КОМПАНИЯ
ИНДИД

ПЕРЕОСМЫСЛЕНИЕ СИСТЕМ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

КОМПАНИЯ
ИНДИД

УЧЕТНЫЕ ДАННЫЕ ПОД УГРОЗОЙ

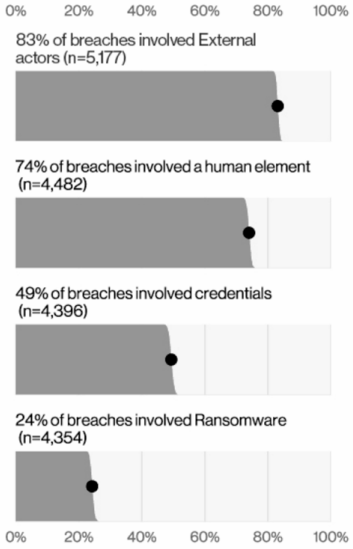


Figure 6. Select key enumerations

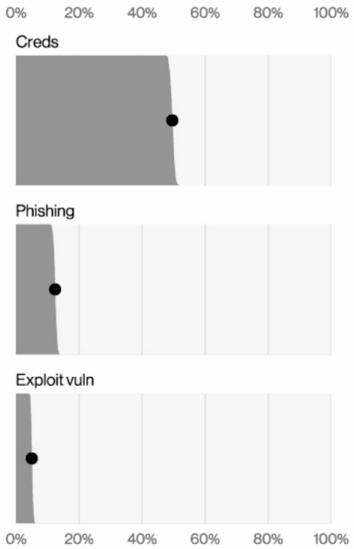


Figure 7. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.

The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

2023 Verizon Data Breach Investigations Report

КОМПАНИЯ
ИНДИД

АВТОМАТИЗАЦИЯ АТАК

BLOODHOUND

BARK
BLOODHOUND ATTACK RESEARCH KIT

КОМПАНИЯ
ИНДИД

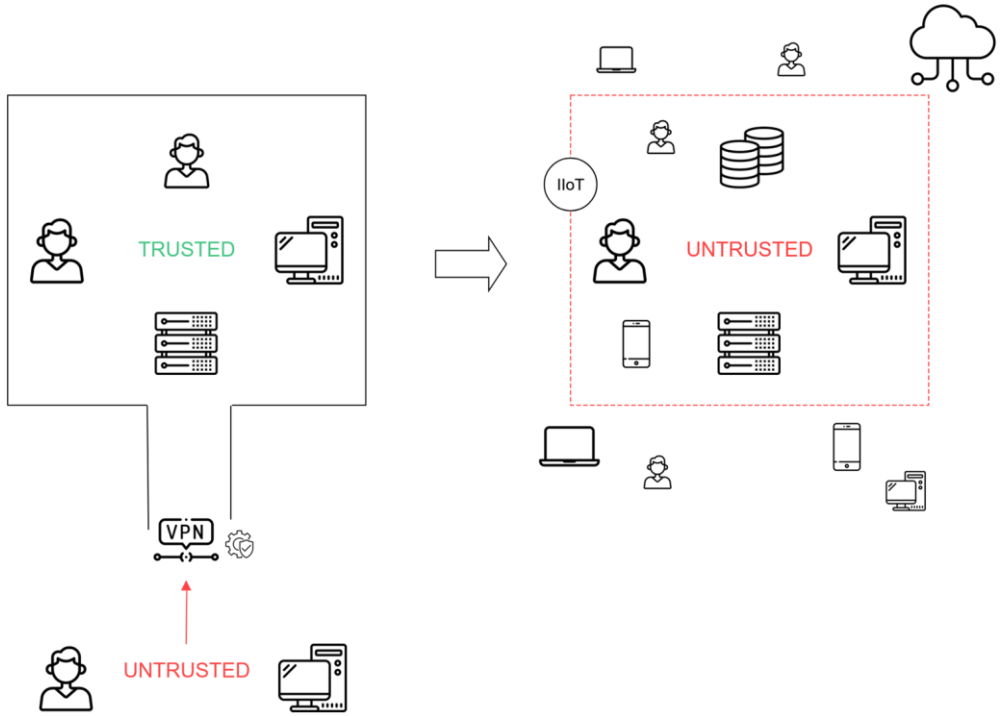
МОНЕТИЗАЦИЯ

- Ransomware
- Cryptojacking
- Продажа доступов в взломанным ресурсам
- Кража информации

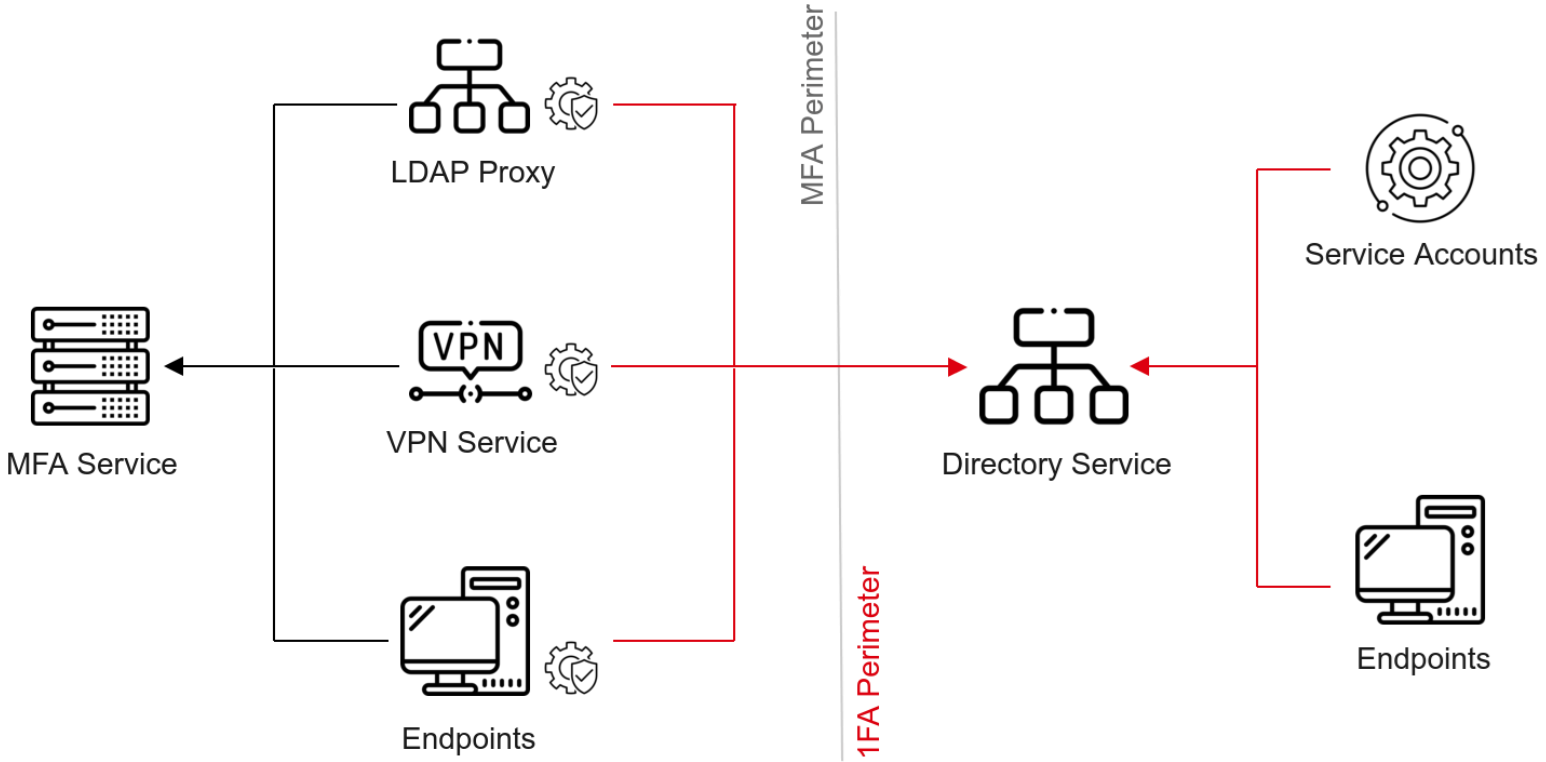
Результат: Усиление мотивации

КОМПАНИЯ
ИНДИД

ИСЧЕЗНОВЕНИЕ ПЕРИМЕТРА



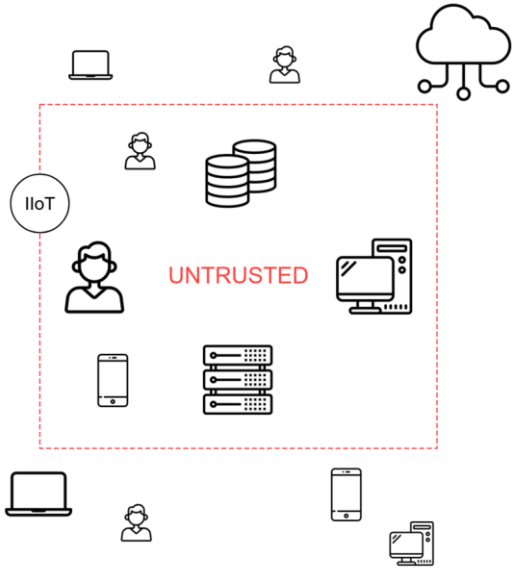
КОМПАНИЯ
ИНДИД



КОМПАНИЯ
ИНДИД

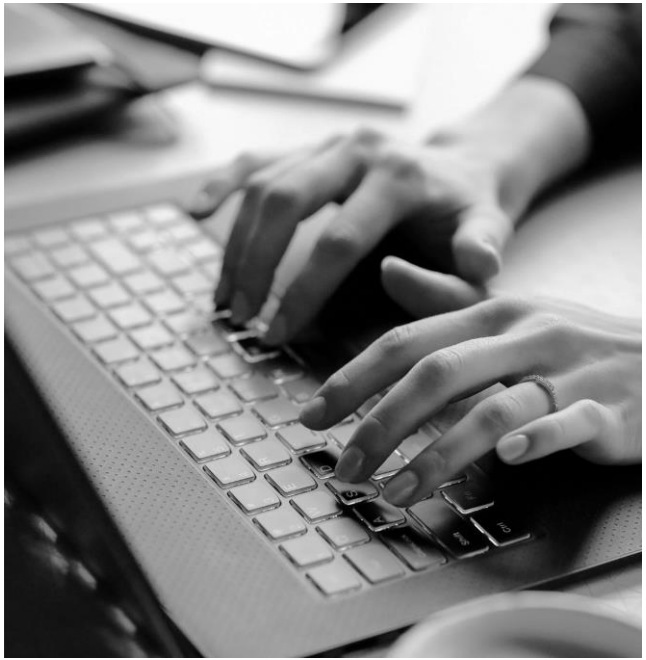
ПРОБЛЕМЫ ТРАДИЦИОННЫХ MFA-РЕШЕНИЙ

- Точечная интеграция в целевые системы
- Отсутствие возможности интеграции в некоторые системы и сценарии
- Необходимость применять несколько продуктов
- Акцент на пользовательские аккаунты
- Невозможность построения единой политики адаптивной аутентификации



КОМПАНИЯ
ИНДИД

РЕШЕНИЕ - INDEED ITDR



Адаптивная платформа многофакторная аутентификации, централизованно интегрируемая в корпоративную сеть и облачные ресурсы

- Не требует изменений на рабочих станциях
- Не требует установки прокси-серверов
- Не требует изменений на серверах приложений
- Противодействует многим известным атакам на учетные данные

КОМПАНИЯ
ИНДИД

ДЕТЕКТ И РЕАГИРОВАНИЕ НА АТАКИ

Без обогащения от других источников данных система может выявлять большинство известных атак на учетные данные и реагировать на них.

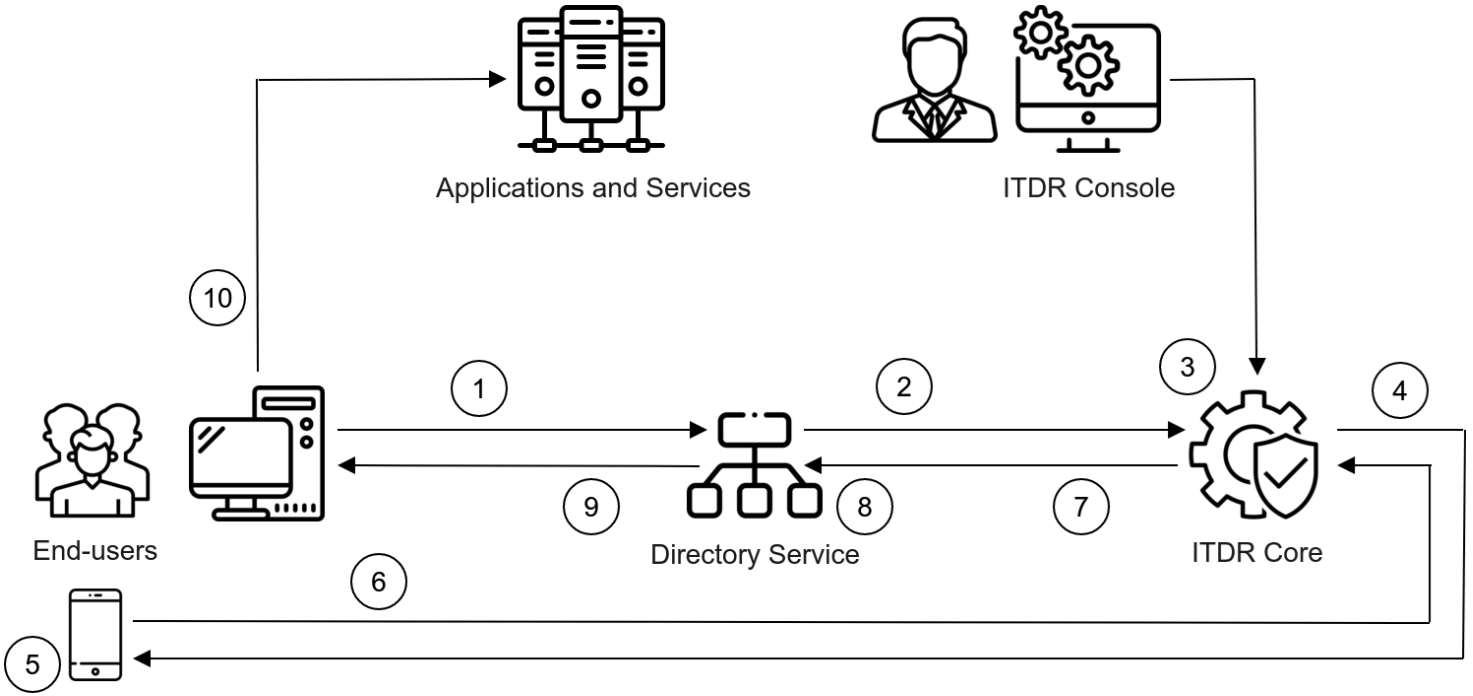
- User Enumeration
- Password Spraying
- AS-REP Roasting
- Kerberoasting
- Golden\Diamond Ticket
- Pass-the-Ticket
- Skeleton Key
- Diamond PAC
- Lateral Movement

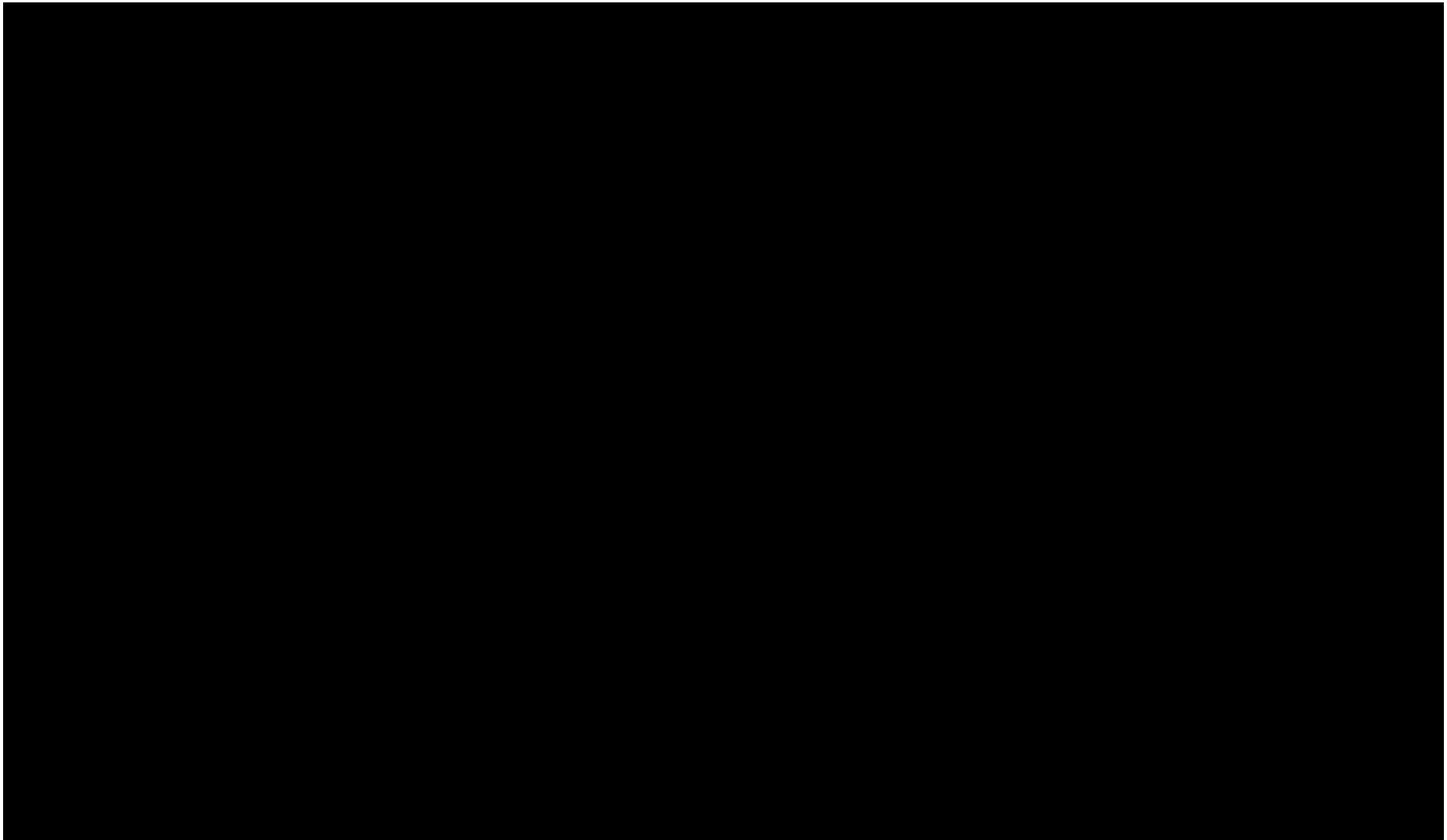
КОМПАНИЯ
ИНДИД

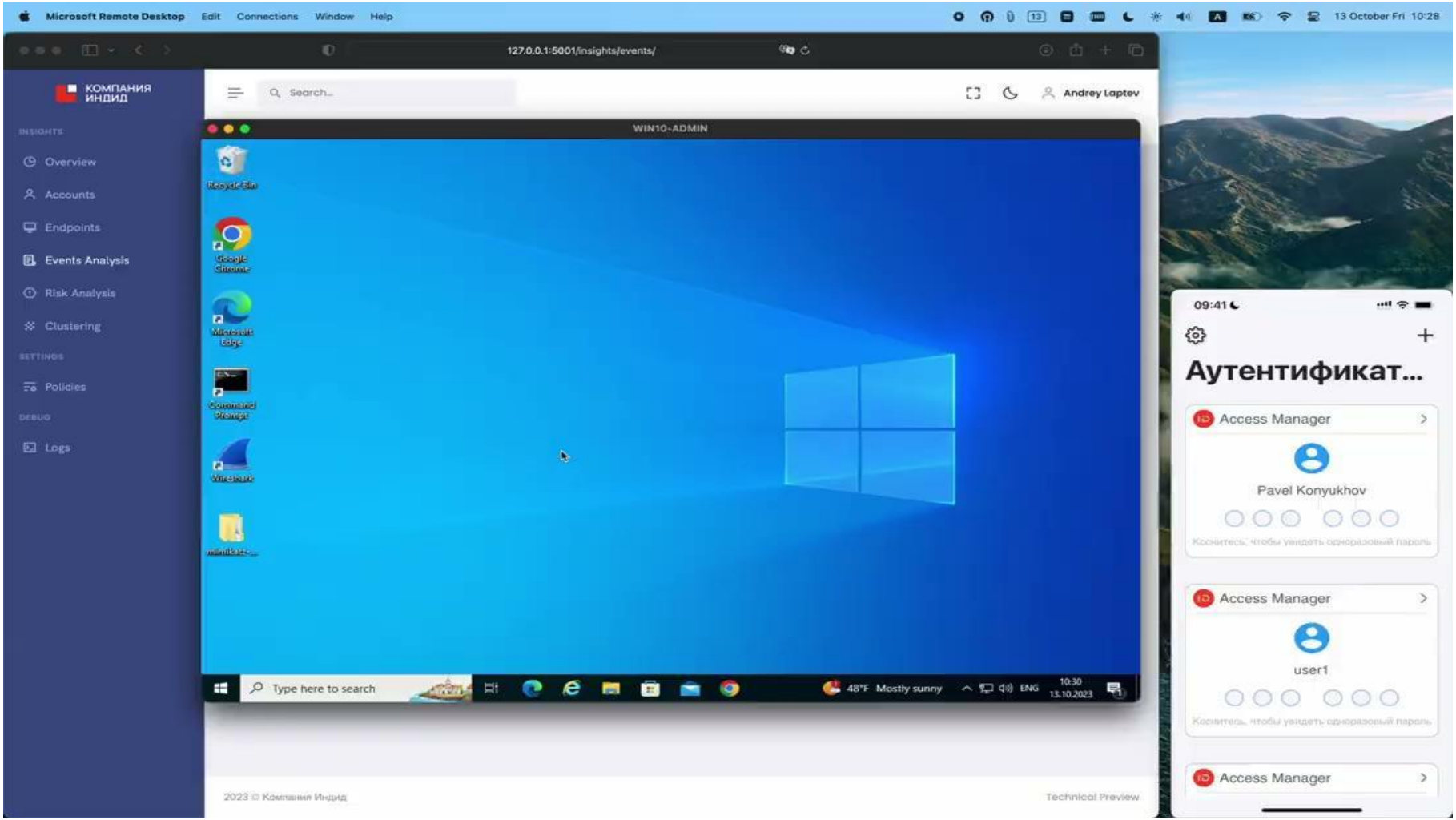
ТЕОРЕТИЧЕСКИЙ МАКСИМУМ ИНФОРМАЦИИ

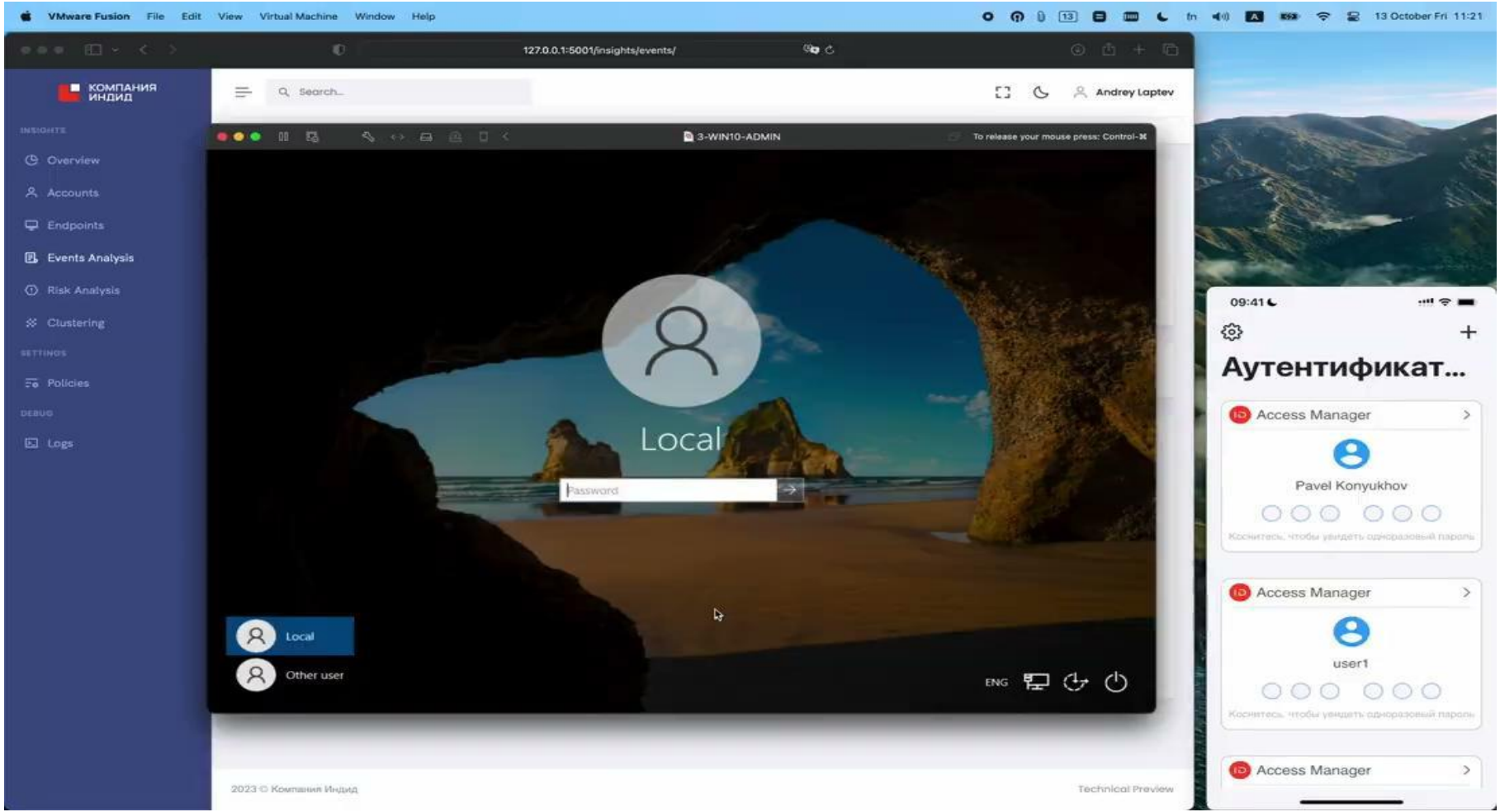
	Date & Time	Protocol	Account Name	Status	Source Endpoint	IP Address	Destination
>	Jul 21 2023 10:08:46	Kerberos	amservice	Access Granted	AM	10.15.3.15	DC
>	Jul 21 2023 10:08:46	Kerberos	amservice	Access Granted	AM	10.15.3.15	DC
v	Jul 21 2023 10:08:45	Kerberos	amservice	Access Denied	AM	10.15.3.15	DC
Domain Controller: dc.indeed.demo		Service: krbtgt/INDEED		Reason: Native Protocol Response	KDC_ERR_PREAUTH_REQUIRED [25]		
>	Jul 21 2023 10:08:44	LDAP	user2	Access Denied	10.10.215.2	10.10.215.2	N/A
>	Jul 21 2023 09:51:28	Kerberos	AM$	Access Granted	AM	10.15.3.15	DC

КОМПАНИЯ
ИНДИД






Microsoft Remote Desktop
Edit
Connections
Window
Help
13 October Fri 10:28
127.0.0.1:5001/insights/events/
КОМПАНИЯ ИНДИД
Search...
Andrey Laptev
INSIGHTS
Overview
Accounts
Endpoints
Events Analysis
Risk Analysis
Clustering
SETTINGS
Policies
DEBUG
Logs
WIN10-ADMIN
Recycle Bin
Google Chrome
Microsoft Edge
Command Prompt
Wireshark
Type here to search
48°F Mostly sunny
ENG
10:30
13.10.2023
2023 © Компания Индид
Technical Preview
09:41
Аутентификат...
Access Manager
Pavel Konyukhov
Коснитесь, чтобы увидеть одноразовый пароль
Access Manager
user1
Коснитесь, чтобы увидеть одноразовый пароль
Access Manager


VMware Fusion File Edit View Virtual Machine Window Help
13 October Fri 11:21
127.0.0.1:5001/insights/events/
КОМПАНИЯ ИНДИД
Search...
Andrey Laptev
INSIGHTS
Overview
Accounts
Endpoints
Events Analysis
Risk Analysis
Clustering
SETTINGS
Policies
DEBUG
Logs
3-WIN10-ADMIN
To release your mouse press: Control-⌘
Local
Password
Local
Other user
ENG
2023 © Компания Индид
Technical Preview
09:41
Аутентификат...
Access Manager
Pavel Konyukhov
Коснитесь, чтобы увидеть одноразовый пароль
Access Manager
user1
Коснитесь, чтобы увидеть одноразовый пароль
Access Manager

КОМПАНИЯ
ИНДИД

СПАСИБО ЗА ВНИМАНИЕ!

КОНТАКТЫ

indeed-company.ru

sales-russia@indeed-company.com

8 800 333-09-06

Андрей Лаптев

andrey.laptev@indeed-company.com

+7 (495) 640-06-09