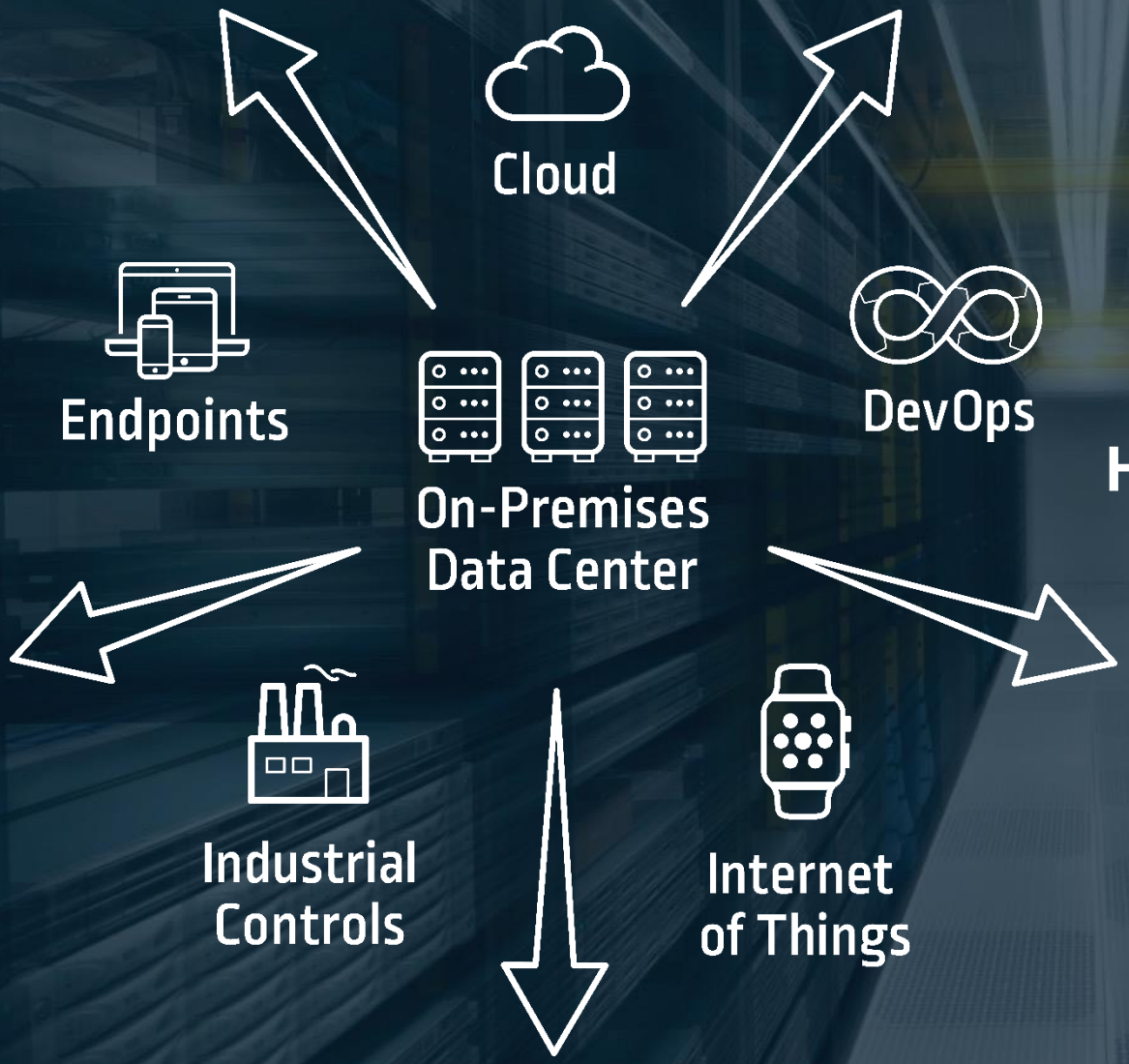

# SOC, НЕДООЦЕНЁННЫЕ ТЕХНОЛОГИИ

Олег Котов, CISSP
Account Executive, Russia & CIS

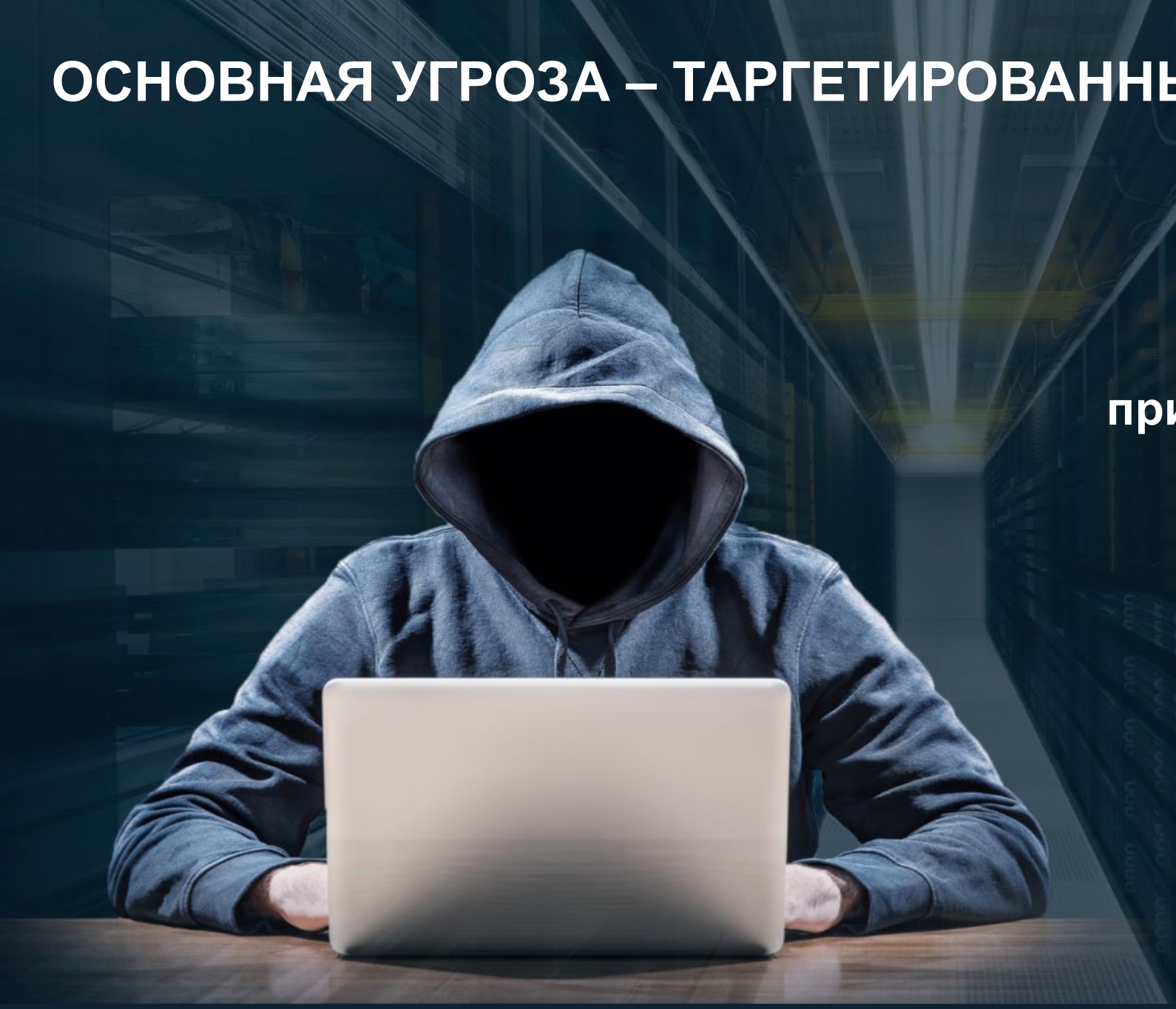
# ПОВЕРХНОСТЬ АТАКИ ПРОДОЛЖАЕТ РАСТИ И ЭТО ОТРАЖАЕТСЯ НА ЗАДАЧАХ SOC




**Не мониторинг событий, а предотвращение инцидентов**

**Не сбор данных для анализа группой специалистов, а максимальная автоматизация всех процессов обнаружения, реагирования и аналитики**

# ОСНОВНАЯ УГРОЗА – ТАРГЕТИРОВАННЫЕ АТАКИ



**Войти незамеченным**

**Поиск засвеченных привилегированных аккаунтов**

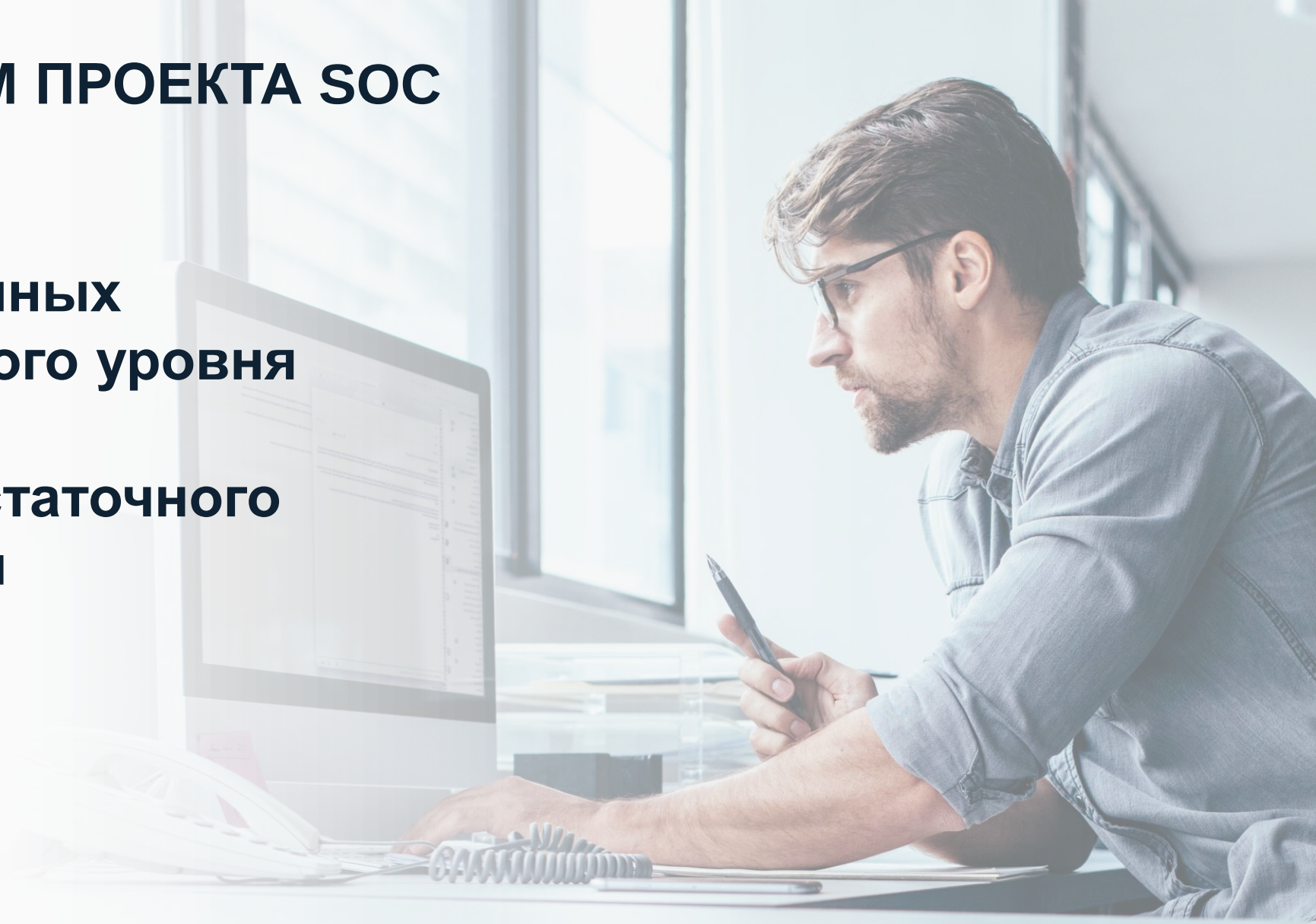
**Эксплуатация известных уязвимостей**

**Получить доступ в обход средств защиты**

# ТИПОВЫЕ ПРОБЛЕМ ПРОЕКТА SOC

1. **Острая нехватка квалифицированных кадров экспертного уровня**

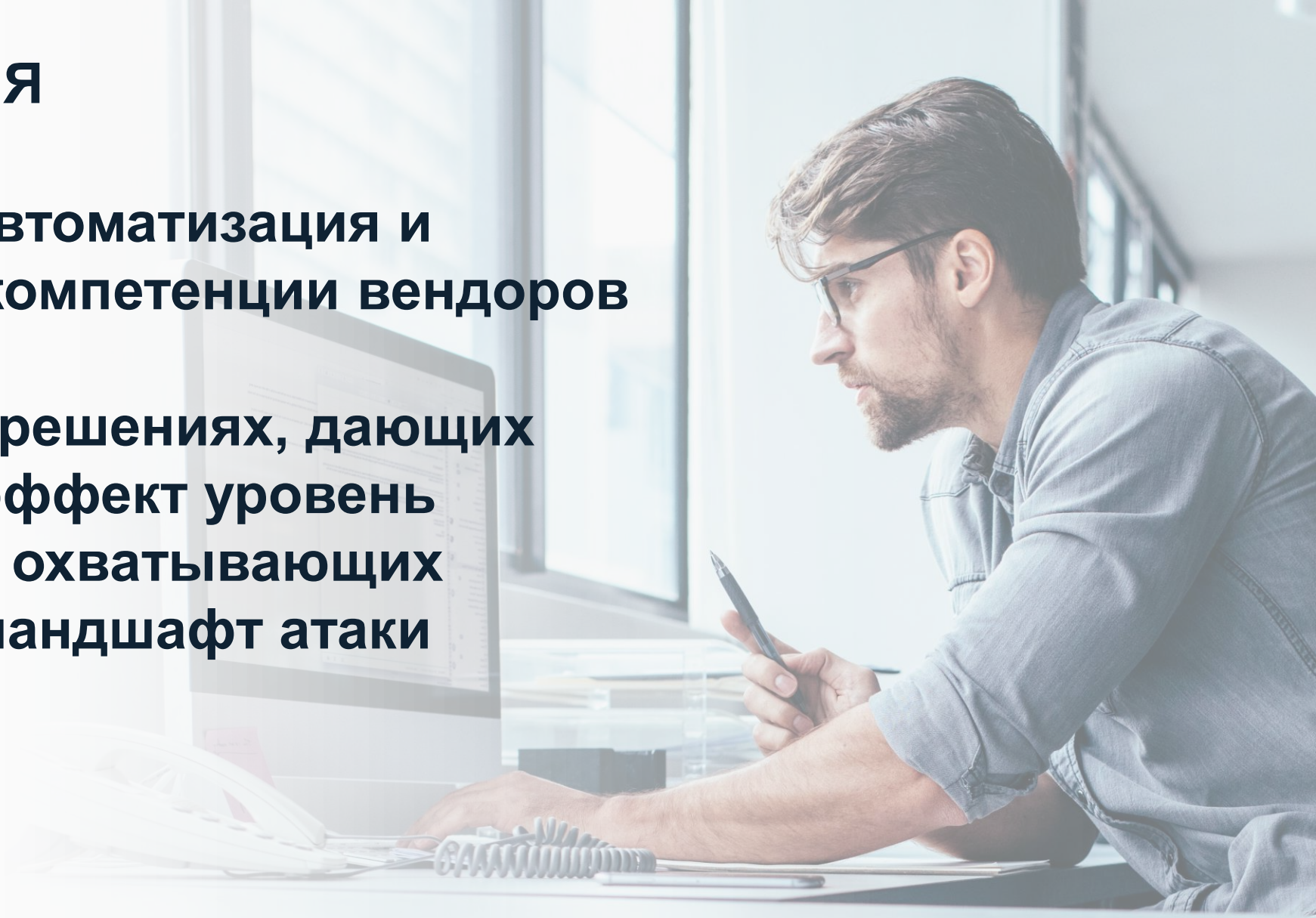
2. **Проблемы недостаточного финансирования**



# СПОСОБЫ РЕШЕНИЯ

1. **Максимальная автоматизация и использование компетенции вендоров**

2. **Фокусировка на решениях, дающих максимальный эффект уровень защищённости и охватывающих максимальный ландшафт атаки**




CYBERARK
ПРИВИЛЕГИИ
ПРИВИЛЕГИРОВАННЫЕ АККАУНТЫ
ПРИВИЛЕГИРОВАННЫЙ ДОСТУП
CYBERARK CORE PAS SOLUTION

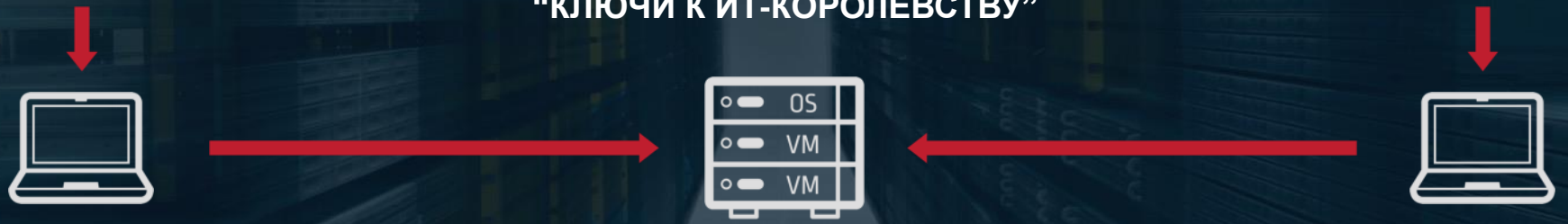
# ПРИВИЛЕГИРОВАННЫЕ АККАУНТЫ – “КЛЮЧИ К ИТ-КОРОЛЕВСТВУ”

ВНЕШНИЙ АТАКУЮЩИЙ


ПРИВИЛЕГИРОВАННЫЕ АККАУНТЫ

“КЛЮЧИ К ИТ-КОРОЛЕВСТВУ”

ВНУТРЕННИЙ ЗЛОУМЫШЛЕННИК

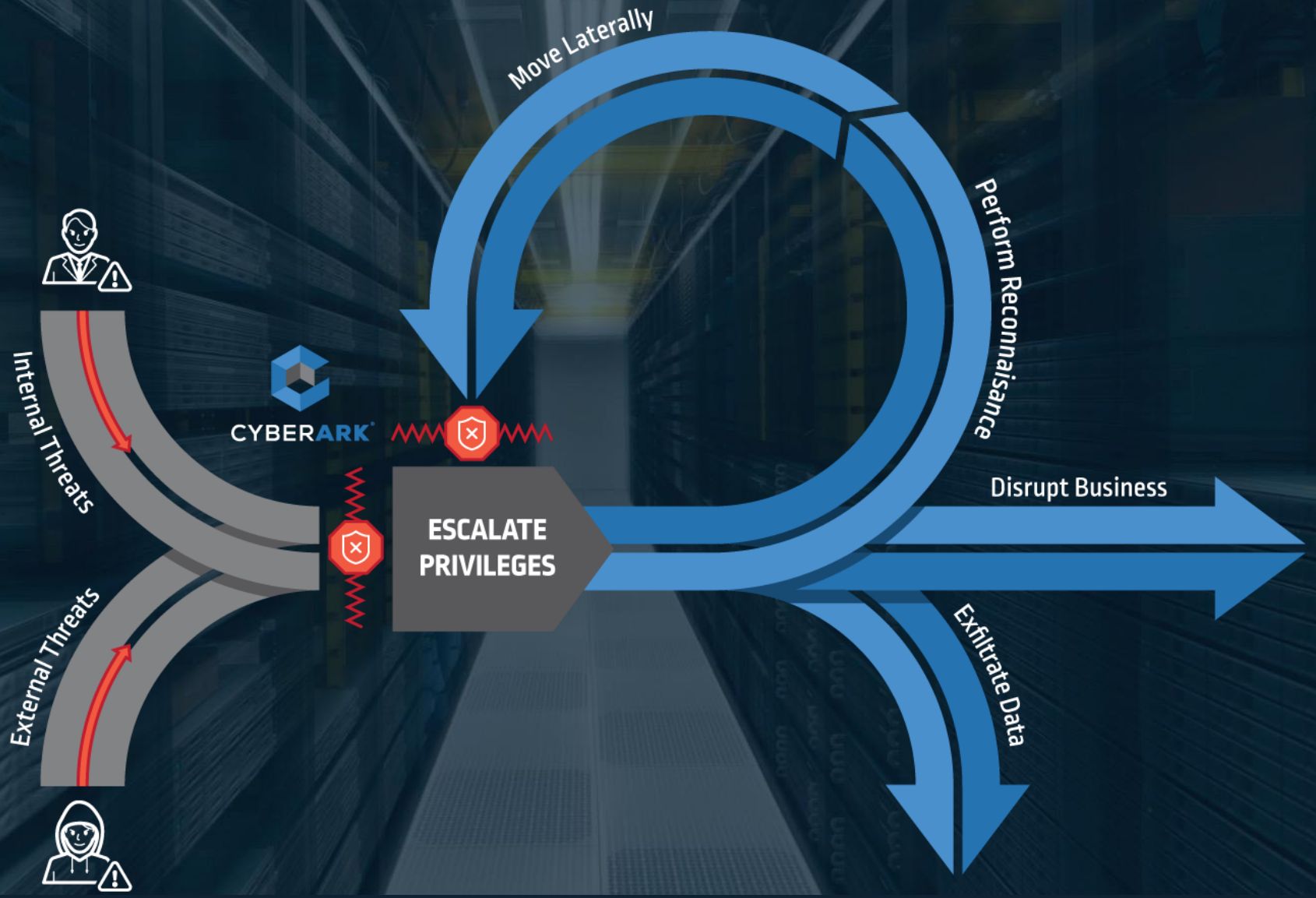



CYBERARK®

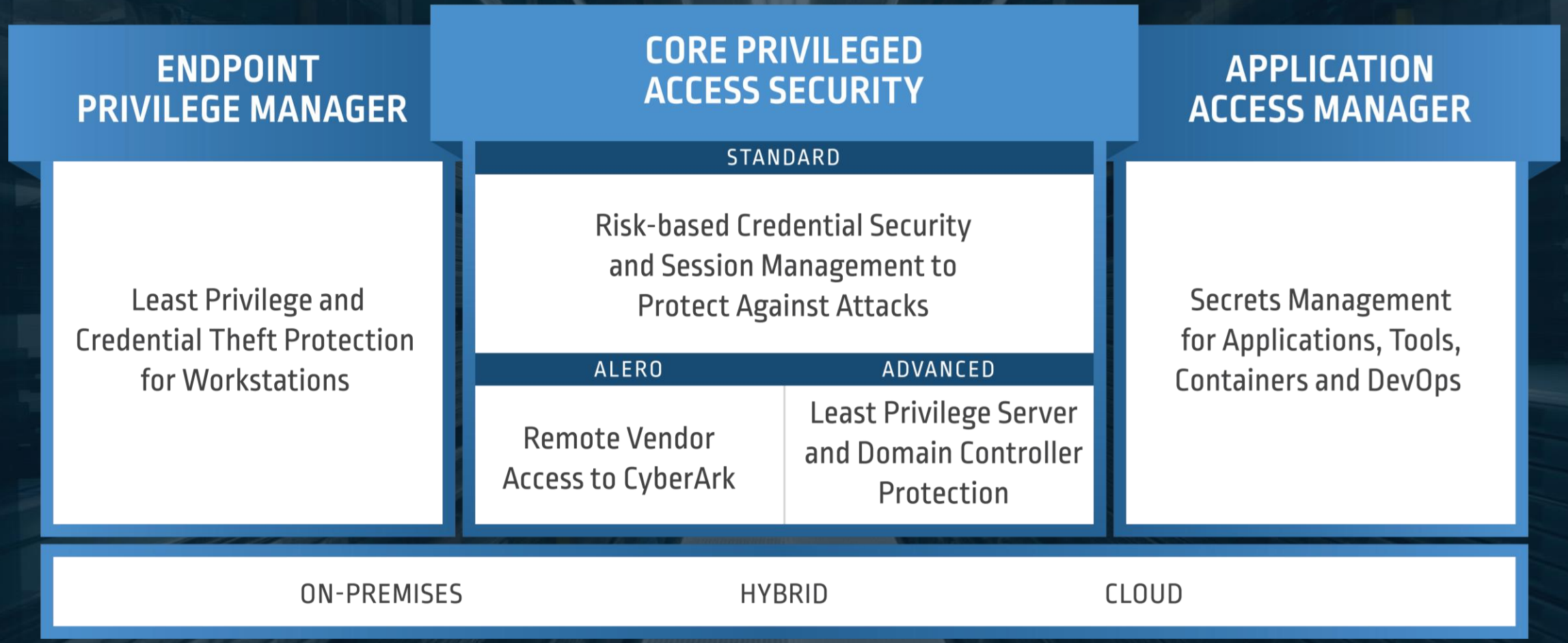
ПРЕДОСТАВЛЯЕТ ПРОАКТИВНУЮ

ЗАЩИТУ И ОБНАРУЖЕНИЕ

# ПРОАКТИВНАЯ ЗАЩИТА ИЗНУТРИ

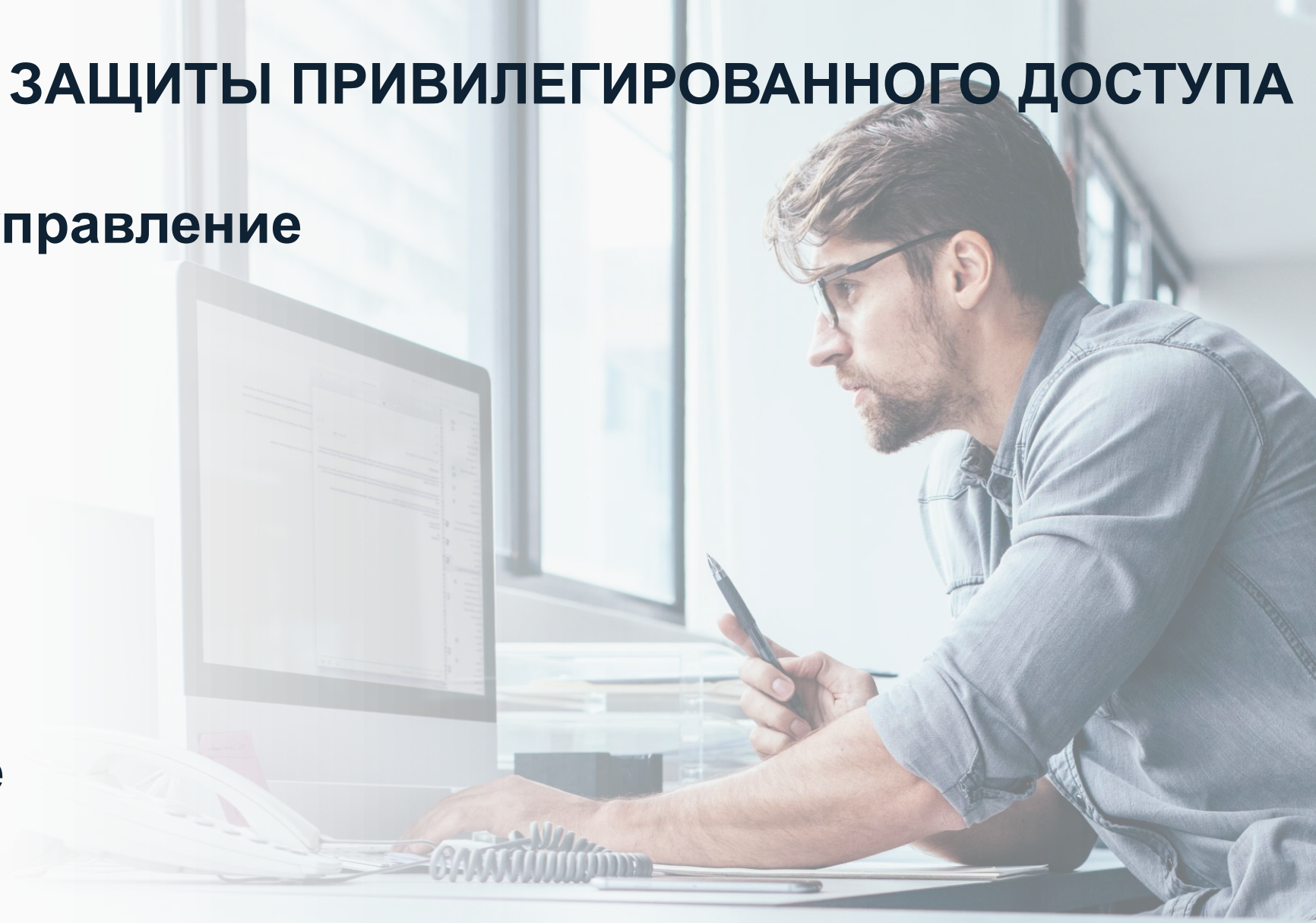


# ПРОАКТИВНАЯ ЗАЩИТА ИЗНУТРИ

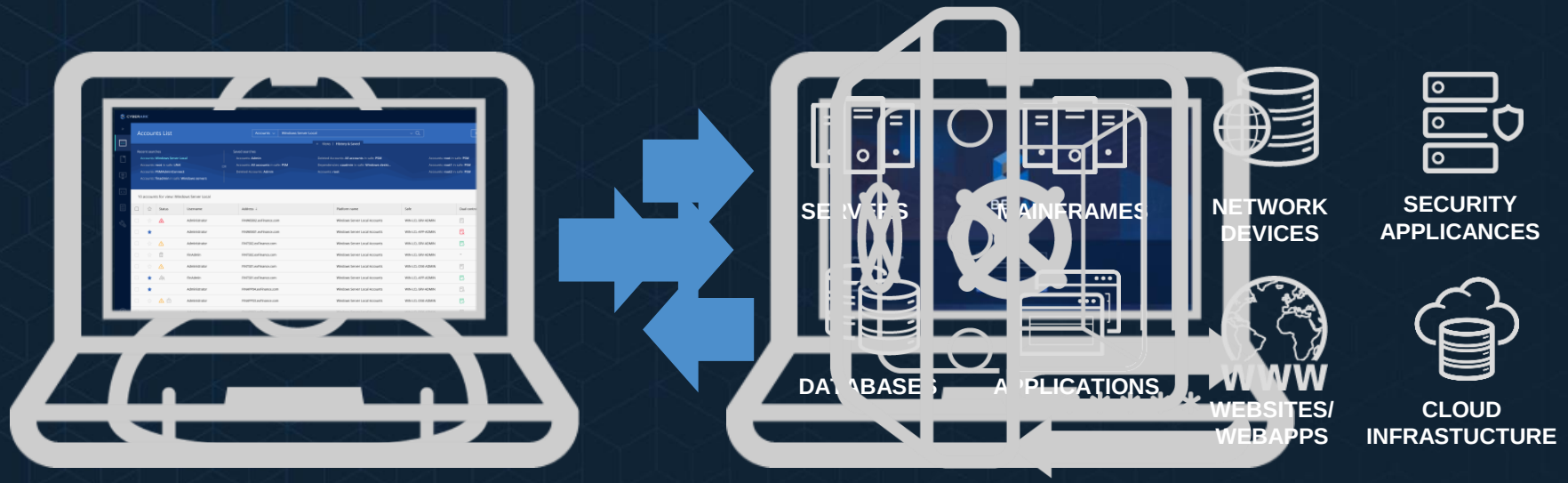


# ЗОЛОТОЙ СТАНДАРТ ЗАЩИТЫ ПРИВИЛЕГИРОВАННОГО ДОСТУПА

1. Обнаружение и управление
2. Изоляция сред
3. Запись и аудит
4. Мониторинг
5. Предотвращение



# ЗАЩИТА УЧЕТНЫХ ДАННЫХ НА ОСНОВЕ РИСКОВ




## *Автоматическая ответная реакция*

**АВТОМАТИЧЕСКАЯ РОТАЦИЯ УЧЕТНЫХ ДАННЫХ В СЛУЧАЕ КОМПРОМЕТАЦИИ ИЛИ КРАЖИ**

CYBERARK

# ЗАЩИТА УЧЕТНЫХ ДАННЫХ НА ОСНОВЕ РИСКОВ

## *Обнаружение*

**СКАНИРОВАНИЕ НА ПРЕДМЕТ ОБНАРУЖЕНИЯ ПРИВИЛЕГИРОВАННЫХ УЧЕТНЫХ ДАННЫХ И АККАУНТОВ**

## *Контроль*

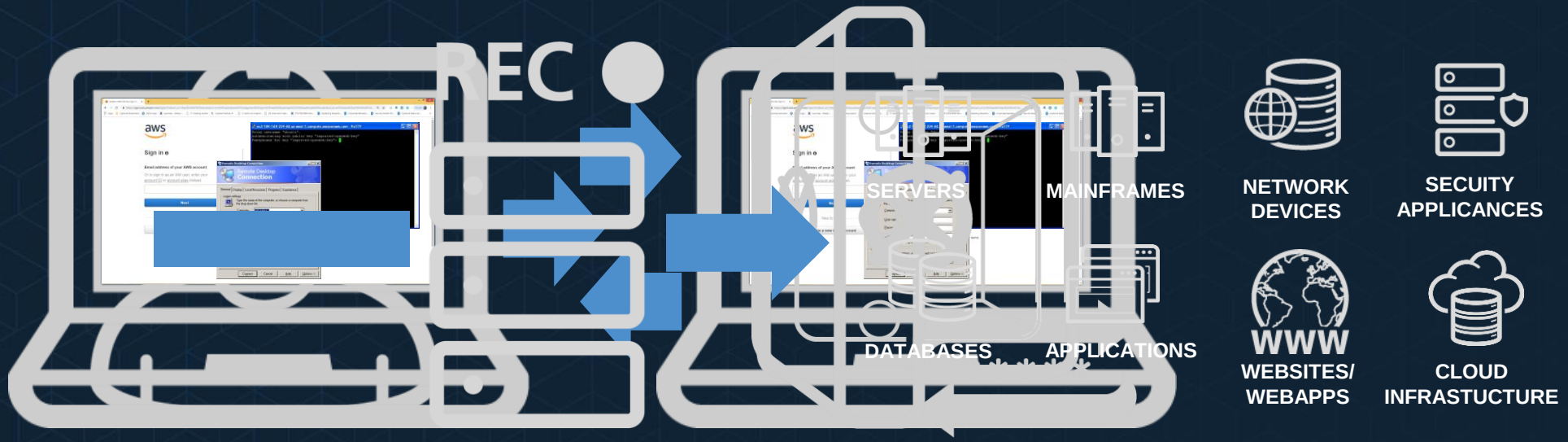
**ПОМЕЩЕНИЕ ПОД КОНТРОЛЬ И ВАЛИДАЦИЯ ПРИВИЛЕГИЙ**

## *Управление*

**ИСПОЛНЕНИЕ ПАРОЛЬНОЙ ПОЛИТИКИ**

CYBERARK

# УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМИ СЕАНСАМИ




## *Автоматическая ответная реакция*

**ПАУЗА ИЛИ ПРЕКРАЩЕНИЕ ПРИВИЛЕГИРОВАННОГО СЕАНСА АВТОМАТИЧЕСКИ НА ОСНОВЕ ОЦЕНКИ РИСКА И АКТИВНОСТИ**

CYBERARK

# УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМИ СЕАНСАМИ

## *Изоляция*

**ОТДЕЛЕНИЕ ПОЛЬЗОВАТЕЛЬСКОЙ СРЕДЫ ОТ ПРИВИЛЕГИРОВАННОЙ ДЛЯ ПРЕДОТВРАЩЕНИЯ ПРОДВИЖЕНИЯ ЗЛОУМЫШЛЕННИКОМ**

## *Аудит*

**МОНИТОРИНГ, ОТСЛЕЖИВАНИЕ И ОБНАРУЖЕНИЕ ПОДОЗРИТЕЛЬНЫХ ДЕЙСТВИЙ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ**

## *Запись*

**РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ С ИСПОЛЬЗОВАНИЕМ ДЕТАЛЬНЫХ ДАННЫХ АУДИТА**

CYBERARK

# МОДУЛЬ АНАЛИТИКИ


CYBERARK

# СПАСИБО

ОЛЕГ КОТОВ
ACCOUNT EXECUTIVE, RUSSIA & CIS

MOBILE +7 916 836 63 68
OLEG.KOTOV@CYBERARK.COM
WWW.CYBERARK.COM

CYBERARK