АЙТИБАСТИОН

www.it-bastion.com

2025

ОТ КОНТРОЛЯ ДО РАССЛЕДОВАНИЯ: ПРАКТИЧЕСКАЯ КИБЕРБЕЗОПАСНОСТЬ С СКДПУ НТ

ИВАН БАРАНОВСКИЙ

КОМПАНИЯ
АЙТИ БАСТИОН

АЙТИБАСТИОН

2014

300+

ОСНОВАНИЕ КОМПАНИИ

10 лет на российском рынке
информационной безопасности

КОМПАНИЯ
АЙТИ БАСТИОН

АЙТИБАСТИОН

300+

250+

ПАРТНЕРОВ-ИНТЕГРАТОРОВ

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

КОМПАНИЯ
АЙТИ БАСТИОН

АЙТИБАСТИОН

250+

>70%

ЗАКАЗЧИКОВ И ПРОЕКТОВ

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

КОМПАНИЯ
АЙТИ БАСТИОН

АЙТИБАСТИОН

>70%

РАМ-РЫНКА РФ

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

КОМПАНИЯ
АЙТИ БАСТИОН

АЙТИБАСТИОН

2014

300+

250+

>70%

ОСНОВАНИЕ КОМПАНИИ
10 лет на российском рынке информационной безопасности

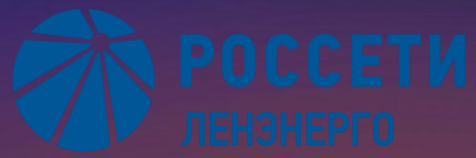
ПАРТНЕРОВ-ИНТЕГРАТОРОВ
Интеграции с компаниями, позволяющие выполнить квалифицированную помощь в реализации защиты инфраструктуры

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

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

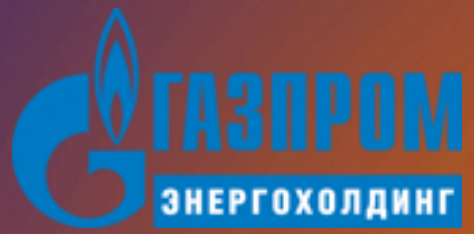
ЗАКАЗЧИКИ

АЙТИБАСТИОН



ПРАВИТЕЛЬСТВО
МОСКВЫ

МИНИСТЕРСТВО
ТРАНСПОРТА РФ



ЧТО ТАКОЕ PAM?

АЙТИБАСТИОН

Privileged Access Management (PAM) – Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам, которое тем самым помогает защитить организации от киберугроз

www.it-bastion.com

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

АЙТИБАСТИОН

Соответствие требованиям

ФЗ-187 «О безопасности КИИ РФ», Приказы ФСТЭК России №239, №235, Приказы ФСТЭК России № 31, № 17, № 21, Указ Президента РФ от 01.05.2022 №250

Базовая ОС

Комплекс работает под управление ОС AstraLinux SE, внесенной в реестр отечественного ПО, и имеет сертификаты ФСТЭК, ФСБ и МО

Варианты поставки

Комплекс может быть реализован как в виртуальной среде, так и в виде ПАК.

Сертификаты и реестр

Включен в реестр отечественного ПО, Сертификат ФСТЭК УД-4, Сертификат МО РФ НДВ-2

Целевые и клиентские ОС

Поддерживается работа с различными ОС как для клиентских, так и для целевых систем – AstraLinux, РЕД ОС, Альт, Windows и др.
Поддержка FreeIPA, ALD Pro и других LDAP

Техническая поддержка

осуществляется сотрудниками компании и специалистами партнера, в т.ч. в режиме 24/7.

www.it-bastion.com

РАМ-ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

Шлюз доступа включает в себя:

- модуль контроля сессий;
- менеджер паролей;
- модуль отказоустойчивости и катастрофоустойчивости.

Мониторинг и аналитика включает в себя:

- модуль мониторинга и отчетности;
- модуль поведенческого анализа, включая детектирование аномалий, инцидентов, реагирование и расширенной статистики

Портал доступа

Кабинет оператора

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

ЕДИНАЯ ТОЧКА ДОСТУПА

Единая точка доступа в инфраструктуру (SSO). Гибкая ролевая модель доступов с возможностью интеграции в существующую инфраструктуру (LDAP, AD, Radius)

ЗАПИСЬ СОБЫТИЙ ДОСТУПА

Полная запись видео и метаданных сессий с созданием долгосрочного архива. Клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и т.д. А наличие сертификата ФСТЭК по УД-4 гарантирует неизменяемость данных для использовании их в качестве доказательно базы

УПРАВЛЕНИЕ ПАРОЛЯМИ

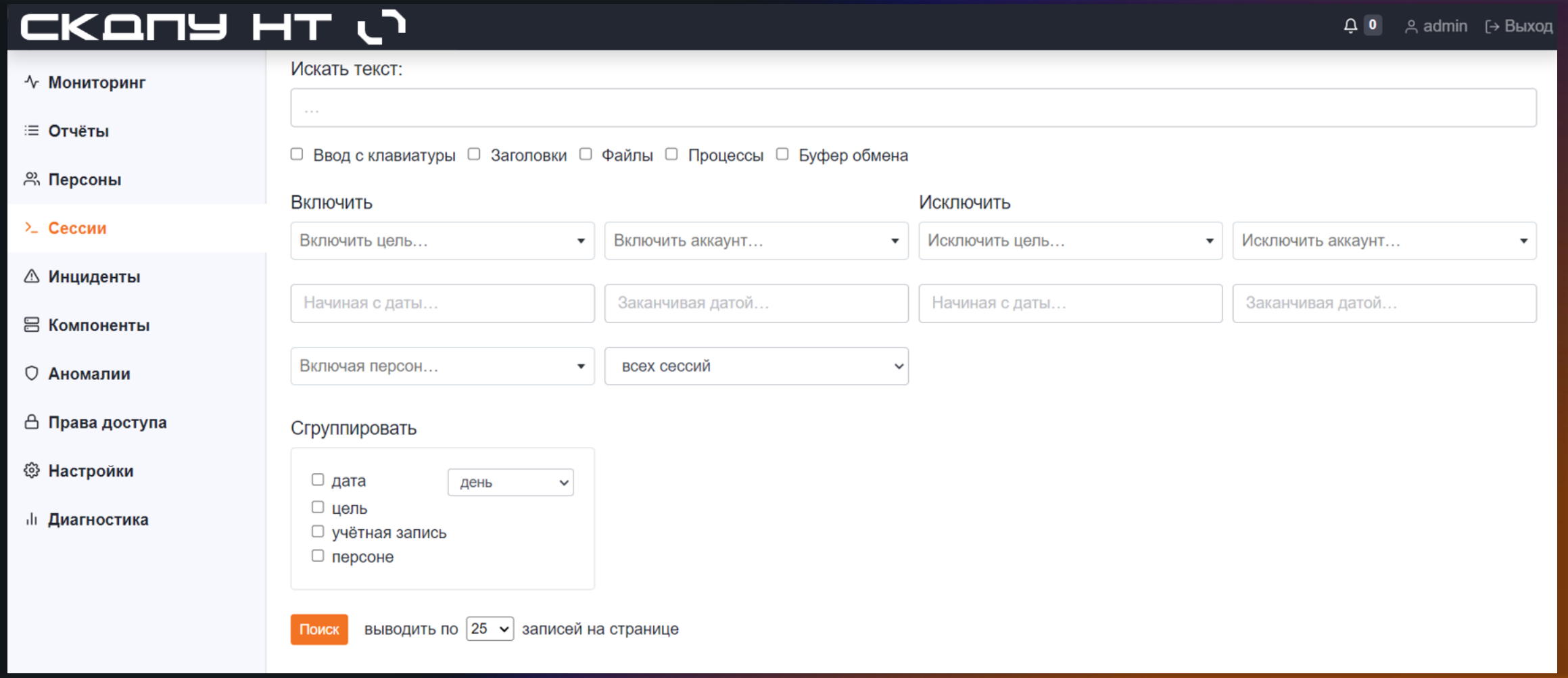
Управление паролями целевых учетных записей без необходимости установки агентов на целевые устройства по настраиваемым политикам

БЕЗ УСТАНОВКИ АГЕНТОВ

Подключение к ЦУ без необходимости установки агентов, что особенно важно при подключении к объектам КИИ

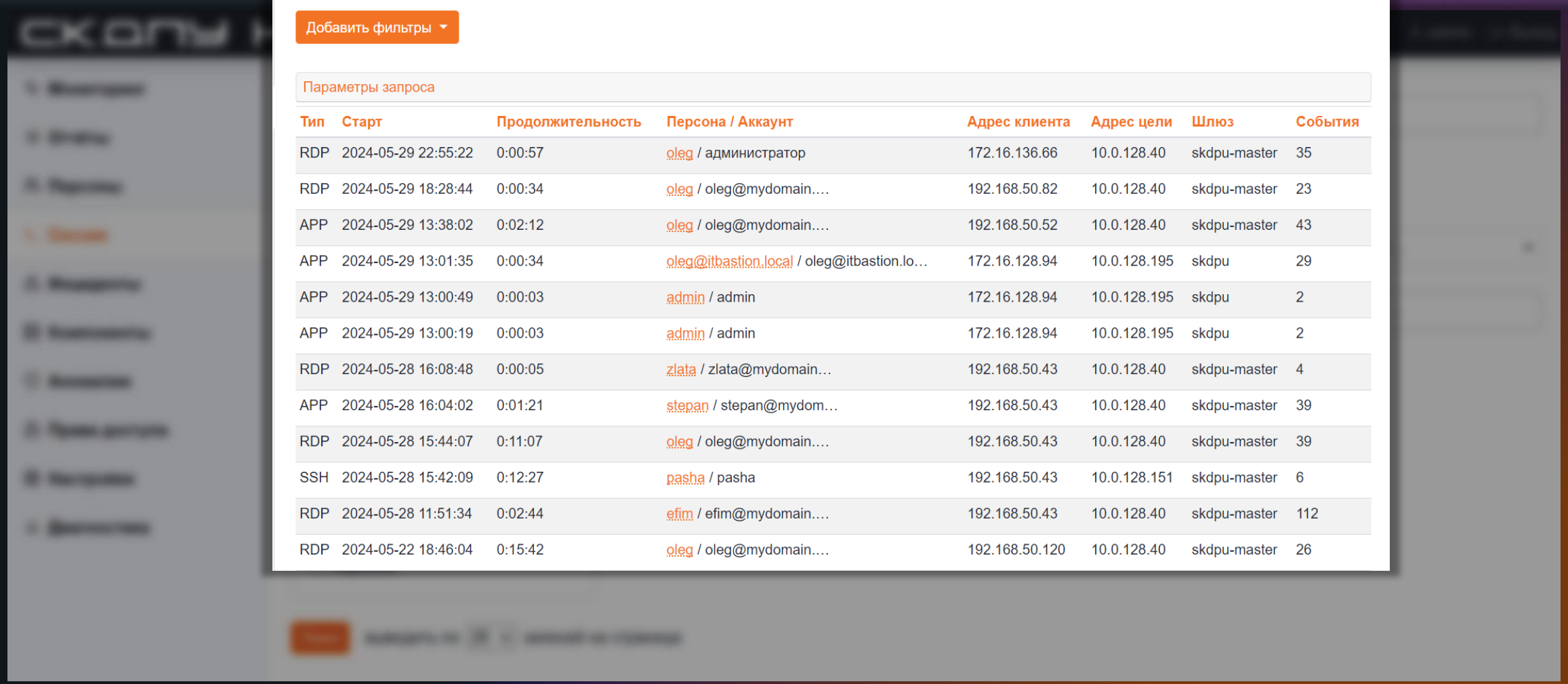
ЦЕНТРАЛИЗОВАННЫЙ АУДИТ ДАННЫХ И СОБЫТИЙ ПО СЕССИЯМ

АЙТИБАСТИОН



ЦЕНТРАЛИЗОВАННЫЙ АУДИТ
ДАННЫХ И СОБЫТИЙ ПО СЕССИЯМ

АЙТИБАСТИОН



Сессии: 620, 2024-06-01 23:10:01

Напечатать

1 2 3 4 5 … 24 25

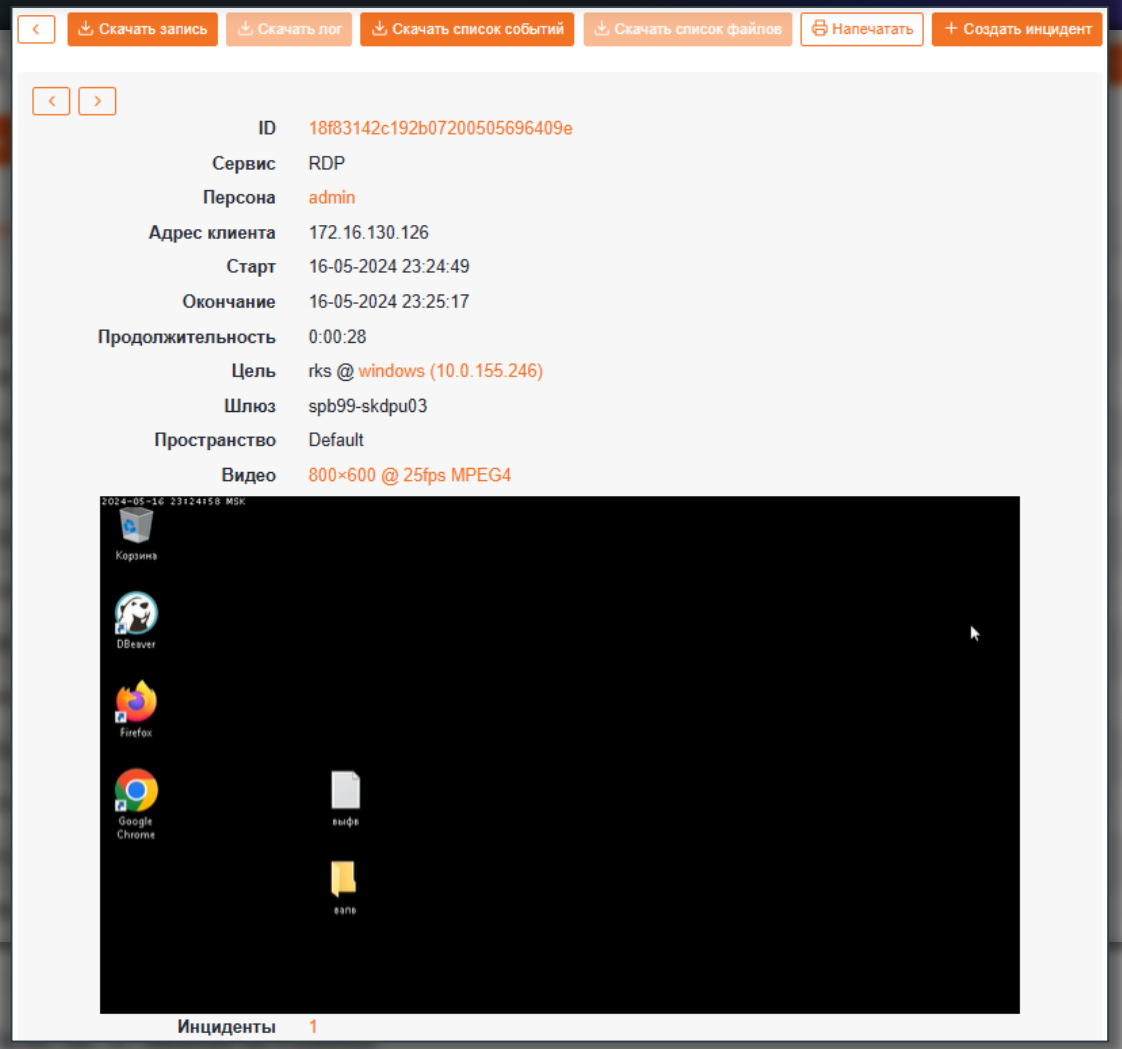
Добавить фильтры

Параметры запроса

Тип	Старт	Продолжительность	Персона / Аккаунт	Адрес клиента	Адрес цели	Шлюз	События
RDP	2024-05-29 22:55:22	0:00:57	oleg / администратор	172.16.136.66	10.0.128.40	skdpu-master	35
RDP	2024-05-29 18:28:44	0:00:34	oleg / oleg@mydomain.…	192.168.50.82	10.0.128.40	skdpu-master	23
APP	2024-05-29 13:38:02	0:02:12	oleg / oleg@mydomain.…	192.168.50.52	10.0.128.40	skdpu-master	43
APP	2024-05-29 13:01:35	0:00:34	oleg@itbastion.local / oleg@itbastion.lo…	172.16.128.94	10.0.128.195	skdpu	29
APP	2024-05-29 13:00:49	0:00:03	admin / admin	172.16.128.94	10.0.128.195	skdpu	2
APP	2024-05-29 13:00:19	0:00:03	admin / admin	172.16.128.94	10.0.128.195	skdpu	2
RDP	2024-05-28 16:08:48	0:00:05	zlata / zlata@mydomain…	192.168.50.43	10.0.128.40	skdpu-master	4
APP	2024-05-28 16:04:02	0:01:21	stepan / stepan@mydom…	192.168.50.43	10.0.128.40	skdpu-master	39
RDP	2024-05-28 15:44:07	0:11:07	oleg / oleg@mydomain.…	192.168.50.43	10.0.128.40	skdpu-master	39
SSH	2024-05-28 15:42:09	0:12:27	pasha / pasha	192.168.50.43	10.0.128.151	skdpu-master	6
RDP	2024-05-28 11:51:34	0:02:44	efim / efim@mydomain.…	192.168.50.43	10.0.128.40	skdpu-master	112
RDP	2024-05-22 18:46:04	0:15:42	oleg / oleg@mydomain.…	192.168.50.120	10.0.128.40	skdpu-master	26

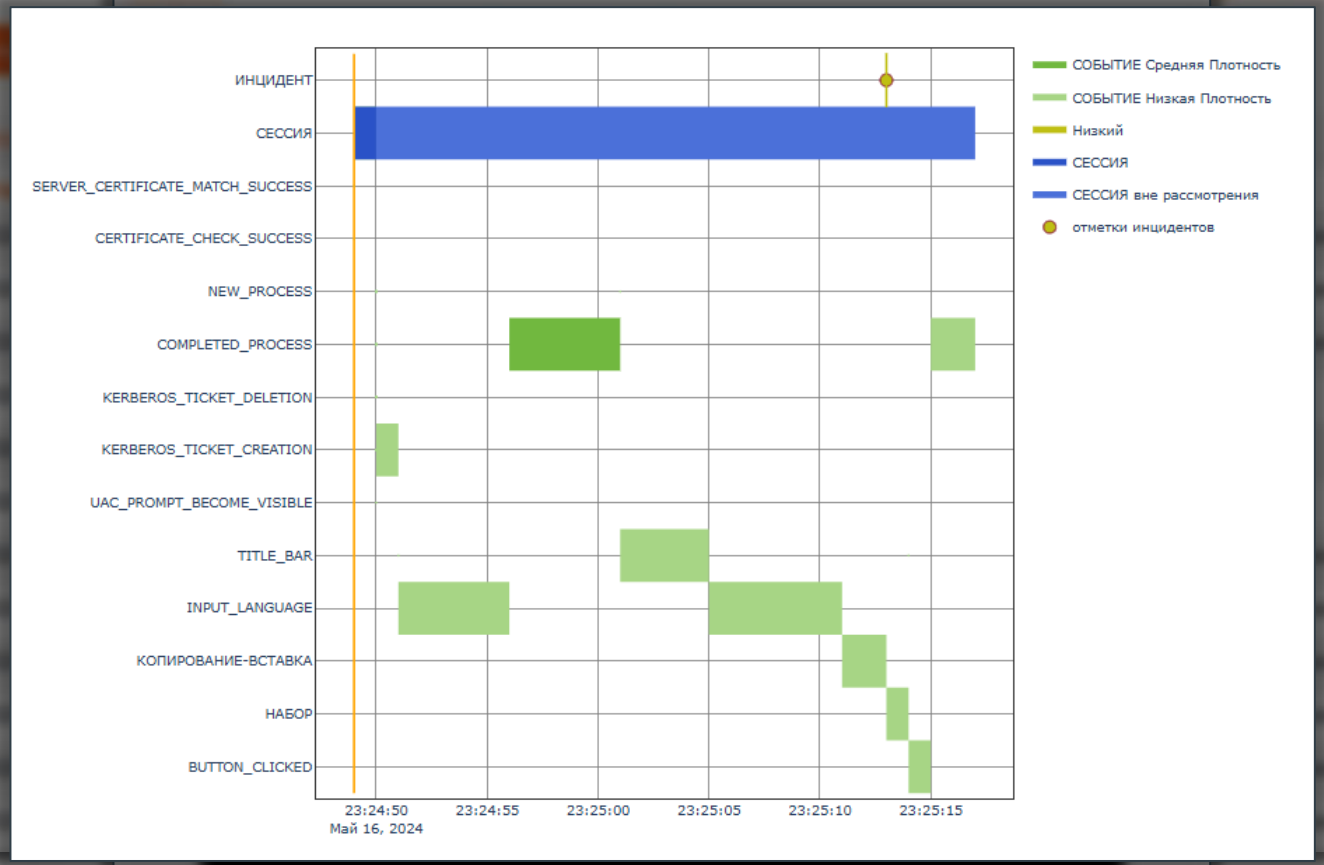
ЦЕНТРАЛИЗОВАННЫЙ АУДИТ
ДАННЫХ И СОБЫТИЙ ПО СЕССИЯМ

АЙТИБАСТИОН



ЦЕНТРАЛИЗОВАННЫЙ АУДИТ
ДАННЫХ И СОБЫТИЙ ПО СЕССИЯМ

АЙТИБАСТИОН



ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

КОНТРОЛЬ ПРИЛОЖЕНИЙ И УЗ В НИХ

Подключение к конечным приложениям без предоставления полного доступа с сокрытием УЗ от приложений.

ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ

Возможность не только контролировать сессию по её результату, но и видеть все действия в режиме реального времени. А в случае необходимости - блокировать сессию пользователя, предотвращая потенциальную угрозу.

РАБОТА ПО ЗАЯВКАМ С ВОЗМОЖНОСТЬЮ ПОДТВЕРЖДЕНИЯ ДОСТУПА

Возможность предоставления доступа по запросу как в момент подключения, так и заранее. Согласование доступа возможно с добавлением одного и более подтверждающих лиц.

КОНТРОЛЬ НА СТОРОНЕ ИС

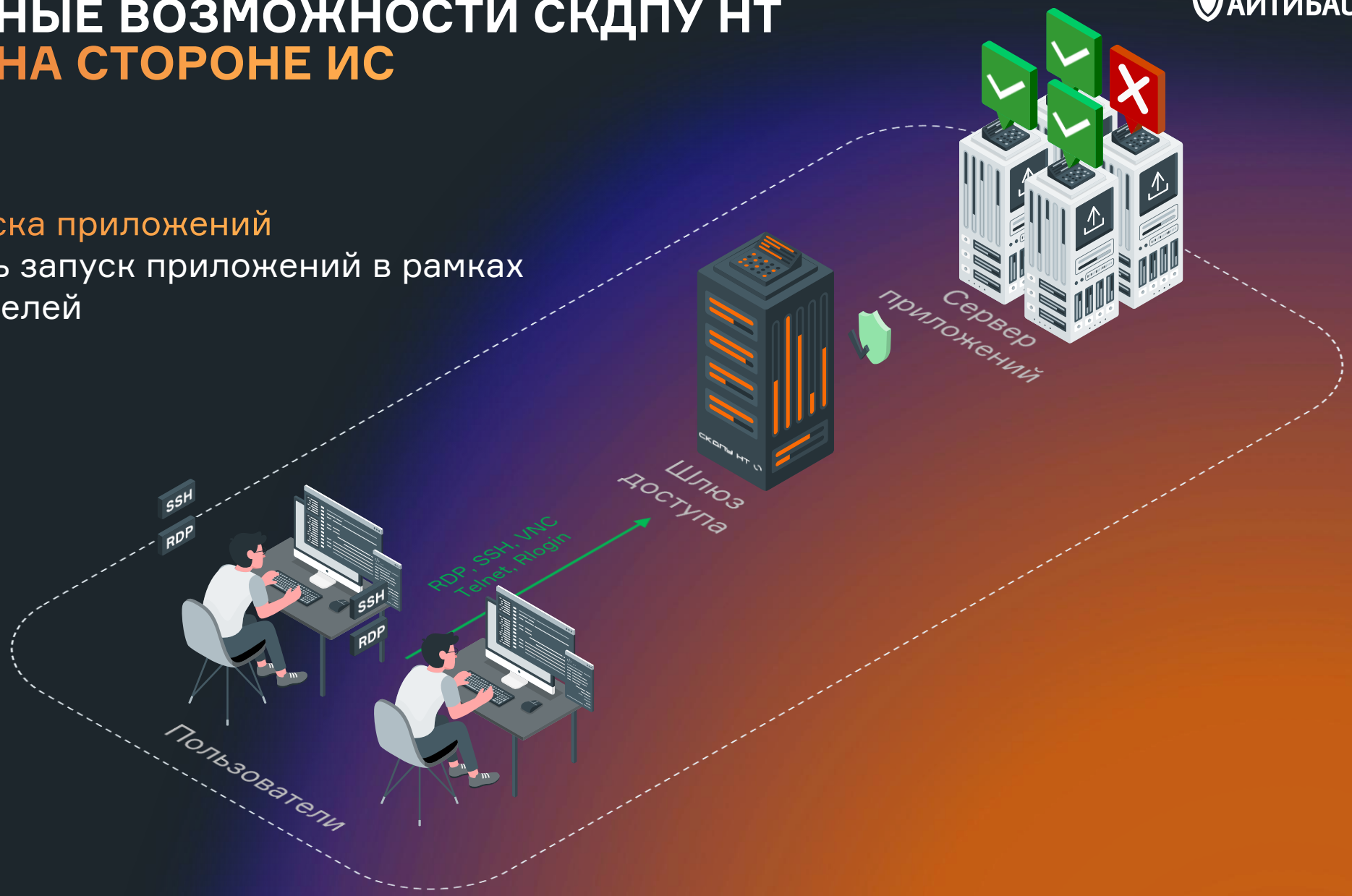
Блокировка туннелей, доступа вне разрешенных диапазонов, запрет на запуск процессов и т.д.

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ СКДПУ НТ
КОНТРОЛЬ НА СТОРОНЕ ИС

АЙТИБАСТИОН

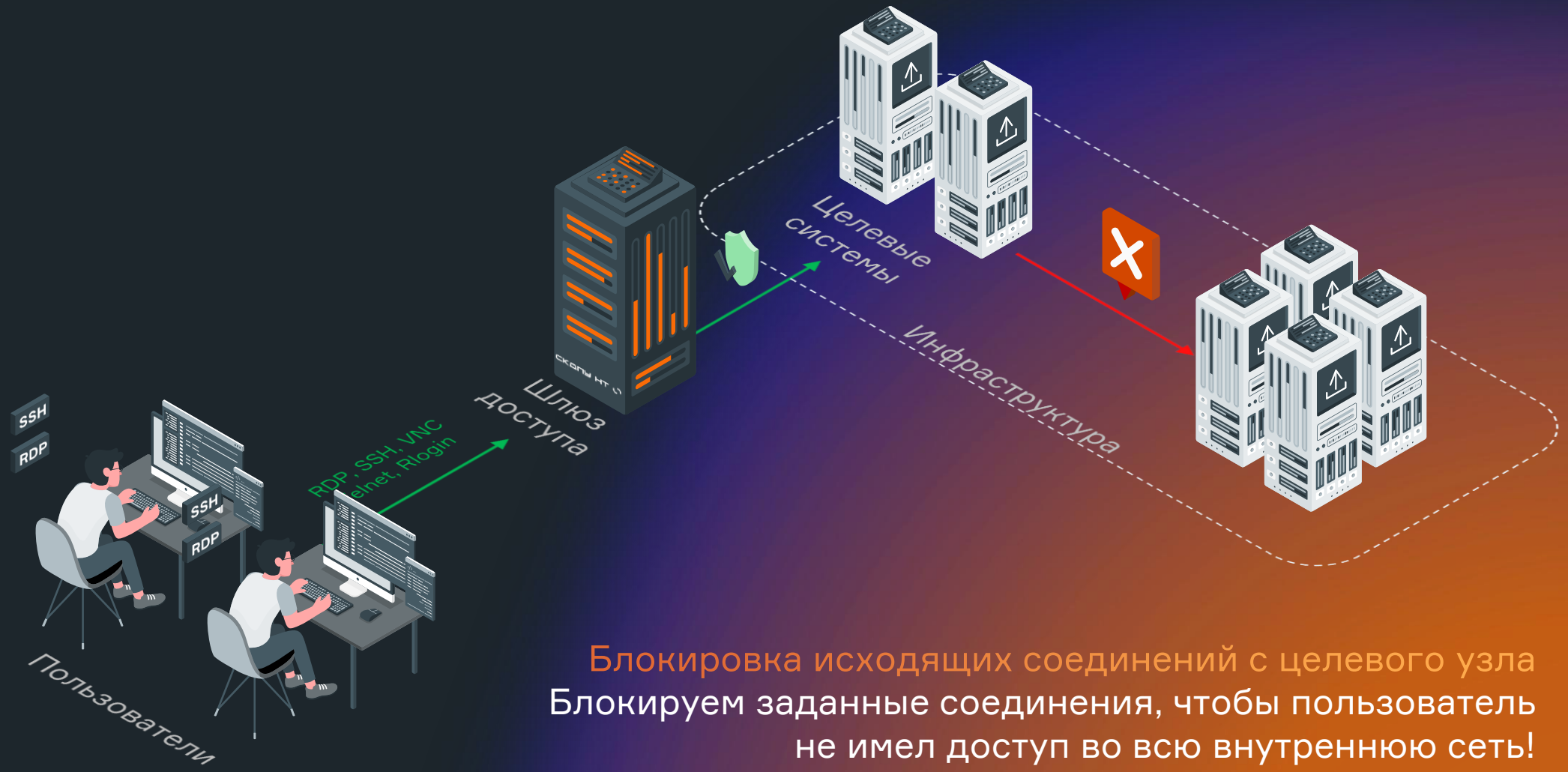
Блокировка запуска приложений

Можем запрещать запуск приложений в рамках сессий пользователей



РАСШИРЕННЫЕ ВОЗМОЖНОСТИ СКДПУ НТ
КОНТРОЛЬ НА СТОРОНЕ ИС

АЙТИБАСТИОН



Блокировка исходящих соединений с целевого узла

Блокируем заданные соединения, чтобы пользователь не имел доступ во всю внутреннюю сеть!

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

ПРОФИЛИРОВАНИЕ И ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

Создание и ведение профилирования пользователей. Анализ всех действий в разрезе «пользователь-цель-действие», машинное обучение и математические модели.

ДЕТЕКТИРОВАНИЕ АНОМАЛИЙ

Предобработка, анализ и детектирование аномального поведения пользователей на основе профилирования и событий

ОТЧЕТЫ И СТАТИСТИКА

Обработка информации и её выдача в виде понятных отчетов от оперативных до сводных, в т.ч. для руководителей.

ОТКАЗОУСТОЙЧИВОСТЬ И МАСШТАБИРОВАНИЕ

Возможность построения действительно отказоустойчивых инсталляций, в т.ч. распределенных между городами и странами. Легкая возможность наращивать мощности как вертикально, так и горизонтально без привязки к территориальному расположению узлов.

НА ПРИМЕРЕ SUPPLY CHAIN

КЕЙС
SUPPLY CHAIN

ДОВЕРЕННЫЙ ПОДРЯДЧИК

Подрядчик, занимающийся поддержкой IT-инфраструктуры компании

УДАЛЕННЫЙ ДОСТУП

Подрядчику предоставлен удаленный доступ под индивидуальными УЗ в контур Заказчика

ОТСУТСТВИЕ РЕГЛАМЕНТА

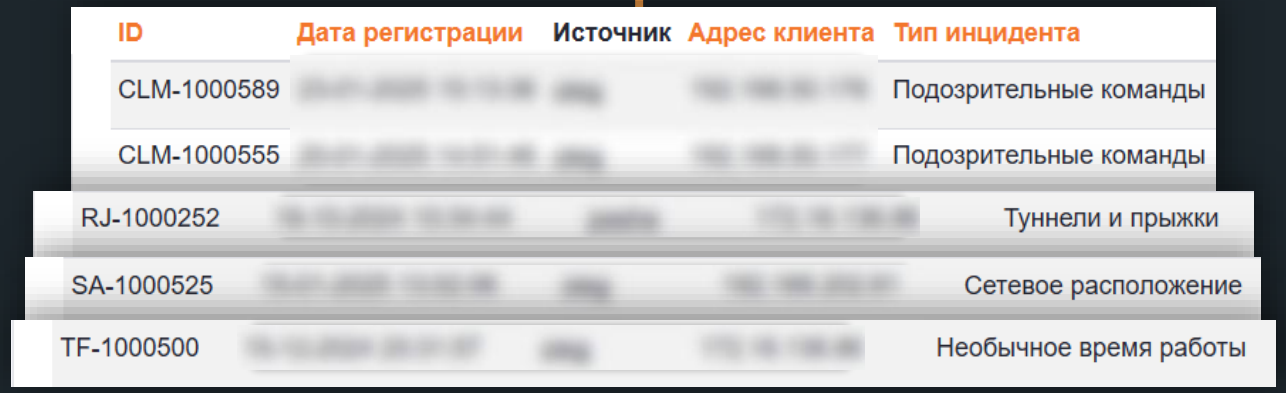
Подрядной организации не предъявляется регламент по ИБ

ФИКСАЦИЯ ИНЦИДЕНТА

Выявление попытки выполнения нетипичных команд в нетипичное для пользователя время.
Автоматические оповещения о подозрительных сетевых взаимодействиях. Подключение с нетипичных адресов.

ОПОВЕЩЕНИЕ

Уведомление подрядчика об аномальном поведении их пользователя



ID	Дата регистрации	Источник	Адрес клиента	Тип инцидента
CLM-1000589				Подозрительные команды
CLM-1000555				Подозрительные команды
RJ-1000252				Туннели и прыжки
SA-1000525				Сетевое расположение
TF-1000500				Необычное время работы

РЕАГИРОВАНИЕ

Разрыв сессии и блокировка пользователя

ФИКСАЦИЯ ИНЦИДЕНТА

Выявление попытки выполнения нетипичных команд в нетипичное для пользователя время.
Автоматические оповещения о подозрительных сетевых взаимодействиях. Подключение с нетипичных адресов.

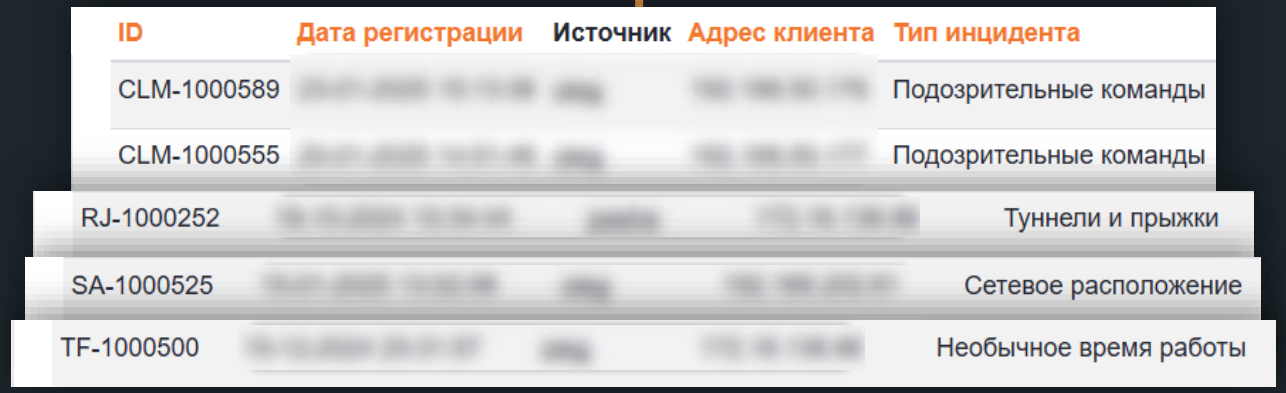
ID	Дата регистрации	Источник	Адрес клиента	Тип инцидента
CLM-1000589	[illegible]	[illegible]	[illegible]	Подозрительные команды
CLM-1000555	[illegible]	[illegible]	[illegible]	Подозрительные команды
RJ-1000252	[illegible]	[illegible]	[illegible]	Туннели и прыжки
SA-1000525	[illegible]	[illegible]	[illegible]	Сетевое расположение
TF-1000500	[illegible]	[illegible]	[illegible]	Необычное время работы

ФИКСАЦИЯ ИНЦИДЕНТА

Выявление попытки выполнения нетипичных команд в нетипичное для пользователя время.
Автоматические оповещения о подозрительных сетевых взаимодействиях. Подключение с нетипичных адресов.

ОПОВЕЩЕНИЕ

Уведомление подрядчика об аномальном поведении их пользователя



ID	Дата регистрации	Источник	Адрес клиента	Тип инцидента
CLM-1000589				Подозрительные команды
CLM-1000555				Подозрительные команды
RJ-1000252				Туннели и прыжки
SA-1000525				Сетевое расположение
TF-1000500				Необычное время работы

РЕАГИРОВАНИЕ

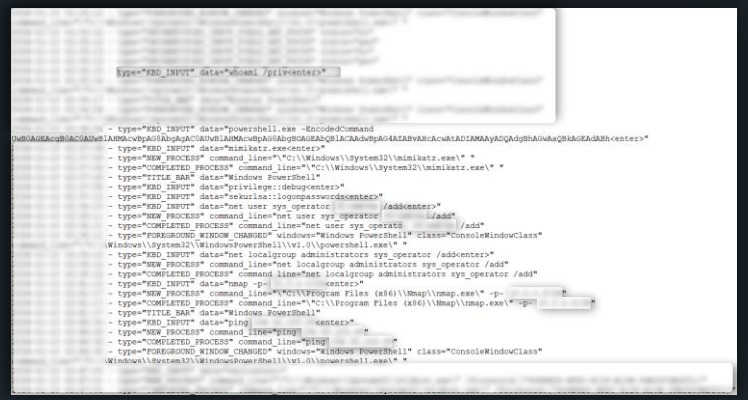
Разрыв сессии и блокировка пользователя

РАССЛЕДОВАНИЕ

Исследование логов для определения вектора атаки.
Выявление попытки выполнения команд, **whoami /priv, nmap, и mimikatz.exe**, а также аномальное использование PowerShell.
Взаимодействие с C2-серверами

ПЕРВИЧНАЯ ЗАЩИТА

Временное ограничение всех привилегий подрядчиков до минимально необходимого уровня

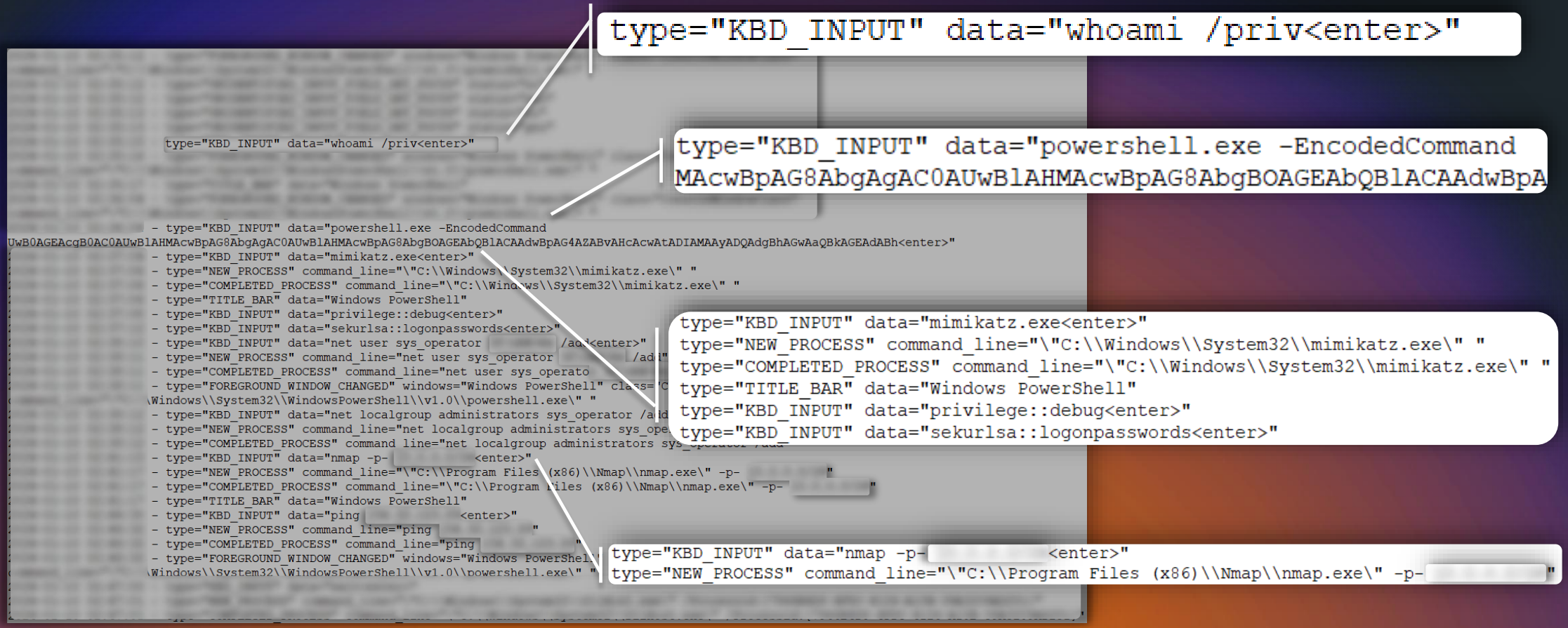


ВЫРАБОТКА МЕР

Блокировка подозрительных команд.
Фильтрация трафика по известным C2-адресам.
Усиление политики доступа подрядчиков.

РАССЛЕДОВАНИЕ

Исследование логов для определения вектора атаки.
Выявление попытки выполнения команд, **whoami /priv, nmap, и mimikatz.exe**, а также аномальное использование PowerShell.
Взаимодействие с C2-серверами

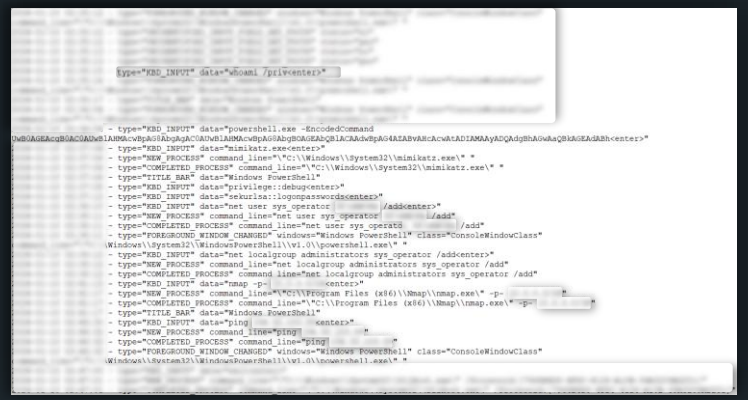


РАССЛЕДОВАНИЕ

Исследование логов для определения вектора атаки.
Выявление попытки выполнения команд, **whoami /priv, nmap, и mimikatz.exe**, а также аномальное использование PowerShell.
Взаимодействие с C2-серверами

ПЕРВИЧНАЯ ЗАЩИТА

Временное ограничение всех привилегий подрядчиков до минимально необходимого уровня



ВЫРАБОТКА МЕР

Блокировка подозрительных команд.
Фильтрация трафика по известным C2-адресам.
Усиление политики доступа подрядчиков.

ИНФОРМИРОВАНИЕ ПОДРЯДЧИКА И ОТРАСЛЕВЫХ ПАРТНЕРОВ

Отчет о векторе атаки, помог закрыть обнаруженные уязвимости и обеспечил информирование других компаний

BACKDOOR

КЕЙС
BACKDOOR

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

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.
##
```

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

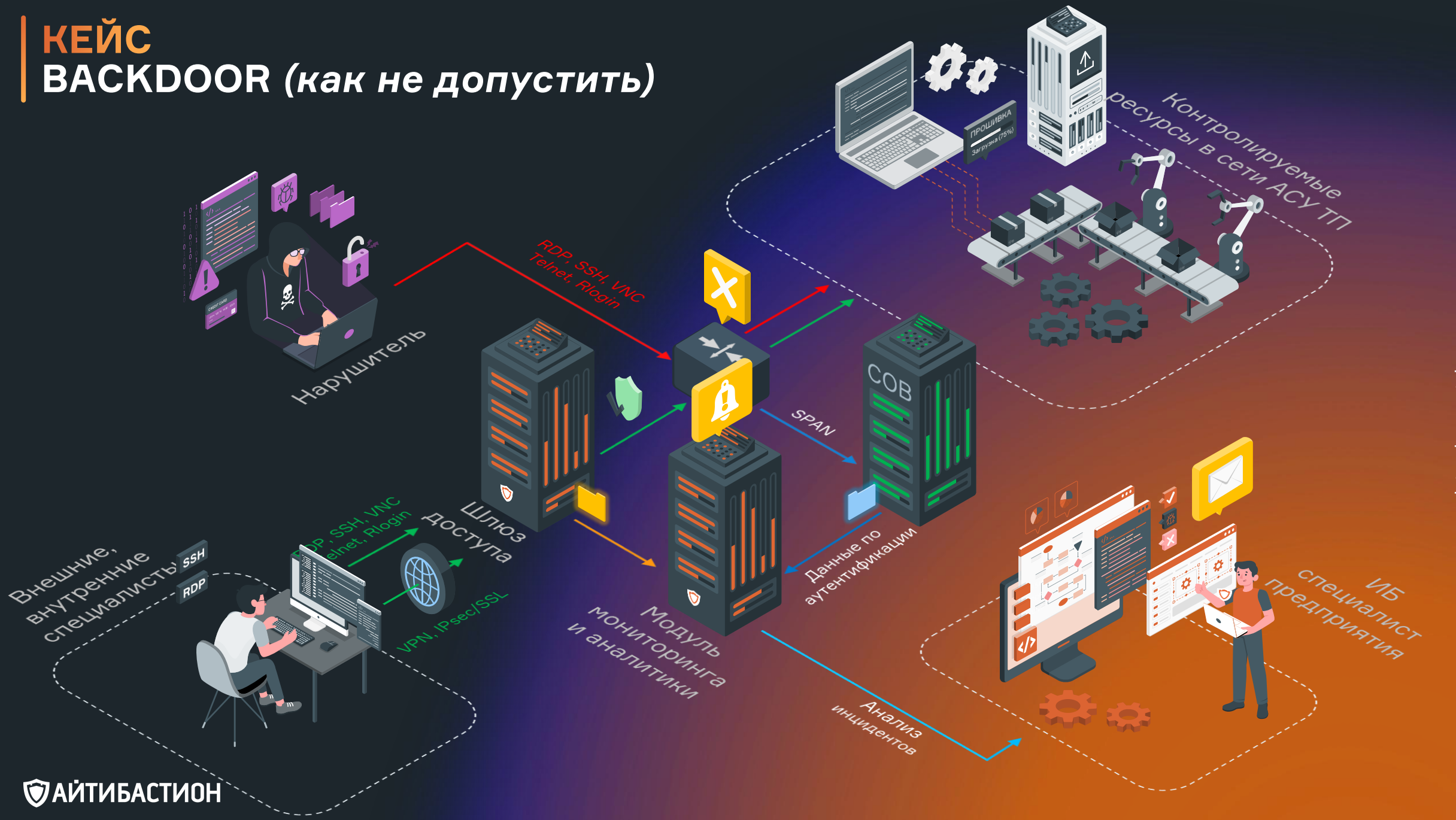
Фиксирование сессии с успешно отработанной командой

ОБНАРУЖЕНИЕ

Обнаружение нарушителя
и применение
административных мер

КАК НЕ ДОПУСТИТЬ ТАКОГО СЦЕНАРИЯ?

КЕЙС
BACKDOOR (*как не допустить*)

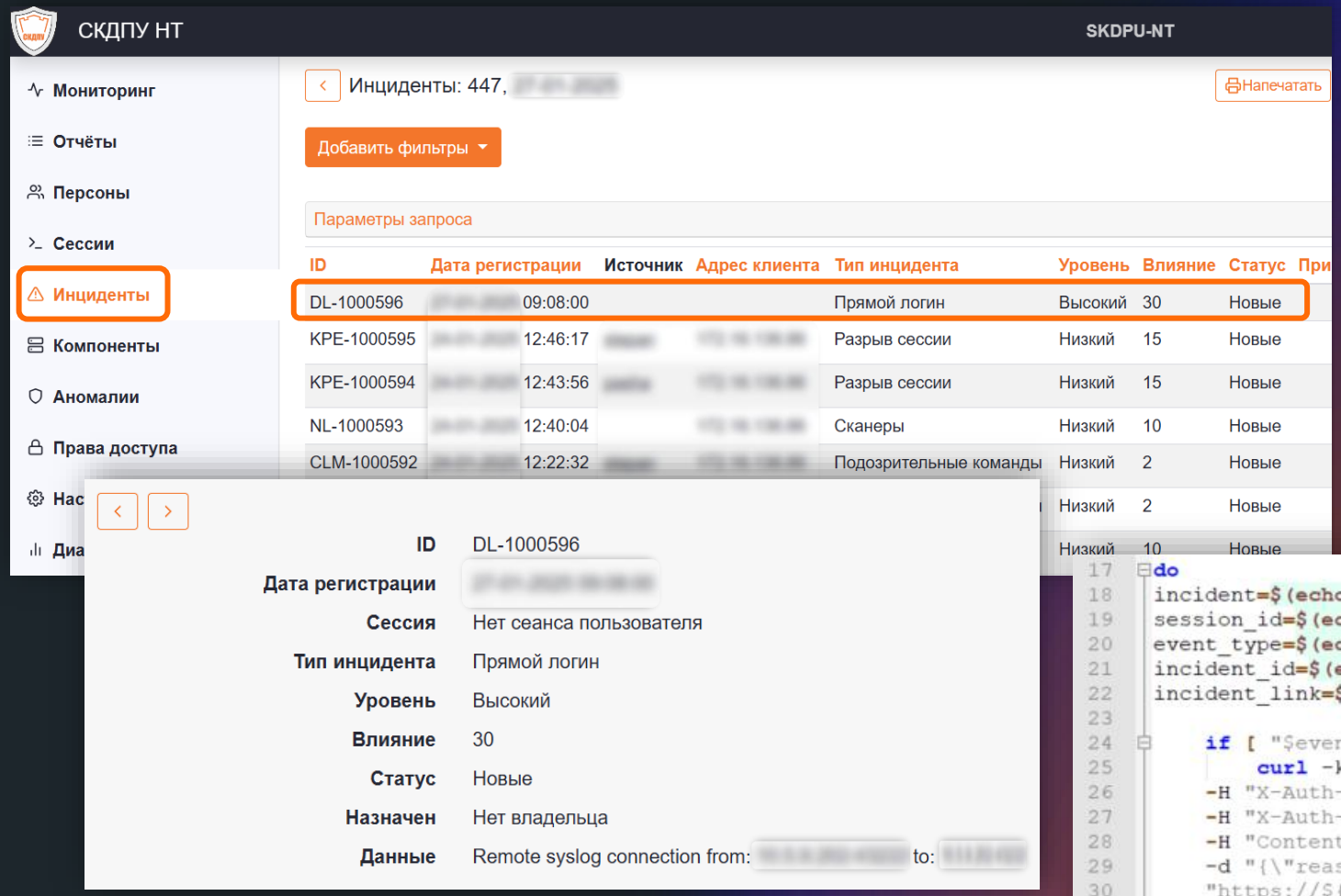


АЙТИБАСТИОН

www.it-bastion.com

КЕЙС
BACKDOOR *(как не допустить)*

АЙТИБАСТИОН



АВТОМАТИЗАЦИЯ

Возможность автоматизации реагирования на инциденты безопасности

```
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
```

ПОРТАЛ ДОСТУПА

www.it-bastion.com

ПОРТАЛ ДОСТУПА
РАМ-ПЛАТФОРМЫ СКДПУ НТ

АЙТИБАСТИОН

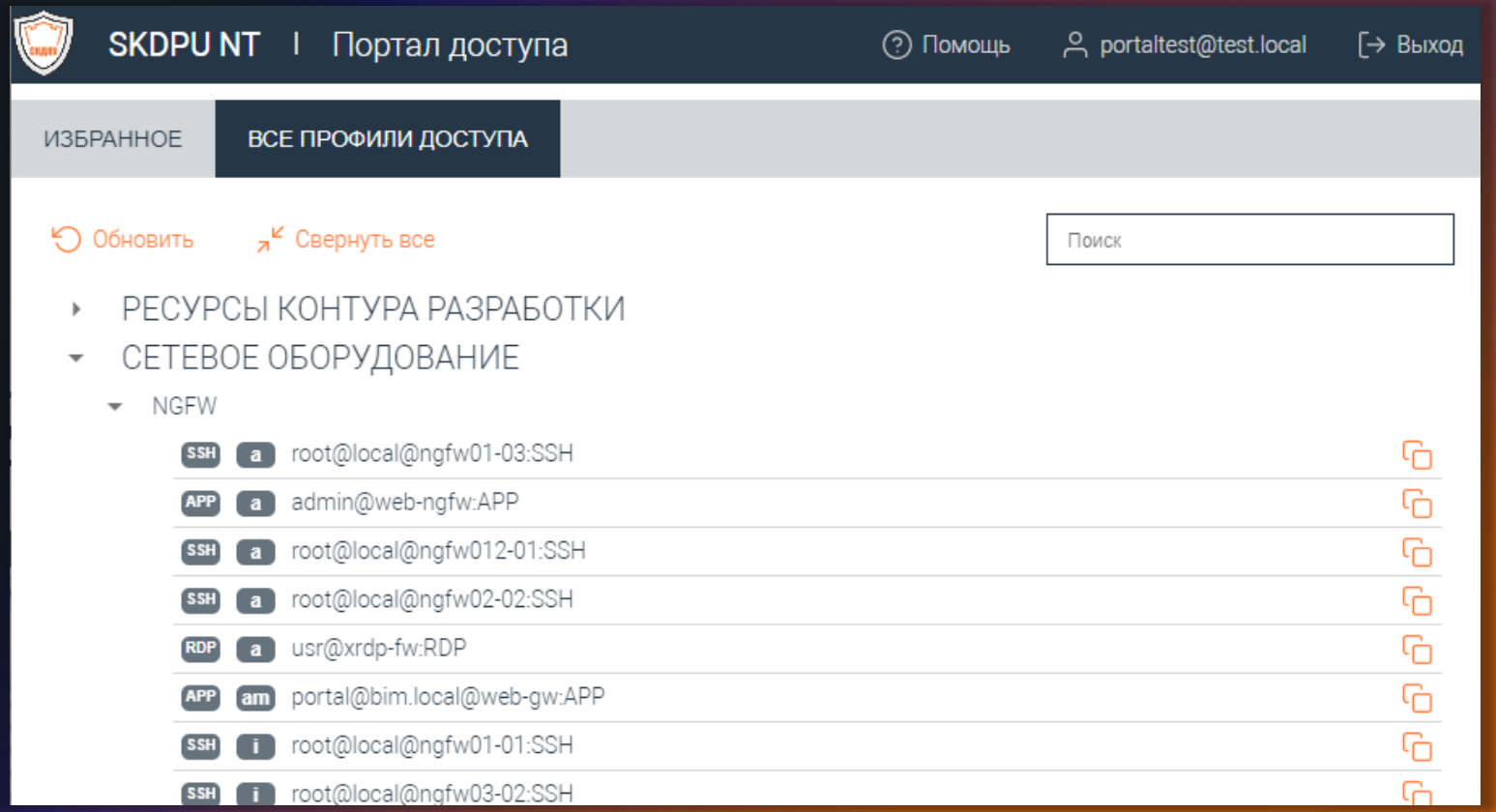
Быстрый и удобный доступ к ресурсам СКДПУ НТ
для всех типов пользователей и при любых размерах ИТ-инфраструктуры

ЕДИНЫЙ ДОСТУП

Единая точка доступа к инфраструктуре шлюзов доступа и запрашиваемым ресурсам в рамках виртуальной инфраструктуры

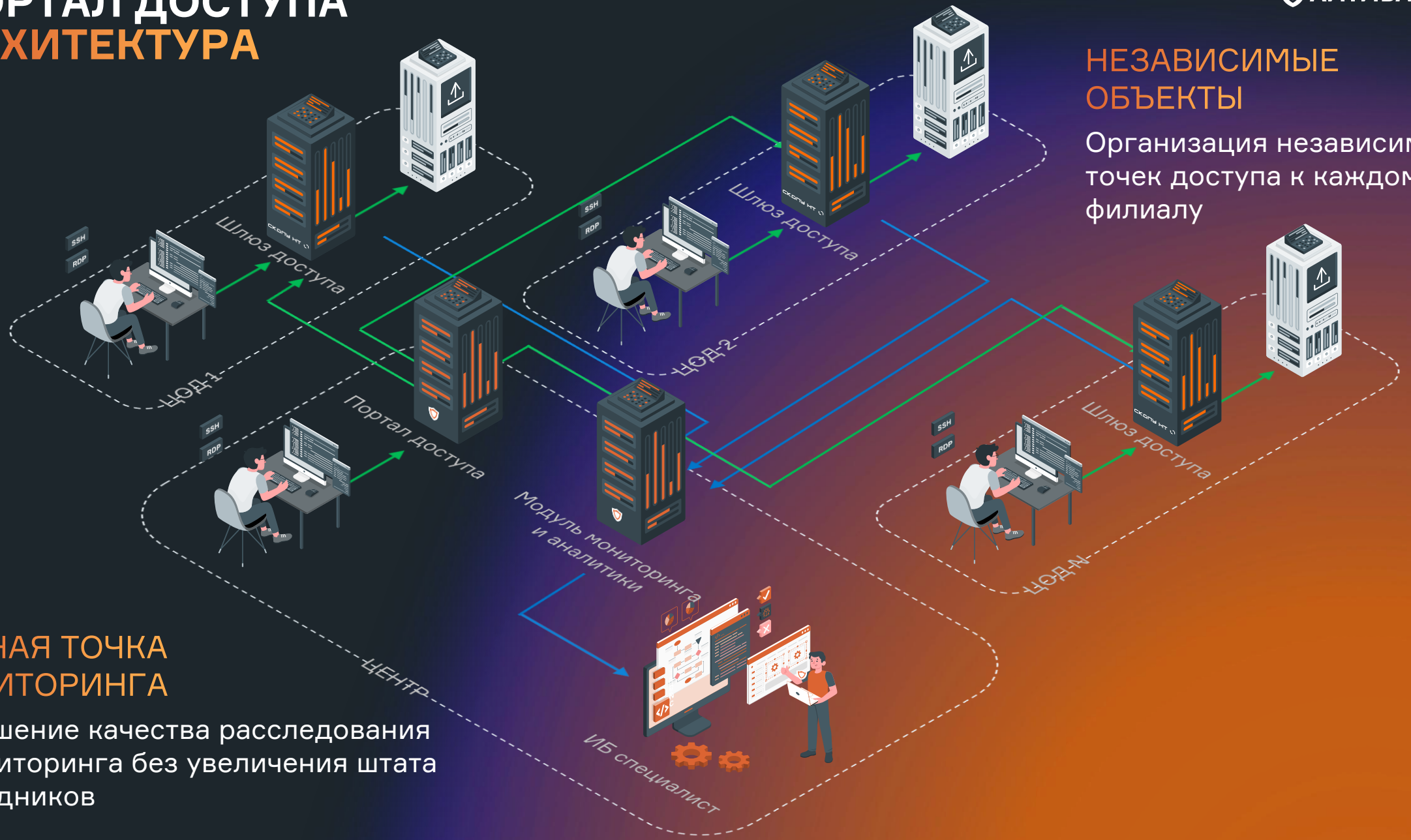
ЕДИНОЕ ОТОБРАЖЕНИЕ

Настраиваемая группировка доступов ко всем доступным ресурсам



ПОРТАЛ ДОСТУПА
АРХИТЕКТУРА

АЙТИБАСТИОН



НЕЗАВИСИМЫЕ ОБЪЕКТЫ

Организация независимых точек доступа к каждому филиалу

ЕДИНАЯ ТОЧКА МОНИТОРИНГА

Повышение качества расследования и мониторинга без увеличения штата сотрудников

КАБИНЕТ ОПЕРАТОРА

www.it-bastion.com

КАБИНЕТ ОПЕРАТОРА

АЙТИБАСТИОН

Модуль PAM-платформы СКДПУ НТ, который позволяет оптимизировать и облегчить управление и администрирование СКДПУ НТ Шлюз доступа при работе с большим количеством целевых систем, пользователей и их доступов, делегируя часть полномочий главного администратора.

Оптимизация управления доступами

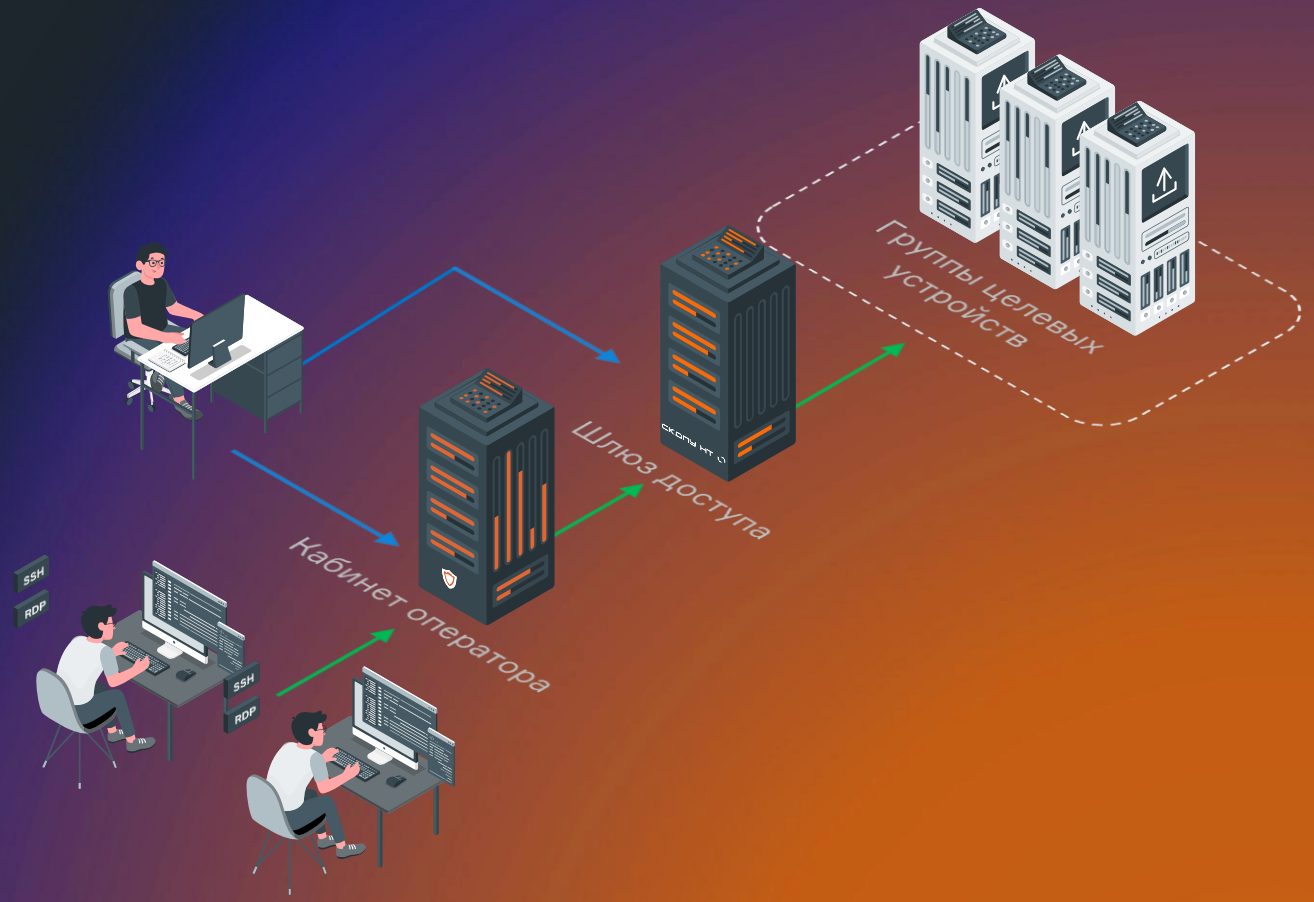
Повышение эффективности работы офицера ИБ

Контроль критичных изменений

Разделение зон ответственности

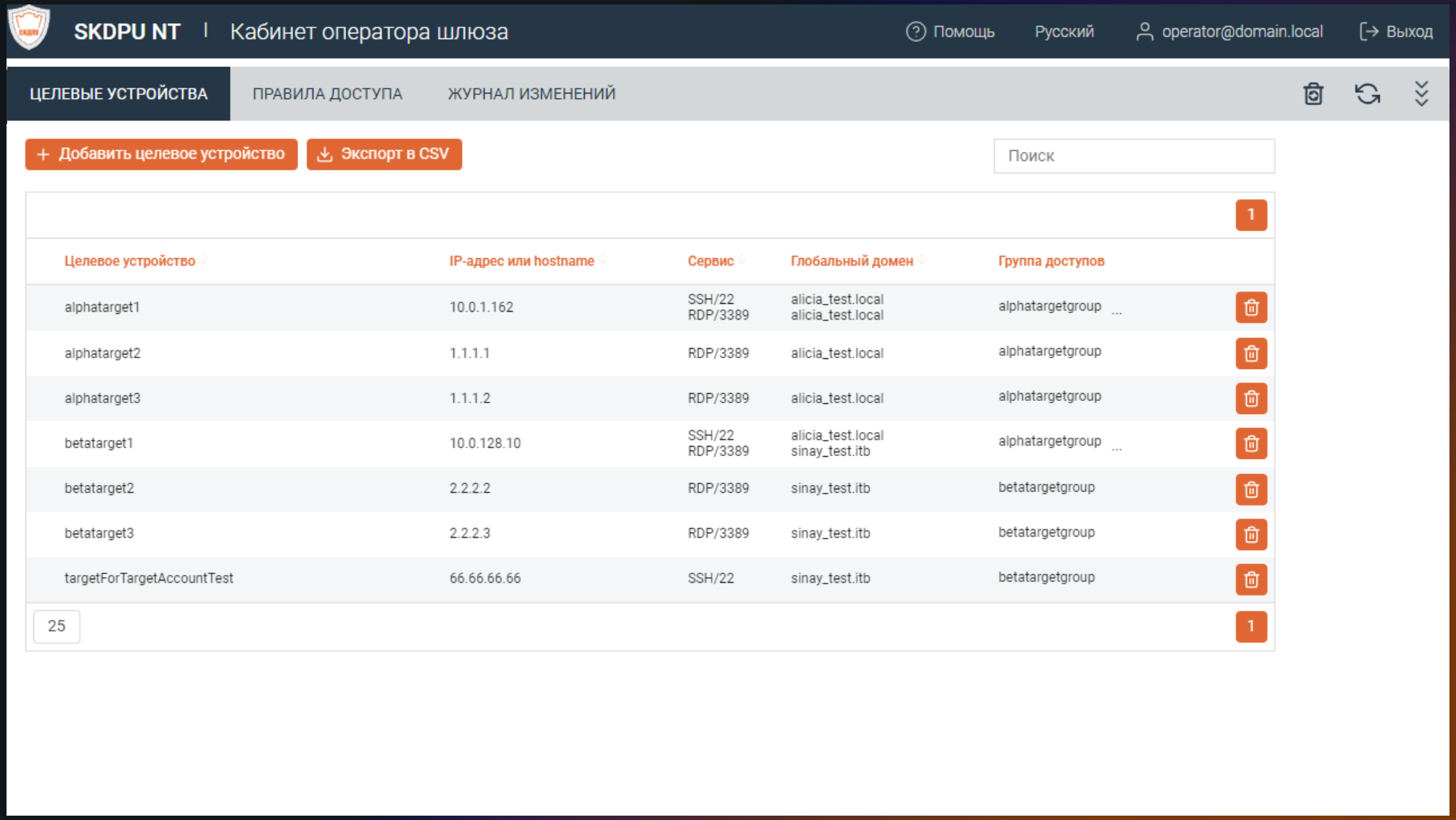
Минимизация ошибочных доступов

Делегирование части полномочий



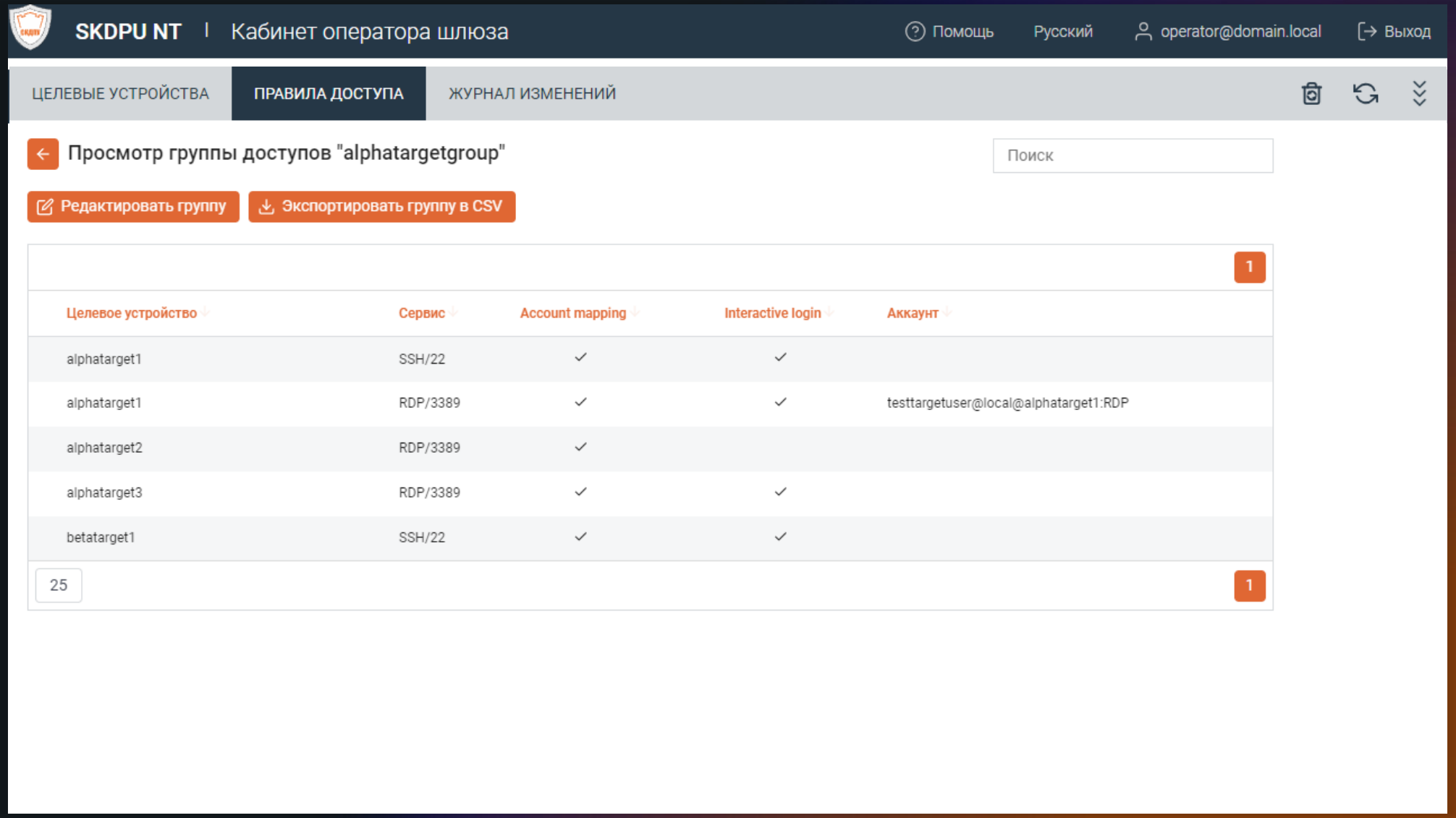
КАБИНЕТ ОПЕРАТОРА
УПРАВЛЕНИЕ ЦЕЛЕВЫМИ РЕСУРСАМИ

АЙТИБАСТИОН



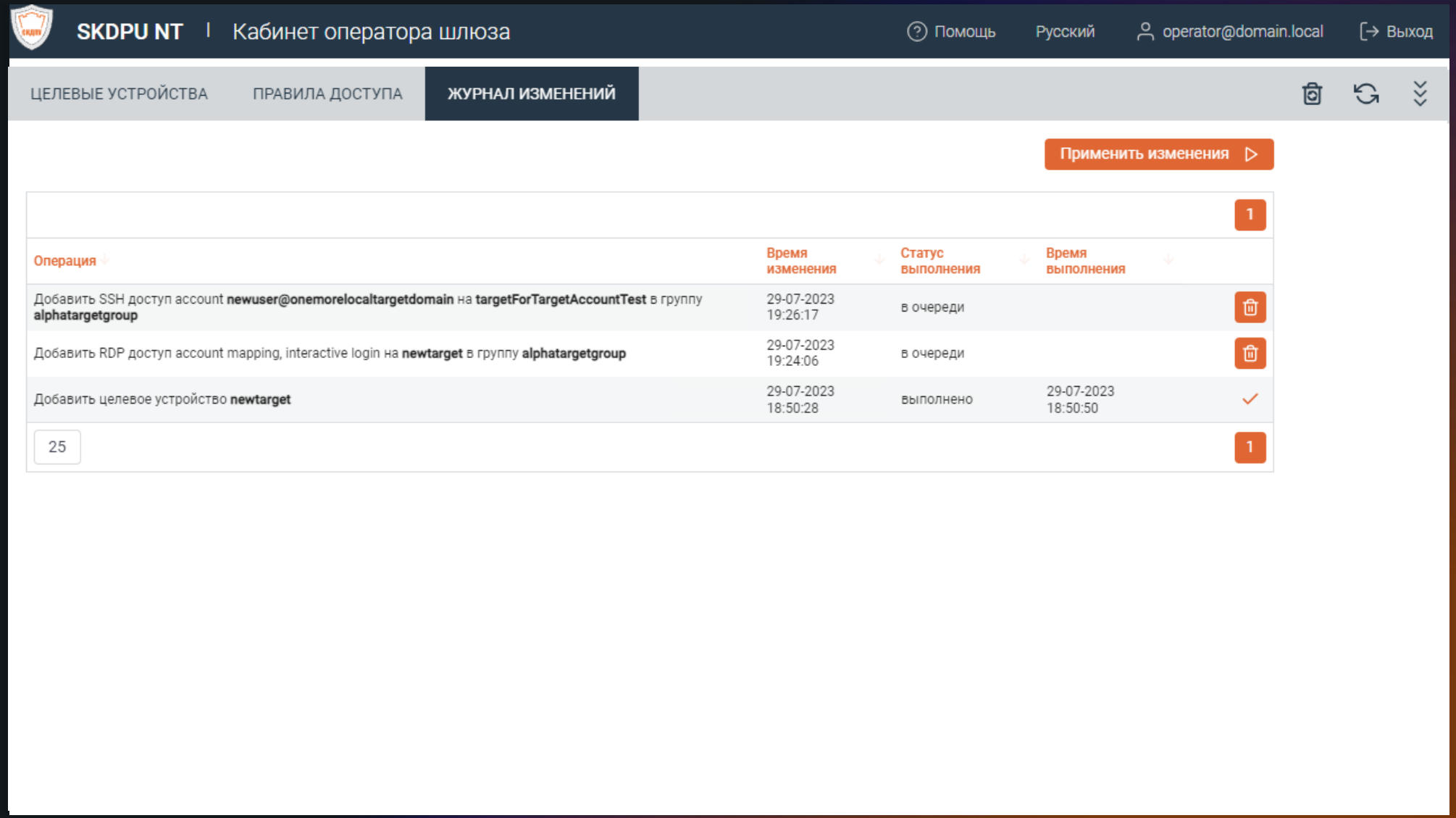
КАБИНЕТ ОПЕРАТОРА
УПРАВЛЕНИЕ ПРАВИЛАМИ ДОСТУПА

АЙТИБАСТИОН



КАБИНЕТ ОПЕРАТОРА
КОНТРОЛЬ ИЗМЕНЕНИЙ

АЙТИБАСТИОН



КАБИНЕТ ОПЕРАТОРА
ВОЗМОЖНОСТИ ОПЕРАТОРА

АЙТИБАСТИОН

ОПЕРАТОРУ ДОСТУПНО

- ✓ Добавление новых устройств
- ✓ Просмотр информации об устройствах группы
- ✓ Просмотр информации о списке доступных устройств в своей группе
- ✓ Добавление доступов пользователям группы
- ✓ Редактирование политики доступов своей группы

ОПЕРАТОРУ ЗАПРЕЩЕНО

- ✗ Полное удаление существующего устройства
- ✗ Редактирование существующих устройств
- ✗ Просмотр информации об устройствах ВНЕ своей группы
- ✗ Любые операции с доступами и пользователями ВНЕ своей группы

ИНТЕГРАЦИИ

АЙТИБАСТИОН

Реализация концепции взаимодополняемых ИТ- и ИБ-систем, где каждая система предоставляет другой профильные данные, обогащая модель событий и предоставляя человеку максимально полный перечень данных для быстрого и точечного реагирования на инциденты

СКДПУ НТ
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

АЙТИБАСТИОН

ASTRA LINUX®

POSITIVE TECHNOLOGIES

kaspersky

INFOWATCH®

Пассворк

Rusiem

GIS
ГАЗИНФОРМ СЕРВИС

ROSA

CyberLympha®

РУТОКЕН

Аладдин

zVirt

alt linux

с•терра®

MULTIFACTOR

UserGate

РЕДОС

КОД безопасности

и другие партнеры

СИНЕЗНИКС

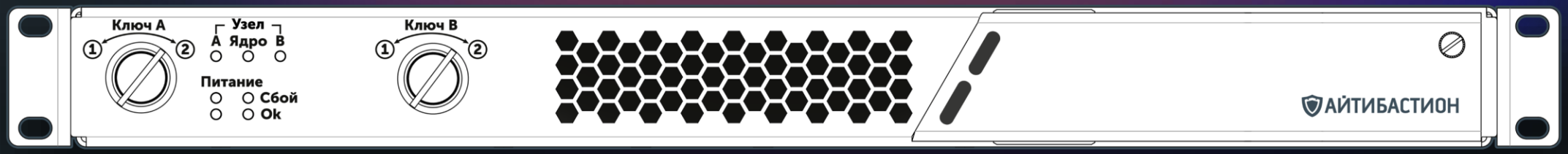
www.it-bastion.com

СИНОНИКС

АЙТИБАСТИОН

«Синоникс» – система контроля информационного обмена

Решение позволяет организовать автоматизированную однонаправленную или двунаправленную передачу данных и файлов между узлами двух сетей, скрывая при этом информацию об их окружении



ПЕРЕДАЧА ДАННЫХ

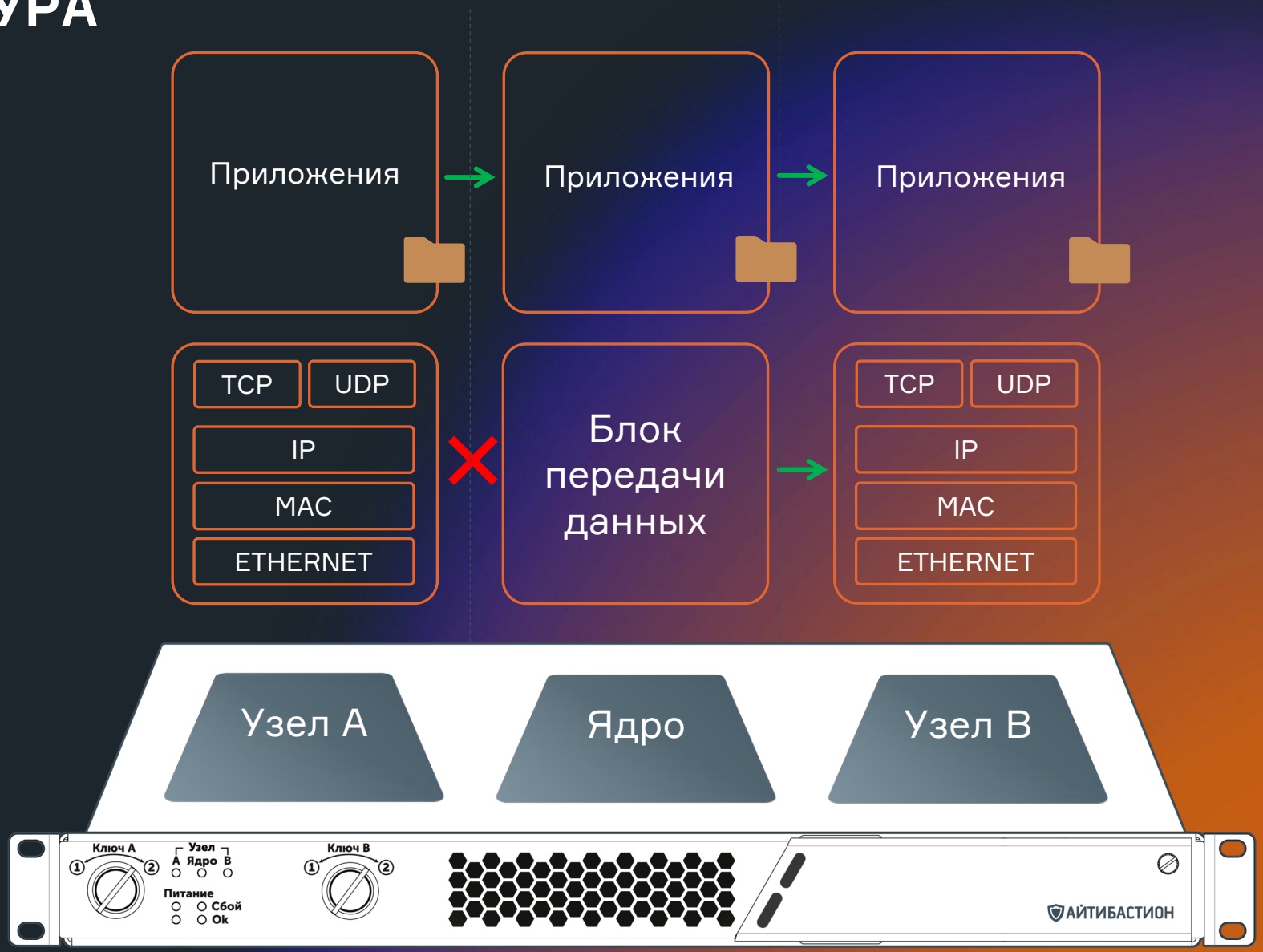
- TCP, UDP, в т.ч. Однонаправленная
- Независимые политики для двух контуров
- Скорость до 1 Гб/с
- Соединение «точка-точка»
- Поддержка работы с МЭ, NGFW и другим сетевым оборудованием

ПЕРЕДАЧА ФАЙЛОВ

- SFTP
- Двусторонняя/односторонняя с выбором направления
- Проверка маски имени, размера и контроль целостности
- Интеграция с ICAP-сервисами (DLP, Sandbox, AV и др.)
- Доставка файлов во внешние хранилища

СИНЕНИКС
АРХИТЕКТУРА

АЙТИБАСТИОН



СИНЕНИКС
НАСТРОЙКА ПРАВИЛ

АЙТИБАСТИОН

Администратор А создает правило, разрешающее передачу данных на определенный **порт**.

Администратор В создает соответствующее правило для направления трафика на нужный адрес.

НОМЕРА ПРАВИЛ НА ОБОИХ УЗЛАХ ДОЛЖНЫ СОВПАДАТЬ

РЕЖИМ РАБОТЫ НА УЗЛАХ ДОЛЖЕН БЫТЬ РАЗЛИЧНЫМ

SSH
RS-232

SSH
RS-232

СИНЕНИКС
НАСТРОЙКА ПРАВИЛ

АЙТИБАСТИОН

ПОЛЬЗОВАТЕЛЬ

ПРАВИЛО

ПРОФИЛЬ

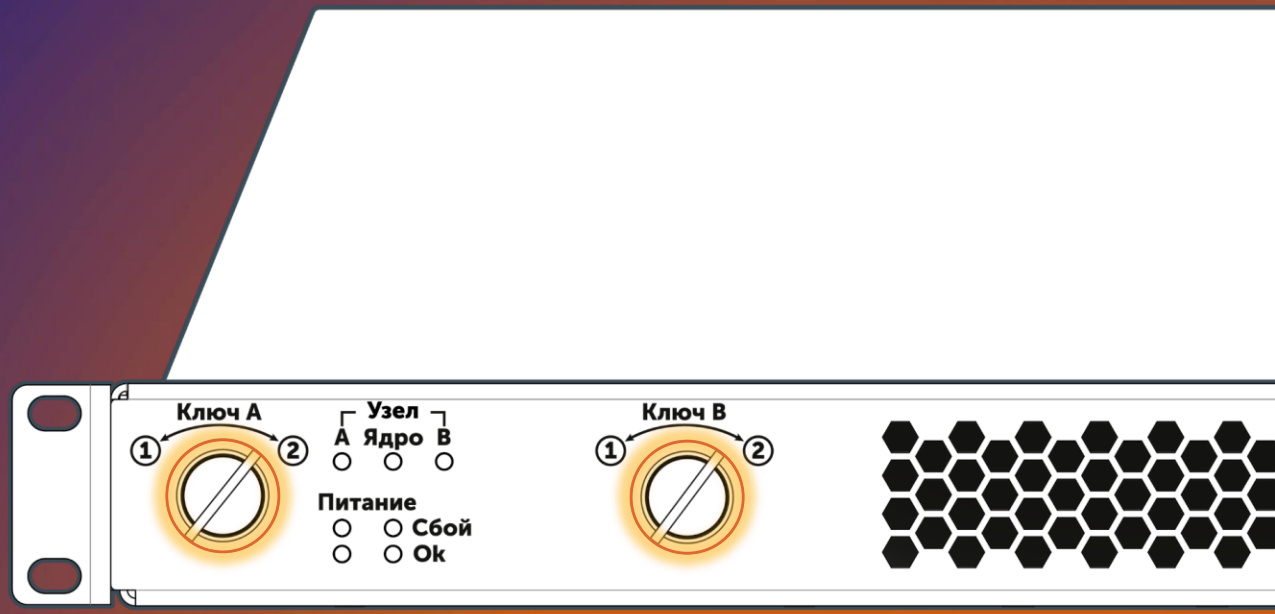
Проверки: размер, маска имени, целостность, ICAP

СИНОНИКС
ДОПОЛНИТЕЛЬНЫЙ КОНТРОЛЬ

АЙТИБАСТИОН

ДОПОЛНИТЕЛЬНЫЙ ФИЗИЧЕСКИЙ КОНТРОЛЬ

Дополнительный контроль обеспечивается с помощью физических пусковых ключей, разделяемых между сотрудниками, каждый из которых ответственен за свою сеть. Ключи разрешают или блокируют передачу данных через Синоникс путем полного отключения питания Ядра. При повороте одного из них, центральная плата отключается.



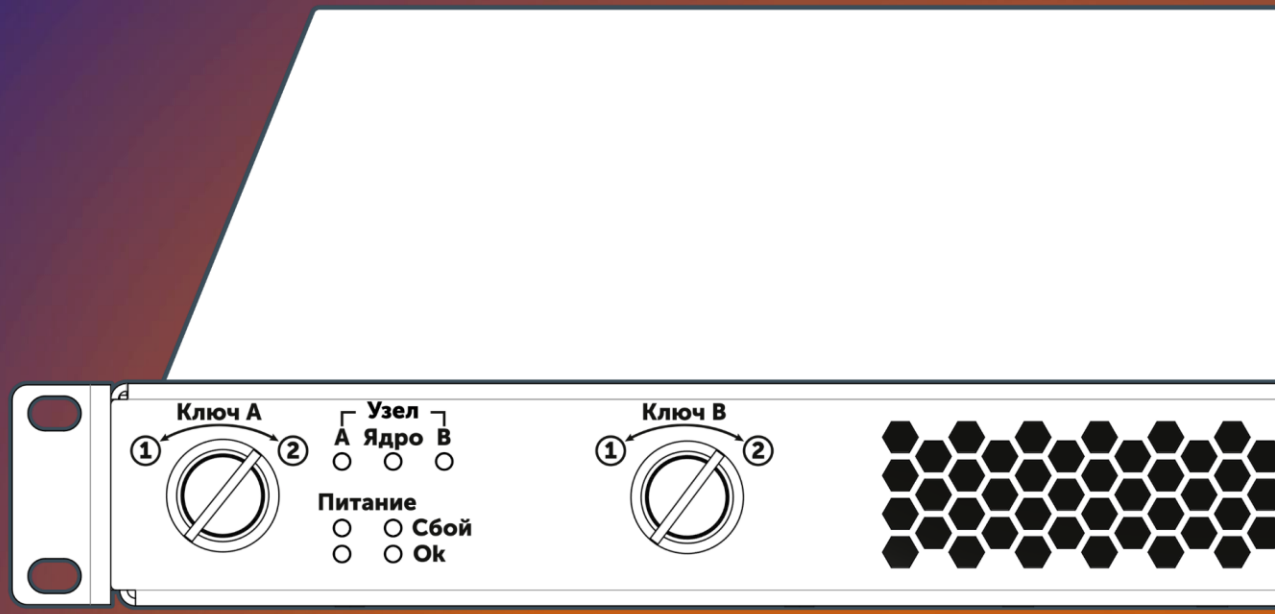
СИНЕНИКС

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

АЙТИБАСТИОН

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИК

AstraLinux 1.7. Special Edition Smolensk
Корпус – 1U
CPU - 4-core 2ГГц
ОЗУ - 8 ГБ
ПЗУ - 128 ГБ
Скорость до 1Гб/с
Кол-во правил передачи - 256

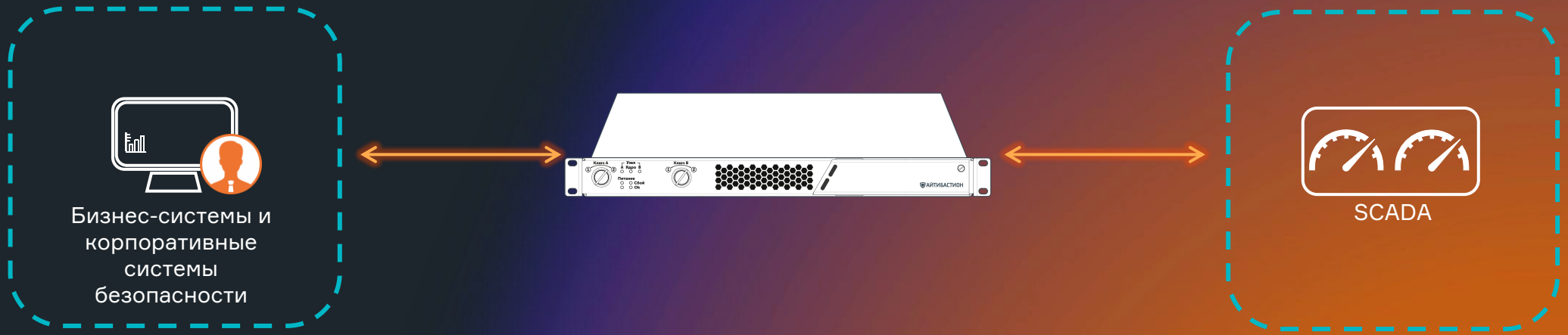


СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

СИНЕНИКС
СЦЕНАРИЙ №1

АЙТИБАСТИОН

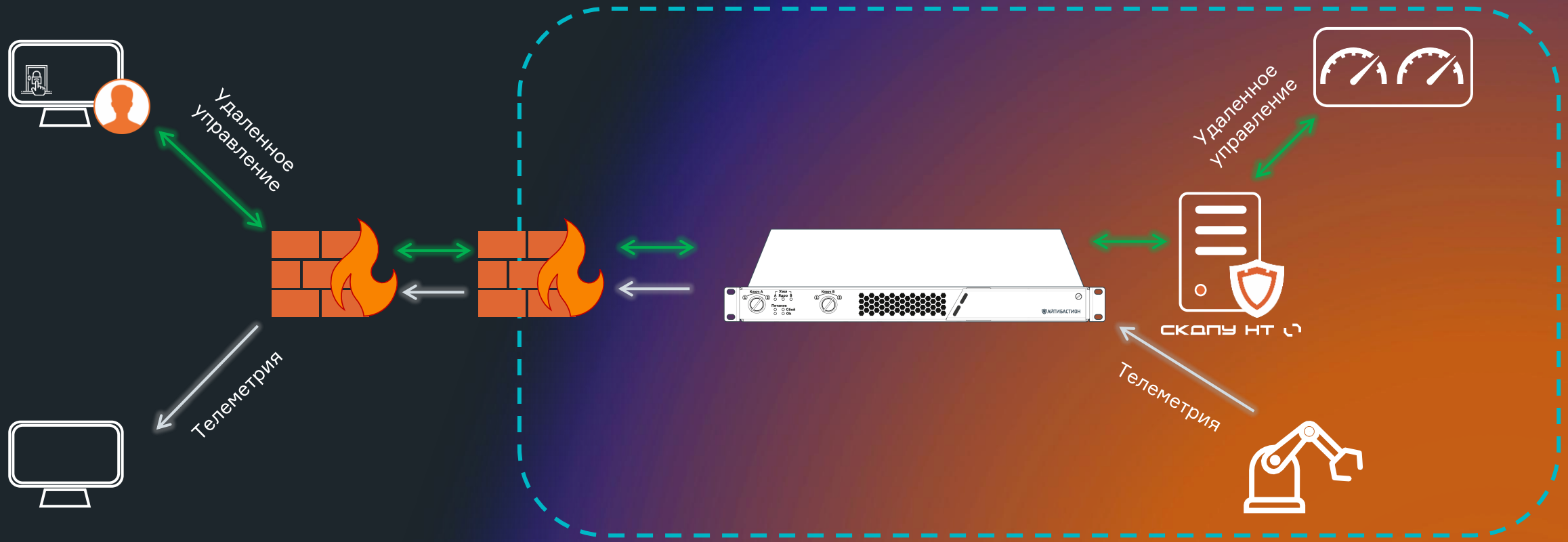
Задача: организовать непрерывный обмен данными между устройствами без сетевой связанности с сокрытием их окружения.



СИНЕНИКС
СЦЕНАРИЙ №2

АЙТИБАСТИОН

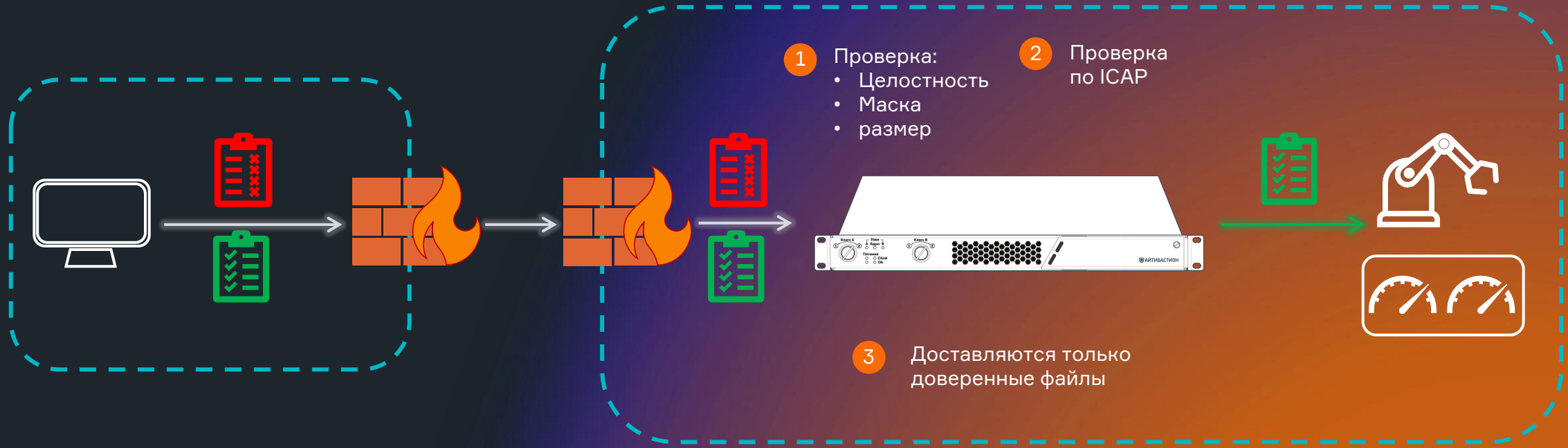
Задача: организовать передачу части данных со стороны одной из несвязанных сетей и обеспечить контролируемый доступ к важным объектам средствами PAM-системы.



СИНЕНИКС
СЦЕНАРИЙ №3

АЙТИБАСТИОН

Задача: развернуть надежную автоматизированную систему для передачи обновлений к системам из разных сетей



СИНЕРГИКС
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

АЙТИБАСТИОН

АНТИВИРУСЫ

kaspersky

Dr.WEB

МЭ/NGFW

КОД безопасности

UserGate

С•Терра®

DLP

INFOWATCH®

SOLAR

и другие решения

www.it-bastion.com

АЙТИБАСТИОН

Спасибо за внимание!

Иван Барановский

i.baranovskiy@it-bastion.com

+7 499 322 3667

it-bastion.com