



ПЛАТФОРМА СКДПУ ИТ
КОМПЛЕКСНЫЙ ПОДХОД
К ОБЕСПЕЧЕНИЮ ЗАЩИЩЕННОСТИ
ПРИВИЛЕГИРОВАННОГО ДОСТУПА

РАМ-платформа СКДПУ ИТ

Многолетний опыт эксплуатации и внедрения решений по контролю доступа в различных сферах с учетом требований доступности, функциональности и автоматизации процессов

300+

Проектов по контролю доступа и анализу действий пользователей

10 лет

Разработки, поддержки и внедрения РАМ-систем

>70%

Отечественного рынка
РАМ-систем

170+

Сотрудников компании

ЧТО МЫ ЗНАЕМ О ПРИВИЛЕГИРОВАННЫХ УЧЕТКАХ?



Привилегированные
учетные записи



Нужны для доступа к критически важным целевым системам



Есть в каждой организации



Сложно контролировать организационно и технически

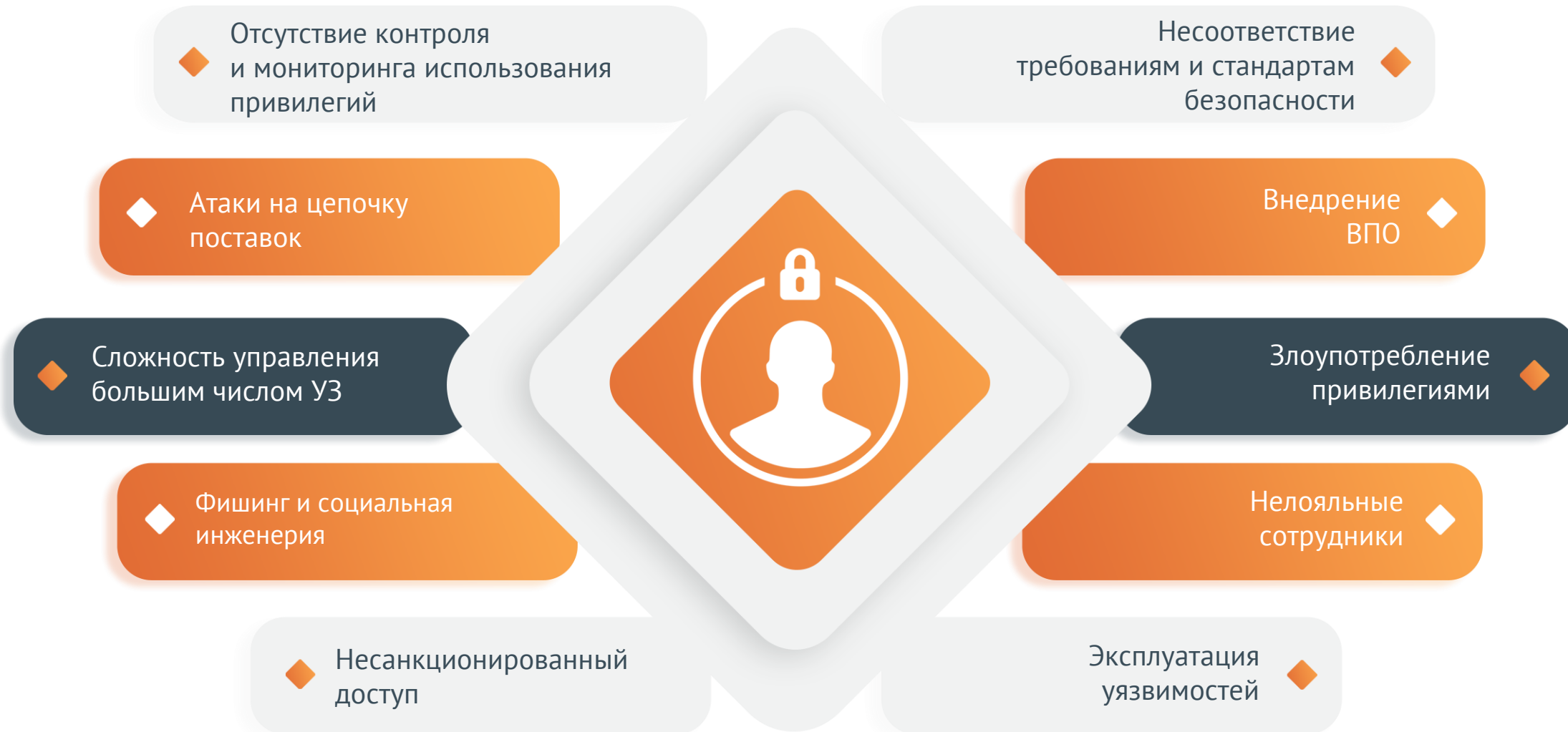


Основная цель атак злоумышленников

ВИДЫ ПРИВИЛЕГИРОВАННЫХ УЧЕТНЫХ ЗАПИСЕЙ



ПРОБЛЕМЫ ПРИВИЛЕГИРОВАННОГО ДОСТУПА



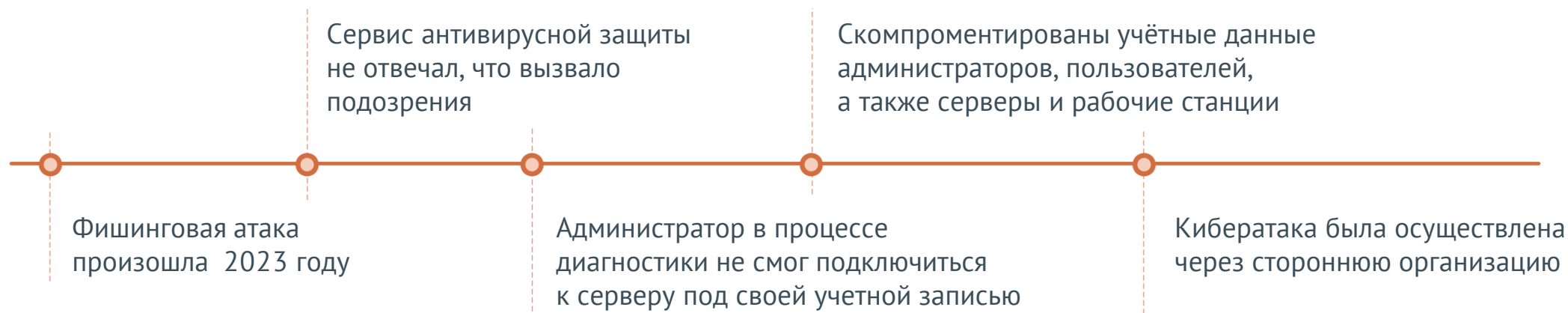
ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ





Кибератака на инфраструктуру интегратора Platformix

Ход атаки



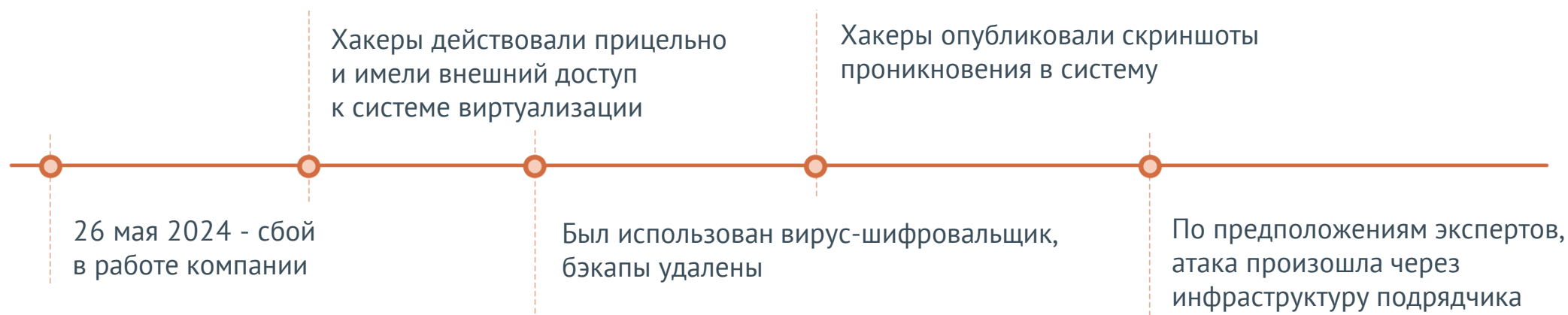
Реальной утечки данных не произошло, однако было потеряно рабочее время сотрудников (2 недели), также Platformix заплатила за привлечение сторонней организации для проведения профессионального ИБ-анализа

ПРИМЕР ИЗ РЕАЛЬНОЙ ЖИЗНИ

Взлом курьерской компании СДЭК

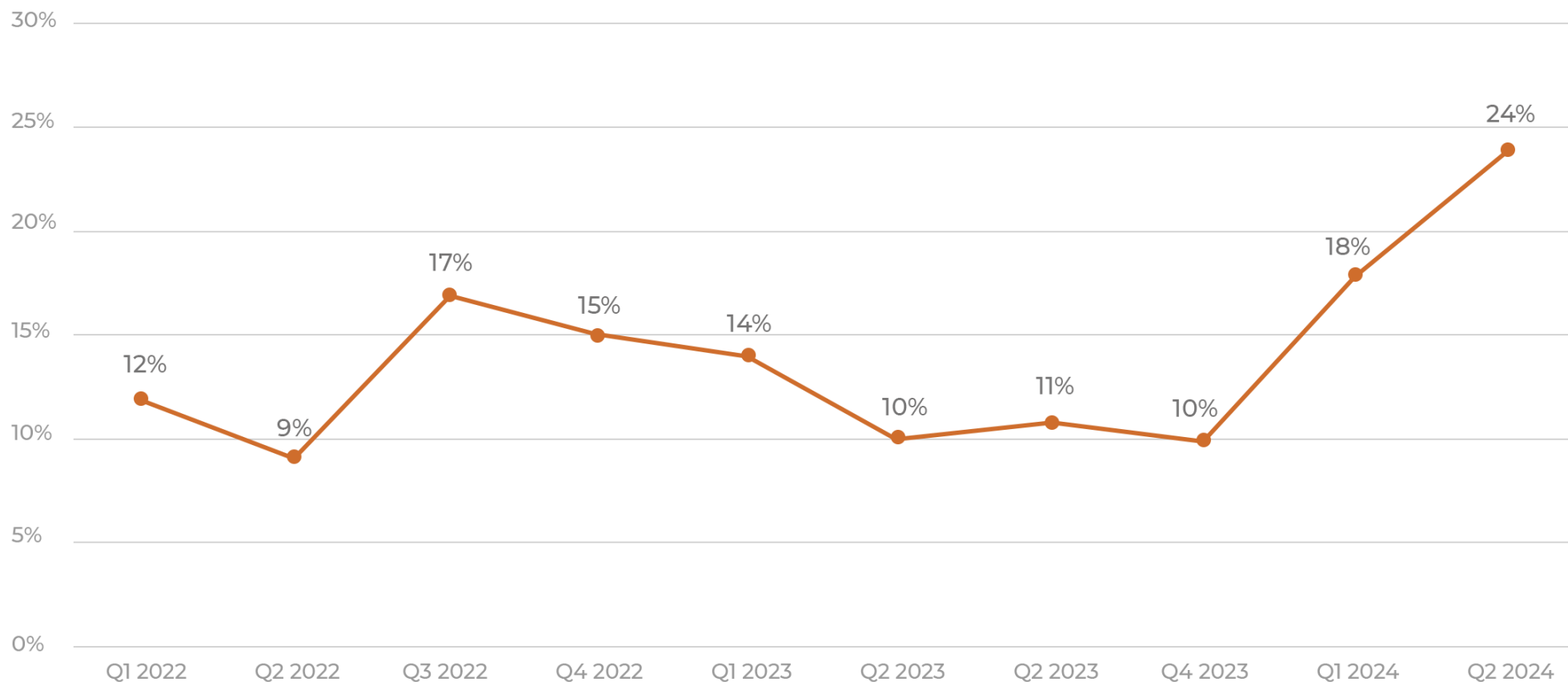
Организаторы – международная хакерская группа Head Mare

Ход атаки



- СДЭК не работала 3 дня
- Пострадали десятки тысяч клиентов, в том числе крупные маркетплейсы
- Задержались доставки 1,75 – 3 миллионов заказов

РОСТ ЧИСЛА УТЕЧЕК УЧЕТНЫХ ДАННЫХ ПОЧЕМУ ЭТО ПРОИСХОДИТ?



Динамика утечек учетных данных у организаций (2022 год – первое полугодие 2024 года). Источник: РТ

СТАНДАРТНЫХ МЕТОДОВ ЗАЩИТЫ НЕДОСТАТОЧНО? ЧТО ДЕЛАТЬ?



СКДПУ НТ

Платформа обеспечения защищенности
привилегированного доступа



Минцифры
России



МИНИСТЕРСТВО ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ



ФСТЭК России

Шлюз доступа

Контроль сессий,
запись событий доступа,
менеджер паролей,
двухфакторная
аутентификация

Портал доступа

Единая точка доступа
к инфраструктуре шлюзов.
Удобная структурированная и
настраиваемая группировка доступов

Кабинет оператора

Оптимизация управления целевыми
устройствами
и правилами доступа.
Разделение зон ответственности



Мониторинг и аналитика

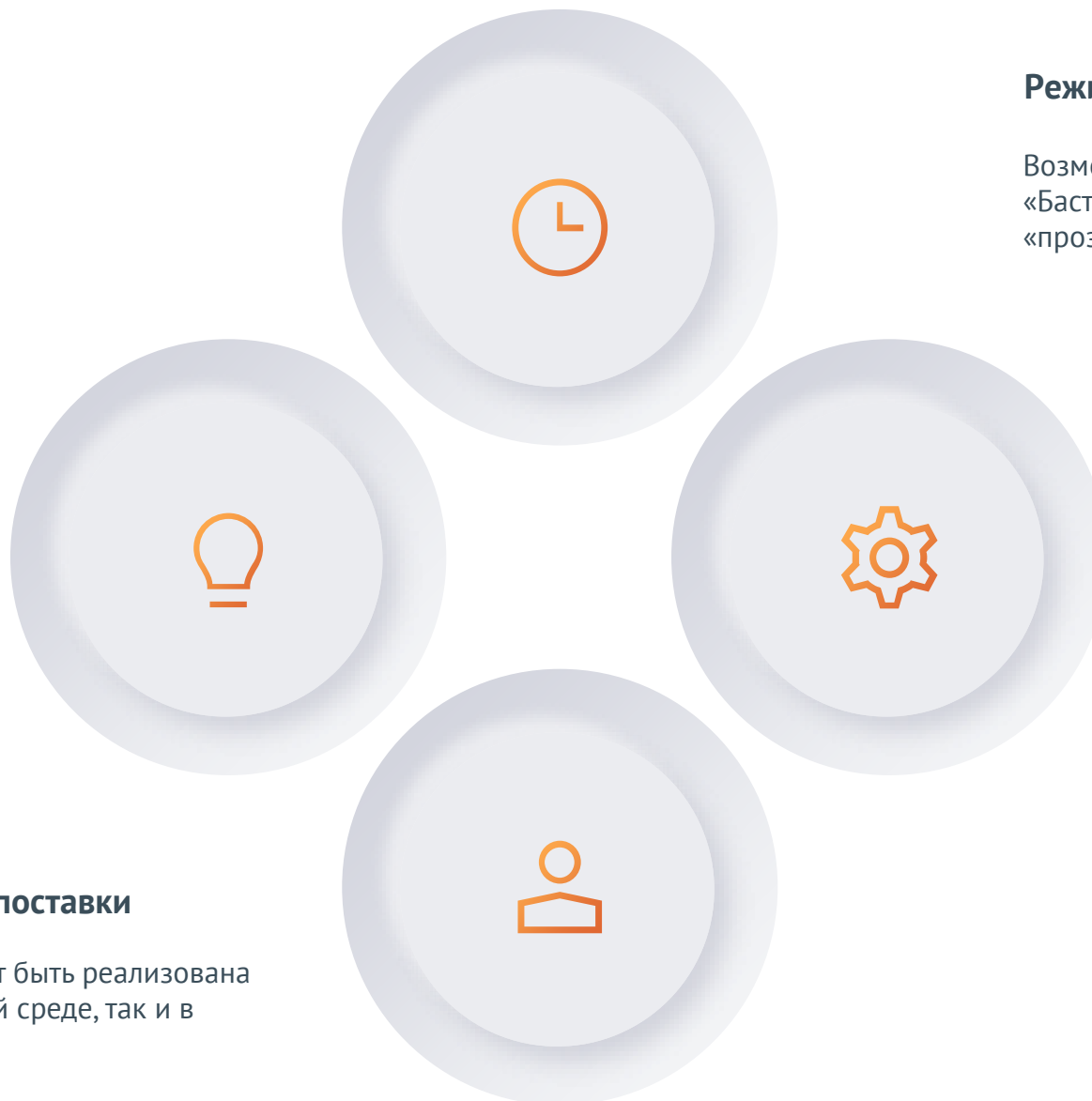
Мониторинг, отчетность
и статистика.
Поведенческий анализ
и детектирование аномалий.
Выявление инцидентов и реагирование
на них

Архив аудита

Централизованное хранение
и просмотр событий доступа.
Оптимизация хранения сессий на
Шлюзах доступа

Агрегатор доступов

Автоматизированный перенос данных
авторизаций и политик доступа к
ресурсам из сторонних систем в
структуру Шлюза доступа



Операционные системы

Платформа базируется на ОС AstraLinux SE. Поддерживается работа с AstraLinux, РЕД ОС, Альт, Windows и другими ОС

Режимы работы

Возможна работа в режиме «Бастион» (прокси) или в «прозрачном» режиме

Интеграционные возможности

Способность к интеграциям с продуктами других классов (SIEM,DLP,NGFW, IDS,VDI и др.)

Варианты поставки

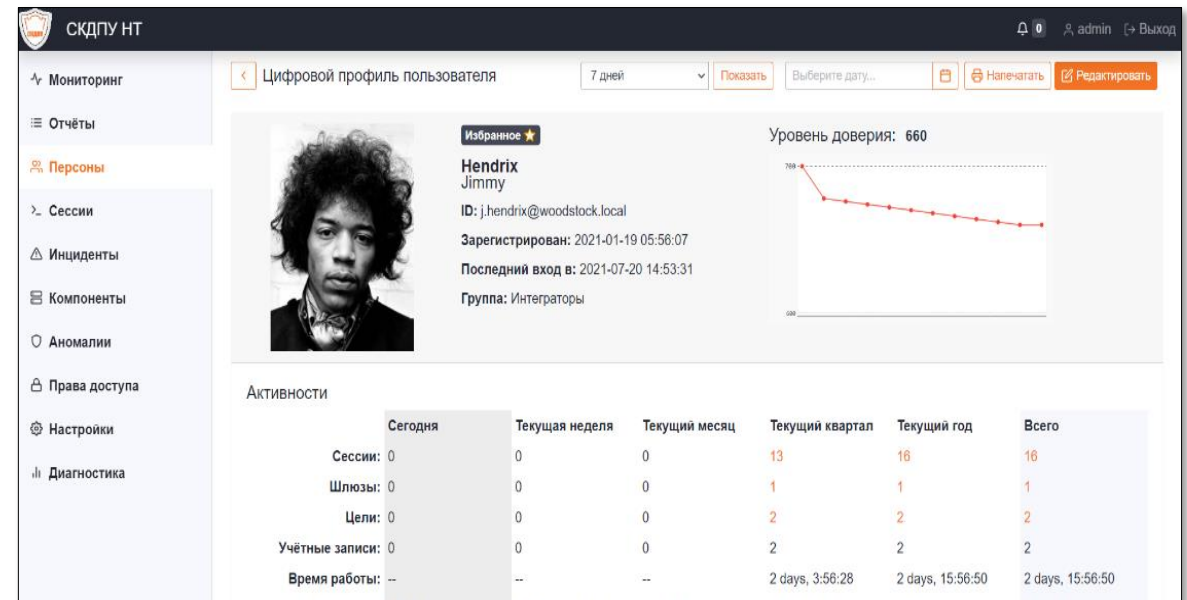
Платформа может быть реализована как в виртуальной среде, так и в виде ПАК

ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ МОНИТОРИНГ И АНАЛИТИКА



- Цифровой профиль
- Поведенческая модель
- Уровень доверия пользователя

Мониторинг и централизованный поиск по всем доступным параметрам



ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ МОНИТОРИНГ И АНАЛИТИКА

Предоставление расширенной статистики по всем действиям и подключениям пользователей, возможность формировать сводные отчеты по различным сценариям

Сессии: 1784, 10-03-2023

Добавить фильтры

Искать текст:

Включить: Ввод с клавиатуры Заголовки

Включить:

Сгруппировать: дата цель учётная запись адрес клиента персона

Параметры запроса

Тип	Старт	Продолжительность	Персона / Аккаунт	Адрес клиента	Адрес цели	Шлюз	События
RDP	09-03-2023 17:47:50	0 02:10	avs@avs16.local / avs@avs16.local	192.168.50.96	10.100.50.16	avs	27
RDP	09-03-2023 16:36:21	0 01:22	avs@avs16.local / avs@avs16.local	192.168.50.96	10.100.50.16	avs	60
SSH	09-03-2023 11:27:23	0 00:00	admin / wabadmin	192.168.50.128	10.100.1.195	skdpu70	1
RDP	09-03-2023 11:14:29	0 00:21	admin / root	172.16.128.58	10.100.1.50	wab-7-0-7	3
SSH	09-03-2023 11:11:59	0 00:16	admin / wabadmin	192.168.50.128	10.100.1.195	skdpu70	7
SSH	07-03-2023 16:07:17	0 00:02	portalltest@test.local / portalltest	172.16.129.6	10.100.1.192	wab-7-0-7	2
RDP	07-03-2023 15:12:53	0 00:21	abezborq / root	172.16.128.186	10.100.1.50	skdpu70	10
SSH	07-03-2023 15:10:34	0 00:07	abezborq / ntadmin177	172.16.128.22	10.100.1.177	skdpu70	3
SSH	07-03-2023 14:40:45	0 00:14	abezborq / ntadmin177	172.16.128.22	10.100.1.177	skdpu70	5
RDP	07-03-2023 14:24:11	0 00:20	admin / root	172.16.129.142	10.100.1.50	skdpu70	19
SSH	07-03-2023 14:23:19	0 00:16	abezborq / ntadmin177	172.16.128.22	10.100.1.177	skdpu70	4
SSH	07-03-2023 14:15:35	0 00:06	abezborq / ntadmin177	172.16.128.22	10.100.1.177	skdpu70	4
RDP	07-03-2023 14:13:40	0 00:11	abezborq / root	172.16.128.186	10.100.1.50	skdpu70	8

выводить по 25 записей на странице

Отчеты Библиотека отчетов История выполнения Профили выполнения Журнал авторизаций

Общие отчеты по системе

- Обобщенная справка
- Учётные записи на целевых системах
- Наиболее часто используемые целевые учётные записи
- Ресурсы системы и их расход
- Обзорный отчет по сессиям
- Обзорный отчет по учётным записям

Отчеты по текущей активности

- Новые сессии
- Целевые системы в использовании

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

Отчеты по безопасности

- Использование УЗ по умолчанию
- Ошибки авторизации
- Ошибки соединения
- Потенциально опасные приложения
- Использование Jump серверов
- Неожиданные команды
- Неожиданное время работы
- Принудительно закрытые сессии
- Контроль изменения уровня доверия
- Детектирование потенциально опасных команд
- Забитая персона
- Количество переданных файлов
- Индикаторы взрывной активности
- Сканеры

Инциденты

- Новые инциденты
- Инциденты без ответственного
- Основные нарушители
- Группы с высоким риском
- Инциденты в работе
- Мои инциденты
- Закрытые инциденты
- Наиболее критичные инциденты по персонам
- Целевые системы с высоким риском

Функционирование системы

- Использование ресурсов
- Доступность шлюзов

ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ МОНИТОРИНГ И АНАЛИТИКА

Настройки детекторов аномалий

- Детектирование потенциально опасных команд
- Детектор разрывов сессий
- Контроль привычного времени работы
- Контроль изменения уровня доверия
- Контроль стандартных команд
- Контроль привычных сетевых адресов работы
- Контроль эффективности работы
- Индикаторы взрывной активности
- Детектор новых доступов
- Детектор проблем с правами доступа к файлам
- Детектор использования средств удаленного доступа
- Детектор входов без средств контроля
- Анализатор ошибок авторизации
- Детектор забытых персон
- Количество переданных файлов
- Детектор сканеров

Детектирование потенциально опасных команд

Активировать

Уровень: Низкий

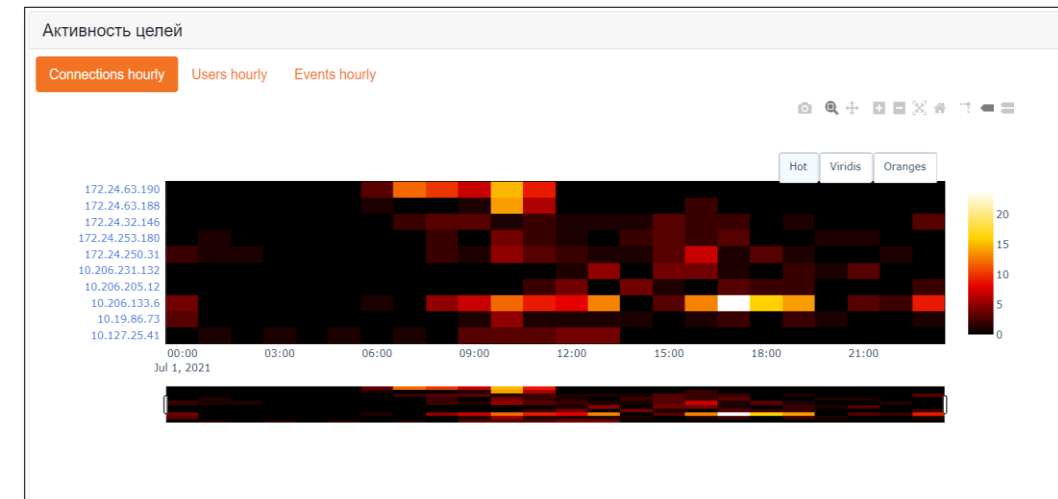
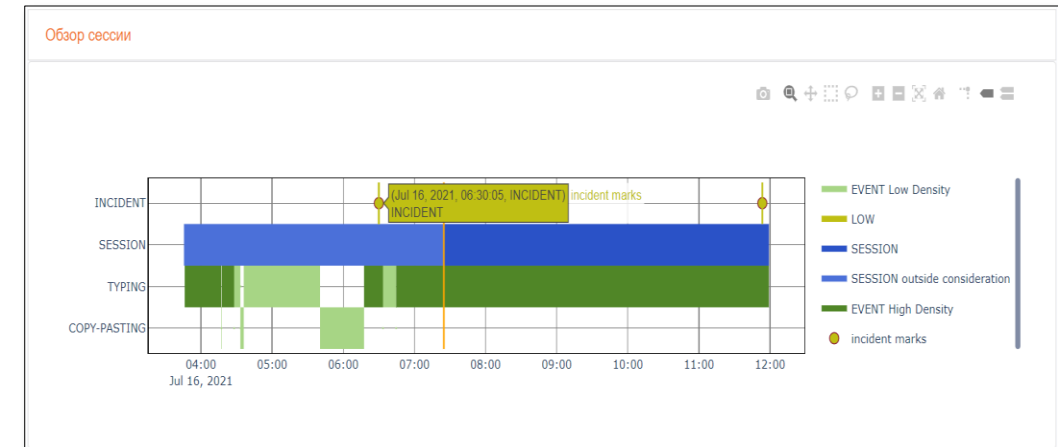
Группы: *

Название списка: black

Коэффициент: 2.0

Шаблоны: ^rm -r, *crypt.*, *hyena.*, *mimikatz.*

Карта событий и тепловая карта активности



Детектирование аномального поведения пользователей и фиксация инцидентов безопасности

ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ МОНИТОРИНГ И АНАЛИТИКА

Настройки детекторов аномалий

- Детектирование потенциально опасных команд
- Детектор разрывов сессий
- Контроль привычного времени работы
- Контроль изменения уровня доверия
- Контроль стандартных команд
- Контроль привычных сетевых адресов работы
- Контроль эффективности работы

Индикаторы взрывной активности

- Детектор новых доступов
- Детектор проблем с правами доступа к файлам
- Детектор использования средств удаленного досту
- Детектор входов без средств контроля
- Анализатор ошибок авторизации
- Детектор забытых персон
- Количество переданных файлов
- Детектор сканеров

CLM-1001562

Дата регистрации: 27-06-2023 20:16:55

Персона: abezboro

Сессия: root win1-RDP
С помощью: skdrp70 продолжительность: 0:01:08

Тип инцидента: Подозрительные команды

Уровень: Низкий

Влияние: 20

Статус: Новые

Назначен: Нет владельца

Адрес клиента: 172.16.128.186

Данные: black: 'Burp.'

Дата и время записи	Тип события	Данные
27-06-2023 20:16:55	KBD_INPUT	data Burp/<enter>

CLM-1000045

Дата регистрации: 13-03-2023 16:44:59

Персона: abezboro

Сессия: root win1-RDP
С помощью: skdrp70 продолжительность: 0:03:40

Тип инцидента: Подозрительные команды

Уровень: Низкий

Влияние: 2

Статус: Новые

Назначен: Нет владельца

Адрес клиента: 172.16.128.186

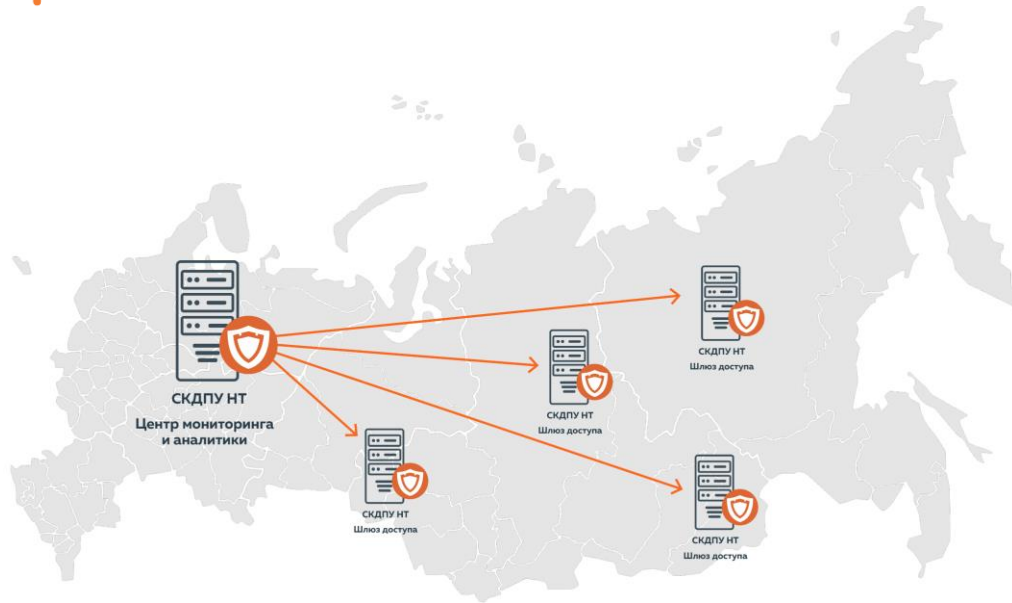
Данные: gray: '.tor-'

Дата и время записи	Тип события	Данные
13-03-2023 16:44:59	NEW_PROCESS	command_line 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe' --type=crashpad-handler 'C:\Users\abezboro\AppData\Local\Google\Chrome\User Data' /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler 'C:\Users\abezboro\AppData\Local\Google\Chrome\User Data\Crashpad'

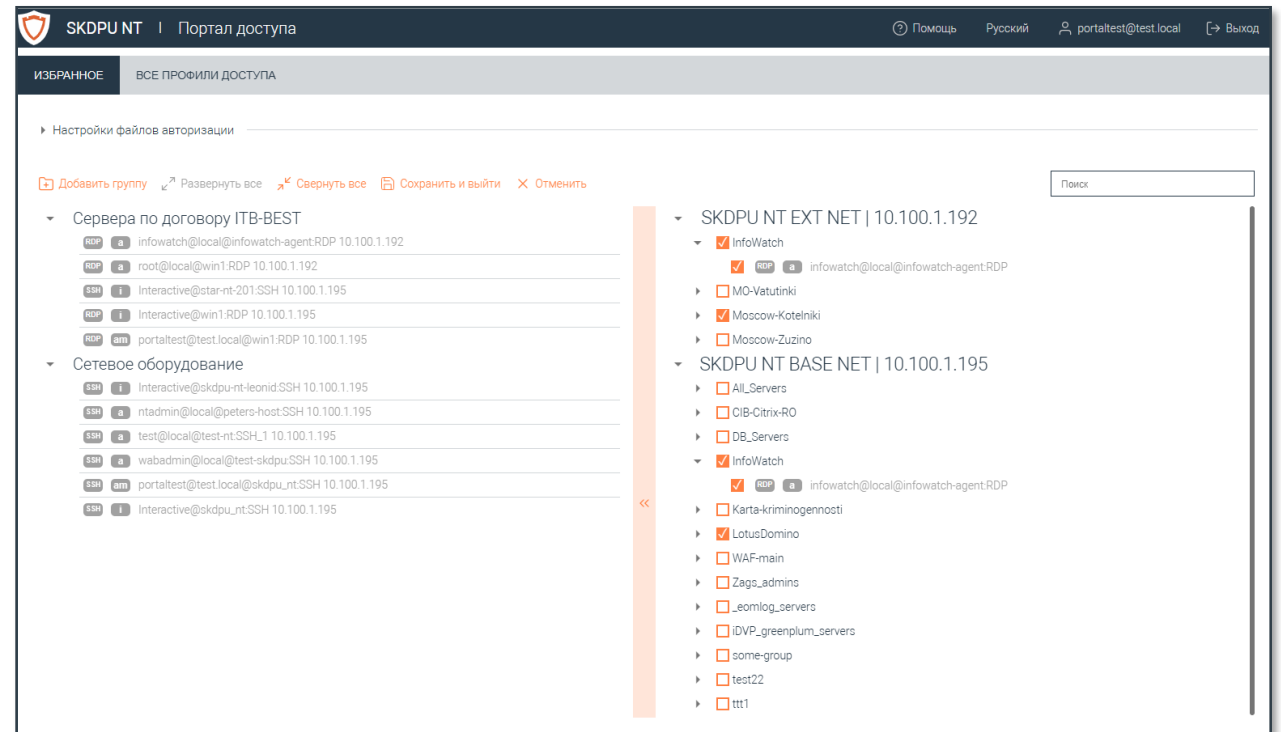
- Индивидуальные модели реагирования
- Подключение функций реагирования на инциденты и интеграция в единую систему реагирования
- Взаимодействие с SOAR/IRP

```
17 do
18   incident=$(echo "${incident}" | base64 --decode)
19   session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
20   event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
21   incident_id=$(echo "${incident}" | jq -r '.data.indent')
22   incident_link=$(echo "${incident}" | jq -r '.incident_link')
23
24   if [ "$event_type" == "NEW_PROCESS" ]; then
25     curl -k -X PUT \
26       -H "X-Auth-Key: $xtoken" \
27       -H "X-Auth-User: $xuser" \
28       -H "Content-Type: application/json" \
29       -d "{\"reason\": \"${incident_id}\n${incident_link}\"} \" \
30       "https://${api_address}/api/sessions?session_id=${session_id}&action=kill"
31   fi
32 done
33
```

ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ ПОРТАЛ ДОСТУПА

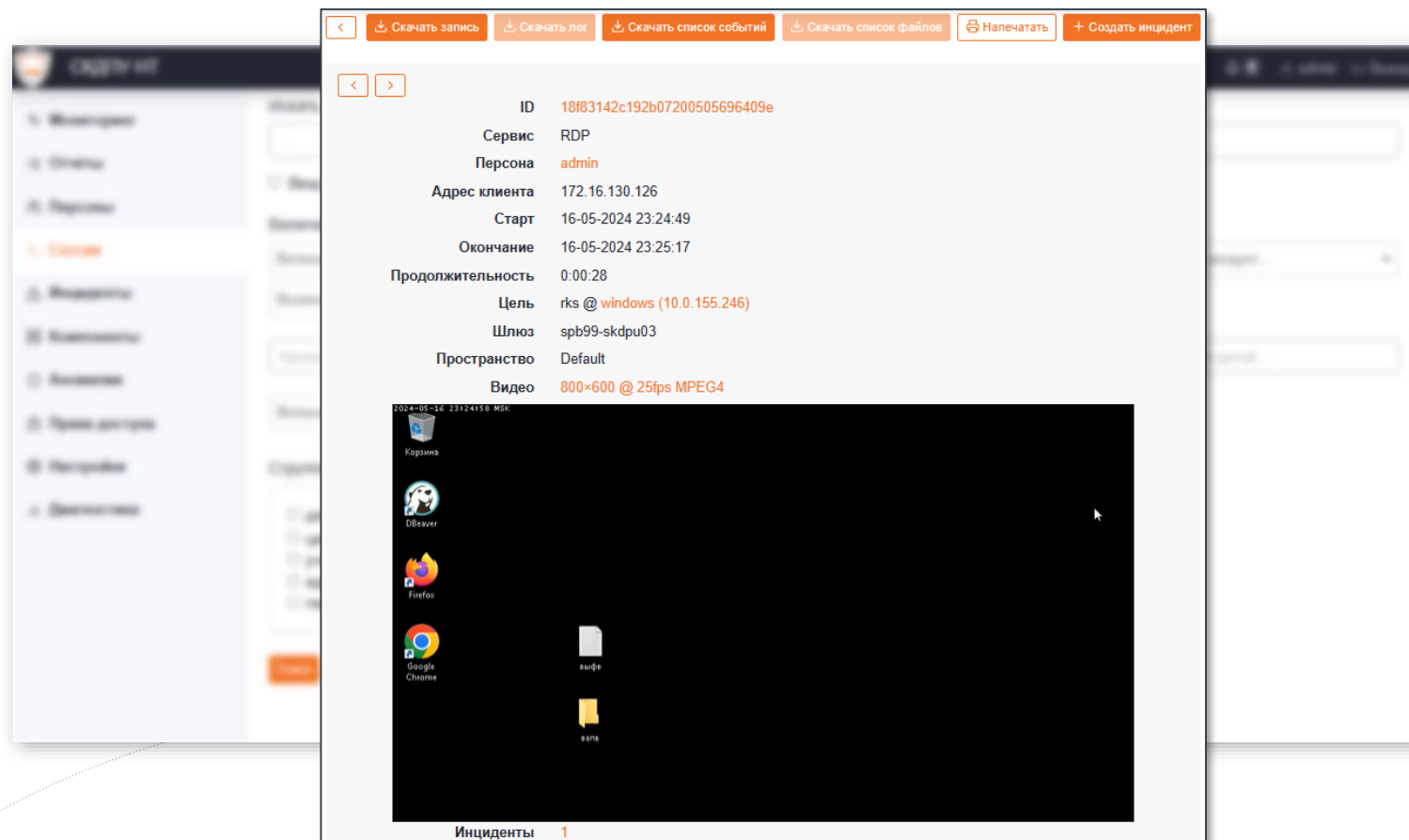


Быстрый и удобный доступ к ресурсам СКДПУ НТ для всех типов пользователей и при любых размерах ИТ-инфраструктуры



- Единая точка доступа к инфраструктуре шлюзов доступа
- Доступ в концепции «нулевого доверия»
- Доступ к приложениям и ресурсам VDI
- Настраиваемая группировка доступов

ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ АРХИВ АУДИТА



Централизованный архив данных и событий по сессиям

- Автоматическое освобождение занятого места на шлюзах
- Выгрузка записей сессий в видеоформате для подтверждения расследований
- Ротация и восстановление данных аудита

ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ КАБИНЕТ ОПЕРАТОРА

- Оптимизация управления доступами
- Разделение зон ответственности
- Делегирование части полномочий
- Минимизация ошибочных доступов
- Контроль критичных изменений

The screenshot displays the 'КАБИНЕТ ОПЕРАТОРА' (Operator Console) interface. The main view is titled 'ЦЕЛЕВЫЕ УСТРОЙСТВА' (Target Devices) and contains a table with the following data:

Целевое устройство	IP-адрес или hostname	Сервис	Глобальный домен	Группа доступов
alphatarget1	10.0.1.162	SSH/22 RDP/3389	alicia_test.local alicia_test.local	alphatargetgroup ...
alphatarget2	1.1.1.1	RDP/3389	alicia_test.local	alphatargetgroup
alphatarget3	1.1.1.2	RDP/3389	alicia_test.local	alphatargetgroup
betatarget1	10.0.128.10	SSH/22 RDP/3389	alicia_test.local sinay_test.itb	alphatargetgroup ...
betatarget2	2.2.2.2	RDP/3389	sinay_test.itb	betatargetgroup
betatarget3				
targetForTargetAccountTest				

An inset window shows the 'ЖУРНАЛ ИЗМЕНЕНИЙ' (Change Log) with the following entries:

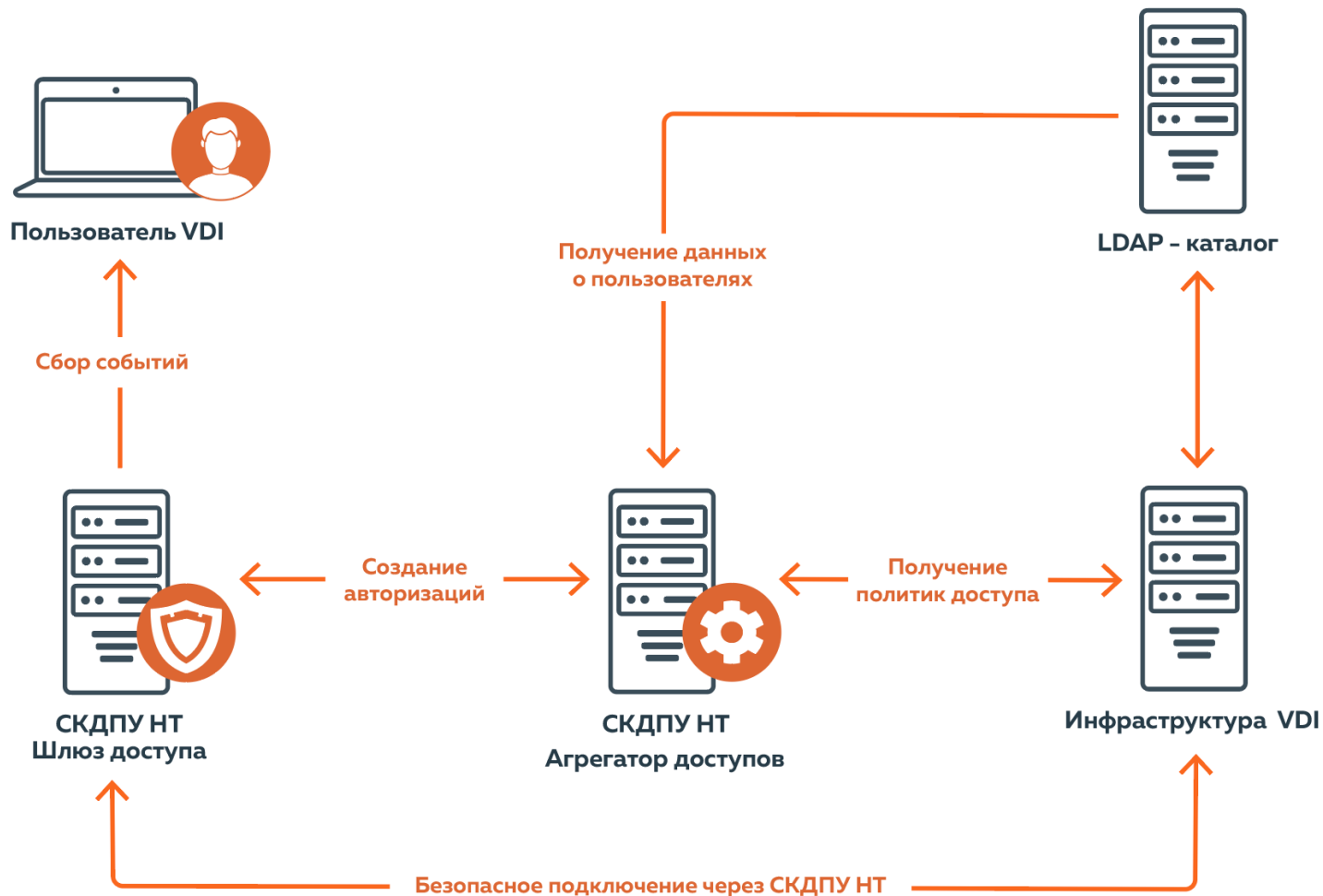
Операция	Время изменения	Статус выполнения	Время выполнения
Добавить SSH доступ account <code>newuser@onemorelocaltargetdomain</code> на <code>targetForTargetAccountTest</code> в группу <code>alphatargetgroup</code>	29-07-2023 19:26:17	в очереди	
Добавить RDP доступ account mapping, interactive login на <code>newtarget</code> в группу <code>alphatargetgroup</code>	29-07-2023 19:24:06	в очереди	
Добавить целевое устройство <code>newtarget</code>	29-07-2023 18:50:28	выполнено	29-07-2023 18:50:50

ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ ШЛЮЗ ДОСТУПА



ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ АГРЕГАТОР ДОСТУПОВ

Автоматическое предоставление доступа к пользовательским ресурсам в виртуальной среде с функциями расширенного контроля и мониторинга действий пользователей



ВОЗМОЖНОСТИ МЕЖВЕНДОРНЫХ ИНТЕГРАЦИЙ



Спасибо
за внимание!



Дмитрий Симак
Менеджер продукта СКДПУ НТ



d.simak@it-bastion.com



+7 910 949 32 75



it-bastion.com

