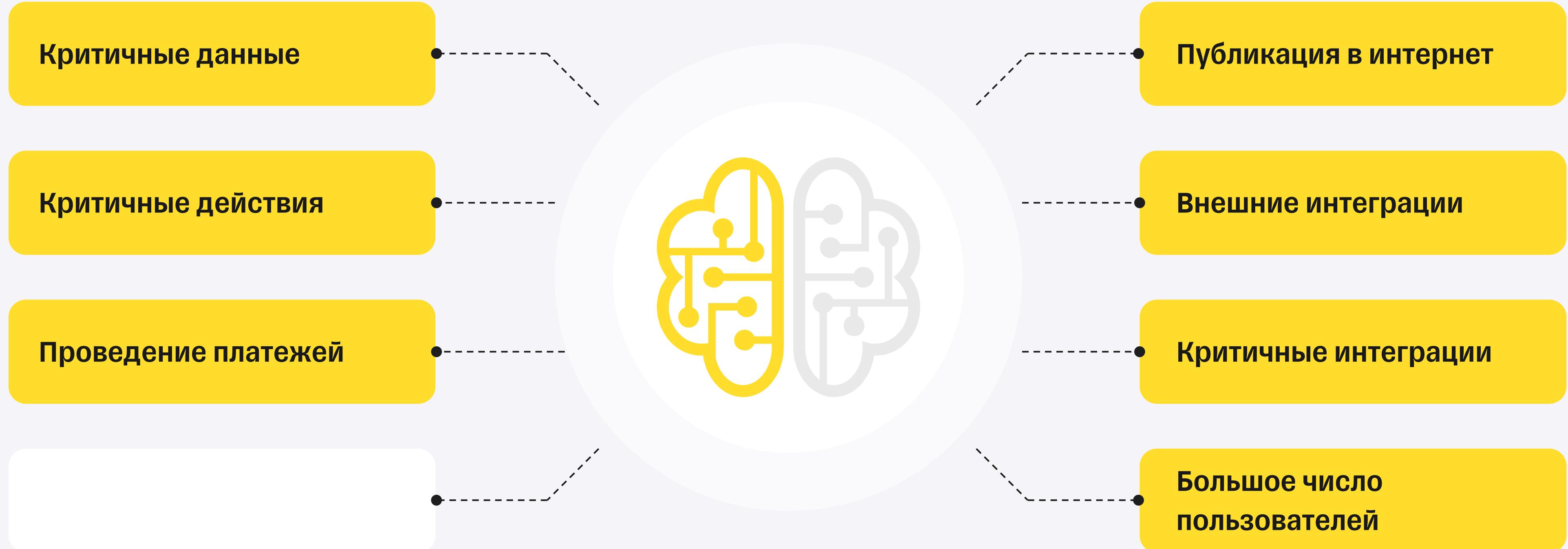
MITRE ATT&CK



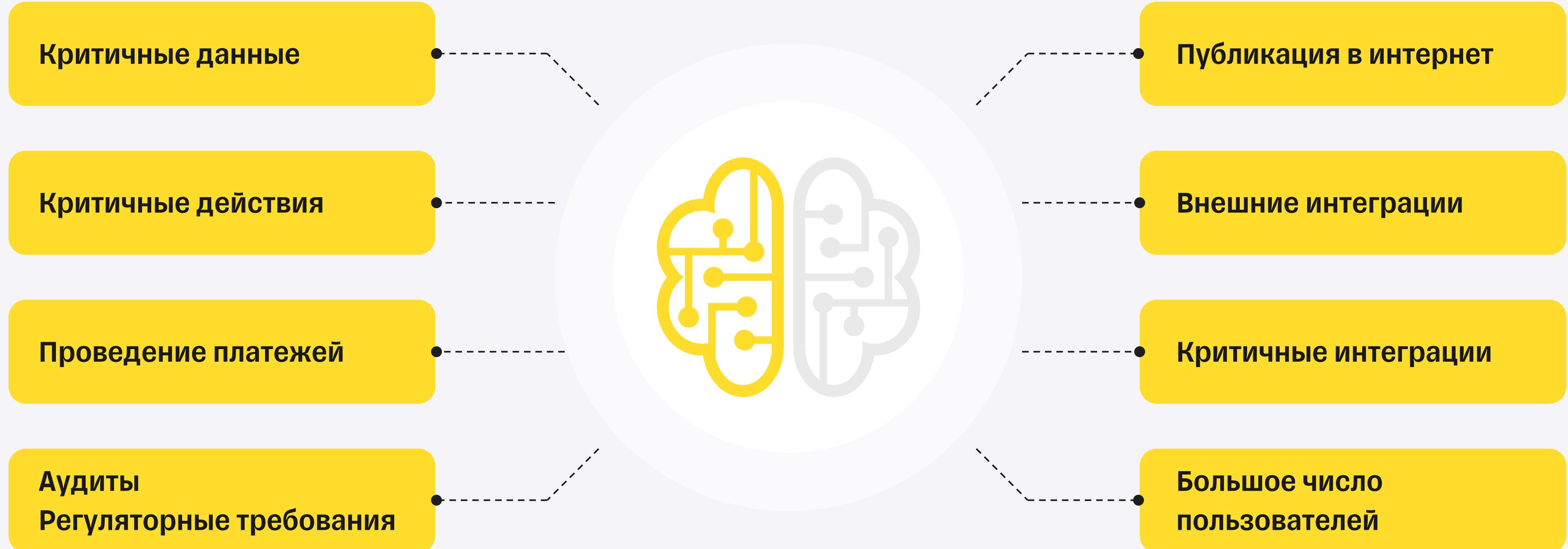
Критичность



Критичность



Критичность

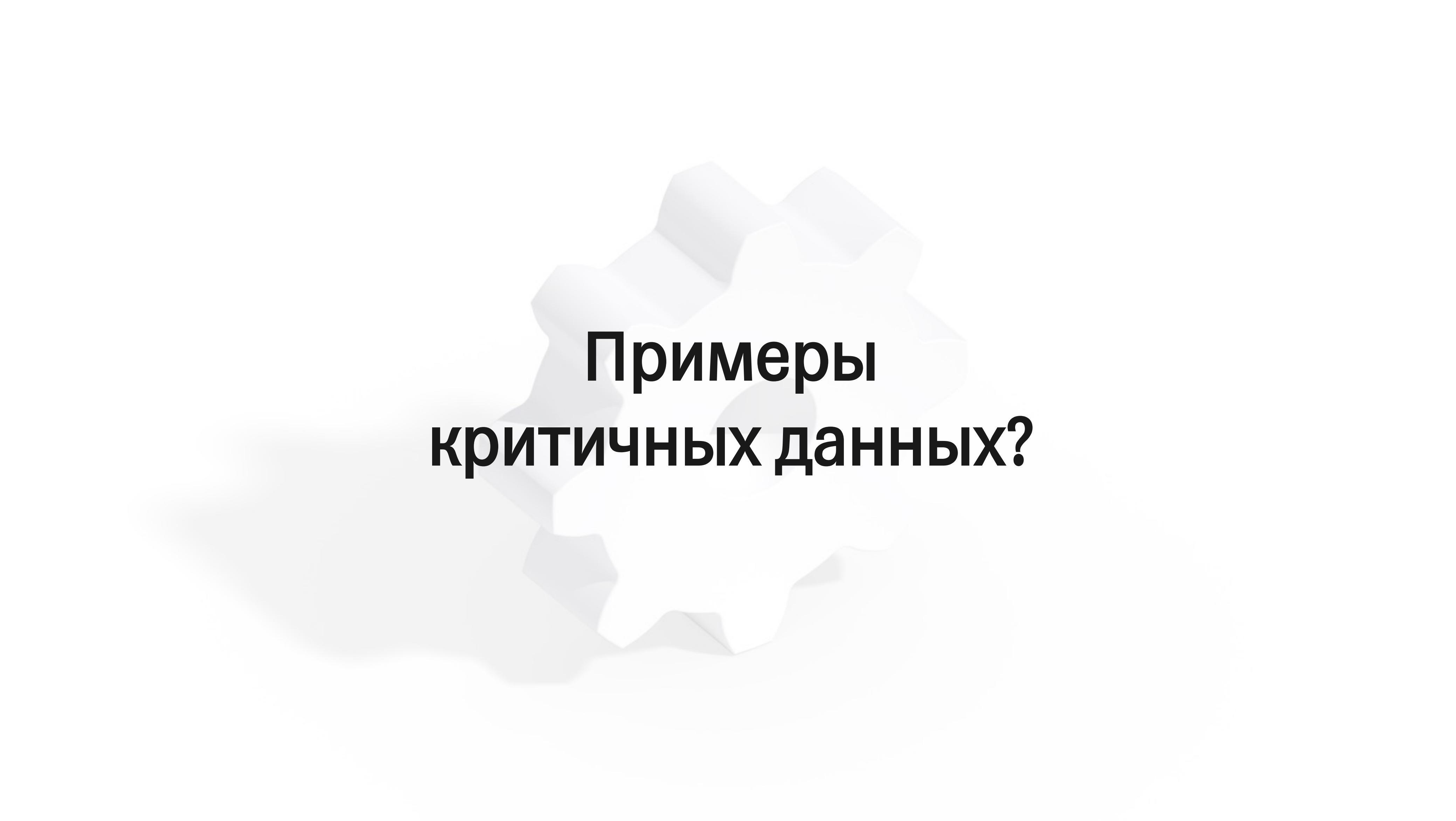




ТИНЬКОФФ

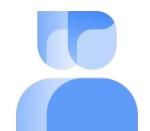
Критичность

Примеры



Примеры критичных данных?

Критичные данные



Персональные данные

Требования Бизнеса

Требования ФЗ-152



Платежные данные

Требования Бизнеса

Требования ЦБ РФ, Требования PCI DSS



Аутентификационные данные

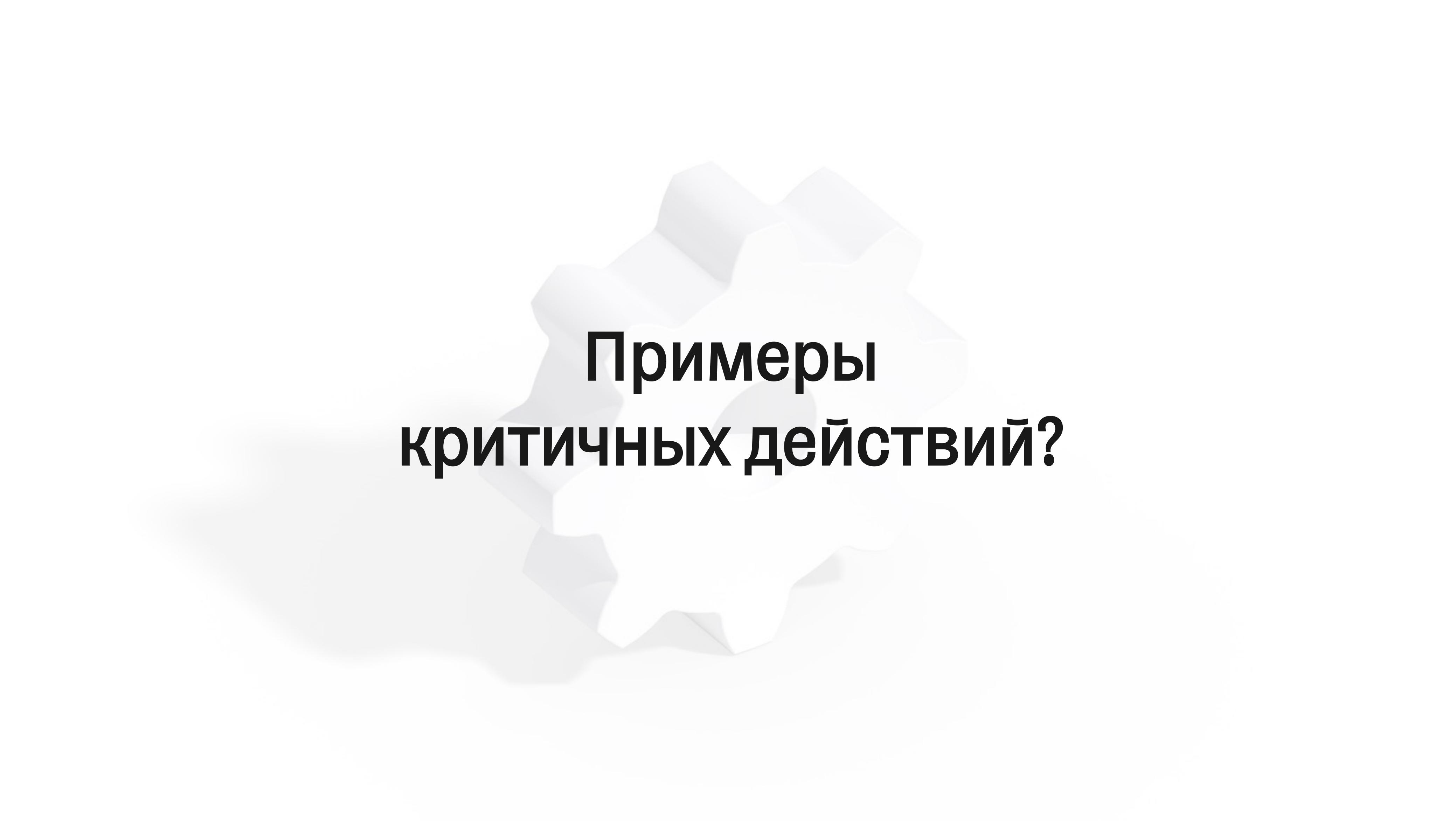
Требование ИБ, связано с реализацией
требований Бизнеса и Регуляторов



Тайна

Банковская, Государственная,

Коммерческая, Связи, Медицинская

The background of the slide features a subtle, abstract geometric pattern composed of overlapping white shapes. These shapes resemble stylized, rounded rectangles or facets, creating a sense of depth and texture without distract from the central text.

**Примеры
критических действий?**

Критичные действия



Блокировка

Карты, номера, токена, аккаунта, счета, клиента, услуги



Управление бонусами и акциями

Начисление списание бонусов, включение в акцию, управление компенсациями



Сброс/замена/перенос

Пароля, токена, SIM/банковской карты, второго фактора, кодового слова



Дубликация/дедубликация

Клиента, абонента

Типовые НПА

Критичные данные



Международные

PCI DSS



РФ

- ФСТЭК - 187-ФЗ П-239 и П-235, 127ПП о КИИ
- РКН - 152 ФЗ, 1119 ПП, П-21 и П-17 ПДн
- ЦБ РФ:
Банки - 683-п, 719-п, 802-п, 787-п, 779-п, 716-п
НФО - 757-п, ГОСТ.Р 57580.1



Других стран

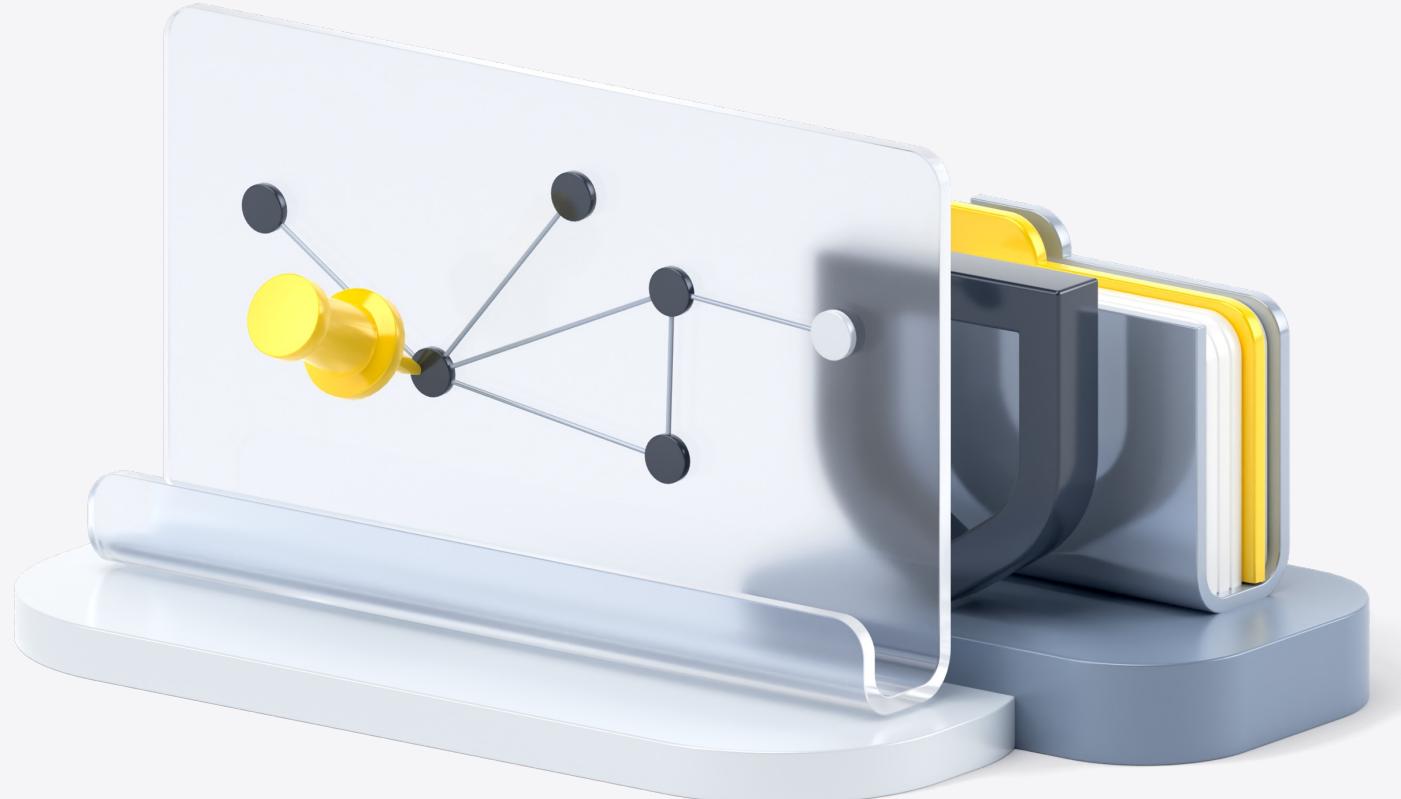
GDPR, HIPPA



ТИНЬКОФФ

Подключение других команд ИБ

Подключение Compliance



На базе типов данных

ПДн, Карточные данные,
Банковская тайна, Тайна связи



На базе процессов

Проведение платежей, Предоставление услуг
связи, Страхование, Брокерские услуги



В связи с отраслью компании

ИБ, Криптография, Банки, Брокеры,
Операторы и т.п.



Объекты [ЗО]КИИ



Security By Design



Asset classification

Security By Design

→ Asset classification

→ Expect attacks

→ Avoid security through obscurity

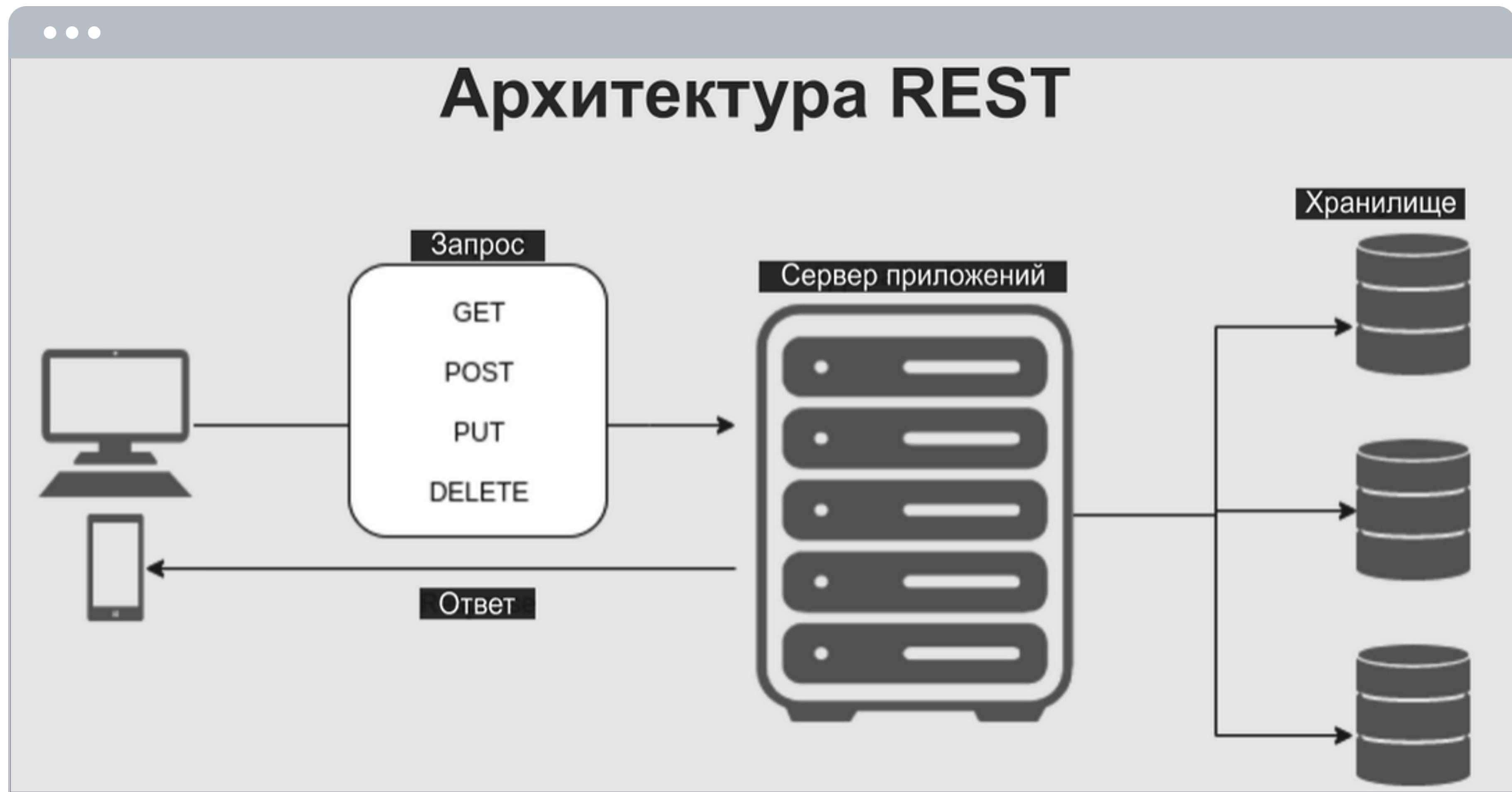
Security By Design

- Asset classification
- Expect attacks
- Avoid security through obscurity
- Minimize attack surface area
- Principle of Least privilege
- Principle of Defense in depth
- Separation of duties
- Keep security simple

Security By Design

Expect attack

Expect attack



Avoid security through obscurity

Avoid security through obscurity

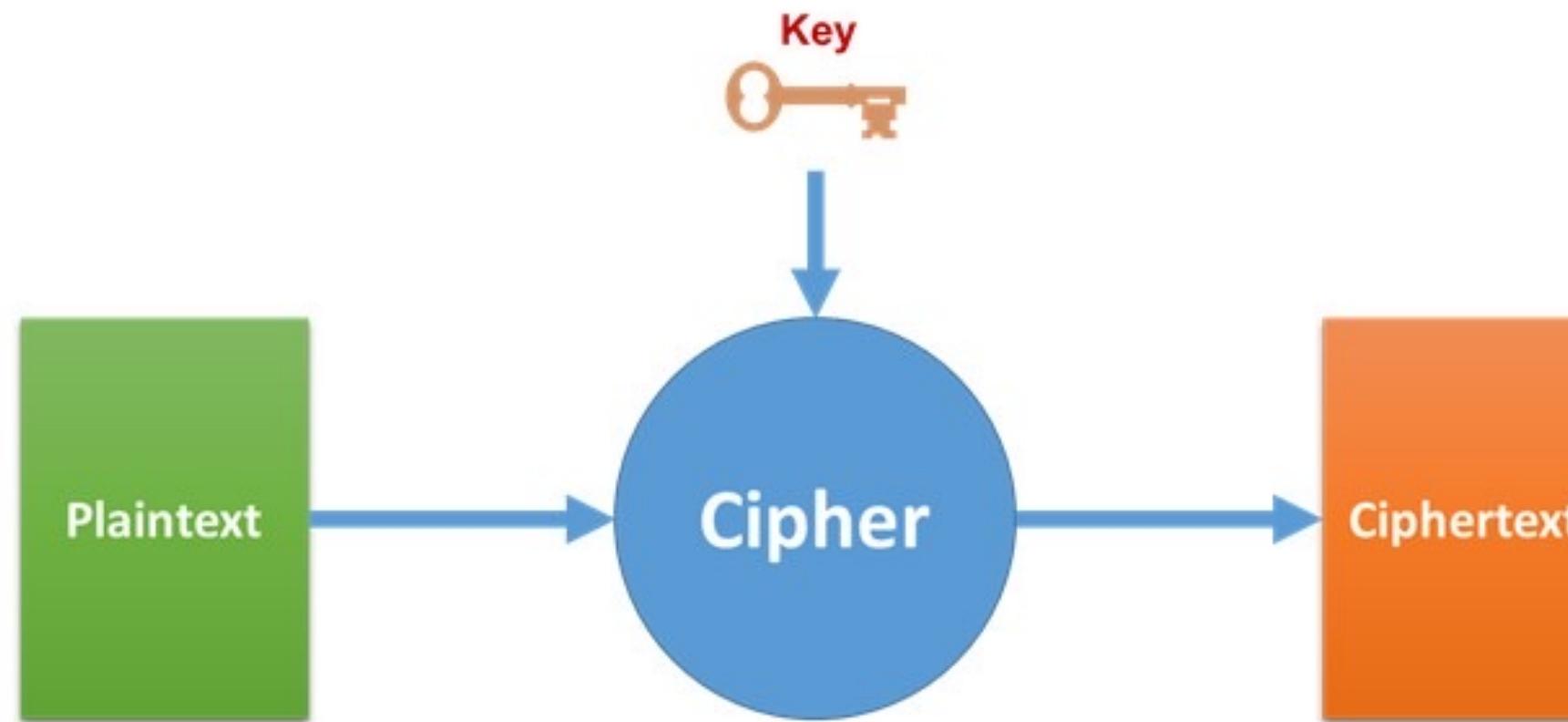


Avoid security through obscurity

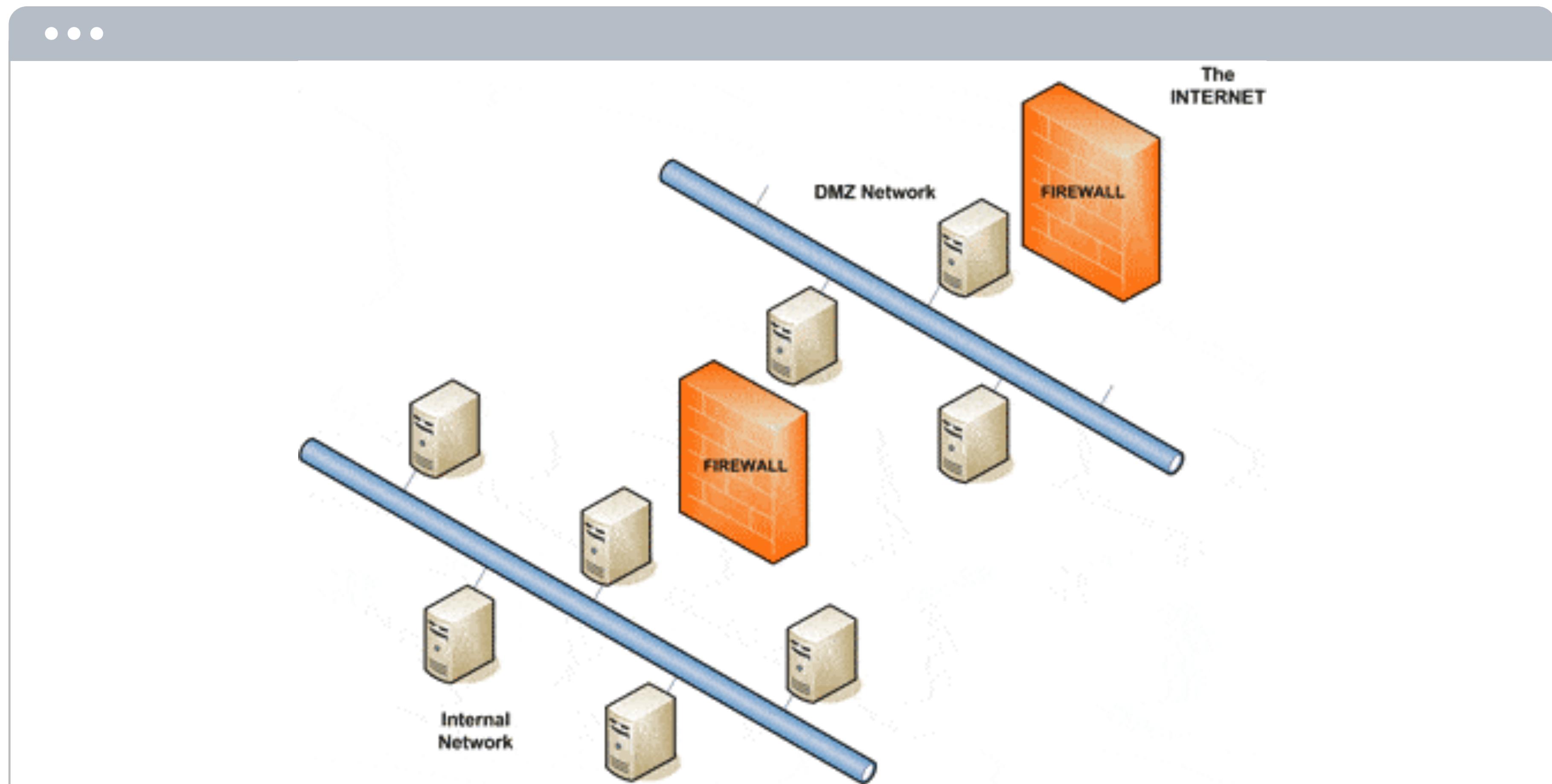
...

The Kerchoff Principle

- A cryptographic system should be secure even if everything about the system, **except the key**, is public knowledge.



Minimize attack surface area



Минимизация поверхности атаки

Сетевой уровень

Уровень компонентов
приложения

Приложение

Минимизация поверхности атаки

Сетевой уровень

- Сетевая сегментация
- Запрещенные порты, протоколы
- VPN
- Сокращение периметра

Уровень компонентов приложения

- Аутентификация
- Роли/группы доступа
- Secure in transit

Приложение

- Минимизация предоставляемых/
запрашиваемых данных

Principle of Least privilege

Principle of Least privilege

Администраторы
системы

Пользователи
системы

Приложение

Значимость этих проблем
настолько очевидна, что начало
повседневной

Principle of Least privilege

Администраторы системы

- Число администраторов

Пользователи системы

- Число пользователей
- Соответствие пользователя и доступной ему роли

Приложение

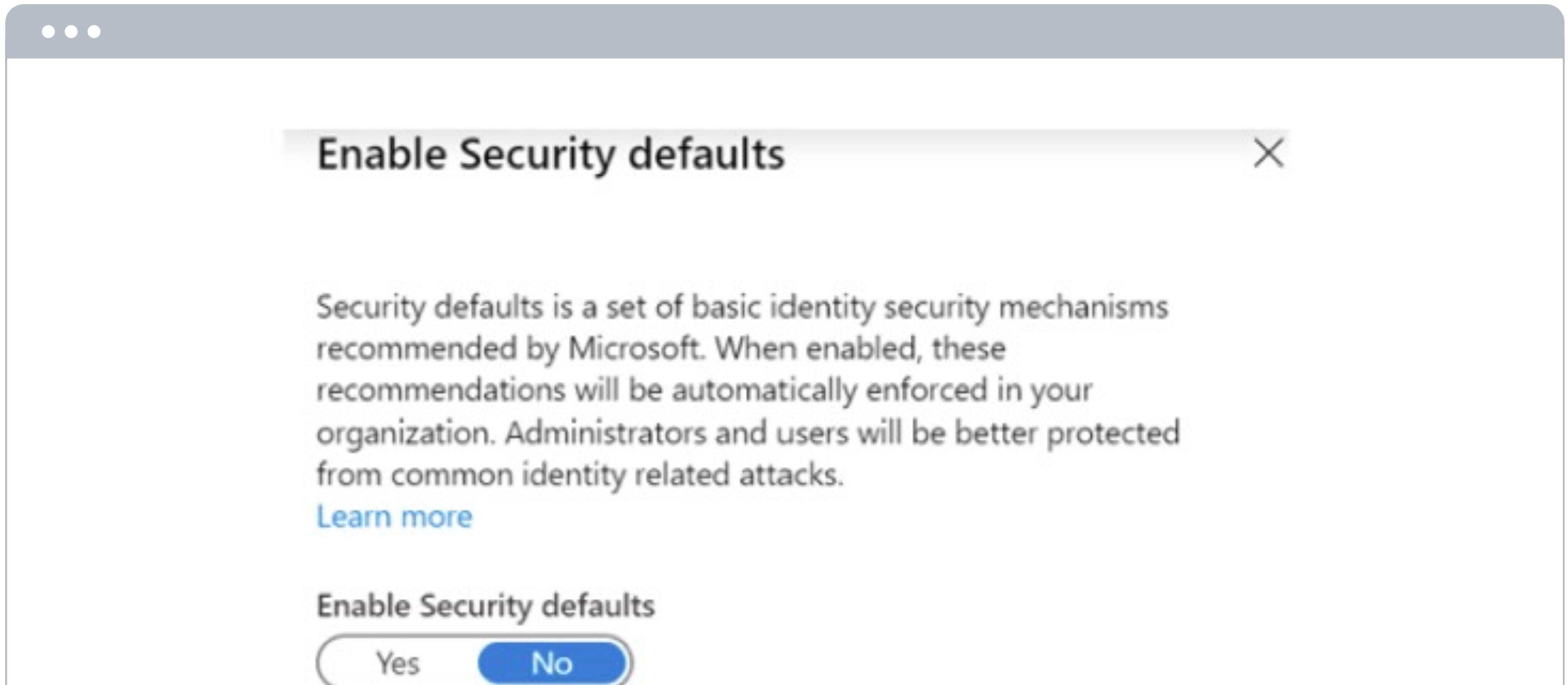
- Внедрение необходимой ролевой модели
- Минимизация критических данных/ функций для каждой роли
- Не хранить лишнее

Secure By default

Secure By default

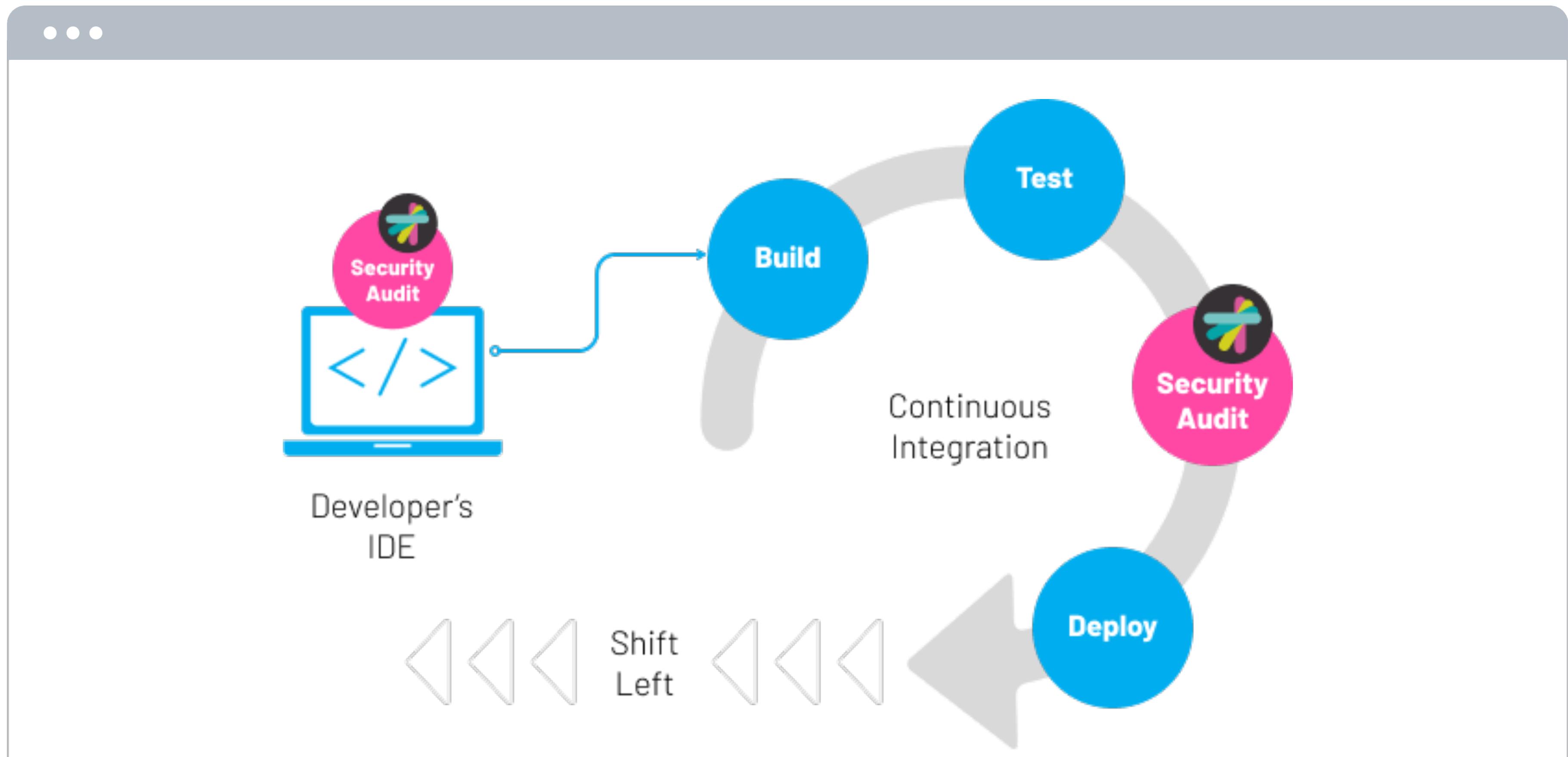


Principle of Defense in depth



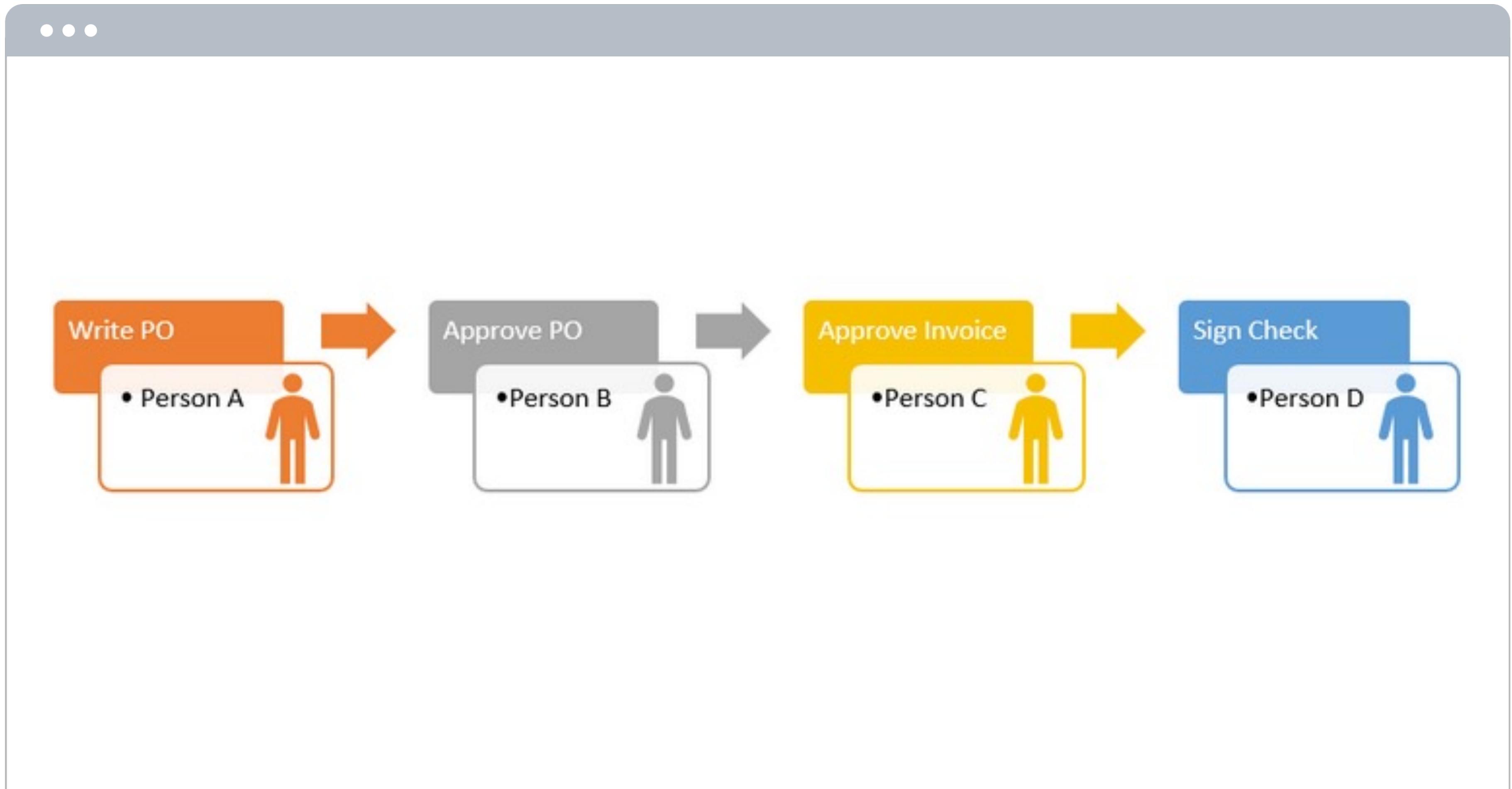
Principle of Defense in depth

Principle of Defense in depth



Separation of duties

Separation of duties



Separation of duties

The diagram illustrates the concept of Separation of Duties. It features two user icons: one purple icon labeled "key admin" with three interlocking gears below it, and one green icon labeled "DBA/Dev" with a database cylinder icon below it. A blue airplane icon is positioned between the two users. The title "Separation of Duties" is displayed above the users in a green, underlined font.

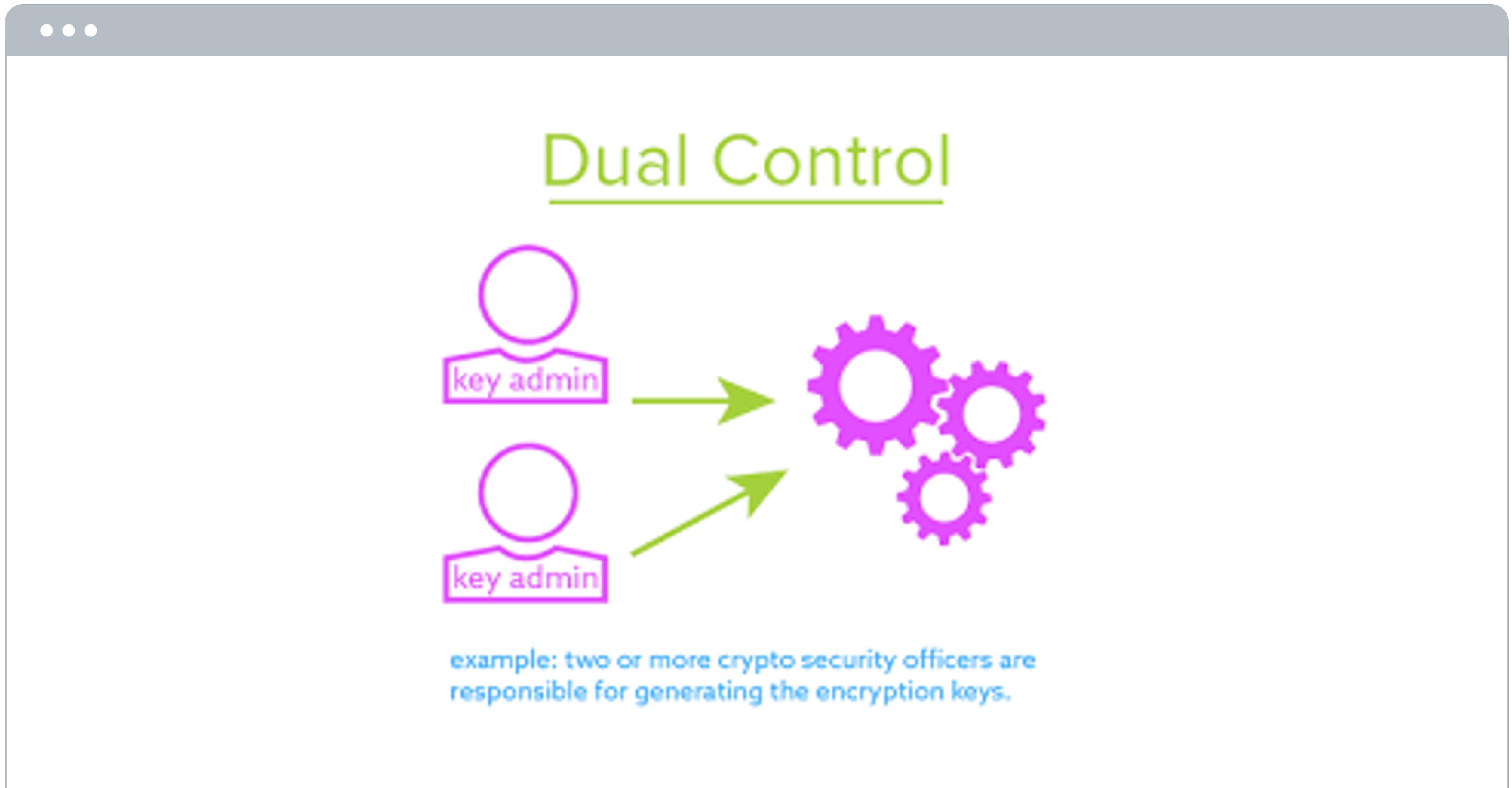
Separation of Duties

key admin

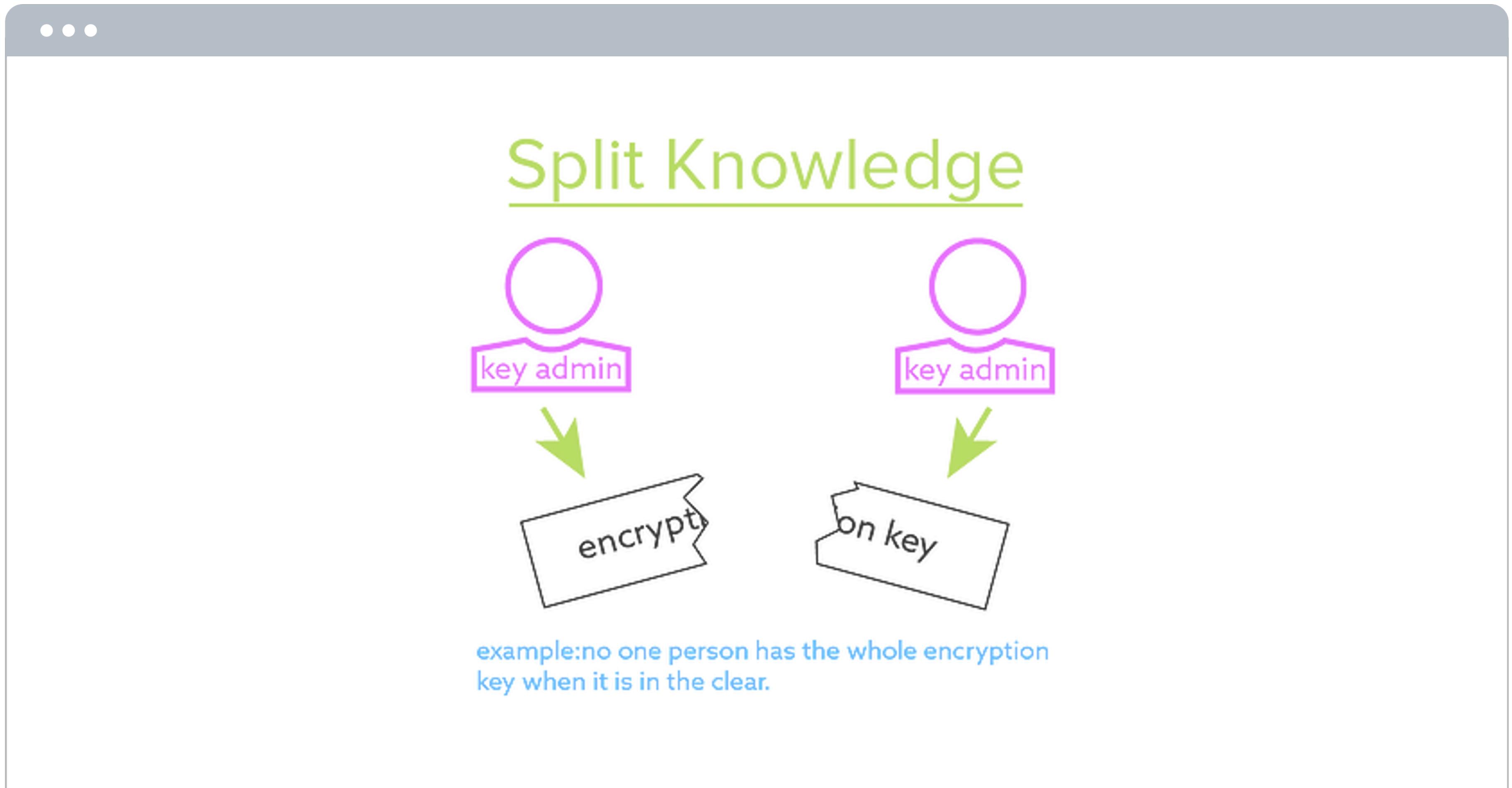
DBA/Dev

example: the crypto security officer is not allowed access to the encrypted data and the data user is not allowed to create/manage keys

Separation of duties

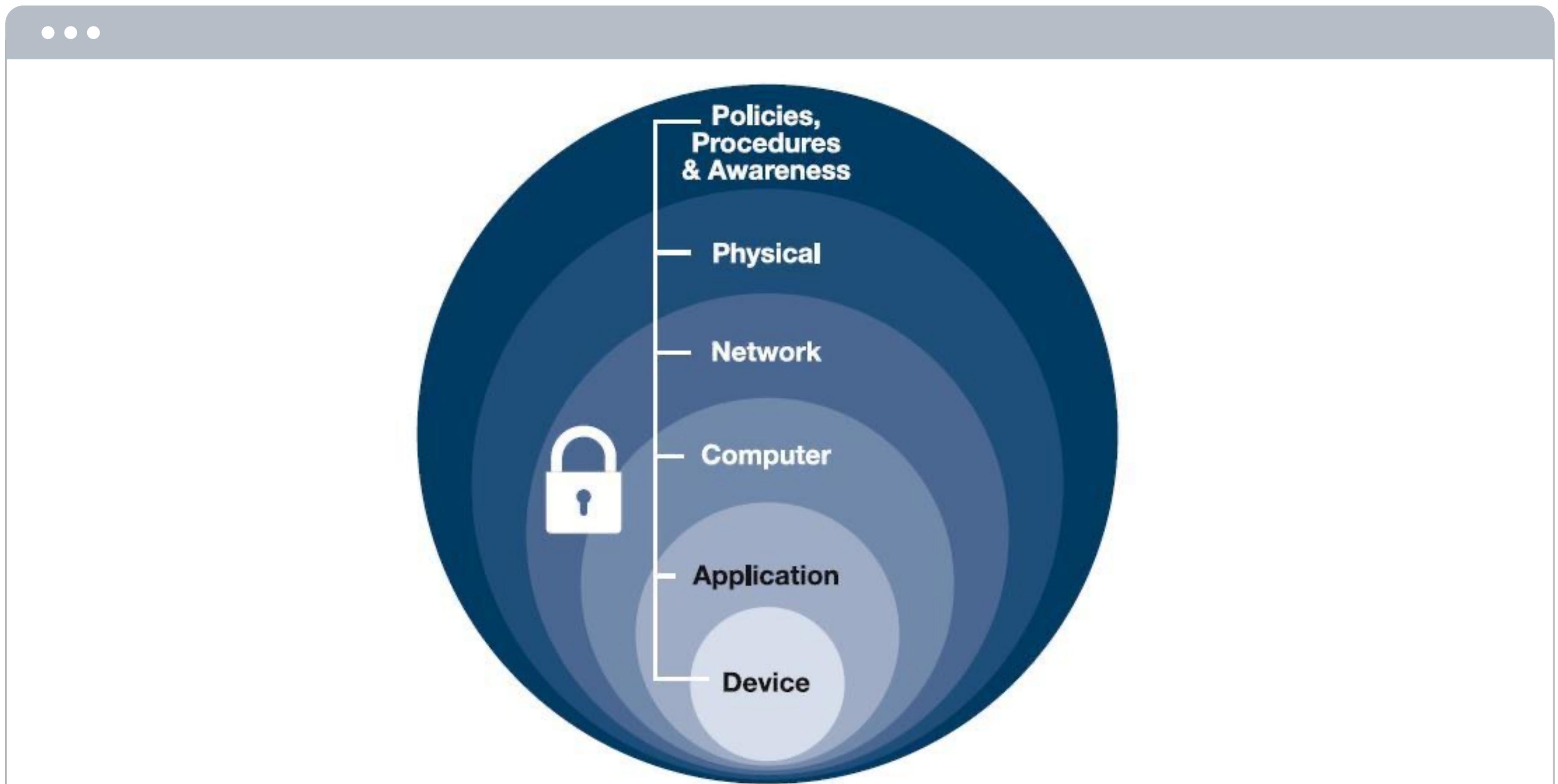


Separation of duties



Principle of Defense in depth

Principle of Defense in depth



Principle of Defense in depth

Сетевой уровень

- Сетевая сегментация
- Запрещенные порты, протоколы
- VPN
- Сокращение периметра

Уровень компонентов приложения

- Аутентификация
- Роли/группы доступа
- Secure in transit

Приложение

- Минимизация предоставляемых/запрашиваемых данных



ТИНЬКОФФ

Конец ч.1