АЙТИБАСТИОН

www.it-bastion.com

КОМПАНИЯ
АЙТИ БАСТИОН

2014

100+

ОСНОВАНИЕ КОМПАНИИ

Более 9 лет на российском рынке информационной безопасности

www.it-bastion.com

КОМПАНИЯ
АЙТИ БАСТИОН

100+

180+

ПАРТНЕРОВ-ИНТЕГРАТОРОВ

Интеграции с компаниями, позволяющие выполнить квалифицированную помощь в реализации защиты инфраструктуры

www.it-bastion.com

КОМПАНИЯ
АЙТИ БАСТИОН

180+

>50%

ЗАКАЗЧИКОВ И ПРОЕКТОВ

Присутствие во всех отраслях от нефтяных компаний до футбольных клубов, от небольших офисов до георасределенных площадок

www.it-bastion.com

КОМПАНИЯ
АЙТИ БАСТИОН

>50%

РАМ-РЫНКА РФ

Комплекс СКДПУ НТ решение, проверенное «в боях» и доказавшее свою эффективность, надежность и качество

www.it-bastion.com

2023

КУДА ПРИВОДИТ РАМ ИЛИ ПОСТРОЕНИЕ ИБ ИНФРАСТРУКТУРЫ НА ОСНОВЕ СКДПУ НТ

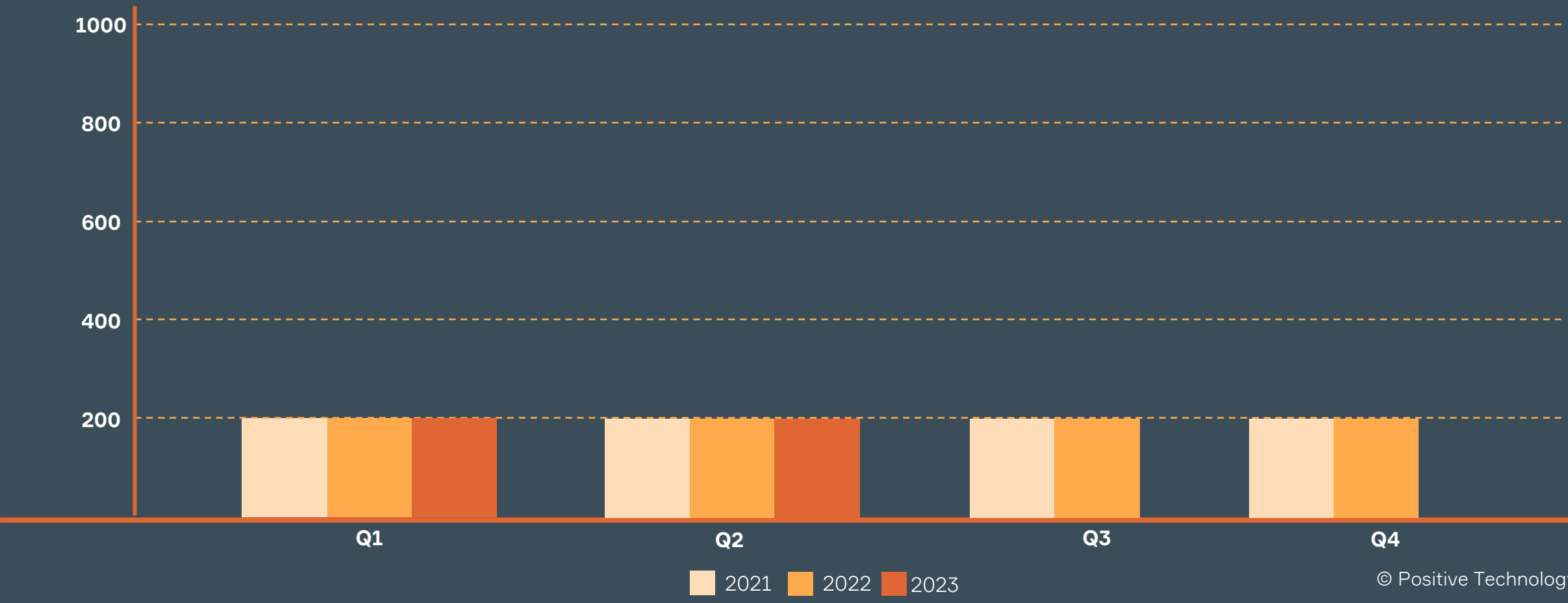
ШИРИКАЛОВ АЛЕКСЕЙ
Руководитель группы
Поддержки продаж

www.it-bastion.com

НЕМНОГО СТАТИСТИКИ
КОЛ-ВО ИНЦИДЕНТОВ

АЙТИБАСТИОН

- Кол-во инцидентов выросло на 20,8%
- Массовые утечки данных
- В 2023 году тенденция показывает еще большее число атак

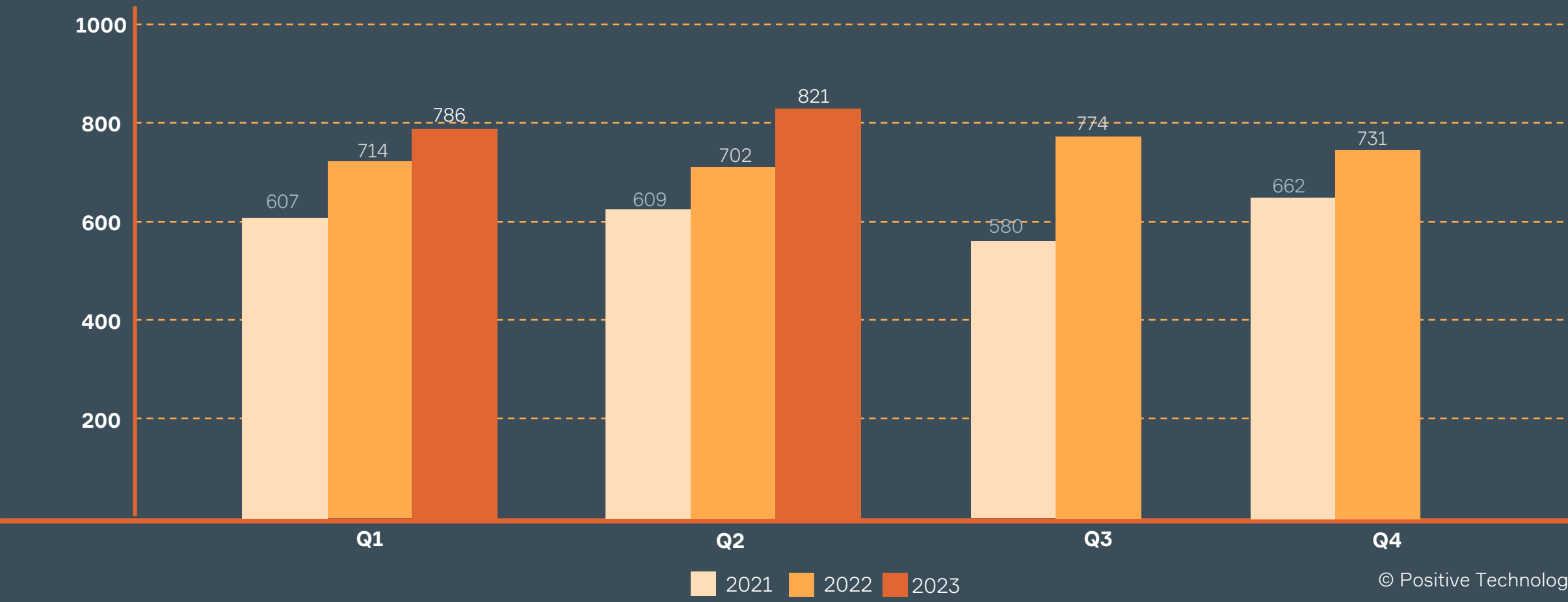


www.it-bastion.com

НЕМНОГО СТАТИСТИКИ
КОЛ-ВО ИНЦИДЕНТОВ

АЙТИБАСТИОН

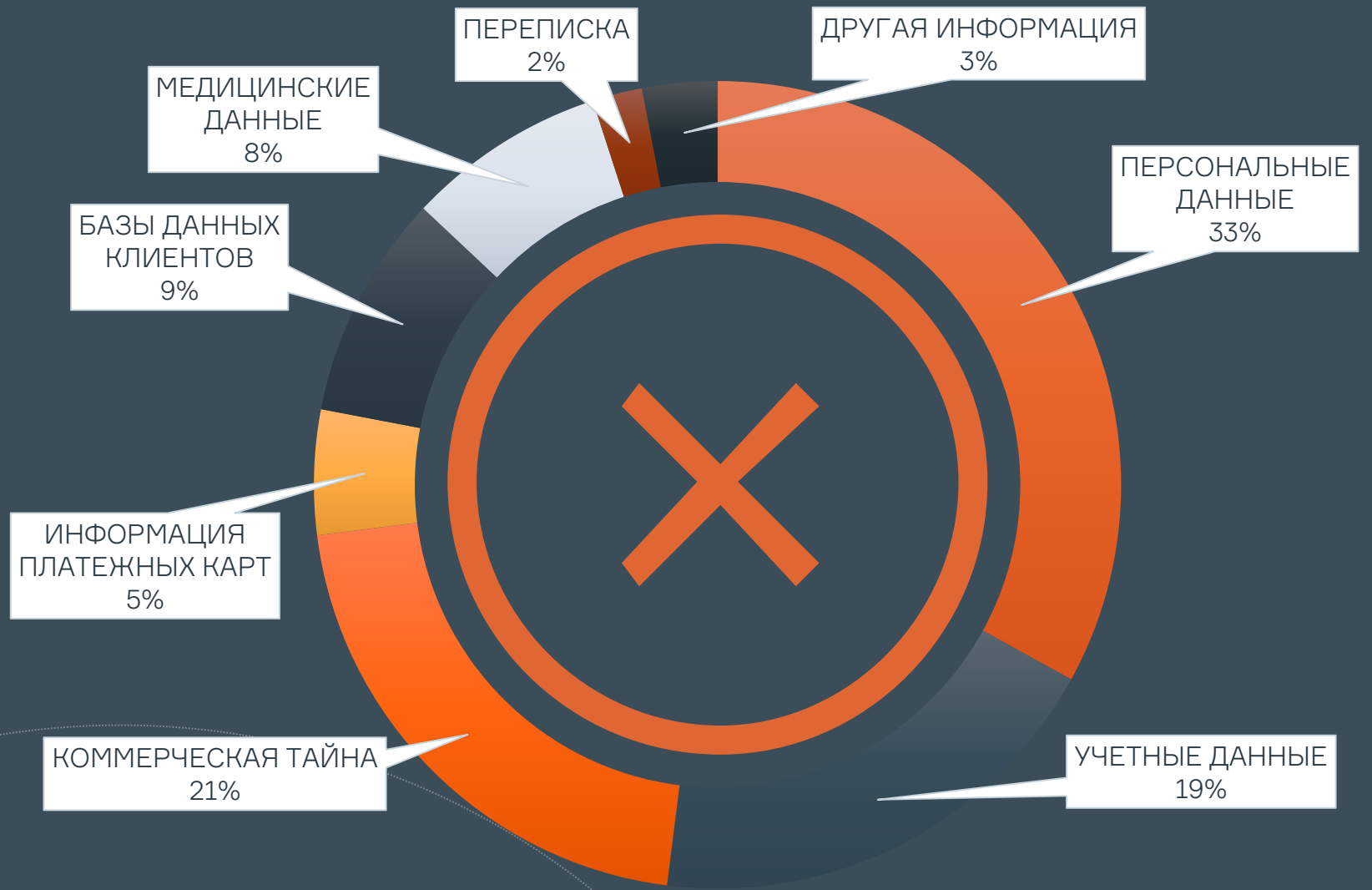
- Кол-во инцидентов выросло на 20,8%
- Массовые утечки данных
- В 2023 году тенденция показывает еще большее число атак



www.it-bastion.com

НЕМНОГО СТАТИСТИКИ
ЦЕЛИ АТАК

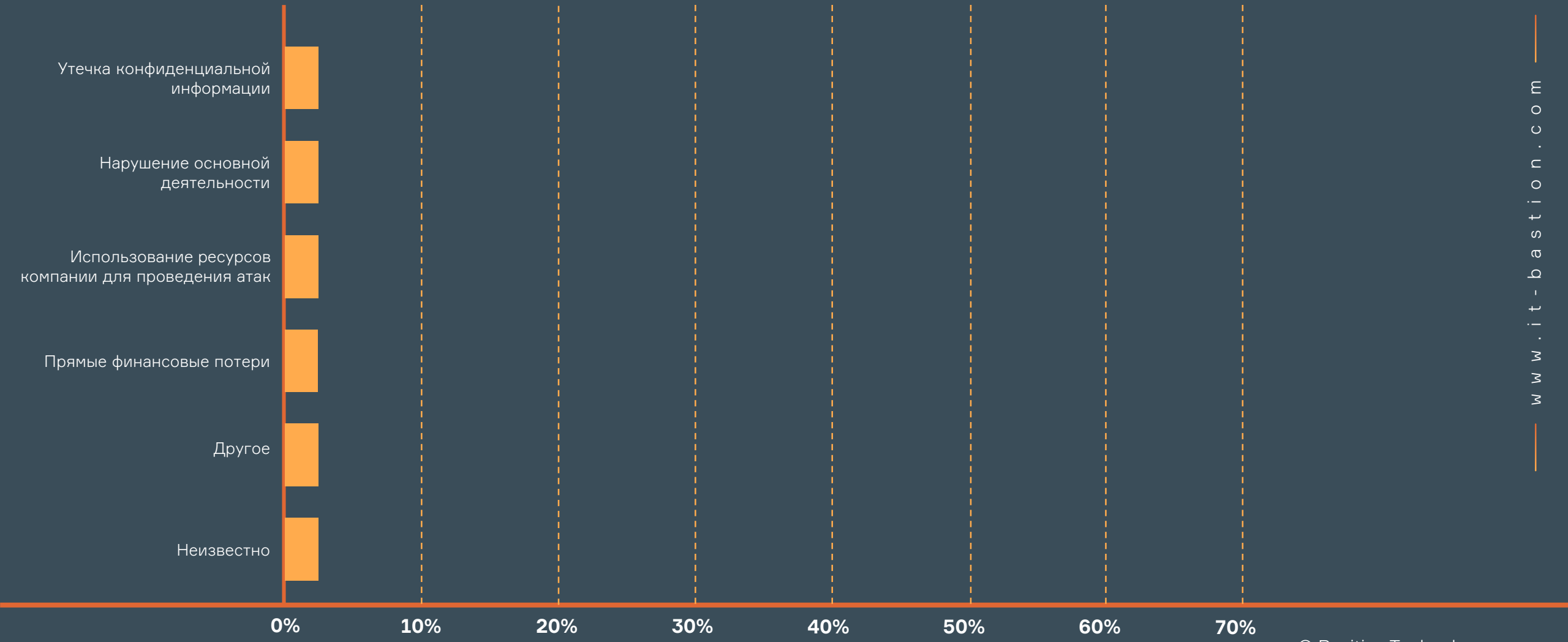
АЙТИБАСТИОН



www.it-bastion.com

НЕМНОГО СТАТИСТИКИ
ПРОЦЕНТ УСПЕШНЫХ АТАК

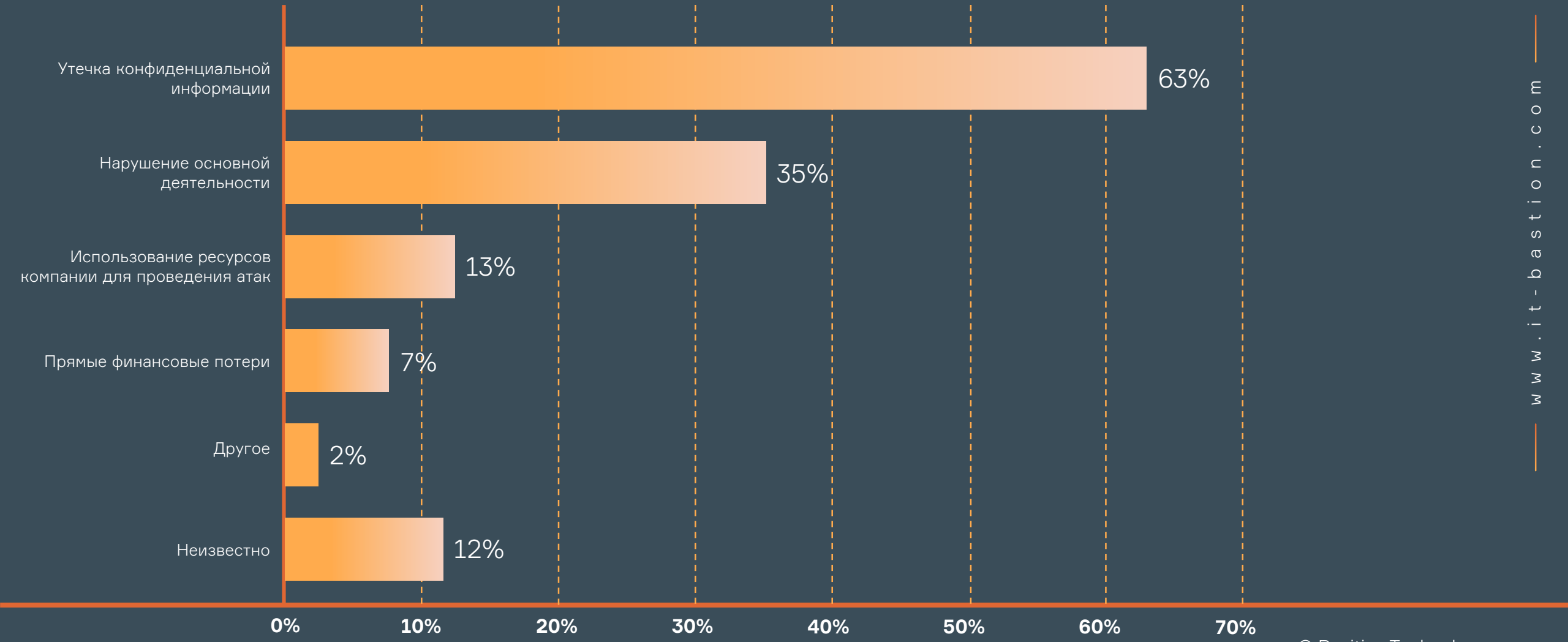
АЙТИБАСТИОН



www.it-bastion.com

НЕМНОГО СТАТИСТИКИ
ПРОЦЕНТ УСПЕШНЫХ АТАК

АЙТИБАСТИОН



www.it-bastion.com

НЕМНОГО СТАТИСТИКИ
ХАРАКТЕР АТАК

АЙТИБАСТИОН

ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ

ПОДБОР ВЕКТОРА АТКИ НА КОНКРЕТНЫЕ ОРГАНИЗАЦИИ ДЛЯ ПОЛУЧЕНИЯ ДАННЫХ ИЛИ НАНЕСЕНИЯ УЩЕРБА ОРГАНИЗАЦИИ

АТАКИ НАПРАВЛЕННЫХ НА ЧАСТНЫЕ ЛИЦА

ПОЛУЧЕНИЕ ДОСТУПА ЗА СЧЕТ АТАКИ НА ПОЛЬЗОВАТЕЛЯ, ИЗНАЧАЛЬНО ИМЕЮЩЕГО ДОСТУП К АТАКУЕМОЙ ИНФРАСТРУКТУРЕ

АТАКИ SUPPLY CHAIN

РЕАЛИЗАЦИЯ АТАКИ ЧЕРЕЗ ПОДРЯДЧИКОВ, КОТОРЫЕ ЗАЧАСТУЮ ИМЕЮТ БОЛЕЕ СЛАБУЮ ЗАЩИТУ

www.it-bastion.com

КОГО КОНТРОЛИРУЕМ?

- ПОДРЯДЧИКОВ
- СИСТЕМНЫХ АДМИНИСТРАТОРОВ
- ИНЖЕНЕРОВ ВЕНДОРА
- АУДИТОРОВ

www.it-bastion.com

АЙТИБАСТИОН

КАК ЗАЩИТИТЬ?

- ЕСТЬ ОПРЕДЕЛЕННЫЙ ПАРК РЕШЕНИЙ
- НЕ ВСЕ РЕШЕНИЯ МОНОВЕНДОРНЫЕ
- ПЕРЕРАБОКА ИНФРАСТРУКТУРЫ
- ИМПОРТОЗАМЕЩЕНИЕ
- СПЕЦИАЛИЗАЦИЯ
- ВЫБОР

АЙТИБАСТИОН

СКДПУ НТ

МА

- Центр анализа
- Мониторинг
- Поведенческая модель
- Уровень доверия
- Инцидент
- Аномалии
- Отчетность

ШД

- Контроль доступа
- 2FA
- Профилирование
- Логирование
- Менеджер паролей
- Паттерны
- Видеозапись
- Политики доступа

www.it-bastion.com

АЙТИБАСТИОН

СКДПУ НТ
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

и другие партнеры

www.it-bastion.com

ПЛАТФОРМЕННОСТЬ

АЙТИБАСТИОН

АЙТИБАСТИОН

КЕЙС 1
2FA

Утечка информации в крупном промышленном предприятии

АЙТИБАСТИОН

КЕЙС №2
ОПЕРАЦИЯ ПОД НОСОМ

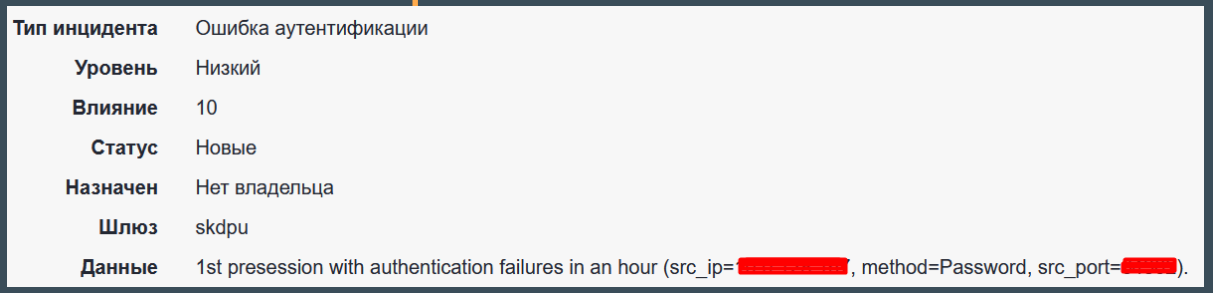
2FA СИСТЕМА В КОМПАНИИ
ВСЕ ПОЛЬЗОВАТЕЛИ ИСПОЛЬЗУЮТ МЕТОД ПОДТВЕРЖДЕНИЯ ВХОДА ЧЕРЕЗ PUSH-УВЕДОМЛЕНИЕ

УДАЛЕННЫЙ ДОСТУП
ВОЗМОЖНОСТЬ ПОДКЛЮЧЕНИЯ В ИНФРАСТРУКТУРУ

ДОМЕННЫЕ УЗ
ИСПОЛЬЗОВАНИЕ ДОМЕННЫХ УЗ ДЛЯ ДОСТУПА К БОЛЬШИНСТВУ ОБЪЕКТОВ

ОШИБКИ АВТОРИЗАЦИИ

НЕСКОЛЬКО НЕУДАЧНЫХ ПОПЫТОК АВТОРИЗАЦИИ



Тип инцидента	Ошибка аутентификации
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Шлюз	skdpu
Данные	1st presession with authentication failures in an hour (src_ip=[redacted], method=Password, src_port=[redacted]).

НЕТИПИЧНОЕ МЕСТО

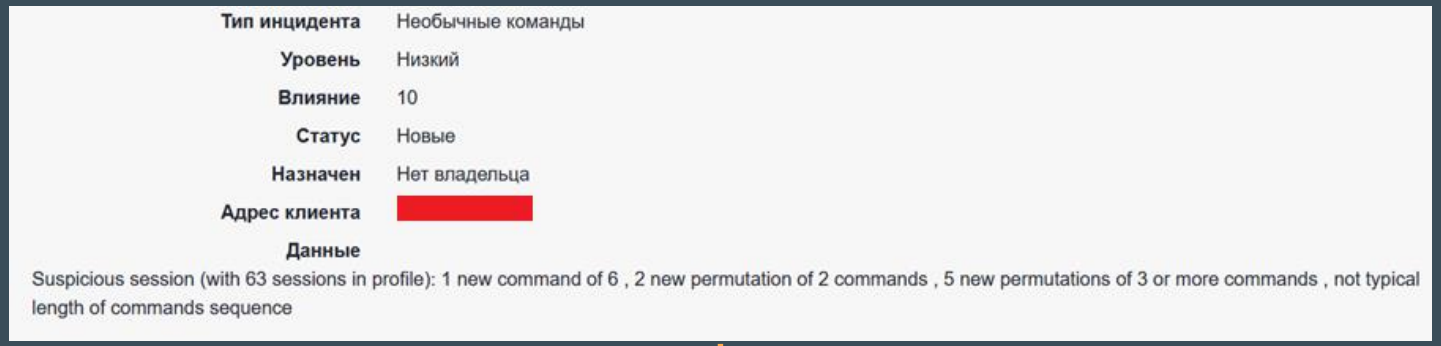
ИСПОЛЬЗОВАНИЕ ДЛЯ ПОДКЛЮЧЕНИЯ НЕСТАНДАРТНЫХ IP

НЕТИПИЧНОЕ ВРЕМЯ

ПОЛЬЗОВАТЕЛЬ ПОДКЛЮЧАЕТСЯ В НЕ РАБОЧЕЕ ВРЕМЯ

НЕТИПИЧНЫЙ ДОСТУП

ПОЛЬЗВОАТЕЛЬ ПЫТАЕТСЯ ПОДКЛЮЧИТЬСЯ К БОЛЬШОМУ КОЛИЧЕСТВУ УСТРОЙСТВ, НЕКТОРЫЕ ИЗ ПОДКЛЮЧЕНИ ТРЕБУЮТ ПОЛУЧЕНИЯ ДОПОЛНИТЕЛЬНОГО РАЗРЕШЕНИЯ

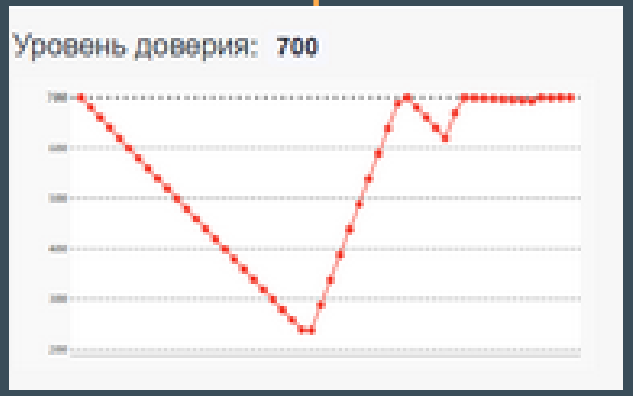


ПОДОЗРИТЕЛЬНЫЕ КОМАНДЫ

ВЫПОЛНЕНИЕ ПОЛЬЗОВАТЕЛЕМ КОМАНД, КОТОРЫЕ ОТЛИЧАЮТСЯ ОТ ПРИВЫЧНЫХ

ПАДЕНИЕ УРОВНЯ ДОВЕРИЯ

РЕЗКОЕ УМЕНЬШЕНИЕ УРОВНЯ ДОВЕРИЯ (УРОВЕНЬ – ДЕМОНСТРИРУЮЩИЙ КОРРЕКТНОСТЬ РАБОТЫ ПОЛЬЗОВАТЕЛЯ)



БЛОКИРОВКА УЗ

ПРЕДОТВРАЩЕНИЕ ДОСТУПА В ИНФРАСТРУКТУРУ

ИТОГ

НЕОБХОДИМО КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

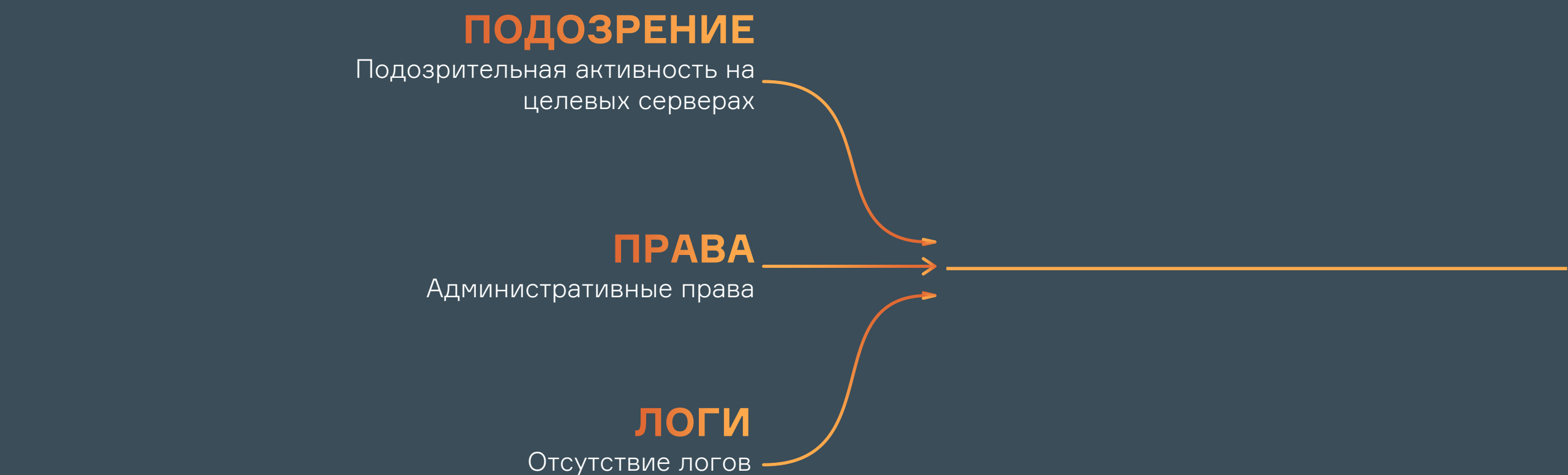
АЙТИБАСТИОН

КЕЙС 2
BACKDOOR

Определение и нейтрализация
несанкционированного доступа

КЕЙС №1
ВРЕМЯ ДЕНЬГИ

АЙТИБАСТИОН



АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

09-08-2023 17:10:25	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:10:45	KBD_INPUT	adduser testuser
09-08-2023 17:10:52	KBD_INPUT	passwd testuser
09-08-2023 17:10:52	KILL_PATTERN_DETECTED	**pattern:** passwd

09-08-2023 17:21:40	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:21:52	KBD_INPUT	adduser test4
09-08-2023 17:21:56	KBD_INPUT	passwd test4
09-08-2023 17:22:07	KBD_INPUT	visudo

ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

09-08-2023 17:10:25	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:10:45	KBD_INPUT	adduser testuser
09-08-2023 17:10:52	KBD_INPUT	passwd testuser
09-08-2023 17:10:52	KILL_PATTERN_DETECTED	**pattern:** passwd

09-08-2023 17:21:40	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:21:52	KBD_INPUT	adduser test4
09-08-2023 17:21:56	KBD_INPUT	passwd test4
09-08-2023 17:22:07	KBD_INPUT	visudo

АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

09-08-2023 17:10:25	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:10:45	KBD_INPUT	adduser testuser
09-08-2023 17:10:52	KBD_INPUT	passwd testuser
09-08-2023 17:10:52	KILL_PATTERN_DETECTED	**pattern:** passwd

09-08-2023 17:21:40	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:21:52	KBD_INPUT	adduser test4
09-08-2023 17:21:56	KBD_INPUT	passwd test4
09-08-2023 17:22:07	KBD_INPUT	visudo

ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

09-08-2023 17:10:25	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:10:45	KBD_INPUT	adduser testuser
09-08-2023 17:10:52	KBD_INPUT	passwd testuser
09-08-2023 17:10:52	KILL_PATTERN_DETECTED	**pattern:** passwd

09-08-2023 17:21:40	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:21:52	KBD_INPUT	adduser test4
09-08-2023 17:21:56	KBD_INPUT	passwd test4
09-08-2023 17:22:07	KBD_INPUT	visudo

ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

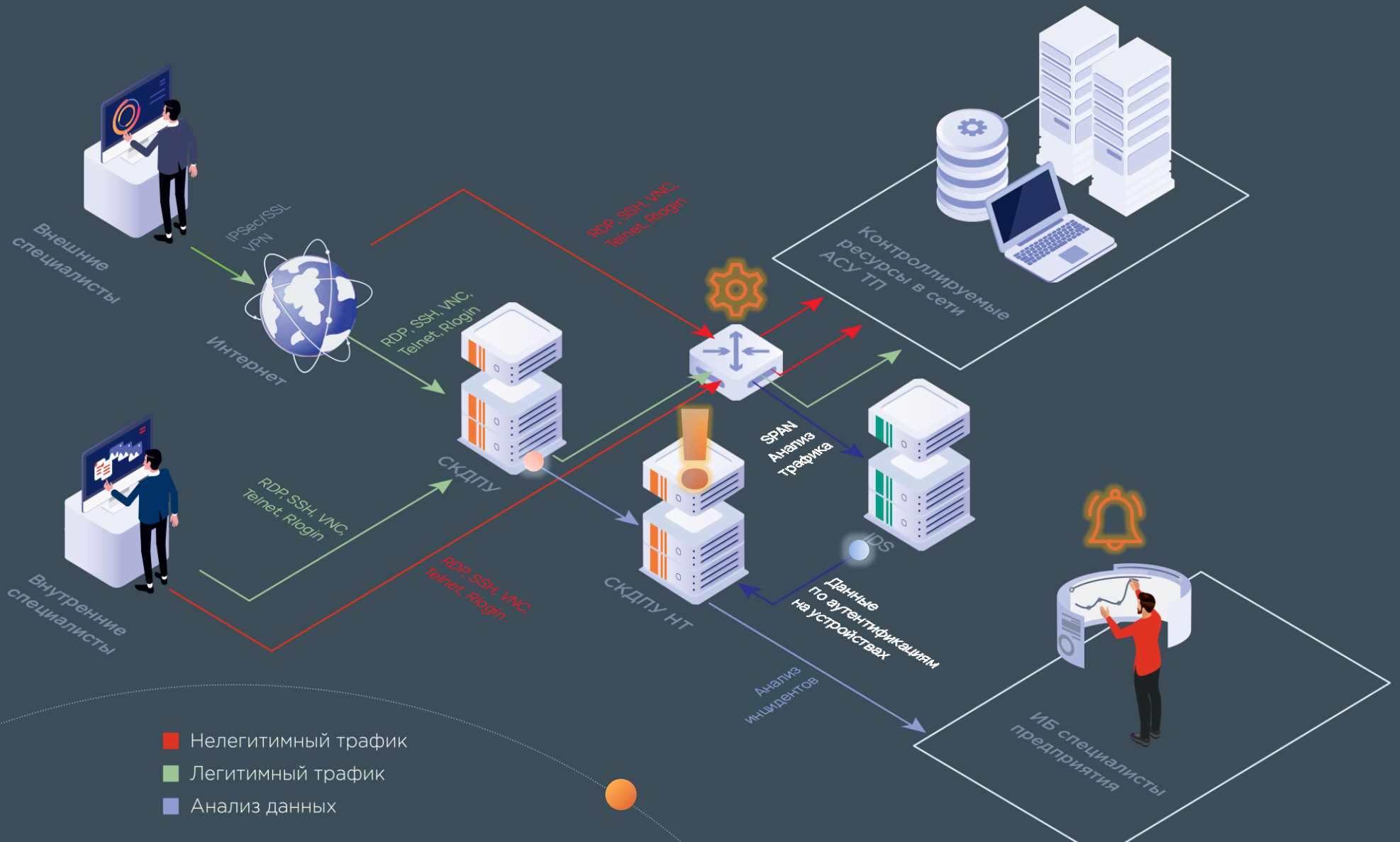
ИТОГ

ЛЮБОЙ СЦЕНАРИЙ РЕАЛИЗУЕМ ПРИ НАЛИЧИИ ВОЗМОЖНОСТИ

КАК НЕ ДОПУСТИТЬ ТАКОГО СЦЕНАРИЯ?

КЕЙС №3
ХИТРЫЙ ДОСТУП *(как не допустить)*

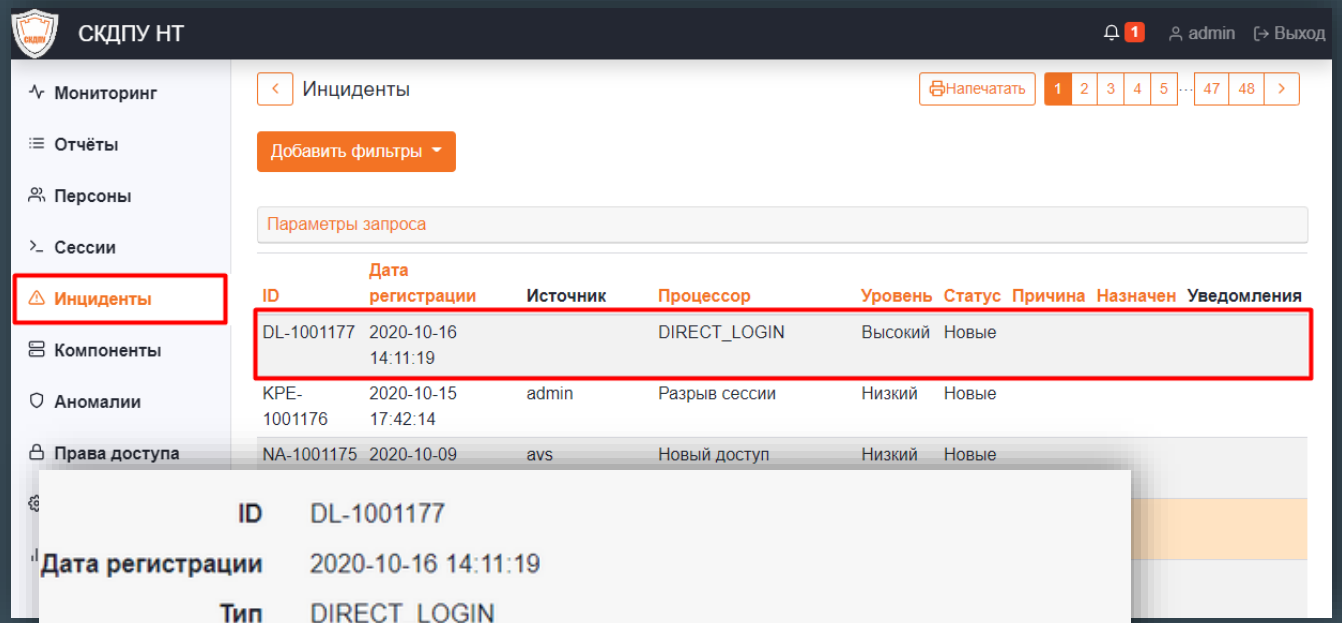
АЙТИБАСТИОН

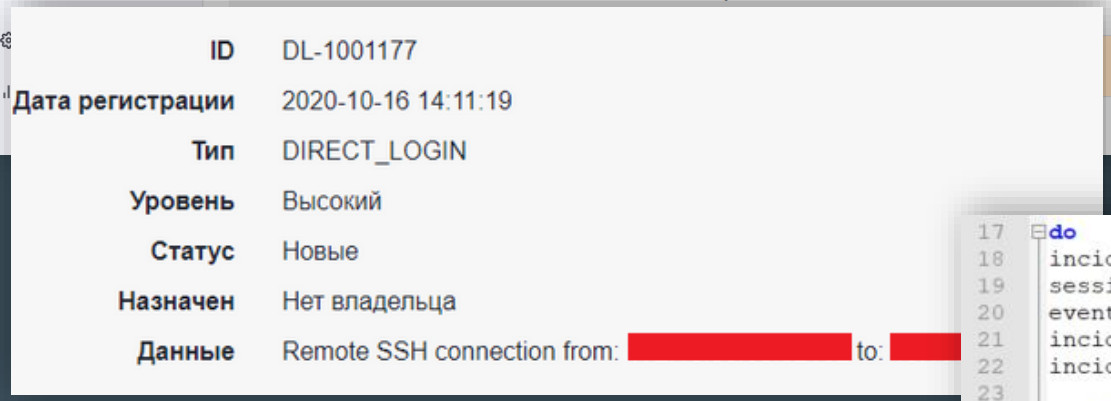


www.it-bastion.com

КЕЙС №3
ХИТРЫЙ ДОСТУП *(как не допустить)*

АЙТИБАСТИОН






```
do
incident=$(echo "${incident}" | base64 --decode)
session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
incident_id=$(echo "${incident}" | jq -r '.data.indent')
incident_link=$(echo "${incident}" | jq -r '.incident_link')

    if [ "$event_type" == "NEW_PROCESS" ]; then
        curl -k -X PUT \
    -H "X-Auth-Key: $xtoken" \
    -H "X-Auth-User: $xuser" \
    -H "Content-Type: application/json" \
    -d "{\"reason\":\"$incident_id\n$incident_link\"}" \
    "https://${api_address}/api/sessions?session_id=${session_id}&action=kill"
    fi
done
```

АВТОМАТИЗАЦИЯ

Возможность автоматизации реагирования на инциденты безопасности

www.it-bastion.com

АЙТИБАСТИОН

КЕЙС 3
ВРЕМЯ - ДЕНЬГИ

Как сохранить деньги при привлечении подрядчиков

КЕЙС №1
ВРЕМЯ ДЕНЬГИ

АЙТИБАСТИОН

ДОП. СОГЛАШЕНИЕ

Заказчик запросил дополнительное соглашение, за дополнительную оплату из-за сложности проводимых работ

РЕАЛЬНОЕ ВРЕМЯ

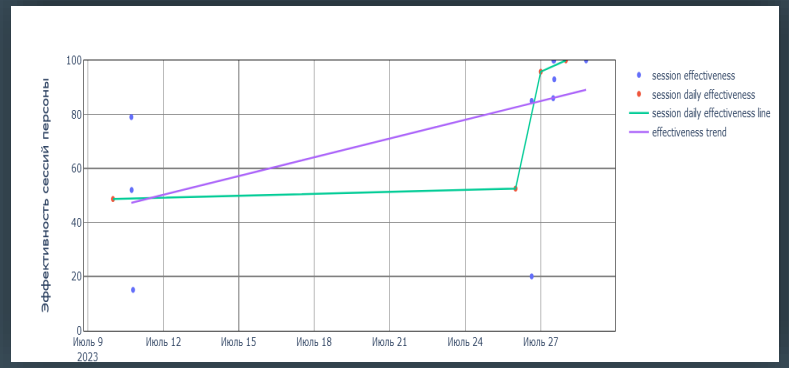
Какое реальное время работы подрядчика?

ОБЪЕМ ВЫПОЛНЕННЫХ РАБОТ

Какой объем выполненных работ?

ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени

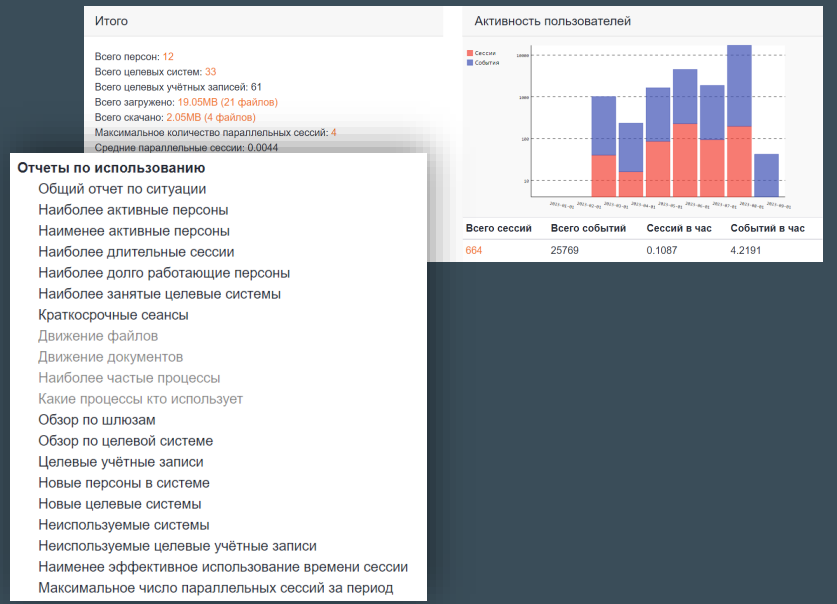


ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени

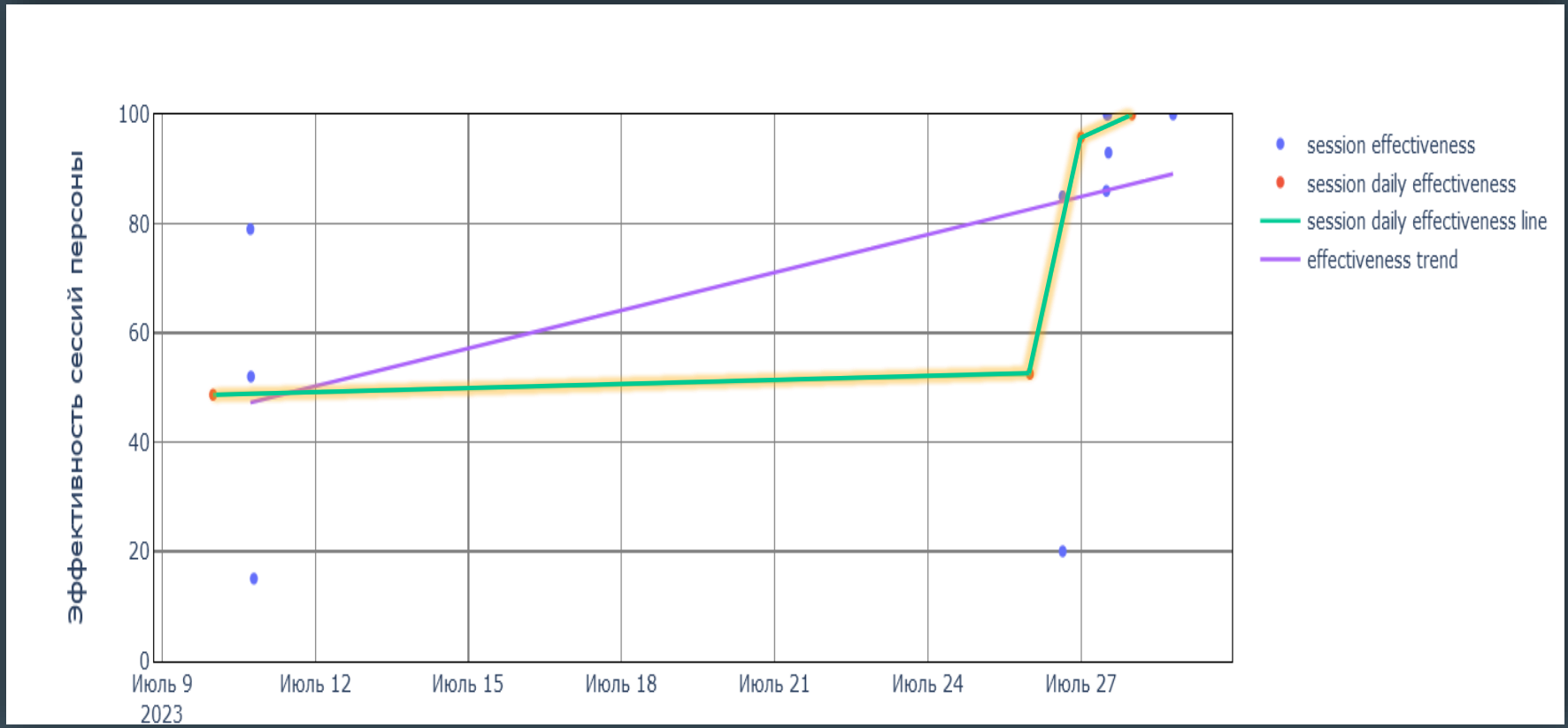
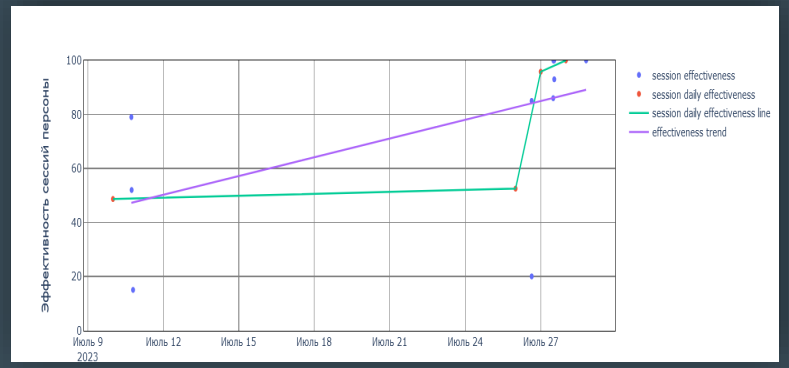


ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



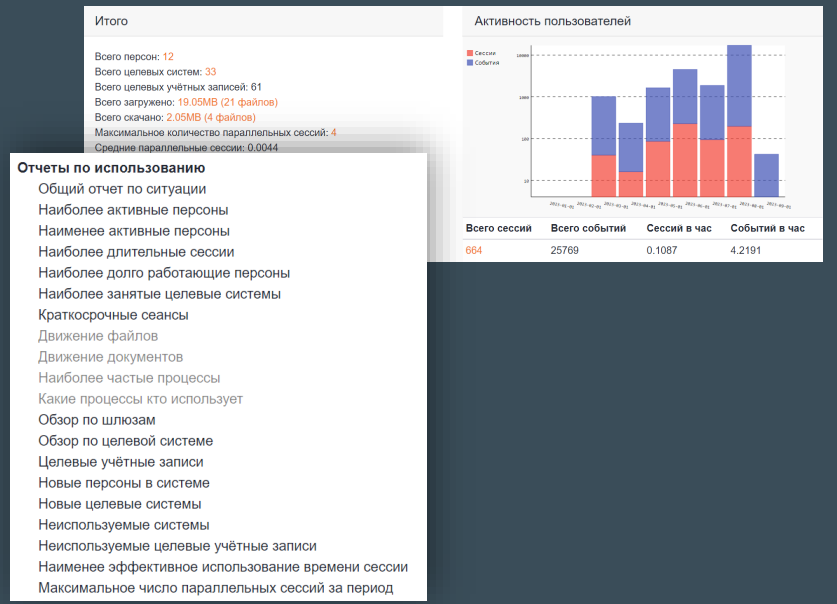
Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени



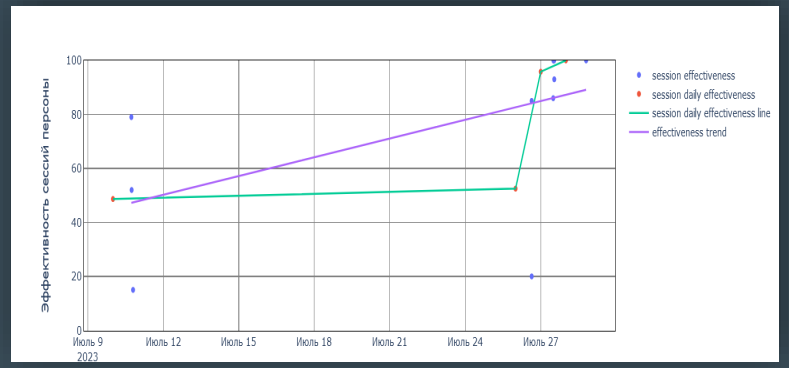
Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



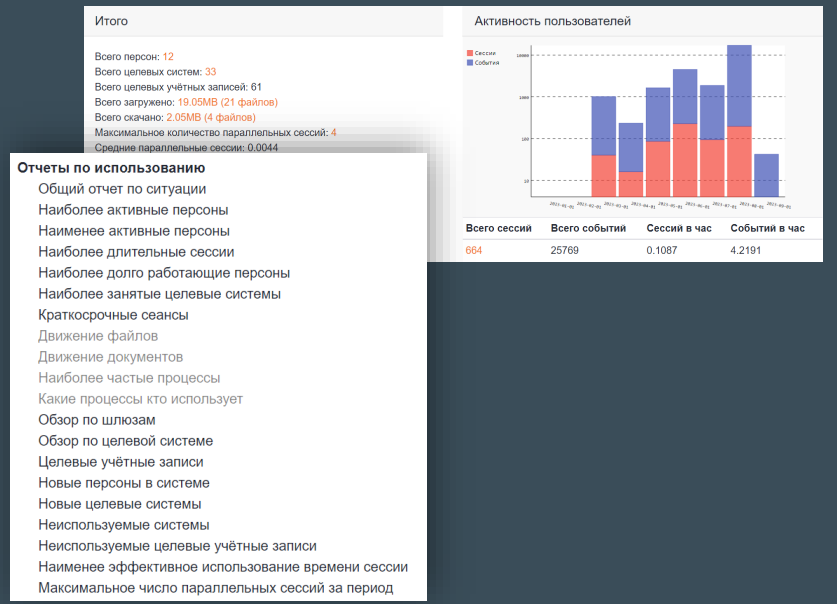
Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени



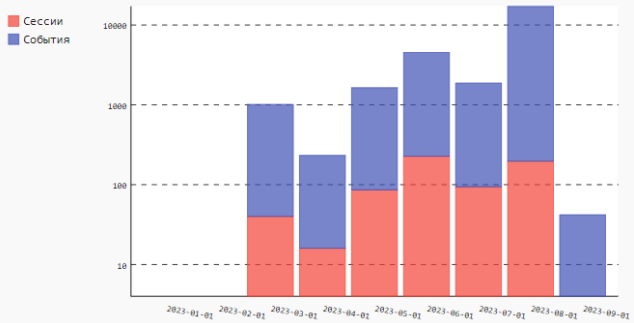
ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени

Итого

Всего персон: 12
Всего целевых систем: 33
Всего целевых учётных записей: 61
Всего загружено: 19.05MB (21 файлов)
Всего скачано: 2.05MB (4 файлов)
Максимальное количество параллельных сессий: 4
Средние параллельные сессии: 0.0044

Активность пользователей



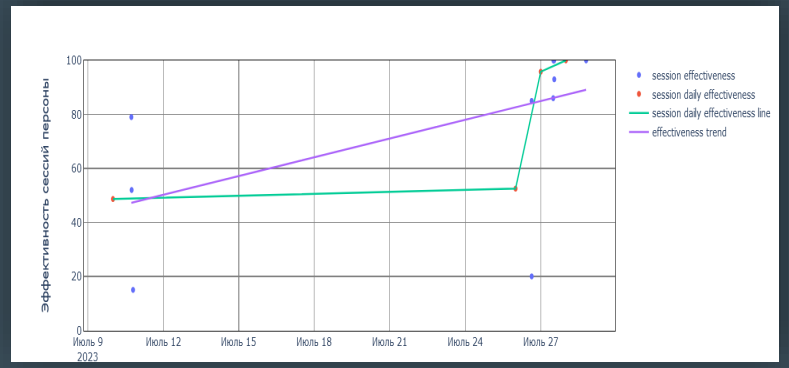
Всего сессий	Всего событий	Сессий в час	Событий в час
664	25769	0.1087	4.2191

Отчеты по использованию

- Общий отчет по ситуации
- Наиболее активные персоны
- Наименее активные персоны
- Наиболее длительные сессии
- Наиболее долго работающие персоны
- Наиболее занятые целевые системы
- Краткосрочные сеансы
- Движение файлов
- Движение документов
- Наиболее частые процессы
- Какие процессы кто использует
- Обзор по шлюзам
- Обзор по целевой системе
- Целевые учётные записи
- Новые персоны в системе
- Новые целевые системы
- Неиспользуемые системы
- Неиспользуемые целевые учётные записи
- Наименее эффективное использование времени сессии
- Максимальное число параллельных сессий за период

ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



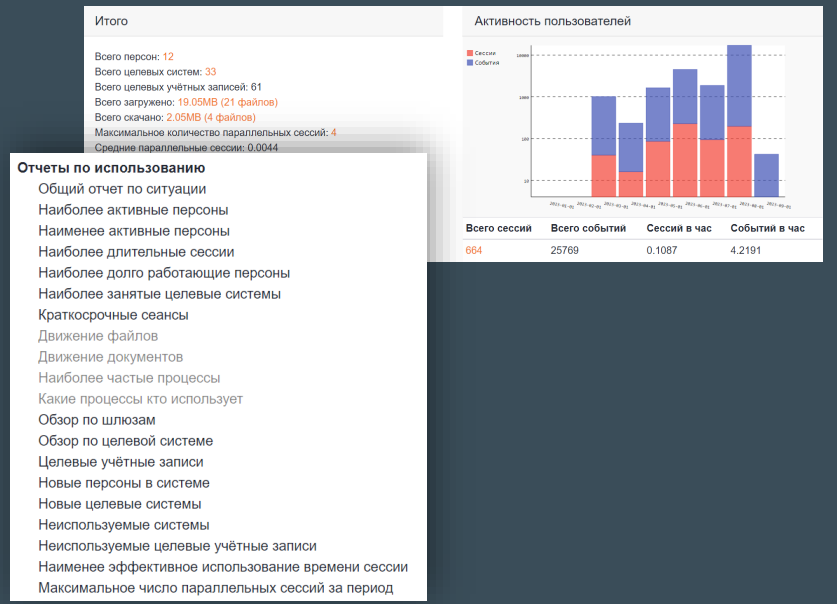
Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени

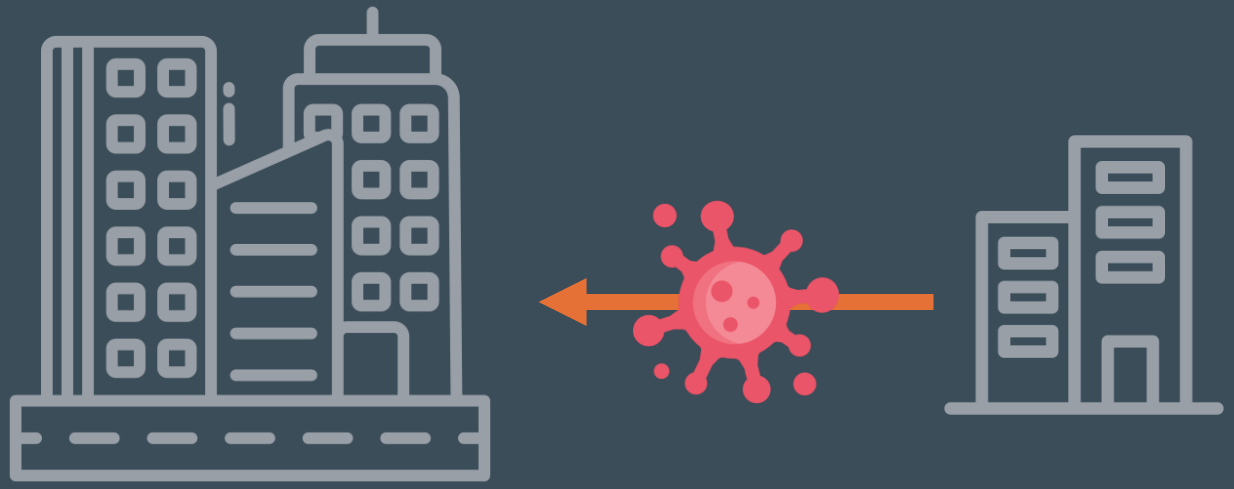


ИТОГ

ЭКОНОМИЯ РЕСУРСОВ И ФИНАНСОВ

АЙТИБАСТИОН

КЕЙС 4
ЧУЖИЕ ОШИБКИ



Предотвращение халатного отношнеия к информационной безопасности

АЙТИБАСТИОН

КЕЙС 5
УВОЛЕН

RJ-1093922 09-08-2023 14:23:29 [redacted] [redacted] Туннели и прыжки Низкий 10

WIN-Администратор@local-RDP-AUT1_otp(68) — [redacted] — Подключение к удаленному рабочему столу

The process 'mstsc.exe' was interrupted in accordance with security policies. (insert key or left click to hide)

ВОЗМОЖНЫ
ДАЛЬНЕЙШИЕ ДЕЙСТВИЯ
ПО СЦЕНАРИЮ КЕЙСА 2

Обезопасить компанию от
намеренного влияния
человеческого фактора

ЧТО МОЖЕТ ДАТЬ PAM?

АЙТИБАСТИОН

- Контроль действий
- Ретросектиктивный анализ
- Реагирование на инциденты
- Однозначная идентификаци
- Ролевая модель
- Поведенческий анализ
- Блокировка воздействия на инфраструктуру
- Предоставление разобранных данных
- Экономия ресурсов
- И т.д.

АЙТИБАСТИОН

Благодарю за внимание!

ШИРИКАЛОВ АЛЕКСЕЙ


a.shirikalov@it-bastion.com


+7 499 322 3667


it-bastion.com