



АЙТИБАСТИОН

ПАК контроль подрядчиков
контроль данные
SSO удаленный доступ
детектор аномалий отчеты
ICAP безопасная передача данных
масштабирование AstraLinux
контроль администраторов

РАМ Цифровой профиль пользователя
отказоустойчивость
КИИ
односторонняя передача
контроль удаленной работы
уровень доверия
аналитика
API
SIEM

СКДПУ НТ
Синоним

АСУ ТП
DLP
поведенческий анализ
однонаправленный шлюз

Отечественная РАМ-платформа СКДПУ НТ

От задачи контроля к экосистеме анализа и
реагирования

Компания «АйТи Бастион»

2014



Основание компании

Более 9 лет на российском
рынке информационной
безопасности

100+



Сотрудников

Команда разработчиков,
инженеров, менеджеров,
маркетинга и пиара,
ориентированная на продукт
и решение реальных задач

180+



Заказчиков и проектов

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

> 50%



РАМ-рынка РФ

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

Что такое PAM для большинства?



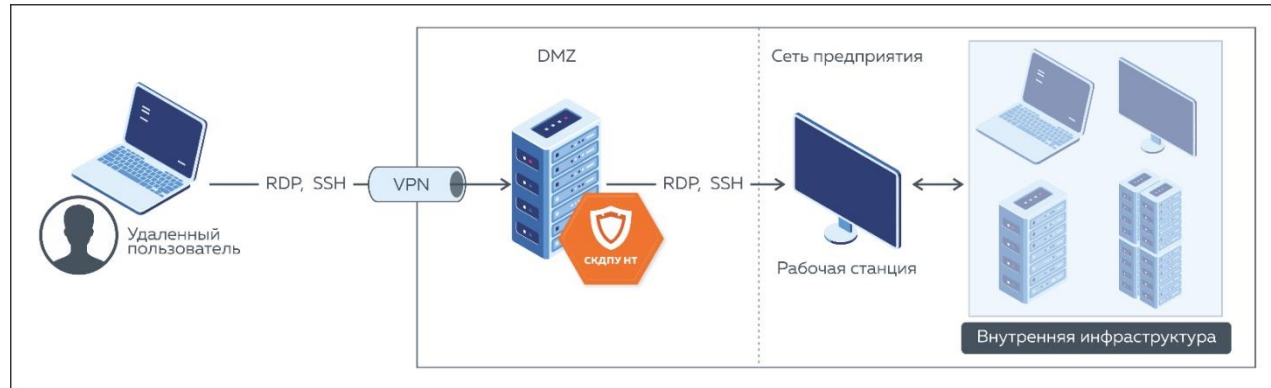
“

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.

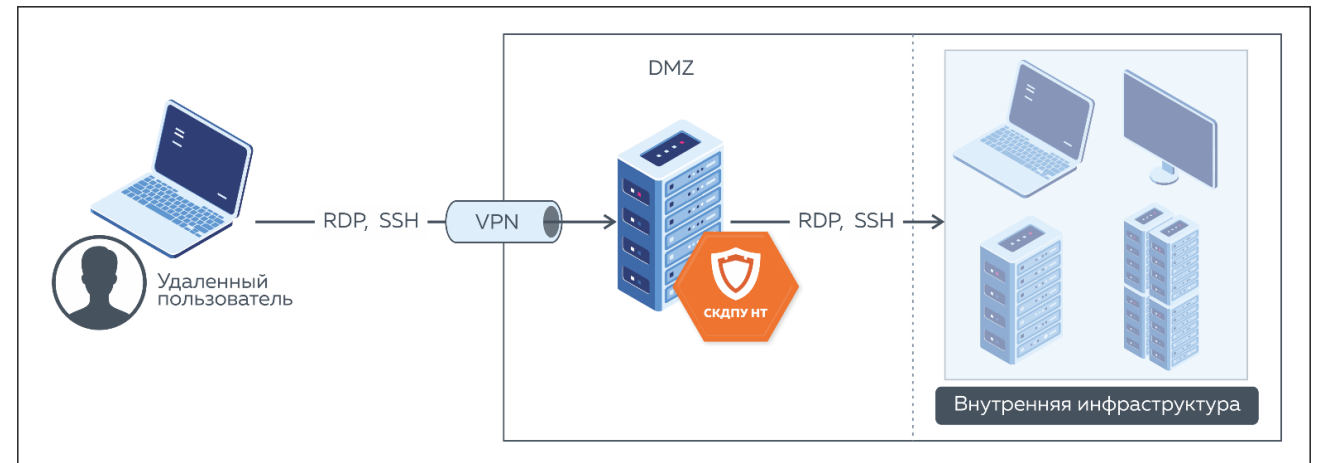
”

Чем помогает РАР-система



- ✓ Привилегии и права на «минимум»
- ✓ Идентификация удаленных устройств
- ✓ Только для «своих» сотрудников
- ✓ Свой домен для удаленных АРМ
- ✓ Двухфакторная аутентификация
- ✓ VPN
- ✓ Запрет постороннего ПО

- ✓ Антивирусная защита
- ✓ Блокировка сеансов при неактивности
- ✓ Реагирование на инциденты
- ✓ Сегментация прав доступа
- ✓ Обновление паролей



Наше видение РАМ-систем

 Технологии

 Люди

 Процессы



Все атаки начинались с утечки учетной записи

Colonial Pipeline

- Атака остановила работу всех трубопроводов системы на пять дней 88 % АЗС в Вашингтоне были без бензина
- Из-за нехватки авиакеросина авиакомпания American Airlines была вынуждена временно изменить некоторые рейсы
- Розничные цены на бензин в США при этом достигли десятилетнего максимума
- В части Северной Каролины, в связи с нехваткой топлива 71 % АЗС были закрыты

Руководство Colonial Pipeline заплатило выкуп в 75 биткоинов (4,5 млн долл. на момент выплаты)

Венесуэльская ГЭС

Атака была направлена на автоматическую систему контроля ГЭС "Гури". Гидроэлектростанция производит 80% электроэнергии, потребляемой в стране. Почти вся страна осталась без электроснабжения до возобновления работы.

Creos Luxembourg S.A

Крупный центральноевропейский оператор электросетей и газопроводов, поставляющий энергию в пять стран ЕС.

Украдено 180 тыс. файлов общим объёмом 150 ГБ, - контракты, соглашения, паспорта, счета и электронную переписку.

Выполнен переход на аварийное обслуживание.

ENI

ENI – Итальянская топливная компания

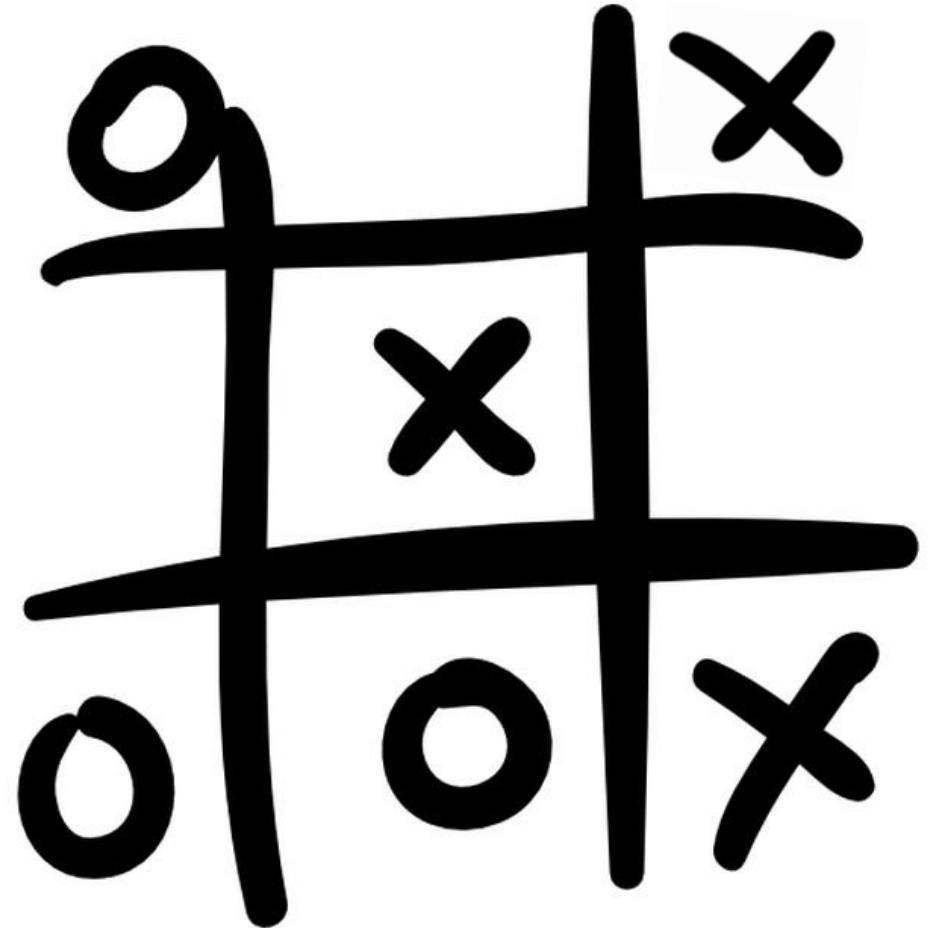
Представитель ENI заявил, что в последние дни внутренние системы защиты обнаружили несанкционированный доступ и быстро пресекли атаку, поэтому последствия были незначительными.

Однако заявляется об утечке конфиденциальной информации и частичным сбоям в работе инфраструктуры.

Про угрозы привилегированного доступа

- Человеческий фактор
- Shadow IT и «обидчивые люди»
- Несоответствие требованиям
- Репутационные риски

- Поставщики услуг
- Цепочки поставок
- Геополитика и санкции



65% атак – целевые атаки

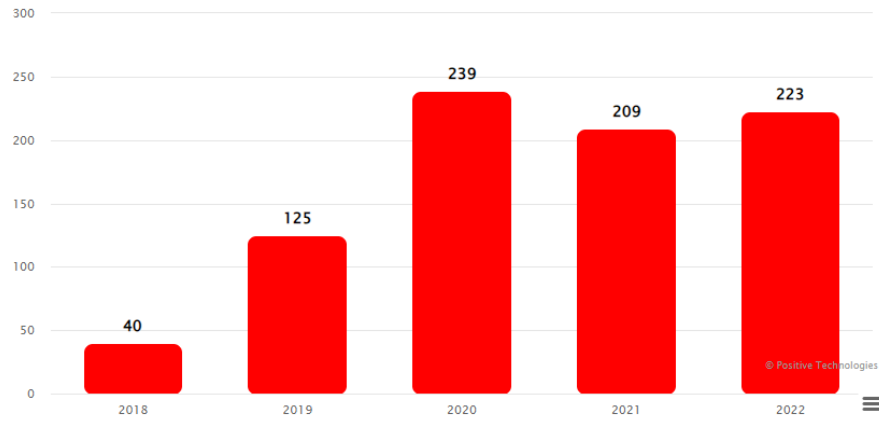


Рисунок 2. Динамика инцидентов (количество по годам)

Инциденты

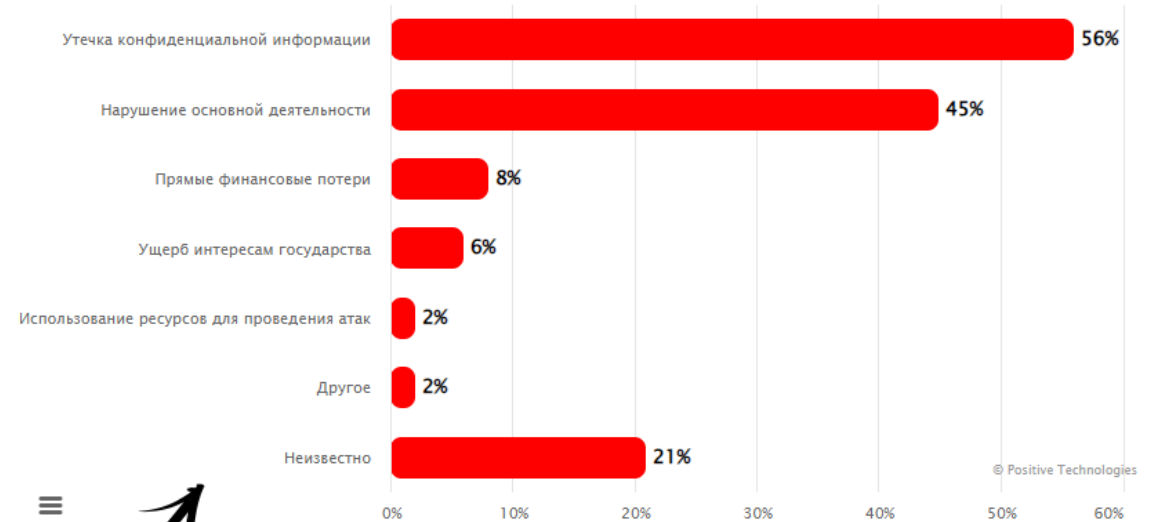


Рисунок 16. Последствия атак на промышленные организации (доля атак)

Последствия

- 75% объявлений в дарквебе про «доступ»
- 45% последствий – нарушение деятельности
- 8% прямые финансовые потери

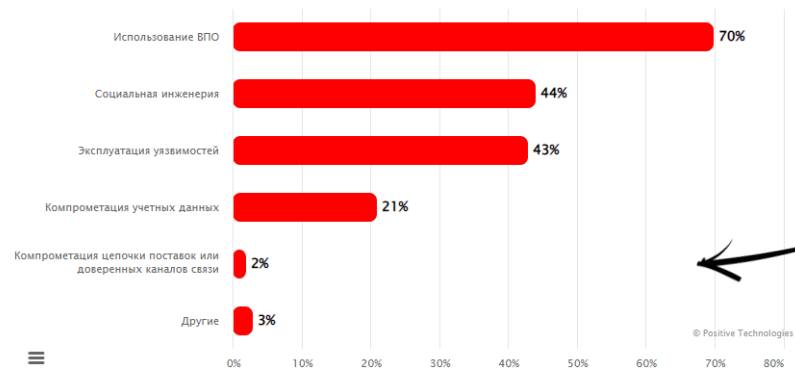
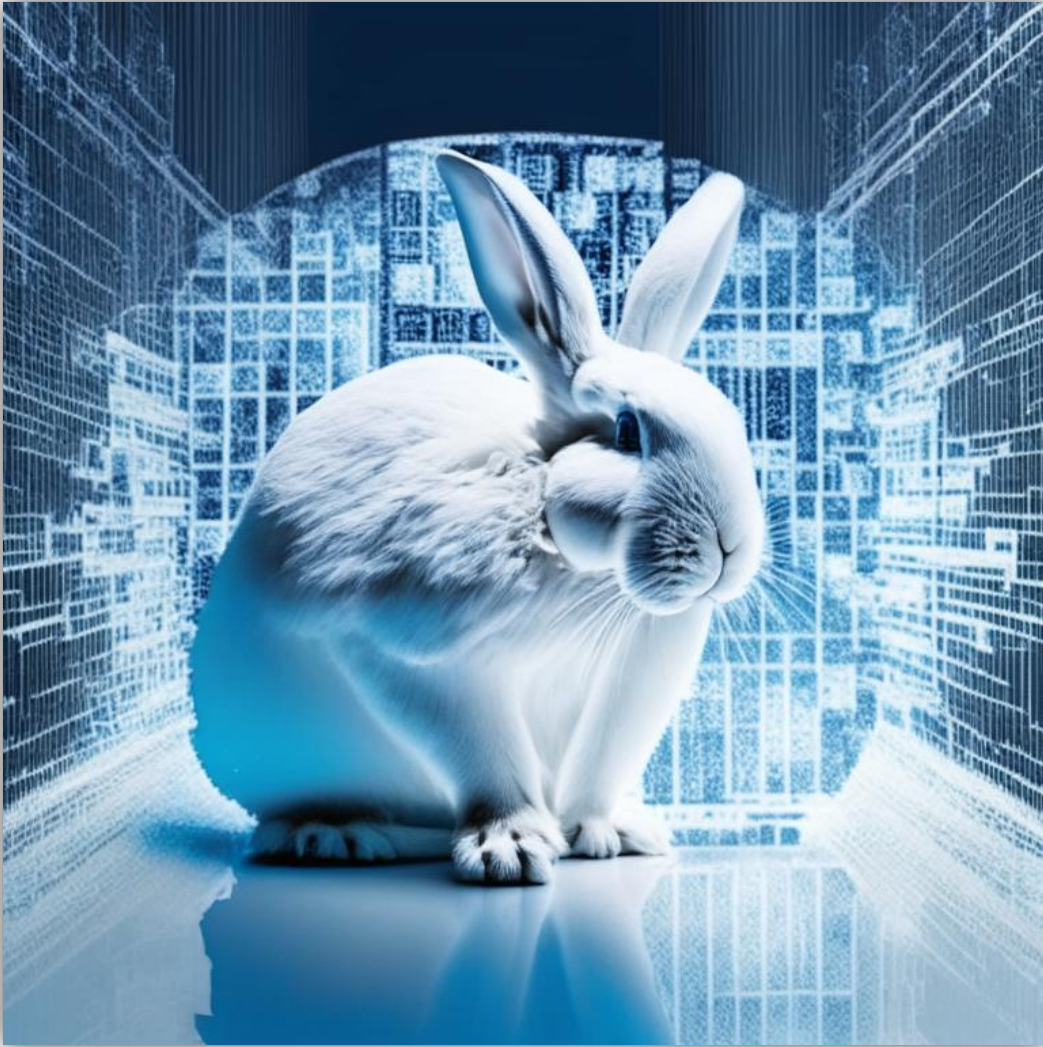


Рисунок 5. Методы атак на промышленные организации (доля атак)

Методы

СКДПУ ИТ – это RAM-платформа



Контроль и активный мониторинг

Фиксация видео и метаданных сессий,
реагирование и сегментация

Скорость анализа

Предварительная обработка «сырых» событий
доступа, UEBA, расширенные инструменты
поиска аномалий

Экосистемный подход

Объединение компетенций сторонних вендоров

Экономия ресурсов

Сокращение времени на анализ потенциальных
инцидентов

Базовые возможности СКДПУ ИТ

ЕДИНАЯ ТОЧКА ДОСТУПА

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

БЕЗ УСТАНОВКИ АГЕНТОВ

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

ПОЛНЫЙ ЦИКЛ УПРАВЛЕНИЯ ПАРОЛЯМИ

От предоставления доступа к гранулярной смене паролей для пользователей и выдачи паролей из сейфа, в т.ч. и для автоматизированных систем

ЗАПИСЬ СОБЫТИЙ ДОСТУПА

Полная запись сессий: клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и др.

REST API И АВТОМАТИЗАЦИЯ

Интеграции с внешними системами для создания и управления доступом

КОНТРОЛЬ НА СТОРОНЕ ИС

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

Централизованный архив данных по сессиям

Сессии: 1784, 10-03-2023

Добавить фильтры

Параметры запроса

Тип	Старт	Продолжительность	Персона / Аккаунт	IP	IP	IP
RDP	09-03-2023 17:47:50	0:02:10	avs@avs16.lo			
RDP	09-03-2023 16:36:21	0:01:22	avs@avs16.lo			
SSH	09-03-2023 11:27:23	0:00:00	admin / wabac			
RDP	09-03-2023 11:14:29	0:00:21	admin / root			
SSH	09-03-2023 11:11:59	0:00:16	admin / wabac			
SSH	07-03-2023 16:07:17	0:00:02	portalltest@tes			
RDP	07-03-2023 15:12:53	0:00:21	abezboro / root			
SSH	07-03-2023 15:10:34	0:00:07	abezboro / ntadmin177	172.16.128.22	10.100.1.177	skdpu70
SSH	07-03-2023 14:40:45	0:00:14	abezboro / ntadmin177	172.16.128.22	10.100.1.177	skdpu70
RDP	07-03-2023 14:24:11	0:00:20	admin / root	172.16.129.142	10.100.1.50	skdpu70
SSH	07-03-2023 14:23:19	0:00:16	abezboro / ntadmin177	172.16.128.22	10.100.1.177	skdpu70
SSH	07-03-2023 14:15:35	0:00:06	abezboro / ntadmin177	172.16.128.22	10.100.1.177	skdpu70
RDP	07-03-2023 14:13:40	0:00:11	abezboro / root	172.16.128.186	10.100.1.50	skdpu70

Искать текст:

...

Ввод с клавиатуры
 Заголовки
 Файлы
 Процессы
 Буфер обмена

Включить
Исключить

Включить цель...
 Включить аккаунт...
Исключить цель...
Исключить аккаунт...

Включить адрес клиента...
 Исключить адрес клиента...

Начиная с даты...
 Заканчивая датой...
Начиная с даты...
Заканчивая датой...

Включая персон...
 Все сессии

Сгруппировать

дата
 день

цель

учётная запись

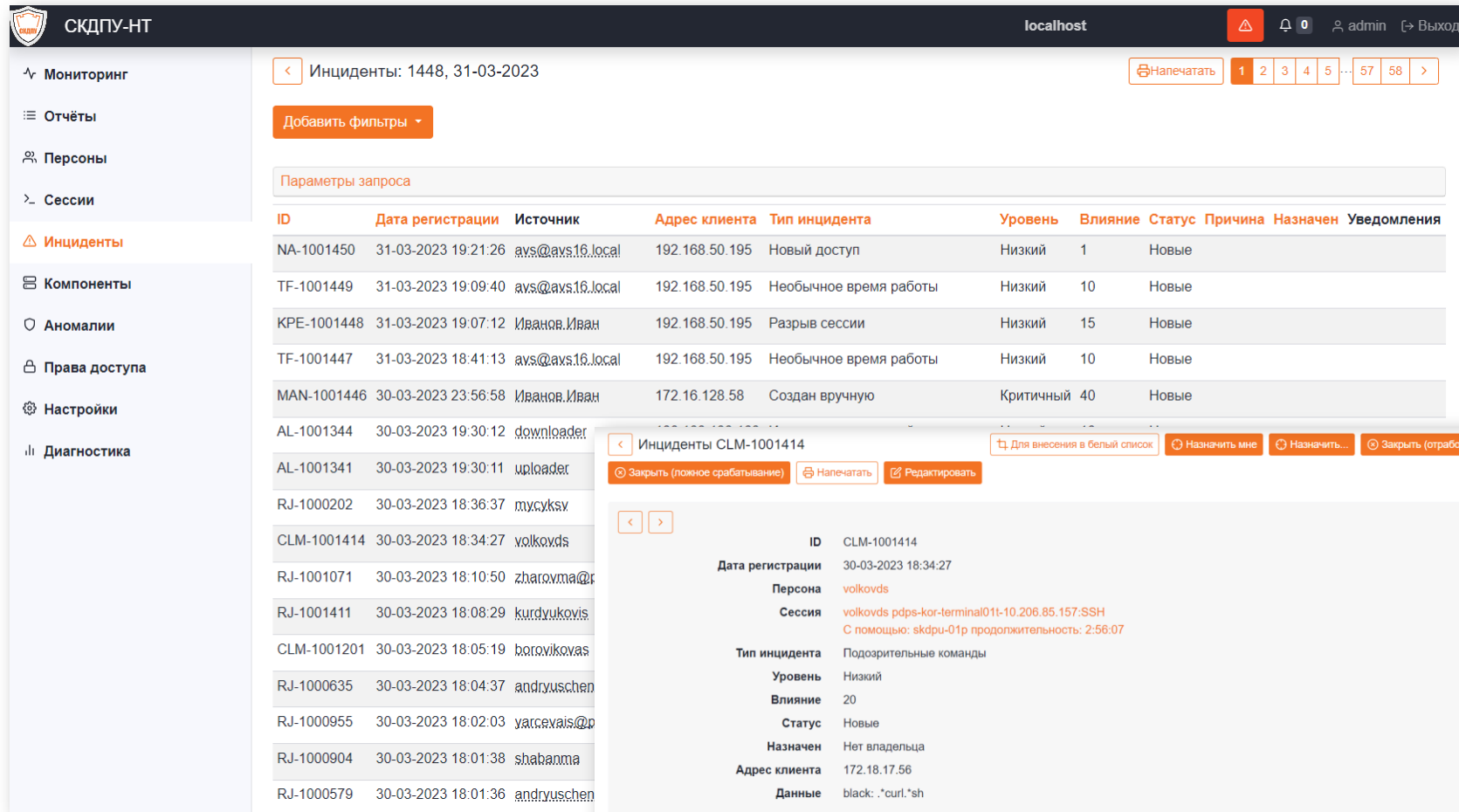
адрес клиента

персона

Поиск
 выводить по 25
записей на странице

Дата и время записи	Тип события	Данные
09-03-2023 16:36:21	SERVER_CERTIFICATE_MATCH_SUCCESS	description: X.509 server certificate match
09-03-2023 16:36:21	CERTIFICATE_CHECK_SUCCESS	description: Connexion to server allowed
09-03-2023 16:36:22	SESSION_ESTABLISHED_SUCCESSFULLY	
09-03-2023 16:36:25	CB_COPYING_PASTING_DATA_TO_REMOTE_SESSION	size: 209 format: CF_TEXT(1)
09-03-2023 16:36:28	COMPLETED_PROCESS	command_line: C:\Windows\system32\WTSTheme.exe -Embedding
09-03-2023 16:36:28	INPUT_LANGUAGE	display_name: Russian (Russia) identifier: 0x0419
09-03-2023 16:36:28	KERBEROS_TICKET_CREATION	client_name: avs@AVS16.LOCAL start_time: 2023/03/09 16:33:11 encryption_type: AES256_CTS_HMAC_SHA1_96(18) end_time: 2023/03/10 02:33:11 renew_time: 2023/03/16 16:33:11 flags: [name_canonicalize ok_as_delegate pre_authent renewable forwardable](0x40a50000)

Управляемая база данных инцидентов



Скриншот интерфейса системы управления инцидентами (СКДПУ-НТ). Вверху отображается информация о количестве инцидентов (1448) на 31-03-2023. В левом меню перечислены основные функции: Мониторинг, Отчёты, Персоны, Сессии, Инциденты, Компоненты, Аномалии, Права доступа, Настройки, Диагностика.

Основная часть экрана содержит таблицу с параметрами запроса и списком инцидентов. Таблица имеет следующие столбцы: ID, Дата регистрации, Источник, Адрес клиента, Тип инцидента, Уровень, Влияние, Статус, Причина, Назначен, Уведомления.

ID	Дата регистрации	Источник	Адрес клиента	Тип инцидента	Уровень	Влияние	Статус	Причина	Назначен	Уведомления
NA-1001450	31-03-2023 19:21:26	avs@avs16.local	192.168.50.195	Новый доступ	Низкий	1	Новые			
TF-1001449	31-03-2023 19:09:40	avs@avs16.local	192.168.50.195	Необычное время работы	Низкий	10	Новые			
KPE-1001448	31-03-2023 19:07:12	Иванов, Иван	192.168.50.195	Разрыв сессии	Низкий	15	Новые			
TF-1001447	31-03-2023 18:41:13	avs@avs16.local	192.168.50.195	Необычное время работы	Низкий	10	Новые			
MAN-1001446	30-03-2023 23:56:58	Иванов, Иван	172.16.128.58	Создан вручную	Критичный	40	Новые			
AL-1001344	30-03-2023 19:30:12	downloader								
AL-1001341	30-03-2023 19:30:11	uploader								
RJ-1000202	30-03-2023 18:36:37	myskyxv								
CLM-1001414	30-03-2023 18:34:27	volkovds								
RJ-1001071	30-03-2023 18:10:50	zharovma@								
RJ-1001411	30-03-2023 18:08:29	kurdyukovis								
CLM-1001201	30-03-2023 18:05:19	borovikovas								
RJ-1000635	30-03-2023 18:04:37	andryuschen								
RJ-1000955	30-03-2023 18:02:03	yatcevais@p								
RJ-1000904	30-03-2023 18:01:38	shabanma								
RJ-1000579	30-03-2023 18:01:36	andryuschen								

Всплывающее окно показывает детали инцидента CLM-1001414:

- ID:** CLM-1001414
- Дата регистрации:** 30-03-2023 18:34:27
- Персона:** volkovds
- Сессия:** volkovds pdps-kor-terminal011-10.206.85.157:SSH
С помощью: skdpu-01p продолжительность: 2:56:07
- Тип инцидента:** Подозрительные команды
- Уровень:** Низкий
- Влияние:** 20
- Статус:** Новые
- Назначен:** Нет владельца
- Адрес клиента:** 172.18.17.56
- Данные:** black: .*curl.*sh

В нижней части всплывающего окна отображены подробности записи:

Дата и время записи	Тип события	Данные
30-03-2023 18:34:27	KBD_INPUT	data curl -H 'cookie: designer-service=qm4apd203gone0nupillgq946m;

- Обучаемая модель детектора аномалий
- Белые списки инцидентов
- Рабочий процесс обработки инцидентов

Детектирование аномального поведения и реагирование

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

Детектирование потенциально опасных команд

Активировать

Уровень

Низкий

Группы

*

Название списка

black

Индикатор

Детектор н

Детектор п

Детектор и

Детектор в

Анализато

Детектор з

Количеств

Детектор сканеров

```

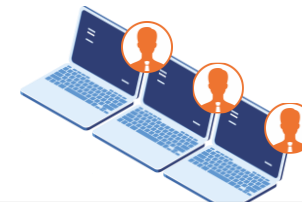
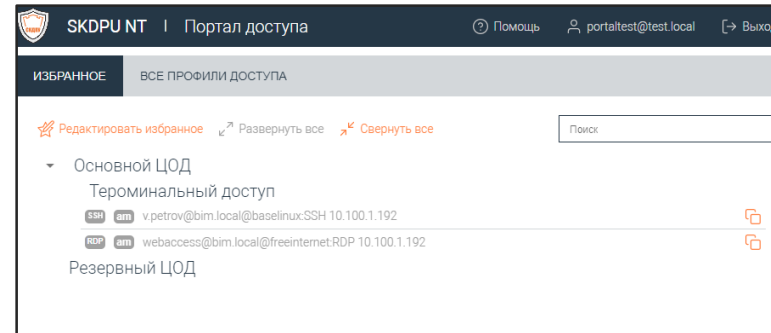
17 do
18   incident=$(echo "${incident}" | base64 --decode)
19   session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
20   event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
21   incident_id=$(echo "${incident}" | jq -r '.data.indent')
22   incident_link=$(echo "${incident}" | 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}\${incident_link}\"} \" \
30         "https://$(api_address)/api/sessions?session_id=${session_id}&action=kill"
31   fi
32 done
33

```

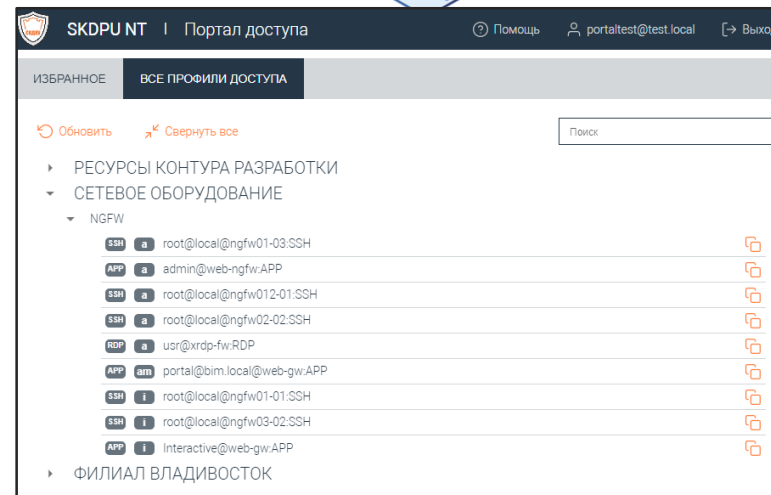
- Детектирование аномалий на основе статистических и математических моделей
- Подключение функций реагирования на инциденты и интеграция в единую систему реагирования
- Индивидуальные модели реагирования
- Взаимодействие с **SOAR/IRP**

Портал доступа. Брокер доступов к ресурсам

- **Единая точка доступа** к инфраструктуре шлюзов доступа
- Поддержка встроенных клиентов доступа без необходимости их установки
- Доступ в концепции «нулевого доверия»
- Доступ к приложениям и ресурсам VDI
- Настраиваемая группировка доступов



Получение доступа по запросу



Новые задачи – новые возможности

- ✓ Организация независимых точек доступа к ресурсам виртуализации и VDI
- ✓ «Терминальный интернет» для сотрудников
- ✓ Поддержка отечественных ОС и каталогов FreeIPA, ALD Pro и других LDAP
- ✓ Сократить до +-5
- ✓ Ограничения в рамках протоколов: файловый обмен, буфер обмена и т.д.
- ✓ Публикация ресурсов на Шлюзе доступа
- ✓ Фиксация действий и событий, в т.ч. видео
- ✓ Интеграция с системой глубокой аналитики СКДПУ ИТ Мониторинг и аналитика

СКДПУ ИТ – это про управление доступом

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**.

От большого к малому



СКДПУ НТ КОМПАКТ

Программно-аппаратный комплекс,
предназначенный для контроля действий
собственных администраторов и внешних
технических специалистов

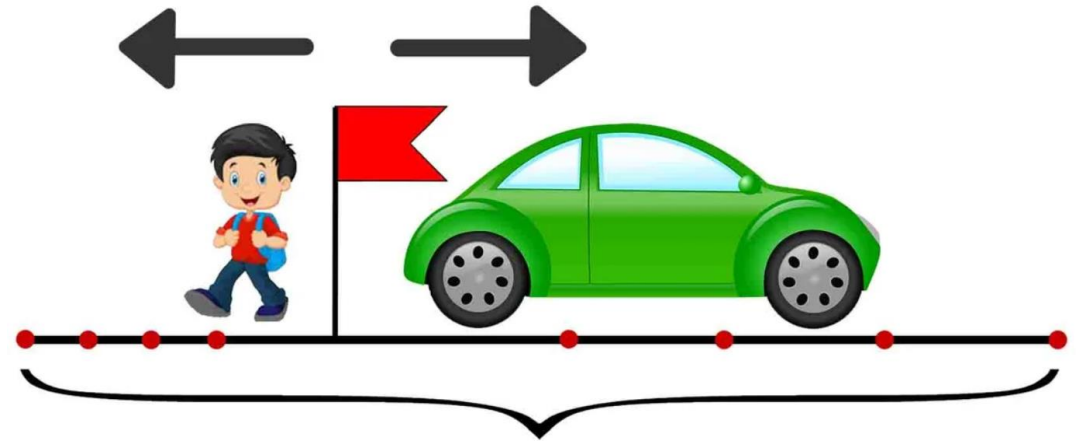
СКДПУ НТ Компакт - компактный ПАК, обладающий
функциональностью шлюза доступа:

- рассчитан на контроль до 10 одновременных сессий
- удобен в использовании в геораспределенной инфраструктуре и небольших компаниях
- доступен по цене

«Из контура А в контур Б подключался...»

Дано:

1. N – собственные сотрудники
2. N+1 – аутсорсеров
3. Наличие данных высокой критичности
4. Распределенная инфраструктура



Проблема:

1. Непрозрачность действий при обработке данных
2. Подключение сторонних организаций
3. Подключение к внутренней сети с личных устройств

Решение от заказчика

Решение:

1. СКДПУ ИТ в качестве единой точки доступа

- «извне» и «внутри»
- с личных и корпоративных устройств
- к критичным системам

2. «Нулевое доверие» с ограничением привилегий

3. Фиксация событий:

- запуска и остановки процессов
- буфера обмена
- команд, окон и др. событий

4. Фиксация активности и аномального поведения, в т.ч. вредоносного ПО



Единый контур ИБ с технологическими партнерами

Единая дополняемая концепция работы

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

- ✓ Система обнаружения вторжений
- ✓ Средства виртуализации и облачные сервисы
- ✓ Многофакторная аутентификация
- ✓ Отечественные ОС
- ✓ IRP/SOAR*
- ✓ SIEM-системы
- ✓ Безопасные рабочие места. Тонкие клиенты и т.п.
- ✓ Криптошлюзы и VPN-туннели
- ✓ Token и Smart Card
- ✓ DLP*

Технологии и партнеры



POSITIVE TECHNOLOGIES



РУТОКЕН



с•терра



и другие партнеры и интеграции...

РАМ-платформа СКДПУ ИТ

Интеграция и обогащение событиями

Единое управление конфигурацией

Реагирование и расследование

«Точно в срок» (Just –in-time)

Поведенческая аналитика (UEBA)

Контроль доступа

Анализ инфраструктуры и поиск УЗ

Нулевое доверие

Сценарный доступ

Управление паролями

Автоматизация и оркестрация



Спасибо за внимание!

Константин Родин

Руководитель направления
по развитию продуктов

k.rodin@it-bastion.com

