АЙТИБАСТИОН

СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ PAM. МЕНЬШЕ СЛОВ, БОЛЬШЕ ПРАКТИКИ

КОНСТАНТИН РОДИН
руководитель направления
по развитию продуктов

www.it-bastion.com

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

РЕАЛЬНАЯ СТАТИСТИКА
АТАК И ИХ ПОСЛЕДСТВИЙ

АЙТИБАСТИОН

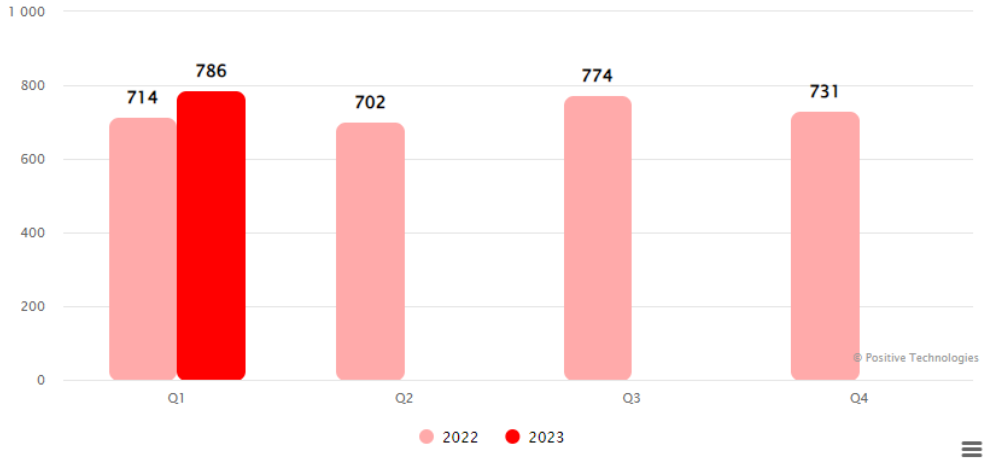


Рисунок 7. Количество инцидентов в 2022 и 2023 годах (по кварталам)

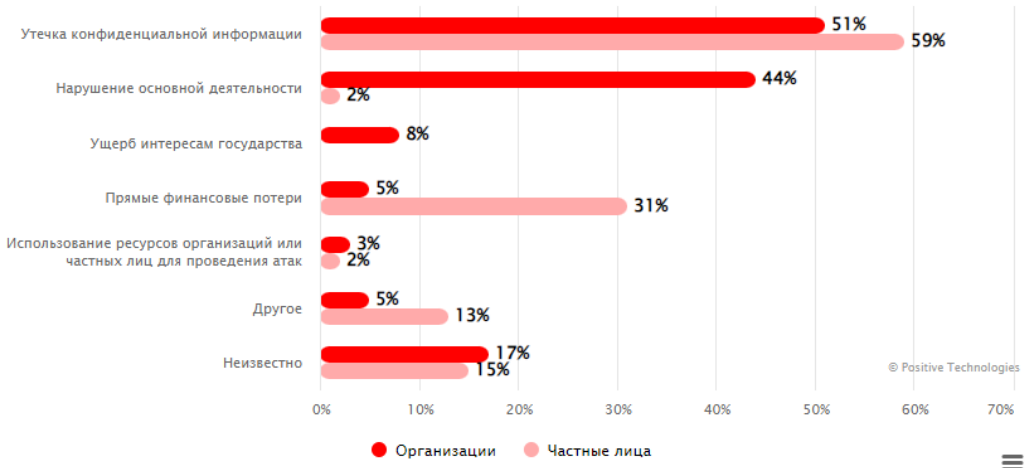


Рисунок 4. Последствия атак злоумышленников (доля атак)

68% атак имели целенаправленный характер

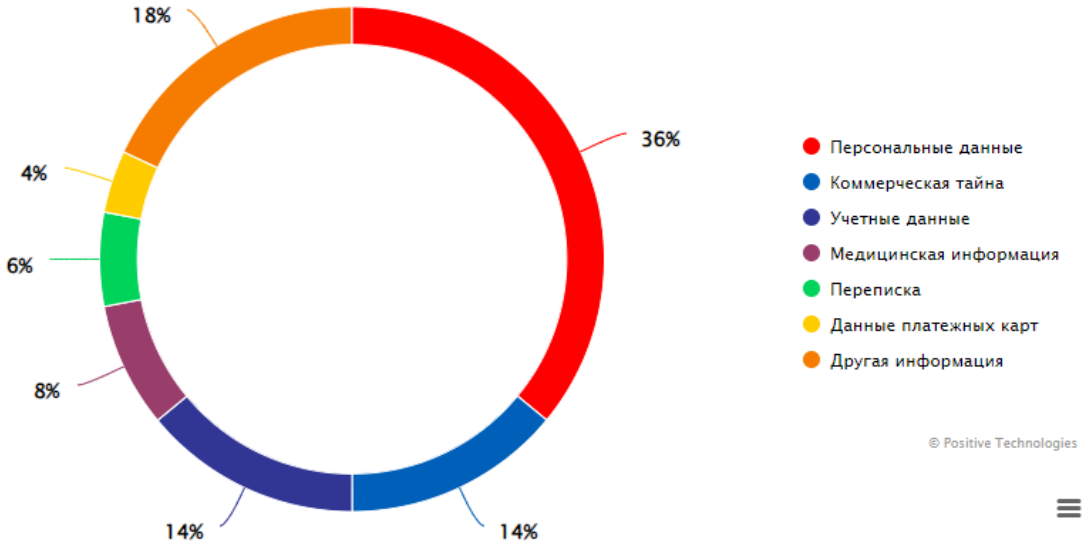


Рисунок 5. Типы украденных данных (в атаках на организации)

https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q1

ПРОБЛЕМАТИКА КОНТРОЛЯ ПРИВИЛЕГИРОВАННОГО ДОСТУПА

АЙТИБАСТИОН

01

Сложность централизованного контроля действий специалистов

02

Кража данных, нарушение работы критичных компонентов

03

Соблюдение требований регуляторов

04

Нарушение безопасности инфраструктуры, простой ресурсов компании

05

Нарушение бизнес-процессов компании

06

Потери в финансах и времени

www.it-bastion.com

ПРИМЕР РЕАЛИЗАЦИИ
АТАКИ В РЕАЛЬНОЙ ЖИЗНИ

АЙТИБАСТИОН

Colonial Pipeline, США

Атака программы-вымогателя.

Доступ в инфраструктуру получен через УЗ сотрудника.

- Отключение трубопровода на несколько дней
- Ущерб потребителям и авиакомпаниям восточного побережья
- Угроза национальной безопасности

100 Гб
Данных утекло

2 часа

www.it-bastion.com

ПРИМЕР РЕАЛИЗАЦИИ
АТАКИ В РЕАЛЬНОЙ ЖИЗНИ

АЙТИБАСТИОН

Uber, США

Взлом методом социальной инженерии.
Доступ в инфраструктуру получен через УЗ сотрудника.

- Утечка переписки, электронных адресов сотрудников, облачных данных
- Утечка данных водительских прав 600 тысяч водителей

57 млн

Человек пострадали от раскрытия личной информации

АЙТИБАСТИОН

Соответствие требованиям

Указ президента РБ №40; Приказ ОАЦ №130; Концепция обеспечения КБ в банковской сфере от 20.11.2019 г.; Концепции ИБ РБ от 18 марта 2019 г. №1; СТБ 34.101.1-2014, СТБ 34.101.2-2014, СТБ 34.101.3-2014; стандарты серии ISO/IEC 27000; PCI DSS

Базовая ОС

Комплекс работает под управление ОС AstraLinux SE. ОС внесена 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 – 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.

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
ПЛАТФОРМА СКДПУ НТ

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 мета-данных сессий с созданием долгосрочного архива. Клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и т.д.

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, особенно важна при подключении к объектам КИИ

ЕДИНЫЙ КОНТРОЛИРУЕМЫЙ ДОСТУП В ЦЕПОЧКАХ ПОСТАВОК

АЙТИБАСТИОН

1. Доступ в контур подрядчика через PAM

2. Доступ в контур заказчика через PAM

3. Выход в контур заказчика через локальный PAM

- Защита сотрудников подрядчика
- Минимизация риска со стороны инсайдеров

www.it-bastion.com

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

КОНТРОЛЬ ПРИЛОЖЕНИЙ И УЗ В НИХ

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

ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ

Полная запись видео и мета-данных сессий с созданием долгосрочного архива. Клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и т.д.

РАБОТА ПО ЗАЯВКАМ И ПОДТВЕРЖДЕНИЕМ

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

КОНТРОЛЬ НА СТОРОНЕ ИС

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

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ КОНТРОЛЯ ДОСТУПА

АЙТИБАСТИОН

Блокировка запуска приложений

Можем запрещать запуск приложений в рамках сессий пользователей

Блокировка исходящих соединений с целевого узла

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

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
ПЛАТФОРМА СКДПУ НТ

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

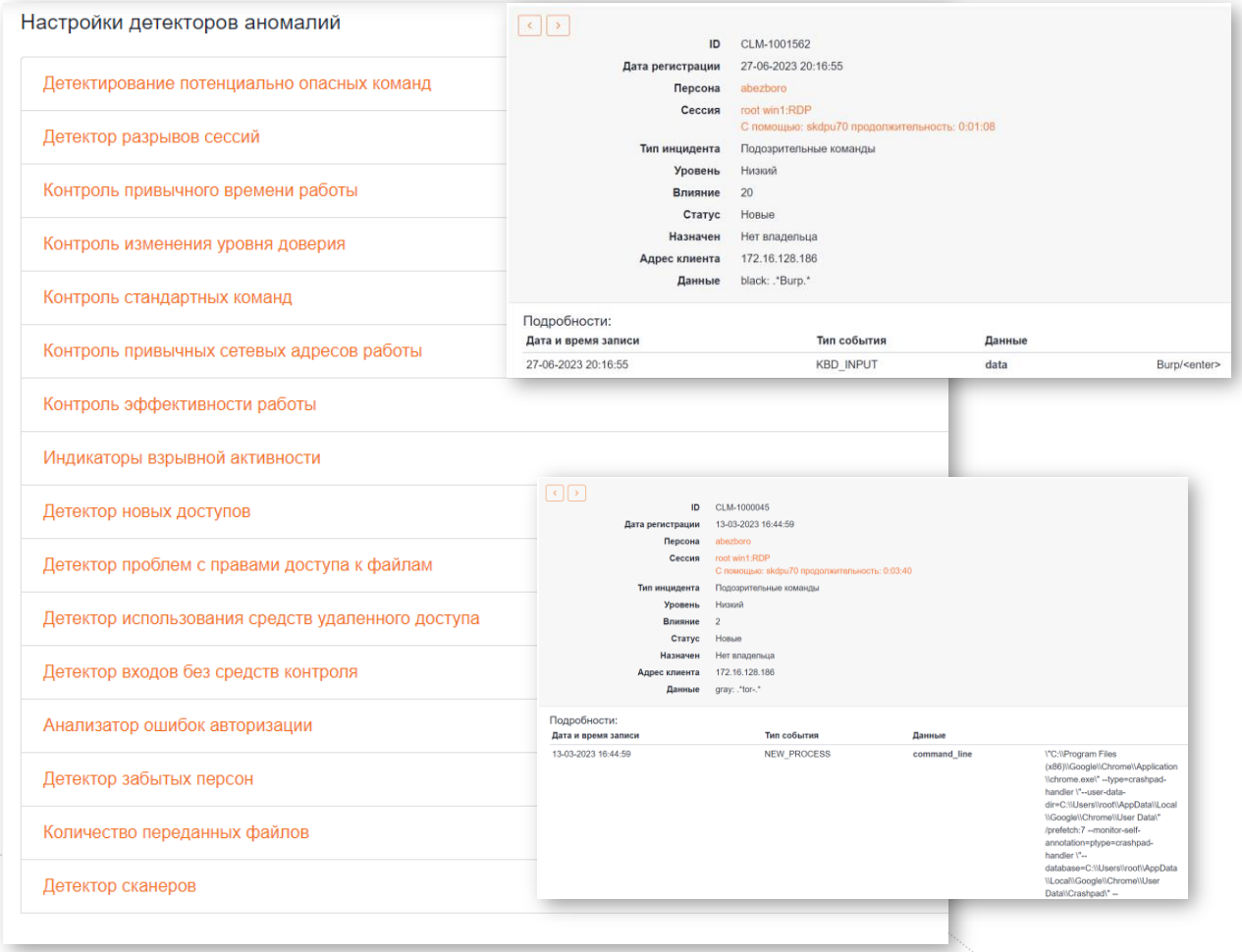
Обработка информации и её выдача в виде понятных отчетов от оперативных до сводных, в т.ч. для руководителей

ОТКАЗОУСТОЙЧИВОСТЬ И МАСШТАБИРОВНИЕ

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

ОТ ПОИСКА ИНЦИДЕНТА К РЕАГИРОВАНИЮ

АЙТИБАСТИОН



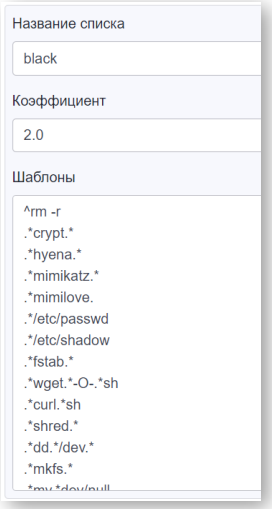
Индивидуальные модели реагирования

```
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
```

Подключение функций **реагирования на инциденты** и интеграция в единую систему реагирования

Взаимодействие с **SOAR/IRP**



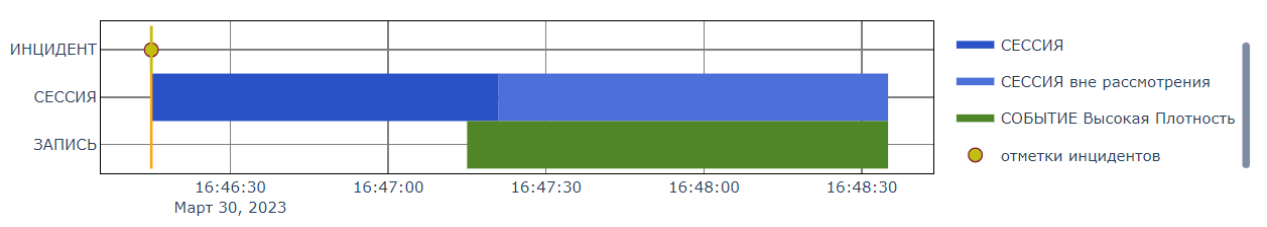
www.it-bastion.com

ПРАКТИКА РАССЛЕДОВАНИЯ НА ПРИМЕРЕ КОМПРОМЕТАЦИИ УЗ И УТЕЧКИ

АЙТИБАСТИОН

ID	eedc27123a22e61edb518fb3f5c9
Тип	RDP
Персона	p.ivan@pas.local
Адрес клиента	172.18.25.5
Старт	30-03-2023 16:46:15
Окончание	30-03-2023 16:48:35
Продолжительность	0:02:20
Цель	admin @ s_vdf-11.23.12.18 (11.23.12.18)
Шлюз	skdpu-03p
Видео	800×600 @ 25fps MPEG4
Инциденты	3

Старт сессии с нестандартного IP в необычное время



Выгрузка большего количества файлов

ID	Дата регистрации	Источник	Адрес клиента	Тип инцидента	Уровень	Влияние	Статус
TF-1000709	30-03-2023 16:46:15	p.ivan@pas.local	172.18.25.5	Необычное время работы	Низкий	10	Новые
SA-1000708	30-03-2023 16:46:15	p.ivan@pas.local	172.18.25.5	Сетевое расположение	Низкий	10	Новые
FT-1085414	30-03-2023 17:06:07	p.ivan@pas.local	172.18.25.5	Количество переданных файлов	Высокий	30	Новые

Дата и время записи	Тип события	Данные
30-03-2023 17:05:24	DRIVE_REDIRECTION_WRITE_EX	**sha256:** 19e037ddcd059235a5ce768c09b09426e8143da8867e7704e07a0f289a856281 **size:** 91452 **file_name:** D:/###Work/
30-03-2023 17:05:24	DRIVE_REDIRECTION_WRITE_EX	**sha256:** cf77028ca36aa3a046b779c77708deb1c23bf8602551994c6a362fe54947d76a **size:** 507918 **file_name:** D:/###Work/
30-03-2023 17:05:25	DRIVE_REDIRECTION_WRITE_EX	**sha256:** 2a7e251086b0729c8dd1071923ecd15a3d46860e4a0f74afc80066ff164e6284 **size:** 525794 **file_name:** D:/###Work/
:25	DRIVE_REDIRECTION_WRITE_EX	**sha256:** b4193f177542e1069852a5e86cd08fef6ef6fbffdb80e5c10985f681524cf508 **size:** 499078 **file_name:** D:/###Work/

www.it-bastion.com

ИДЕНТИФИКАЦИЯ ВРЕДОНОСНОГО ПО И АТАК

АЙТИБАСТИОН

Анализ запущенных процессов

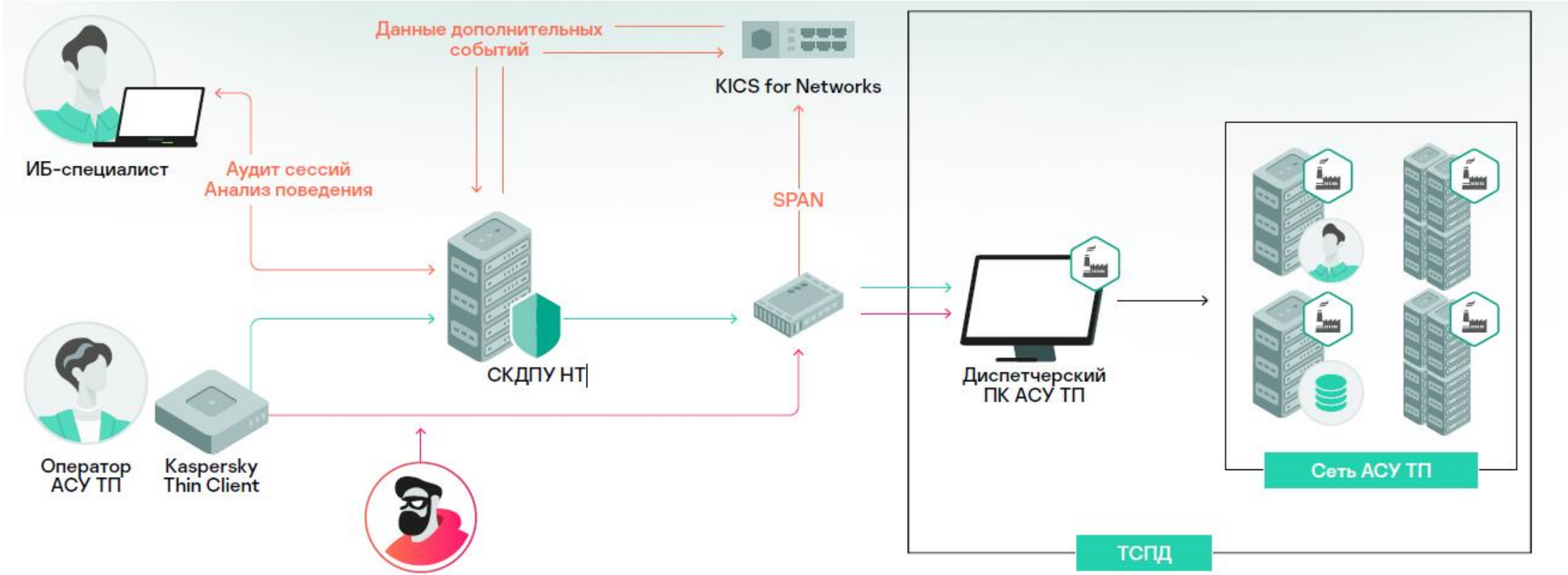
Сбор и накопление событий

Детектирование аномалий

«В правилах стоял детект на типичные thread injection, и в случае выполнения тех или иных команд даже в фоновом режиме - сессия сотрудника обрывалась. Удалось задетектировать подобную вредоносную активность, расследовать её комплексом сзи и отозвать доступ к системам компании N.»

СЕГМЕНТИРОВАНИЕ И ОГРАНИЧЕНИЕ ФИЗИЧЕСКОГО ДОСТУПА

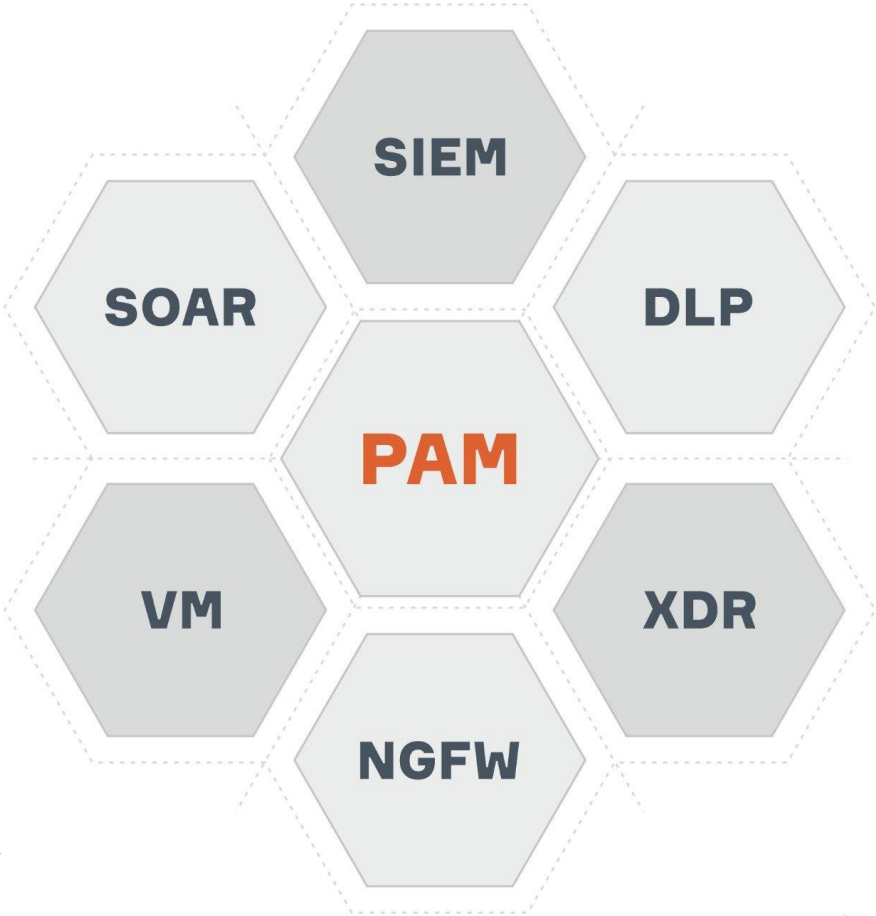
АЙТИБАСТИОН

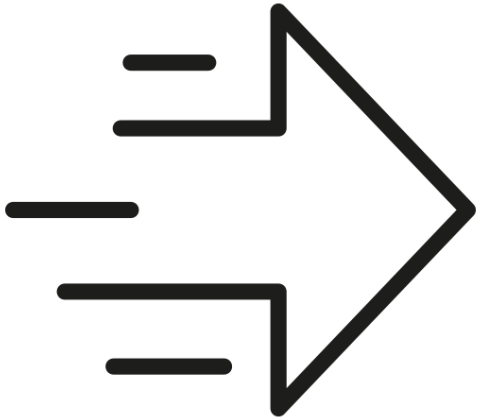


Регламентированный доступ из внешнего помещения через
систему контроля удаленного доступа с защищенного тонкого клиента

ПРОБЛЕМА «ИЗОЛИРОВАННОСТИ» СРЕДСТВ ИБ

АЙТИБАСТИОН



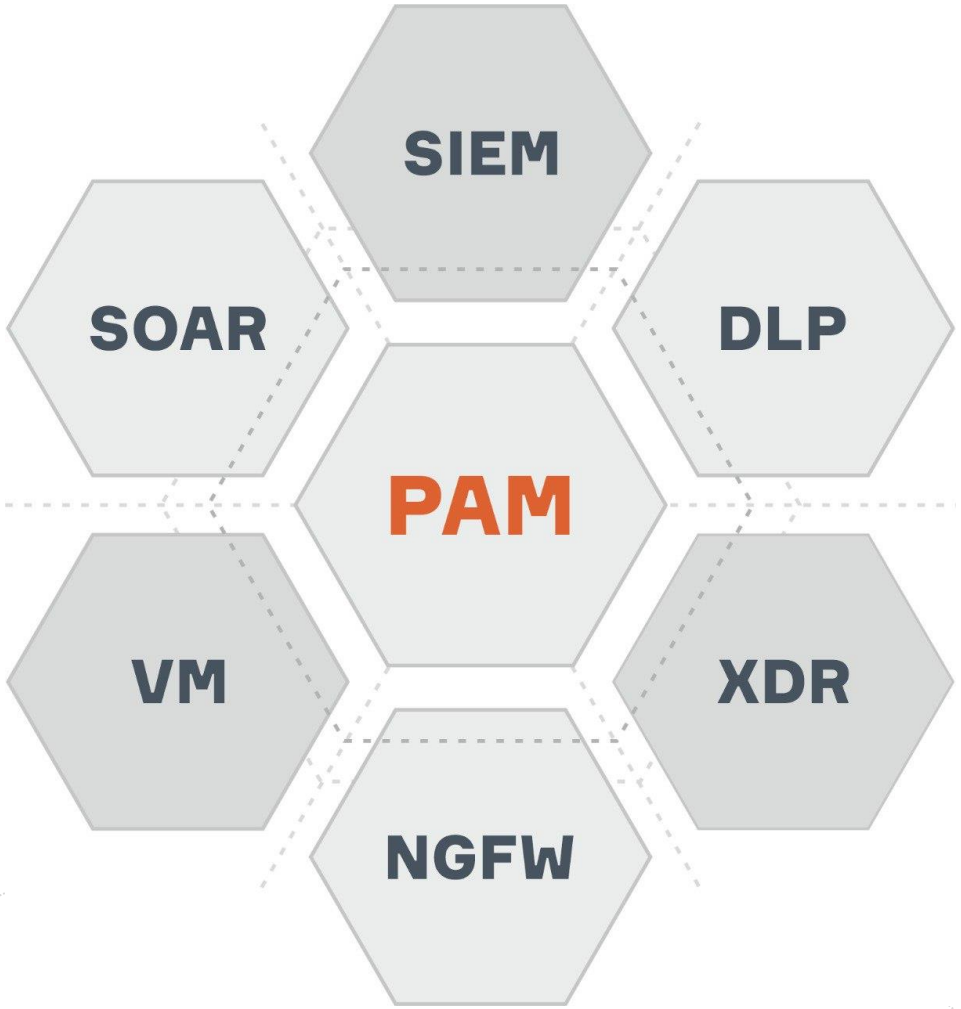


«зазор» средств защиты

эксплуатация «зазора»

БОЛЬШЕ ВОЗМОЖНОСТЕЙ
СКДПУ НТ

АЙТИБАСТИОН



Контроль и мониторинг доступа

Выявление инцидентов

Реагирование на инциденты

Кроссвендорная интеграция

Контроль доступа к информации

ЕДИНАЯ ДОПОЛНЯЕМАЯ КОНЦЕПЦИЯ РАБОТЫ РАМ-ПЛАТФОРМЫ СКДПУ НТ

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.

1. Система обнаружения вторжений
2. Средства виртуализации и облачные сервисы
3. Многофакторная аутентификация
4. Отечественные ОС
5. IRP/SOAR
6. HoneyPot
7. SIEM-системы
8. Безопасные рабочие места, тонкие клиенты и т.п.
9. Криптошлюзы и VPN-туннели
10. Token и Smart Card
11. Межсетевые экраны
12. DLP*

www.it-bastion.com

ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ
«АйТи БАСТИОН» и СКДПУ НТ

АЙТИБАСТИОН

ASTRA LINUX®

POSITIVE TECHNOLOGIES

kaspersky

INFOWATCH®

Passwork ®

DATALINE

GIS
ГАЗИНФОРМ
СЕРВИС

ROSA

CyberLympha®

РУТОКЕН

Аладдин

zVirt

alt linux

с•терра®

MULTIFACTOR

UserGate

Rusiem

КОД
безопасности

РЕДОС

и другие партнеры

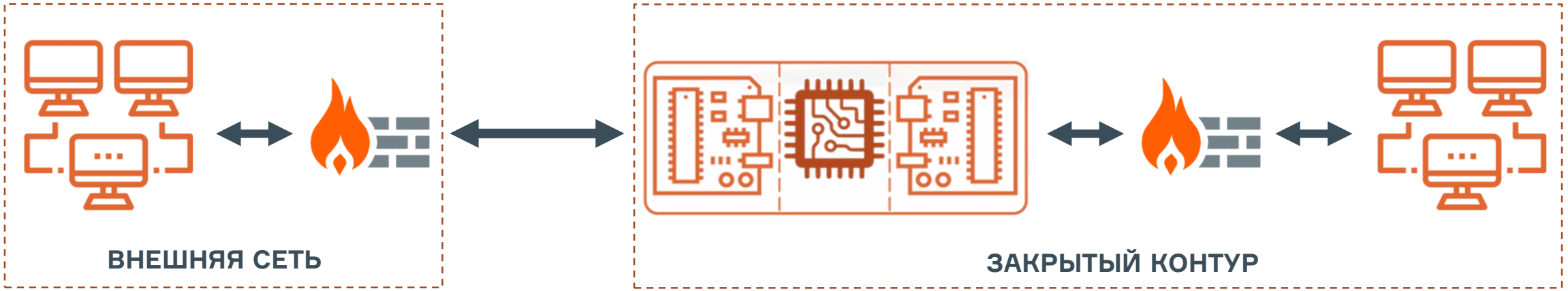
www.it-bastion.com

НЕ ТОЛЬКО РАМ, НО И
ШЛЮЗ БЕЗОПАСНОГО ОБЪЕДИНЕНИЯ СЕТЕЙ

Предназначен для использования в автоматизированных системах для обработки информации с максимальным уровнем конфиденциальности информации **не выше «совершенно секретно»** (включительно).

ВОЗМОЖНОСТИ ШЛЮЗА СИНОНИМ

АЙТИБАСТИОН



ПЕРЕДАЧА ДАННЫХ

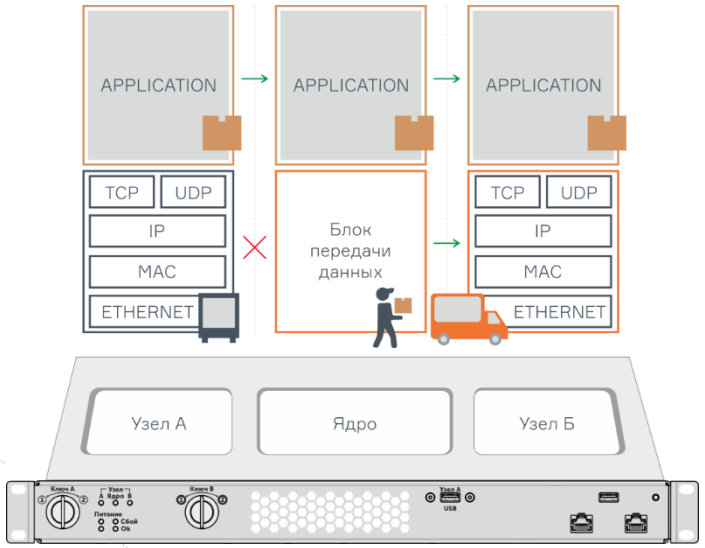
Передача данных между ИЗОЛИРОВАННЫМИ сетями.

- TCP, UDP
- Независимые политики для двух контуров
- Скорость до 1 Гб/с

ПЕРЕДАЧА ФАЙЛОВ

Передача файлов между ИЗОЛИРОВАННЫМИ сетями с дополнительными правилами проверки файлов на соответствие политикам передачи.

- SFTP
- Выбор направления передачи
- Проверка маски, ЭЦП
- Интеграция с ICAP-сервисами (DLP, Sandbox, AV и др.)



Работа на транспортном уровне:

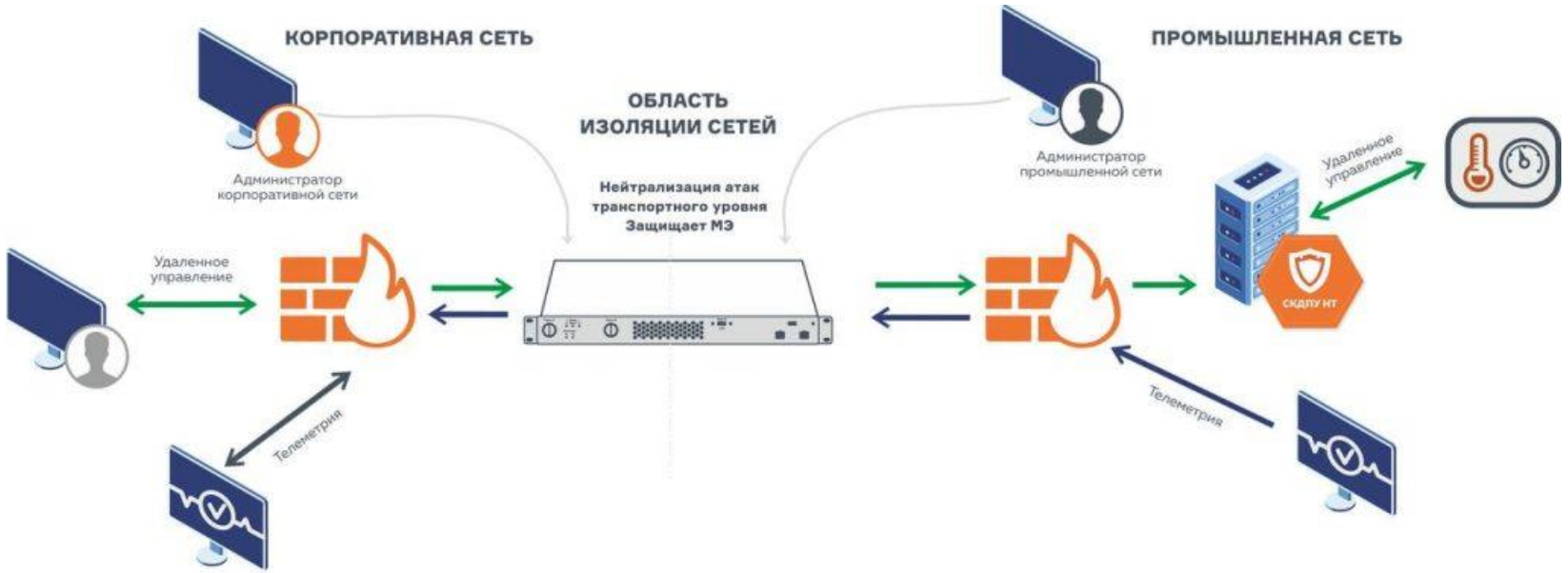
- Изоляция сети
- Нейтрализация сетевых атак

Противодействие 0-day

Контентная фильтрация данных:

- Валидация и проверка файлов
- Работа в цепочке сетевого оборудования

СЦЕНАРИЙ ПРИМЕНЕНИЯ СОВМЕСТНО С PAM
ЗАДАЧА



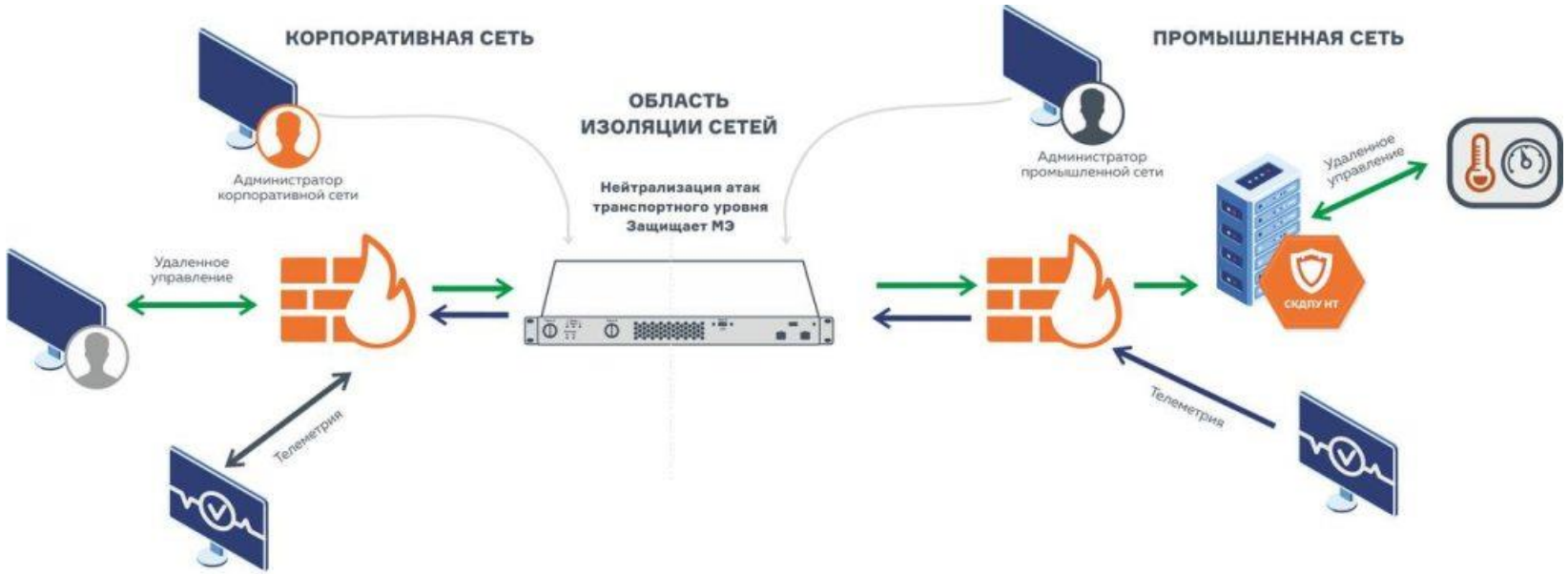
Цель: обеспечение дополнительной степени защиты при передаче данных в закрытый сегмент и организация безопасного контролируемого доступа в него.

Задача: организовать изоляцию сегментов сетей с возможностью передачи части данных из закрытого контура и обеспечить контролируемый доступ к критически важным объектам средствами PAM-системы.

Предпосылки, условия и компромиссы:

Получение актуальных и оперативных данных из закрытых, изолированных сегментов является актуальной, но не единственной задачей в современных реалиях глобальной цифровизации бизнеса. Также важно оперативно обеспечить удаленный доступ к объектам в таких сегментах при условии, что он не только регламентирован, но и надежно защищен и соответствует всем предъявляемым к этим объектам требованиям регуляторов.

СЦЕНАРИЙ ПРИМЕНЕНИЯ СОВМЕСТНО С PAM
РЕШЕНИЕ



Решение:

Для достижения цели используется шлюз безопасного стыка сетей Синоним в сочетании с PAM-системой СКДПУ НТ.

В рамках организованного безопасного канала между двумя сетями располагается Синоним. Он предоставляет дополнительный контроль и фильтрацию пакетов на транспортном уровне и обеспечивает связь между заранее определенными системами двух сетей, одной из которой является СКДПУ НТ. NGFW, который размещается после Синонима, создает базовую защиту изолированной сети. Далее со стороны закрытого сегмента – СКДПУ НТ, через которую проходит контролируемый безопасный доступ к целевой системе. Таким образом обеспечивается не только высокий уровень контроля проходящей между сетями информации, фильтрация и защита от атак на транспортном уровне, но и управление привилегированным доступом внутри закрытого сегмента.

ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ
«АйТи БАСТИОН» и СКДПУ НТ

АЙТИБАСТИОН

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%

PAM-рынка РФ

Комплекс СКДПУ НТ
Проверенное решение, доказавшее свою эффективность, надежность и качество

www.it-bastion.com

Спасибо за внимание!

АЙТИБАСТИОН

Константин Родин
Руководитель направления
по развитию продуктов

k.rodin@it-bastion.com

+7 916 560 50 66

it-bastion.com