



POSITIVE  
TECHNOLOGIES

Сетевые аномалии при удаленной работе:  
**Диалог MaxPatrol SIEM и PT NAD**

**Исаев Антон**

Эксперт отдела мониторинга событий ИБ

**Станислав Черкасов**

Менеджер по продвижению продуктов

[ptsecurity.com](https://ptsecurity.com)



# Что в программе

РТ

- Проблематика работы через удаленный доступ
- Кейс #1: Прокрастинация и как ее выявлять
- Кейс #2: Простой
- Кейс #3: Интересный
- Ответы на вопросы
- Послесловие

# Проблематика удаленки



- **Непривычные условия работы для сотрудников**
- **Отсутствие налаженных процессов и методов взаимодействия**
- **Отсутствие контроля за сотрудниками**
- **Домашние компьютеры – ворота в инфраструктуру**
- **Сложность соблюдения безопасных условий работы**

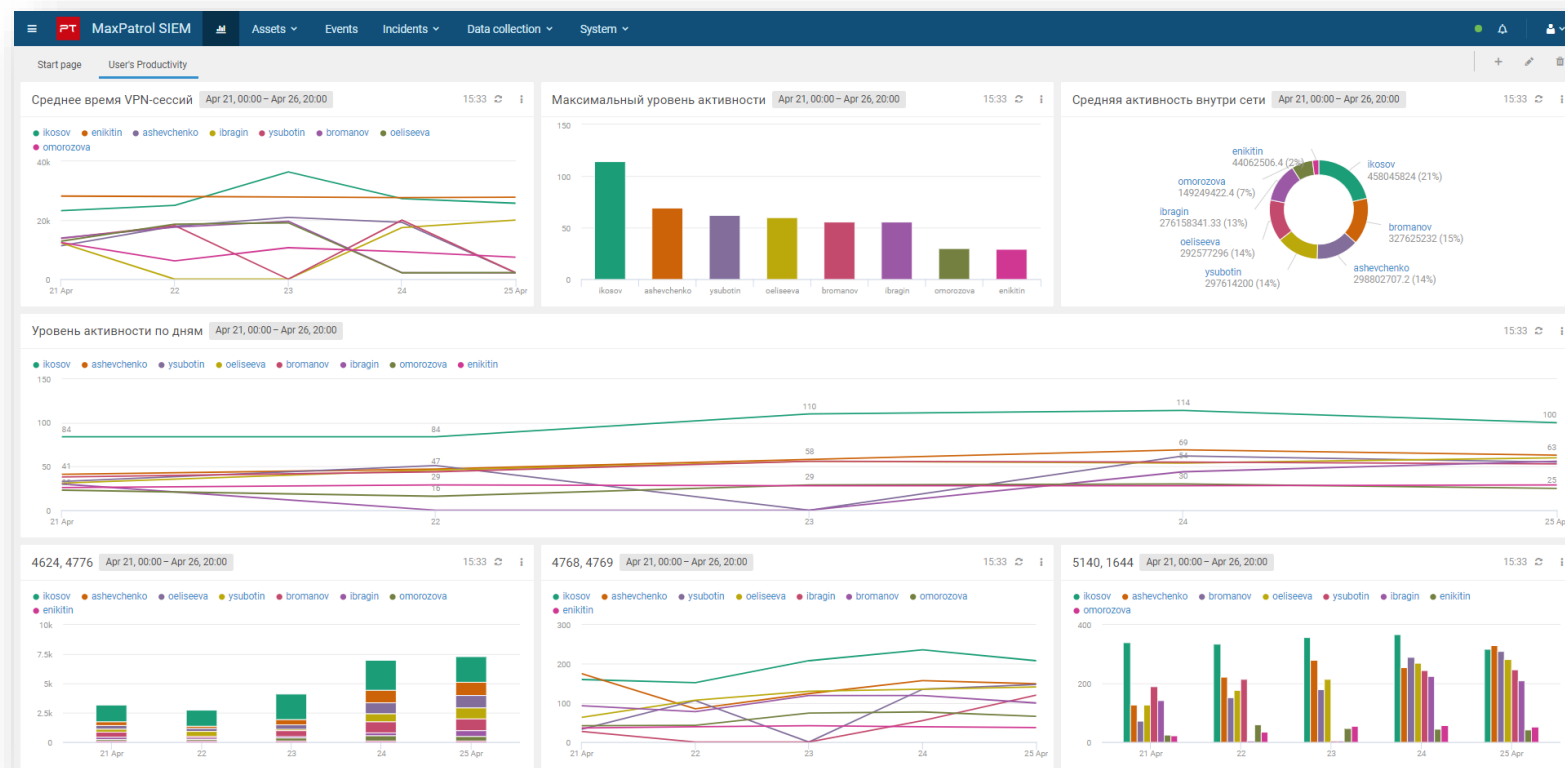


# Кейс №1: активность пользователей

PT

**Пользователи могут быть неактивными в силу многих причин:**

1. Отсутствие задач
2. Прокрастинация
3. Отсутствие релевантной активности
4. Проблемы с доступом



# Активность пользователей. Демо

РТ

## Делаем анализ на основе:

- Продолжительности VPN-сессий
- Объема внутреннего трафика пользователя
- Авторизаций на контроллерах домена
- Обращений к ресурсам внутри домена

Колонки	Название	Тип данных	Ключевое поле 🔑	Индексируемое	Может содержать null
::	user	string	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
::	activity_coefficient	number	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	work_days	number	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	actual_date	datetime	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	actual_intranet_ip	string	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
::	avg_vpn_duration	string	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	sum_vpn_duration_today	string	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	avg_intranet_data_size	string	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	sum_intranet_data_size_today	string	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	avg_ad_logins	number	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	sum_ad_logins_today	number	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	avg_ad_ticket_requests	number	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	sum_ad_ticket_requests	number	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	avg_ad_share_objects_access	number	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
::	sum_ad_share_objects_access	number	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>



# Активность пользователей.

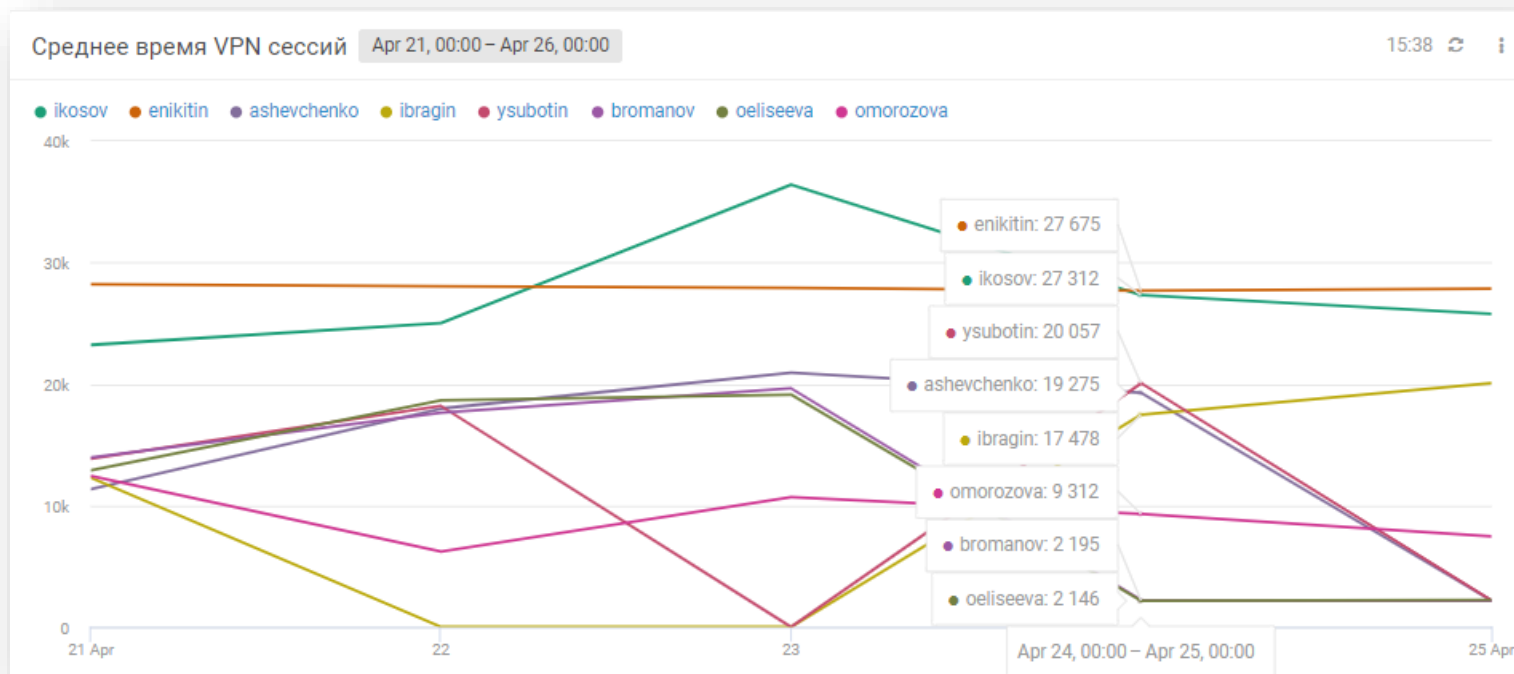
## Демо

РТ

## Продолжительность VPN-сессии

События для анализа:

- Cisco VPN
- Check Point VPN
- OpenVPN
- И т.д...



# Активность пользователей. Демо

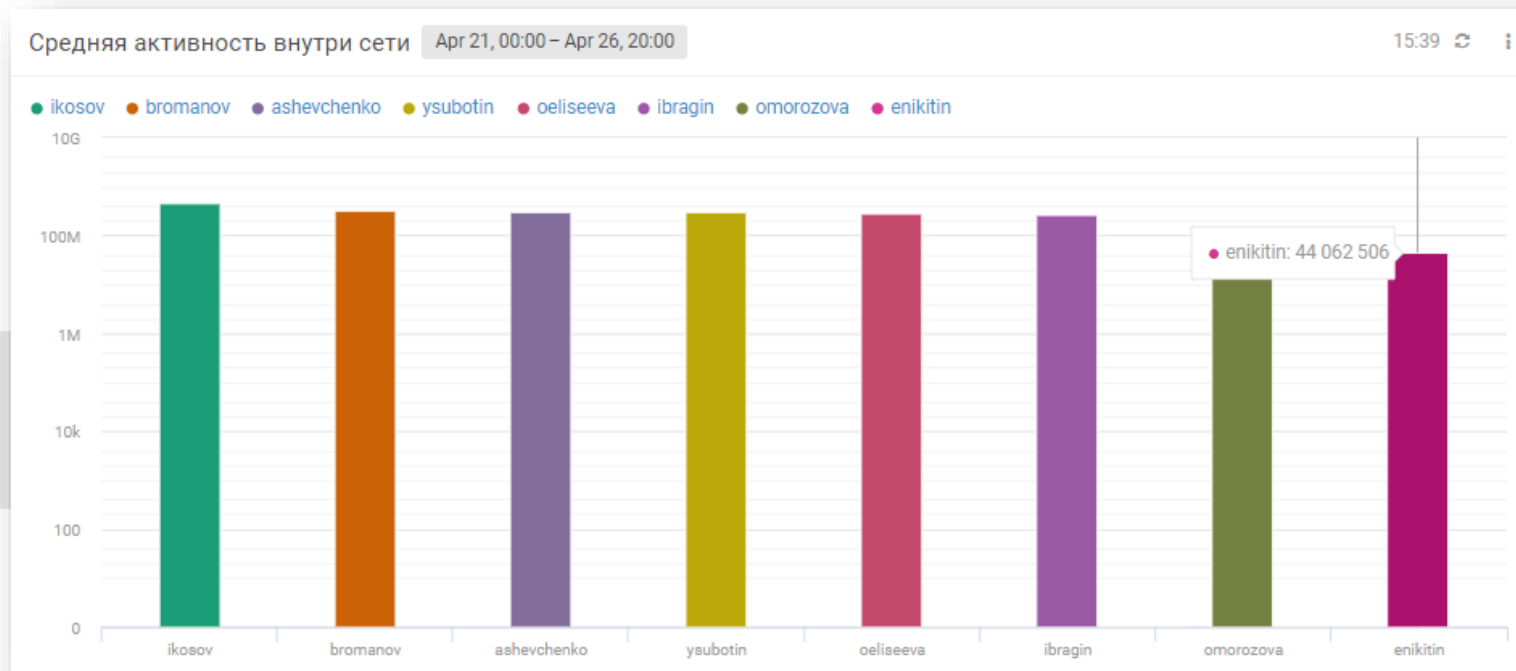
PT

## Объем внутреннего трафика пользователя

События для анализа:

PT Network Attack Discovery  
(NAD Sensor)

Анализ протоколов/портов/подсетей  
для сужения «поля зрения»





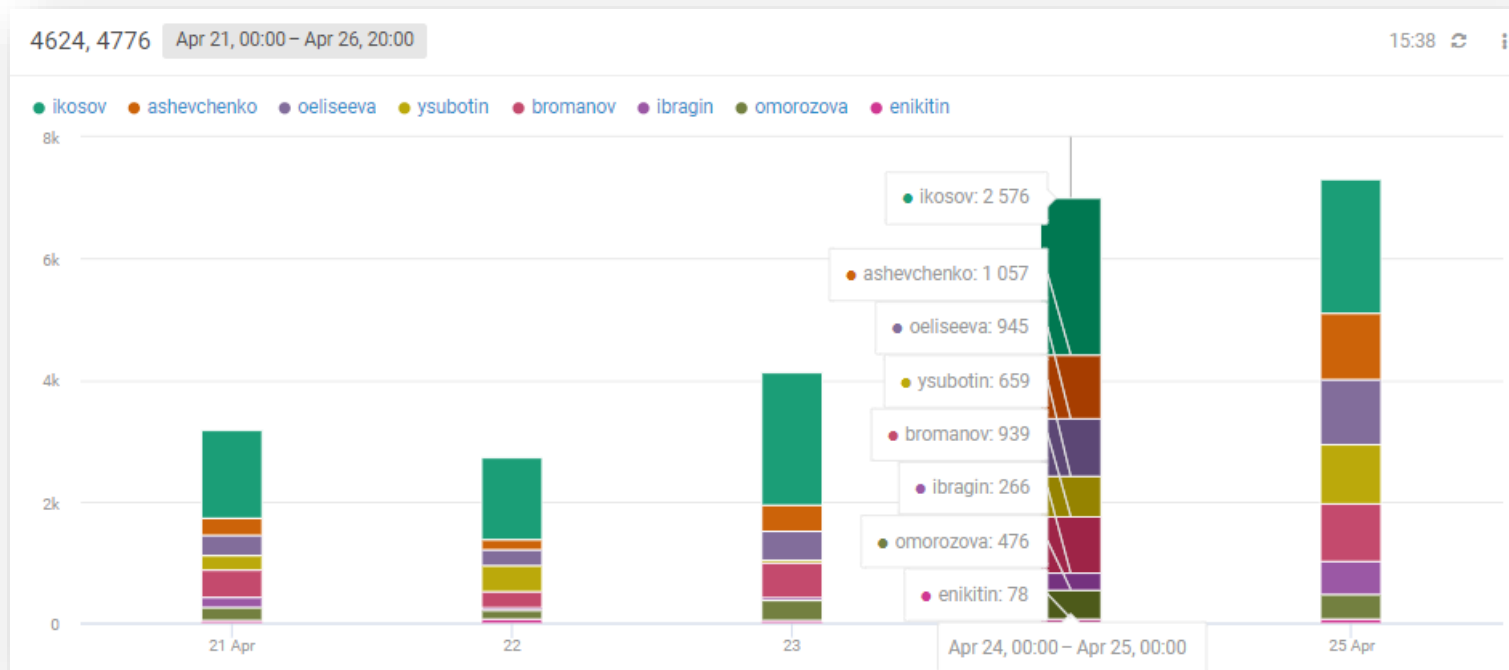
# Активность пользователей. Демо



## Авторизация на контроллерах домена

События для анализа:

Active Directory  
(Авторизация в домене)





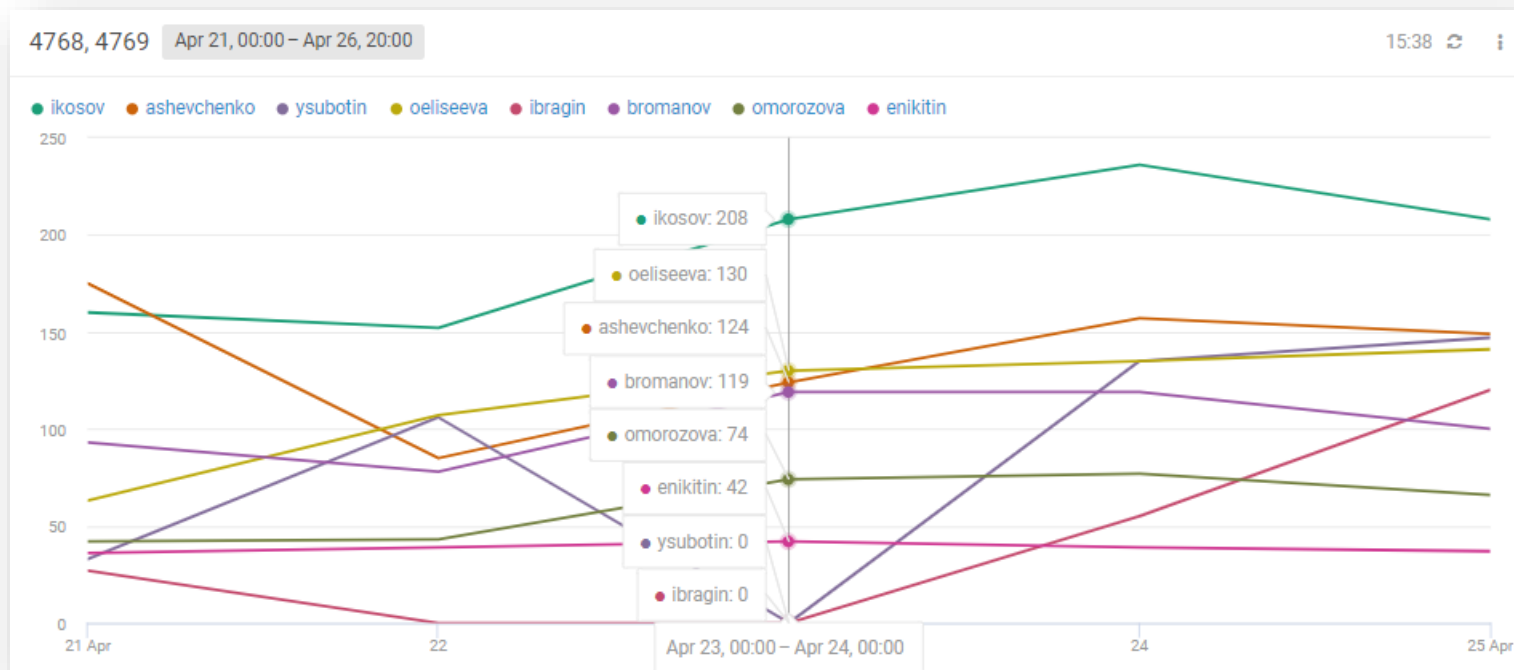
# Активность пользователей. Демо

РТ

## Авторизация на контроллерах домена

События для анализа:

Active Directory  
(Запрос Kerberos билетов)



# Активность пользователей. Демо

РТ

## Обращения к ресурсам внутри домена

События для анализа:

Active Directory  
(Получение доступа к ресурсам/  
объектам внутри организации)



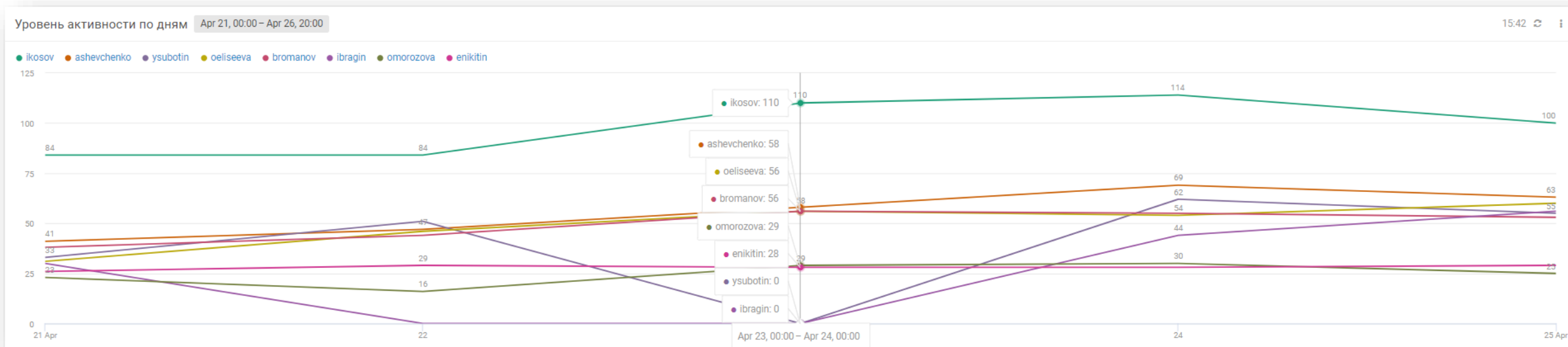


# Активность пользователей. Демо



## Что в итоге:

Визуализация пользовательской активности по заданным метрикам



# Активность пользователей. Демо

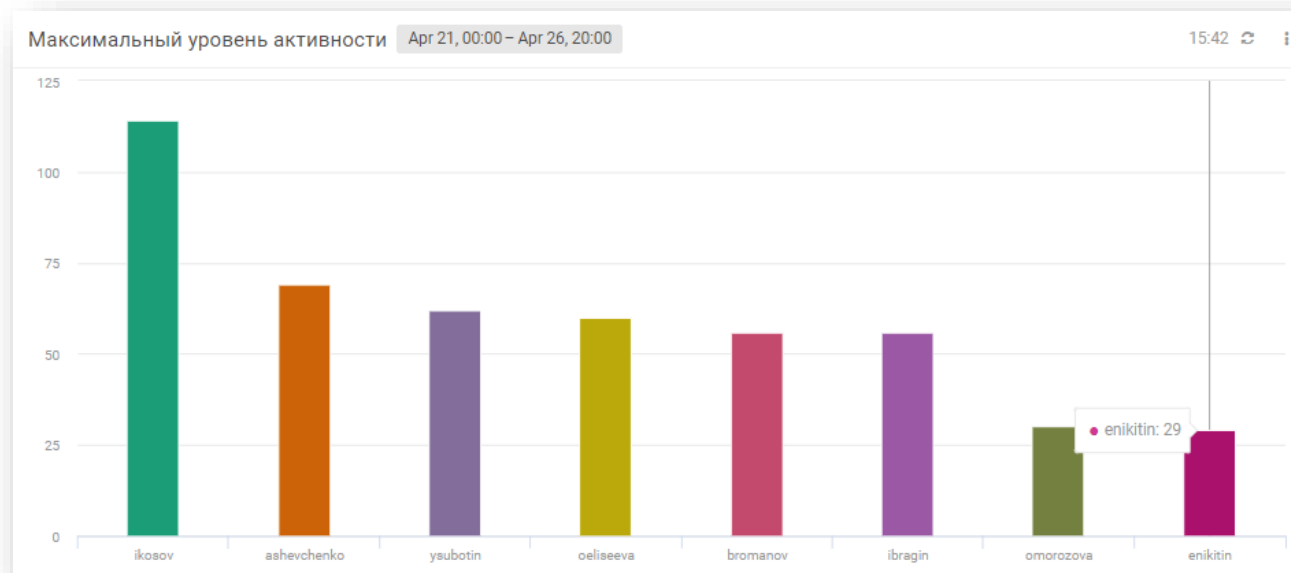
РТ

## Что в итоге:

Визуализация пользовательской активности по заданным метрикам

Поделимся примерами по запросу:

- табличные списки
- правила обогащения





# Практические сценарии. PT NAD и MaxPatrol SIEM

PT

## ВНИМАНИЕ:

Последующие материалы предназначены исключительно для демонстрации возможностей продуктов MaxPatrol SIEM и PT NAD.

Демонстрационные материалы не предназначены для использования в каких-либо целях, отличных от данной презентации. **Использование материалов для совершения злонамеренных действий преследуется по закону, согласно Уголовному Кодексу Российской Федерации.**

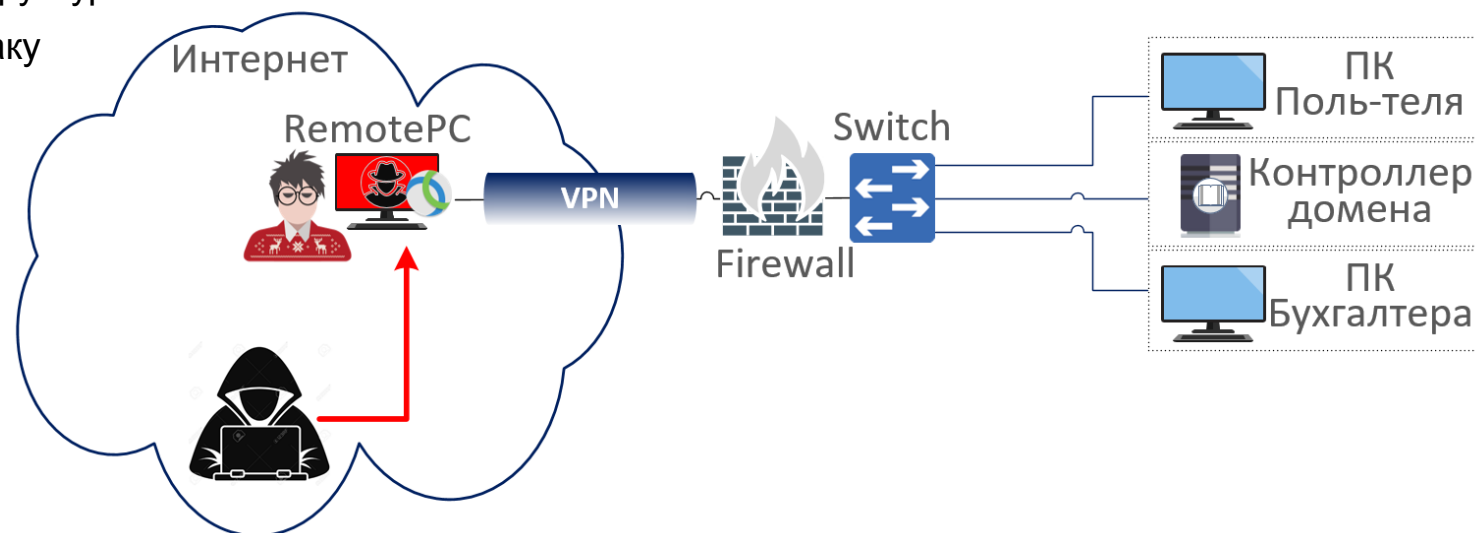


# Кейс №2: цепочка атаки PT NAD > MaxPatrol SIEM

PT

## Что происходит:

1. Домашний компьютер пользователя скомпрометирован
2. Злоумышленник находит жертву внутри инфраструктуры
3. MaxPatrol SIEM с помощью PT NAD выявляет атаку



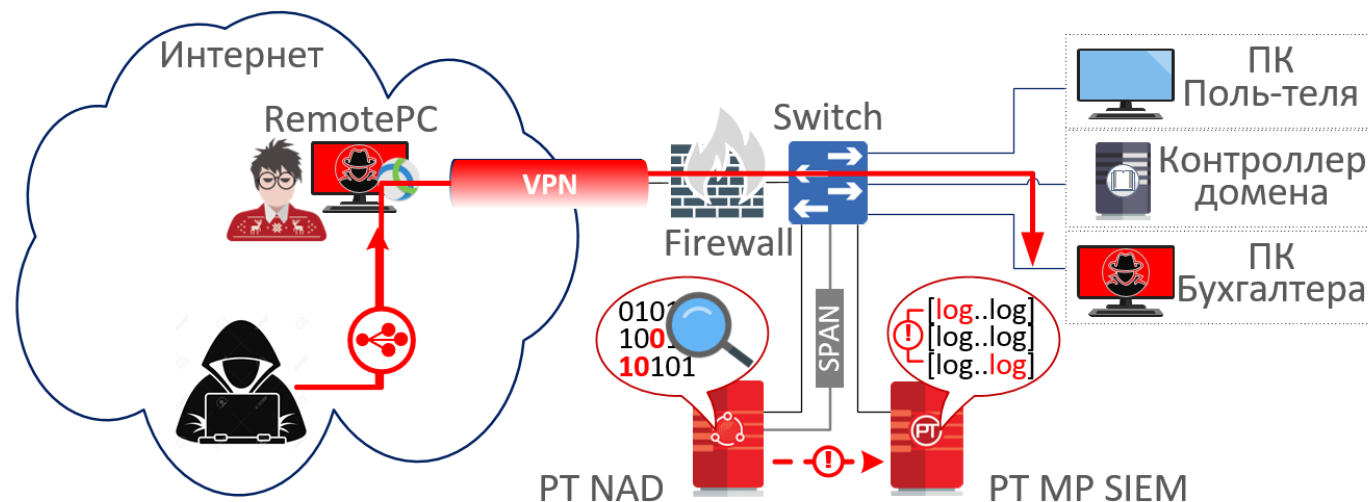


# Кейс №2. Часть 1: действия злоумышленника

РТ

## Что происходит:

1. Злоумышленник сканирует инфраструктуру в поисках жертвы
2. Обнаруживает компьютер бухгалтерии, уязвимый для MS17-010
3. Получает доступ к системе
4. Организует обратное соединение до первоначально скомпрометированного узла



# Кейс №2. Часть 1

РТ



**Демо: действия злоумышленника**



# Кейс №2. Часть 2: обнаружение



## Что происходит:

1. PT NAD сообщает в MaxPatrol SIEM о происходящем, анализируя трафик
2. MaxPatrol SIEM на основе полученных данных выстраивает цепочку атаки с помощью правила корреляции
3. Эта информация позволяет службе ИБ на ранней стадии зафиксировать инцидент и принять его в работу

# Кейс №2. Часть 2

РТ



**Демо: обнаружение атаки**



# Кейс №3: от простого к сложному

PT

## Что происходит:

1. Злоумышленник компрометирует жертву – домашний компьютер пользователя, оказывается внутри корпоративной сети
2. Находит жертву и закрепляется в сети
3. Связка PT NAD и MaxPatrol SIEM выявляет атаку

# Кейс №3. Часть 1

РТ



**Демо: действия злоумышленника**

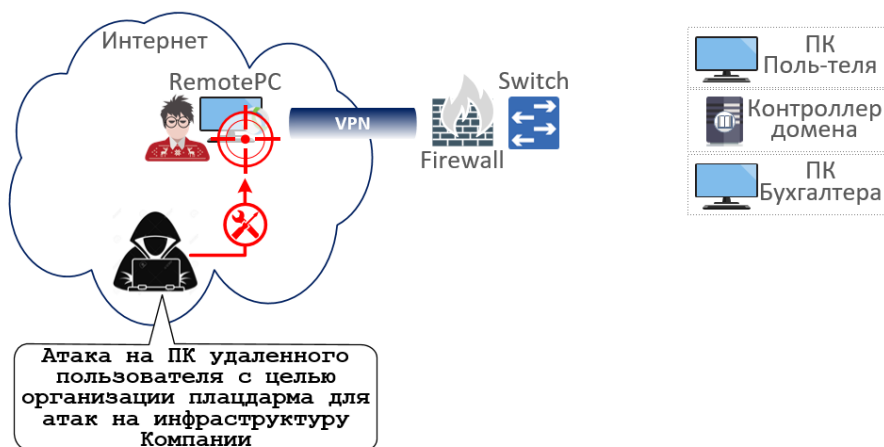


# Кейс №3. Часть 1: действия злоумышленника

РТ

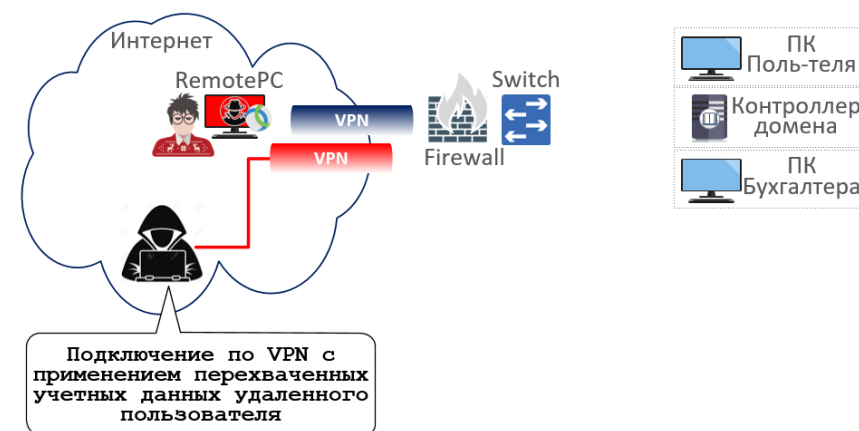
## Что происходит:

1. Злоумышленник компрометирует жертву – домашний компьютер пользователя



## Что происходит:

2. Украдв учетные данные от VPN, злоумышленник использует их, для организации собственного подключения, минуя жертву



# Кейс №3. Часть 1

РТ



**Демо: действия злоумышленника**

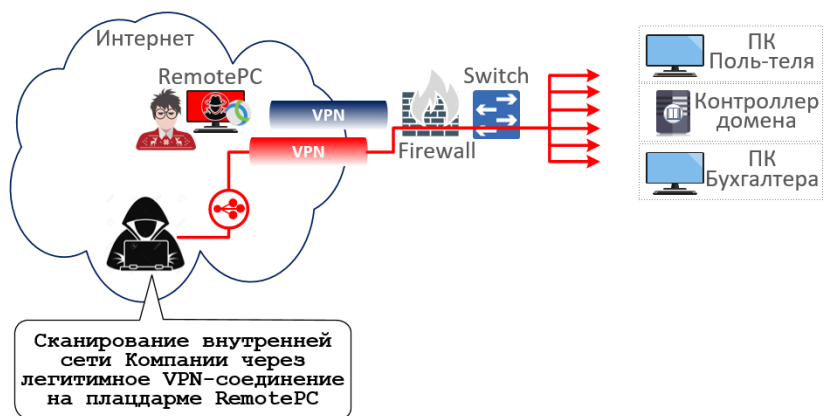


# Кейс №3. Часть 1: действия злоумышленника

РТ

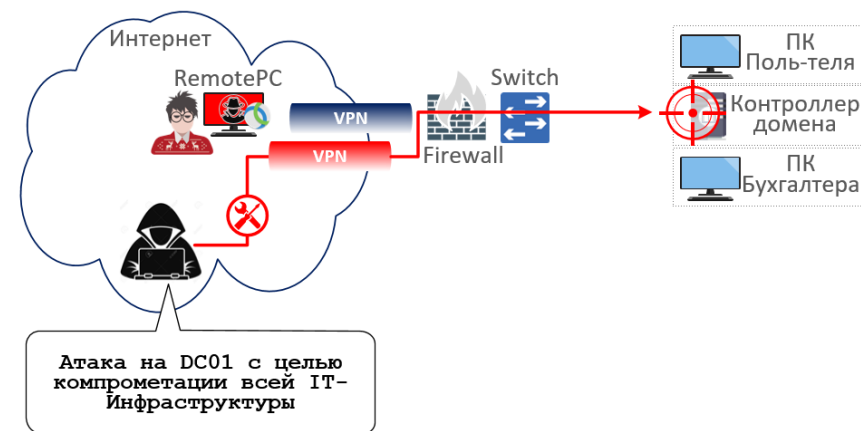
Что происходит:

3. Злоумышленник «осматривается», сканирует сеть для поиска целей



Что происходит:

4. Находит доменный контроллер и пытается его скомпрометировать



# Кейс №3, часть 1

РТ



**Демо: действия злоумышленника**

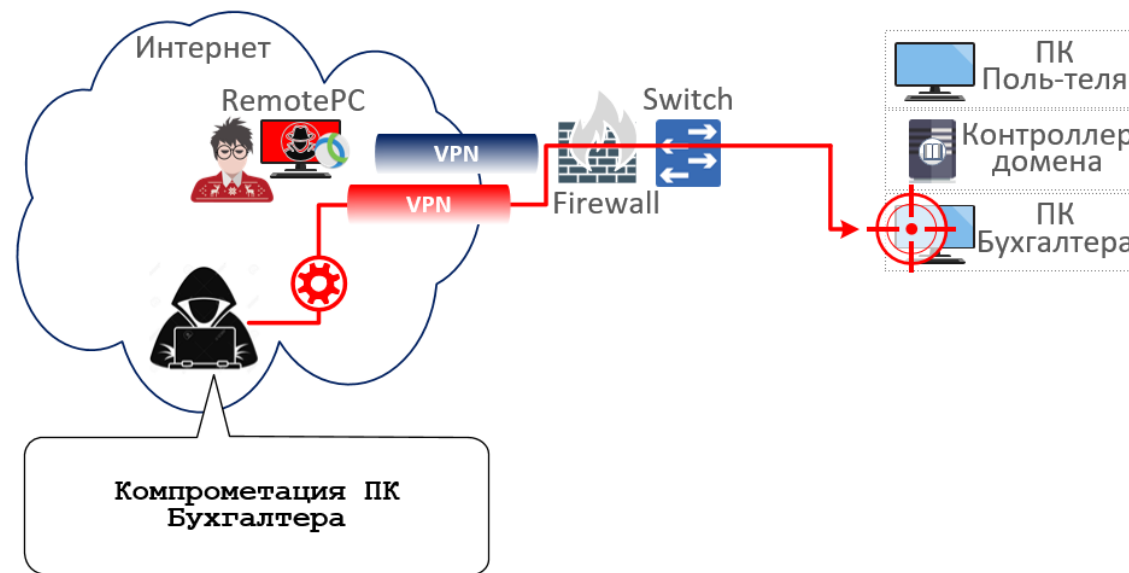


# Кейс №3. Часть 1: действия злоумышленника

РТ

## Итог:

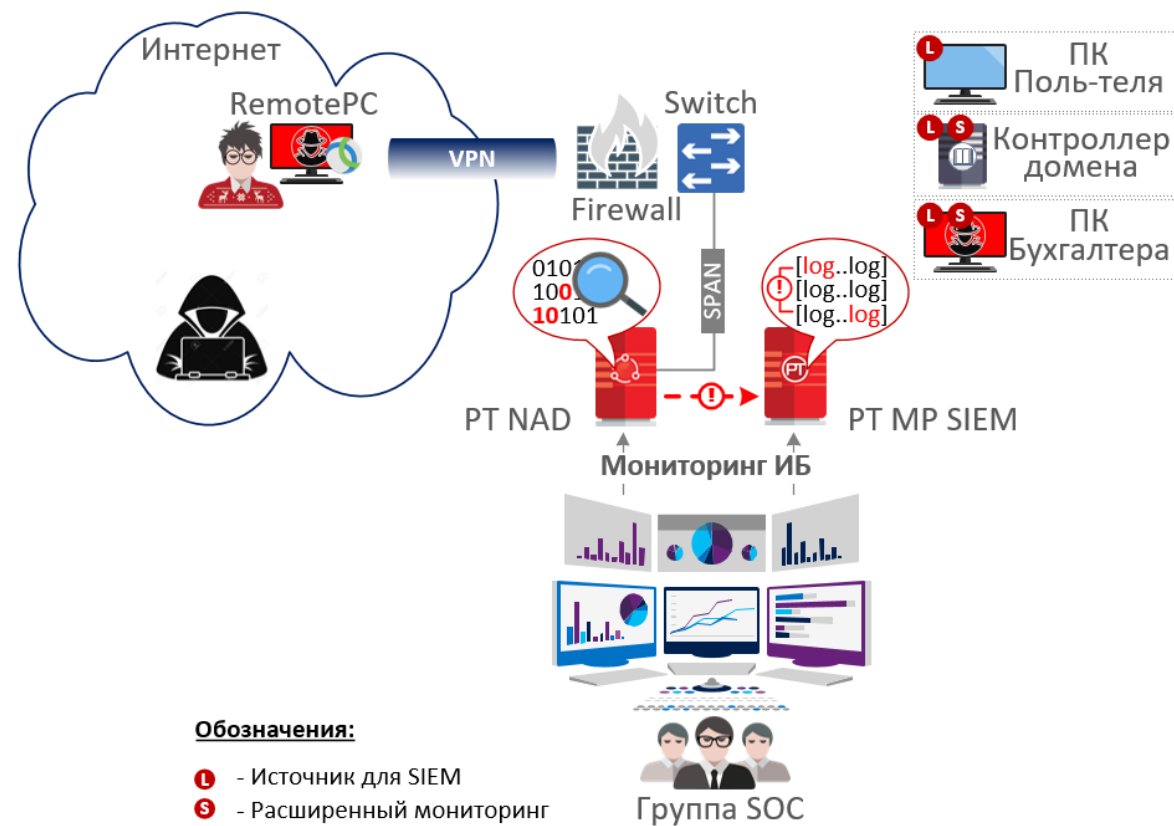
Злоумышленнику не удастся напрямую скомпрометировать доменный контроллер, он использует информацию из ПК Пользователя в инфраструктуре, и попутно находит новую жертву – ПК Бухгалтера с чувствительной информацией



# Кейс №3. Часть 2: обнаружение

РТ

## Выявление инцидента с помощью РТ NAD и MaxPatrol SIEM





# Кейс №3. Часть 2

РТ



**Демо: обнаружение атаки**

# Заключение



- Мир меняется у нас на глазах, меняются и подходы
- Связка MaxPatrol SIEM и PT NAD не заменяет других решений, но дополняет картину защищенности
- Мы работали и будем продолжать работы в этом направлении



# Ответы на вопросы

# Послесловие



## ○ Проведенный Positive Technologies опрос показал, что:

- Только лишь в 11% ответов значилось, что удаленный доступ был организован в связи с пандемией
- Абсолютное большинство респондентов указало, что для доступа используются их личные домашние устройства
- Наиболее популярные способы организации доступа: OpenVPN, Cisco VPN и RDG

Данные исследования скоро появятся на [ptsecurity.com/ru-ru/research/analytics/](https://ptsecurity.com/ru-ru/research/analytics/)

## ○ Анонс: 28 мая вебинар по работе с новым пакетом экспертизы, посвященному удаленной работе



# Что дальше:



Обновить версию:

[support.ptsecurity.com](https://support.ptsecurity.com)

Заказать пилот:

[ptsecurity.com/ru-ru/solutions/secure-remote-work/](https://ptsecurity.com/ru-ru/solutions/secure-remote-work/)

Пройти обучение:

[edu@ptsecurity.com](mailto:edu@ptsecurity.com)

Купить:

[sales@ptsecurity.com](mailto:sales@ptsecurity.com)



Антон Исаев

Специалист по системам мониторинга безопасности



Станислав Черкасов

Менеджер по продвижению продуктов