АЙТИБАСТИОН

www.it-bastion.com

2024

ПО КЛАССИКЕ КОНЦЕПЦИИ ZERO TRUST

КАК ДОВЕРИТЬСЯ ПРИВИЛЕГИРОВАННОМУ ПОЛЬЗОВАТЕЛЮ И КАК ИЗОЛИРОВАТЬ ВЗАИМОДЕЙСТВИЕ МЕЖДУ СИСТЕМАМИ

ШИРИКАЛОВ АЛЕКСЕЙ
Руководитель группы
Поддержки продаж

КОМПАНИЯ АЙТИ БАСТИОН

2014

ОСНОВАНИЕ КОМПАНИИ

10 лет на российском рынке информационной безопасности

300+

ПАРТНЕРОВ-ИНТЕГРАТОРОВ

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

250+

ЗАКАЗЧИКОВ И ПРОЕКТОВ

Присутствие во всех отраслях от нефтяных компаний до футбольных клубов, от небольших инфраструктур до георапределенных площадок

>70%

РАМ-РЫНКА РФ

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

PAM

Privileged Access Management (PAM)

Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам.

Сертификация

Работа продукта на базе
операционной системы Astra Linux SE

ASTRA LINUX®

К ЧЕМУ ПРИШЛИ
РАМ-ПЛАТФОРМЫ В 2024 ГОДУ

АЙТИБАСТИОН

- Расширенный контроль доступа
- Непрерывный мониторинг
- Управление секретами и их хранение
- Выявление и обработка инцидентов
- Поиск и выявление аномалий
- Реагирование на инциденты

Комплексный подход к обеспечению защищенности

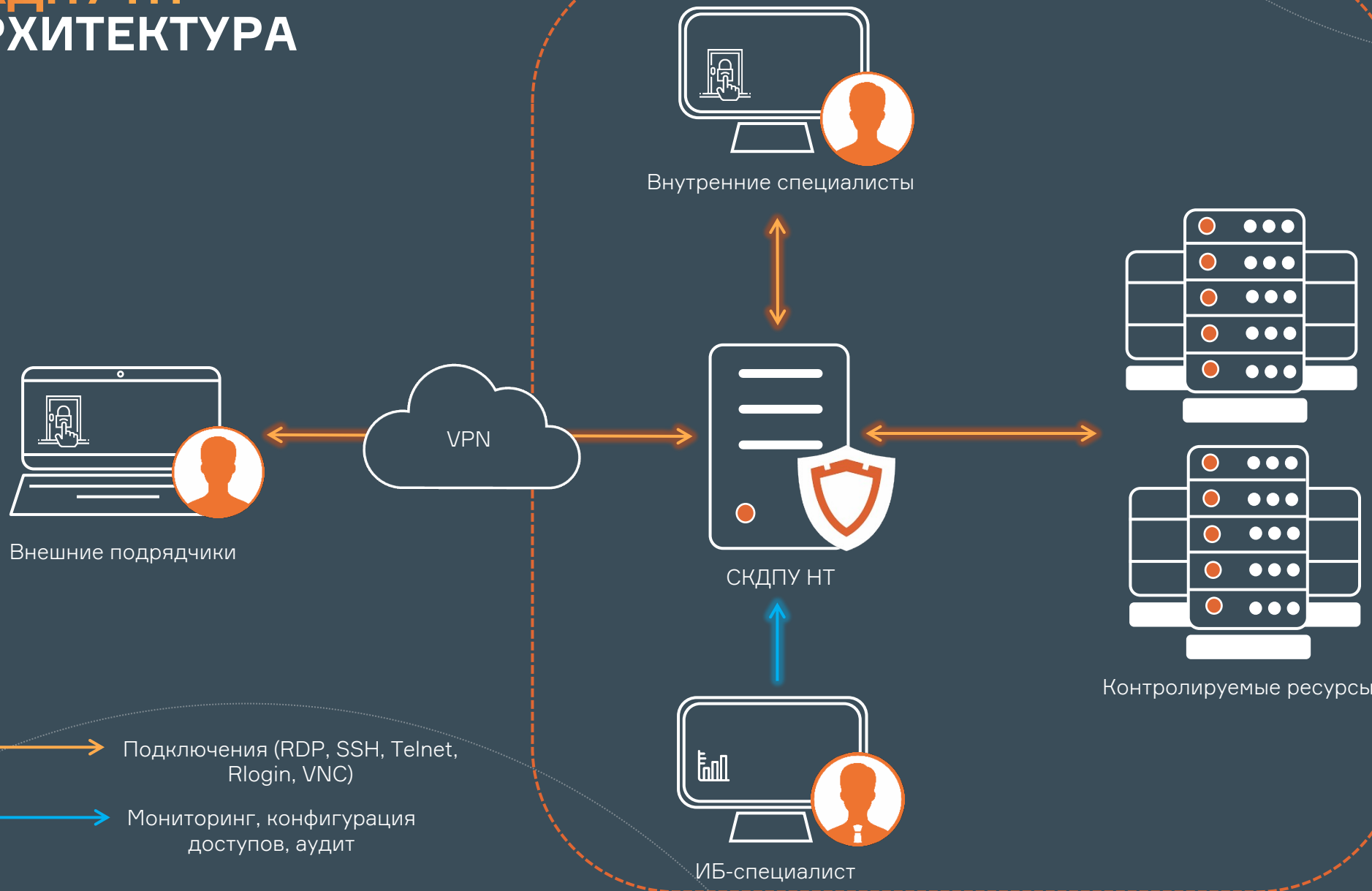
Классическая PAM-система

- Контроль доступа
- Фиксация событий доступа
- Управление паролями

www.it-bastion.com

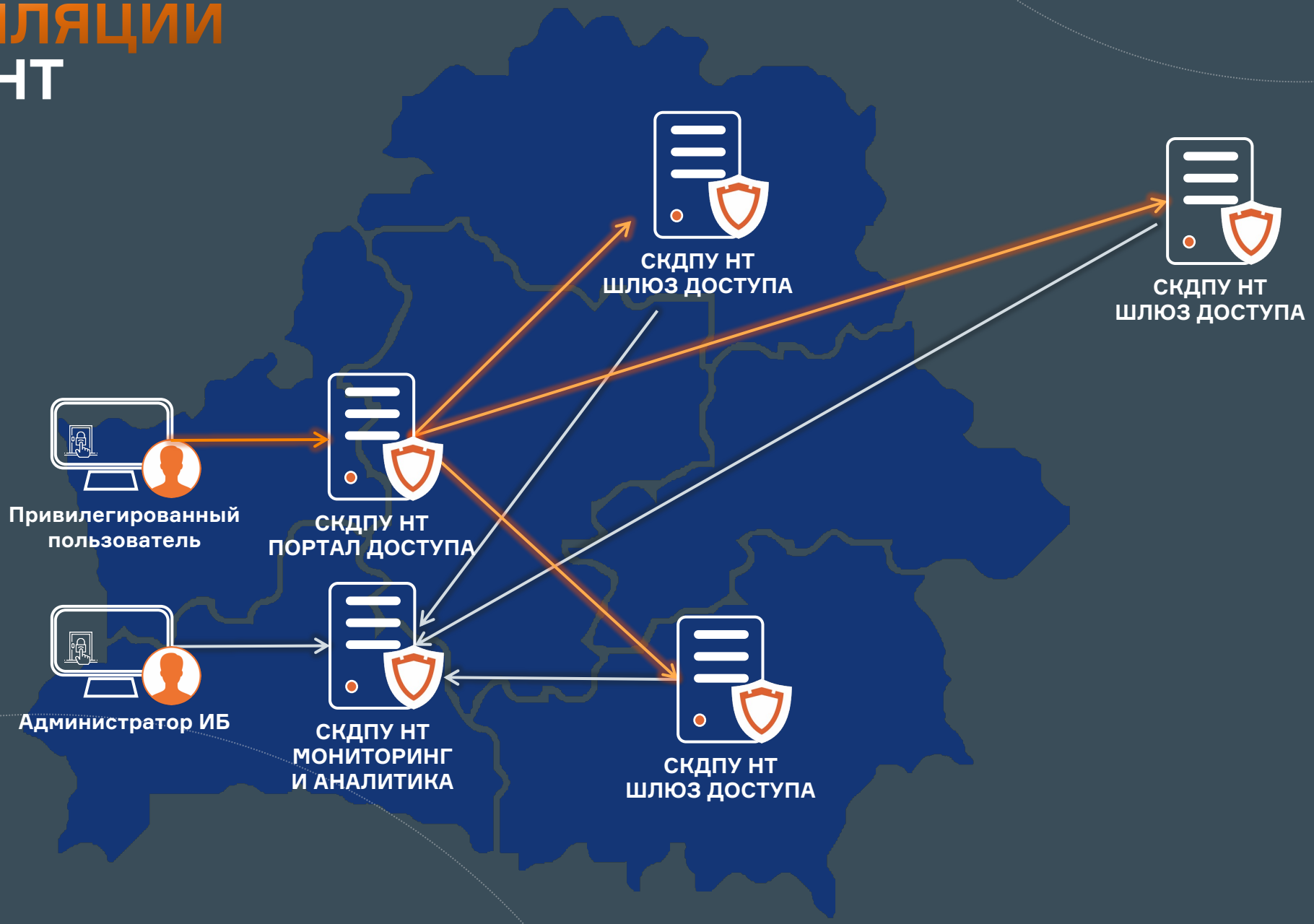
СКДПУ НТ
АРХИТЕКТУРА

АЙТИБАСТИОН



www.it-bastion.com

ИНСТАЛЛЯЦИИ
СКДПУ НТ



www.it-bastion.com

АЙТИБАСТИОН

ВОЗМОЖНОСТИ
МЕЖВЕНДОРНЫХ ВЗАИМОДЕЙСТВИЙ

СКДПУ НТ
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЁРСТВА

ASTRA LINUX®

POSITIVE TECHNOLOGIES

kaspersky

INFOWATCH®

Пассворк

DATALINE

GIS
ГАЗИНФОРМ СЕРВИС

ROSA

CyberLympha®

РУТОКЕН

Аладдин

zVirt

alt linux

С•Терра®

MULTIFACTOR

UserGate

Rusiem

КОД безопасности

РЕДОС

и другие партнеры

ZERO TRUST

КОГО КОНТРОЛИРУЕМ?

Наиболее распространённые сценарии

ВНУТРЕННИХ ПОЛЬЗОВАТЕЛЕЙ

Системные администраторы, операторы и другие привилегированные пользователи с доступом к серверам КИИ

ПОДРЯДЧИКОВ

При их привлечении для решения задач на объектах КИИ

АУДИТОРОВ

При необходимости осуществления доступа к чувствительной инфраструктуре

ИНЖЕНЕРОВ ВЕНДОРА

При обслуживании ПО/оборудования, сервисных работах

АЙТИБАСТИОН

www.it-bastion.com

АЙТИБАСТИОН

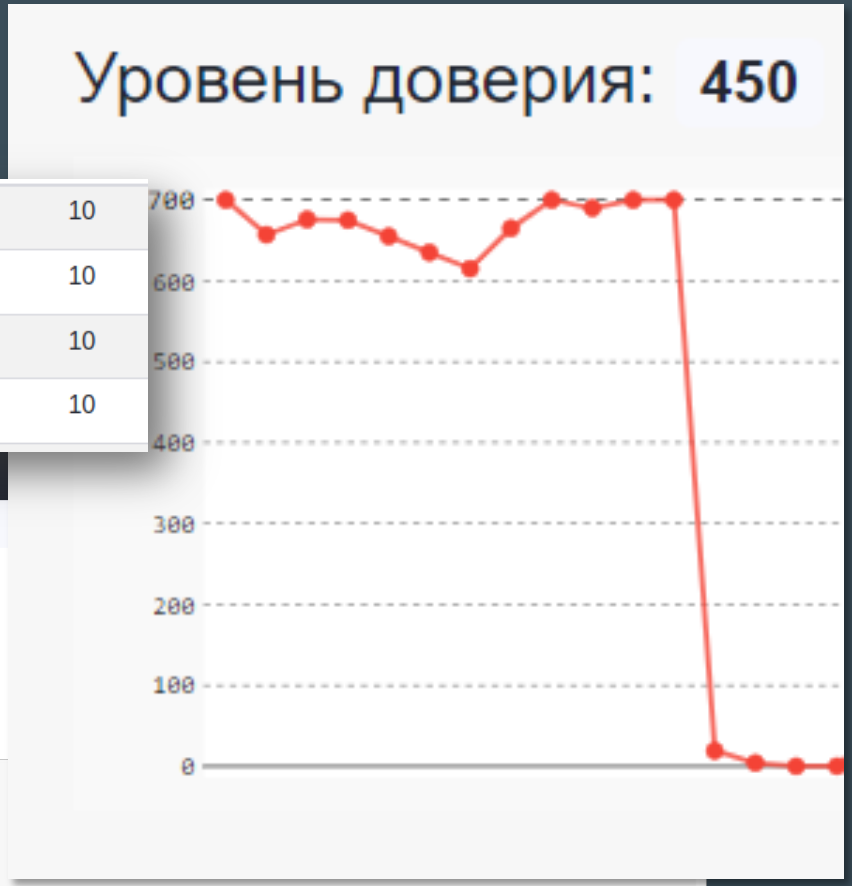
Примеры выявления нелегитимных действий привилегированного пользователя

- Подозрительная активность
- Эффективность работы
- Человеческий фактор
- Автоматизация
- Цепочки поставок

РЕАЛИЗАЦИЯ
ПОДОЗРИТЕЛЬНАЯ АКТИВНОСТЬ

АЙТИБАСТИОН

AF-1000232	05-03-2024 07:13:01	admin		Ошибка аутентификации	Низкий	10
TF-1000231	05-03-2024 07:03:20	admin	172.16.137.42	Необычное время работы	Низкий	10
SA-1000230	05-03-2024 07:03:20	admin	172.16.137.42	Сетевое расположение	Низкий	10
TF-1000229	05-03-2024 06:29:55	admin	172.16.130.62	Необычное время работы	Низкий	10



SKDPU

Текущие соединения

Обновить статус

Обновлять автоматически :

Частота : 5 sec

пауза...

Показать элементы 10

Статус Пользователь

admin@172.16.130.6

1 - 1 / 1

Подтвердите действие на 10.0.129.59

Подтвердите разрыв для сессии : admin@172.16.130.62 -> admin@demowin:3389 (RDP/RDP) ?

OK Отмена

Тип инцидента	Необычные команды
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Адрес клиента	
Данные	

Suspicious session (with 63 sessions in profile): 1 new command of 6 , 2 new permutation of 2 commands , 5 new permutations of 3 or more commands , not typical length of commands sequence

РЕАЛИЗАЦИЯ
ЭФФЕКТИВНОСТЬ РАБОТЫ

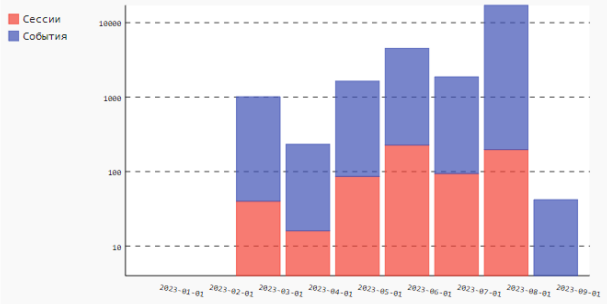
АЙТИБАСТИОН

www.it-bastion.com

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

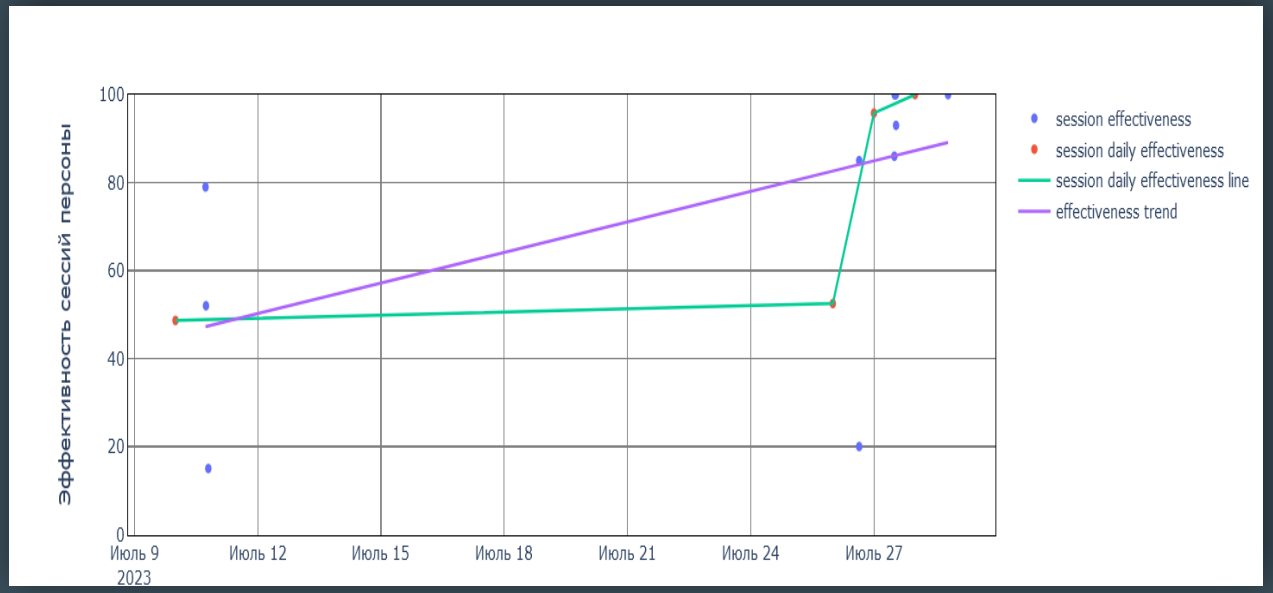
Активность пользователей



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

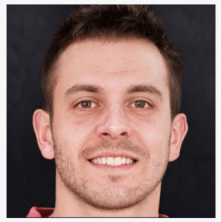


СКДПУ НТ
ЧЕЛОВЕЧЕСКИЙ ФАКТОР

АЙТИБАСТИОН

www.it-bastion.com

Цифровой профиль пользователя | 7 дней | Показать | Выберите дату... | Напечатать | Редактировать



Избранное

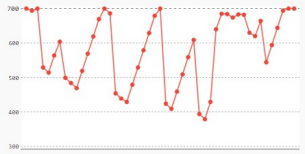
ID: admin

Зарегистрирован: 16-10-2023 13:58:00

Последняя активность: 06-03-2024 11:24:00

Группа: Интеграторы

Уровень доверия: **700**



Активности

	Сегодня	Текущая неделя	Текущий месяц	Текущий квартал	Текущий год	Всего
Сессии:	0	0	15	70	70	208
Шлюзы:	0	0	2	3	3	5
Цели:	0	0	4	6	6	15
Учётные записи:	0	0	3	4	4	7
Время работы:	--	--	0:40:21	2:00:21	2:00:21	7:58:44
Загруж						
Скач						

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

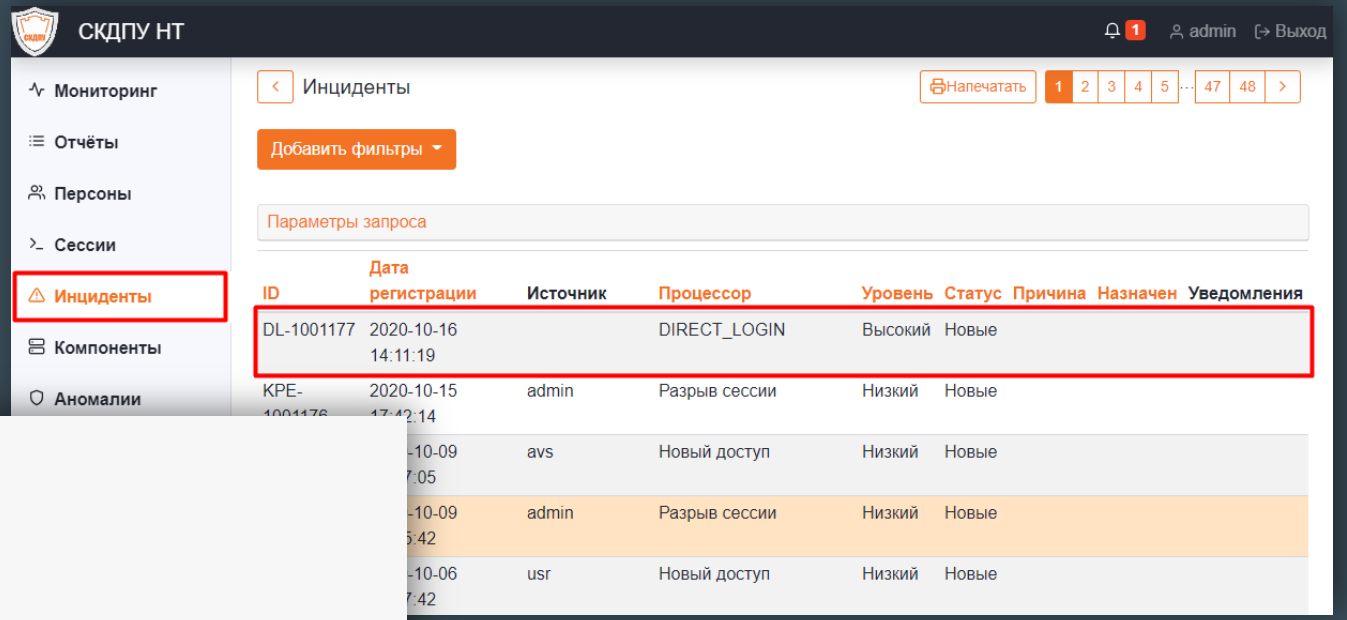
RJ-1093922 09-08-2023 14:23:29 [redacted] [redacted] Туннели и прыжки Низкий 10

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)

СКДПУ НТ
ЧЕЛОВЕЧЕСКИЙ ФАКТОР

АЙТИБАСТИОН



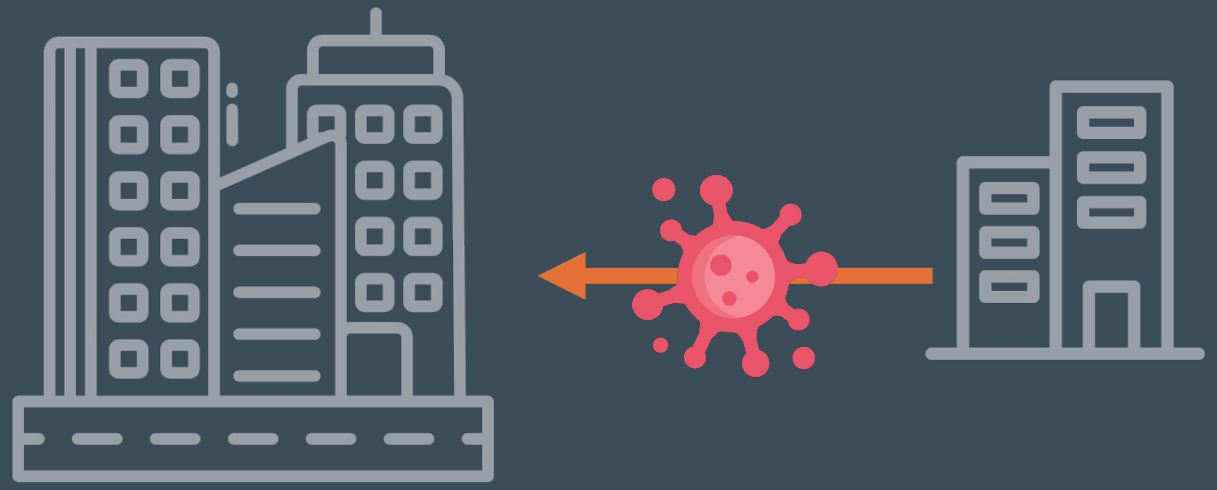
ID	DL-1001177
Дата регистрации	2020-10-16 14:11:19
Тип	DIRECT_LOGIN
Уровень	Высокий
Статус	Новые
Назначен	Нет владельца
Данные	Remote SSH connection from: [redacted] to: [redacted]

```
do
incident=$(echo "${
session_id=$(echo "
event_type=$(echo "
incident_id=$(echo
incident_link=$(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
```

СКДПУ НТ
ЦЕПОЧКИ ПОСТАВОК

АЙТИБАСТИОН



СКДПУ НТ
ЦЕПОЧКИ ПОСТАВОК

АЙТИБАСТИОН

x10

ПРОБЛЕМНЫЕ ВОПРОСЫ СОГЛАСНО РЕЗУЛЬТАТАМ ГОСУДАРСТВЕННОГО КОНТРОЛЯ *

АЙТИБАСТИОН

01

Уязвимость цепочек поставок

02

Наличие неучтенных или незащищенных подключений

03

Использование слабых паролей

04

Отсутствие регулярных обновлений баз АВЗ и СОВ

05

Низкая вовлеченность персонала в вопросы ИБ

06

Отсутствие анализа защищенности периметра

07

Наличие архитектурных уязвимостей

08

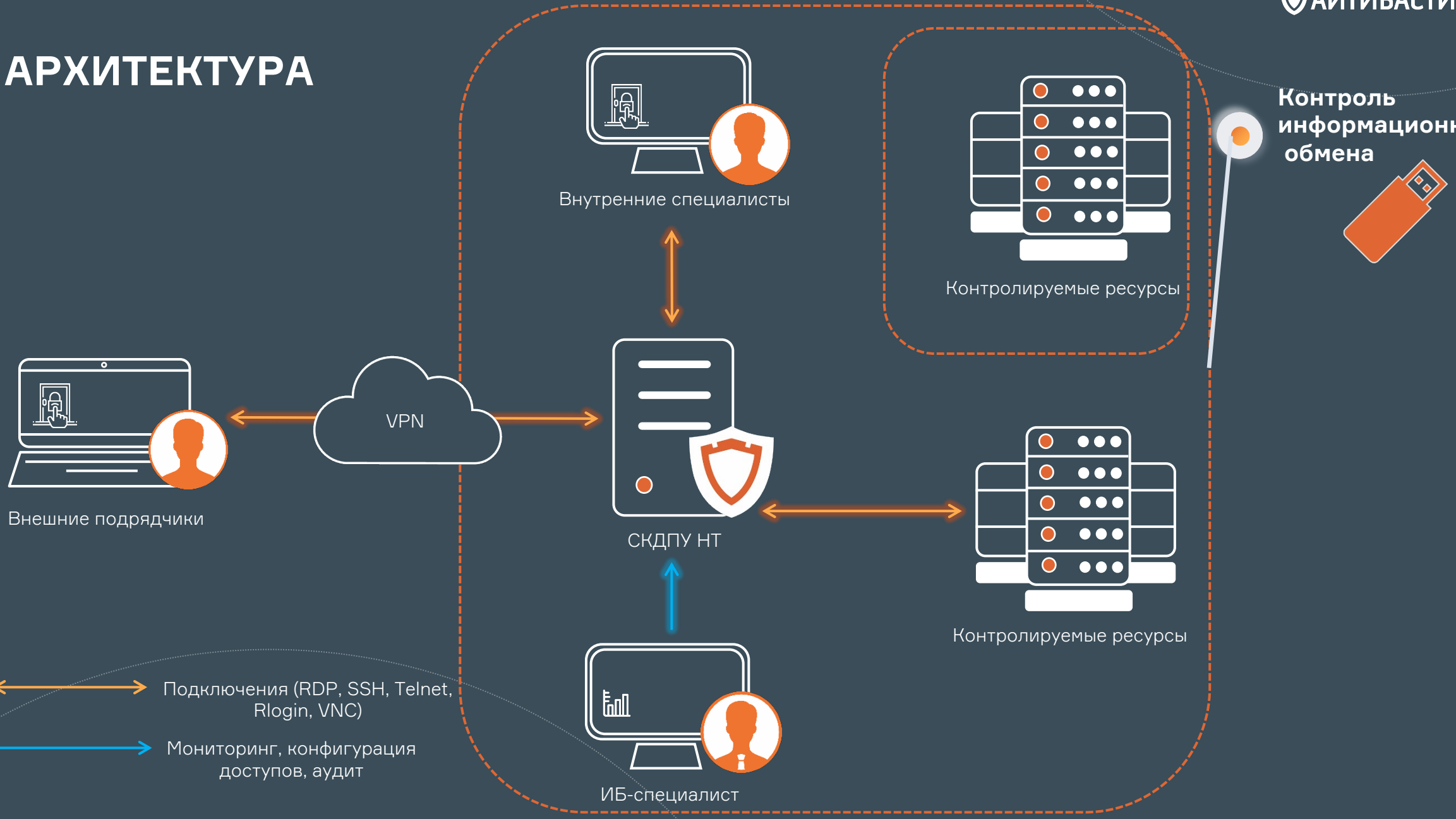
Наличие уязвимостей без реализации компенсирующих мер

* на основе доклада ФСТЭК РФ на ИБ АСУ ТП КВО 2024

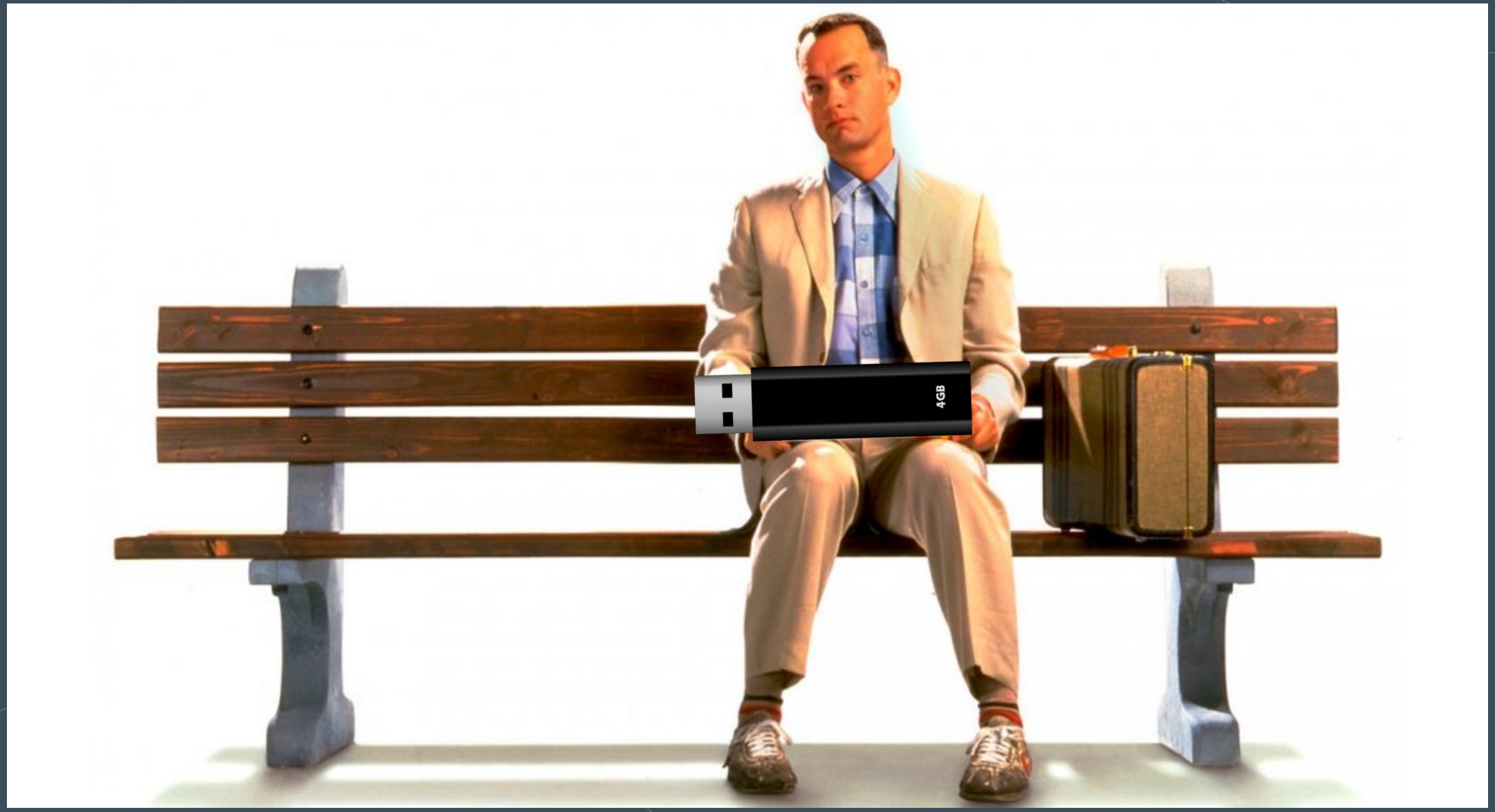
www.it-bastion.com

АЙТИБАСТИОН

АРХИТЕКТУРА



www.it-bastion.com


4GB

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СЕТЯХ

АЙТИБАСТИОН

Внешние, внутренние специалисты

VPN, IPsec/SSL

www.it-bastion.com

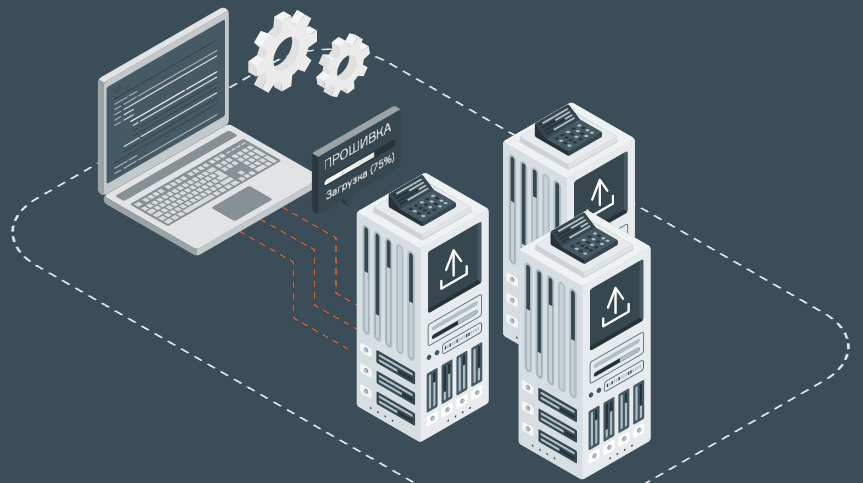
ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СЕТЯХ

АЙТИБАСТИОН

Передача в контур

Обновление
Настройка
Базы
Файлы
Иные данные

Внешние, внутренние специалисты



www.it-bastion.com

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СЕТЯХ

АЙТИБАСТИОН

Передача из контура

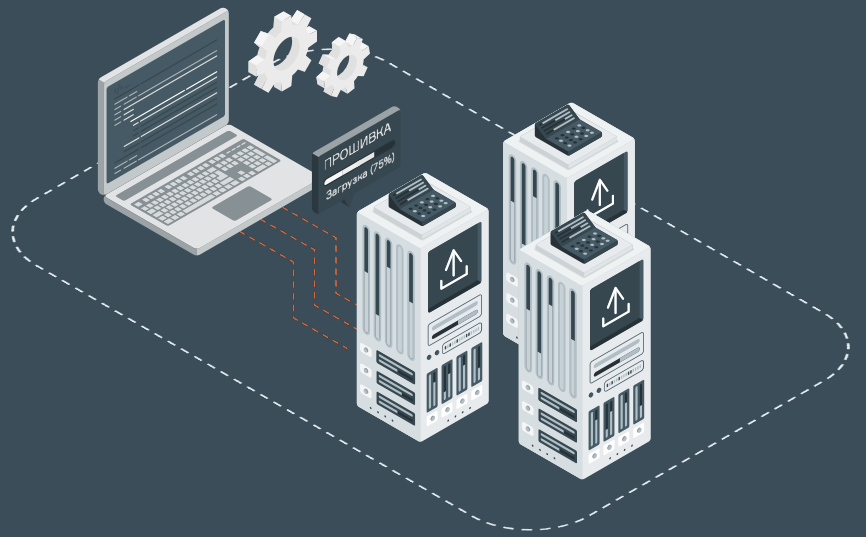
Телеметрия

Логи

Базы

Иные данные

Внешние, внутренние специалисты

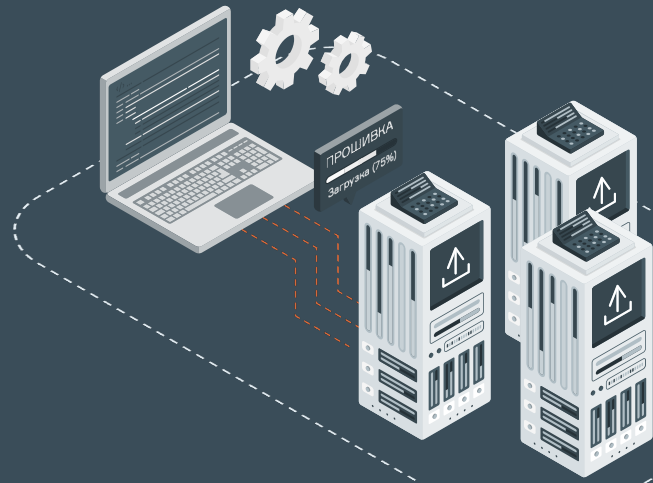


www.it-bastion.com

АЙТИБАСТИОН

Внешние, внутренние специалисты

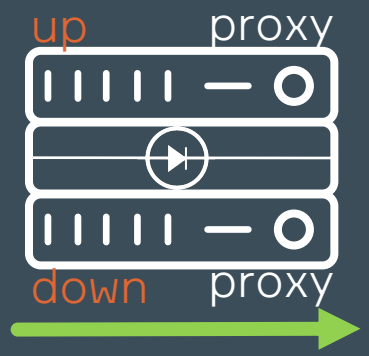
VPN, IPsec/SSL



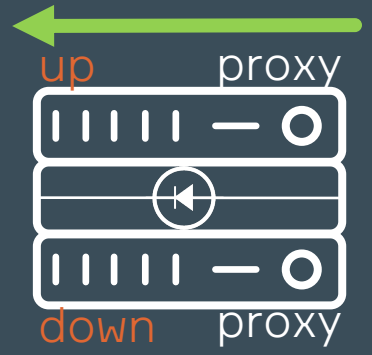
www.it-bastion.com

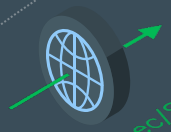
АЙТИБАСТИОН

TCP



Внешние, внутренние специалисты





VPN, IPsec/SSL

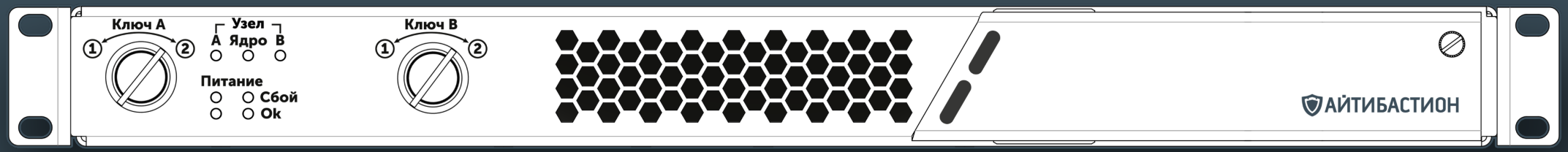
www.it-bastion.com

СИНОНИКС

АЙТИБАСТИОН

Система контроля информационного обмена

Система позволяет организовать безопасный обмен информацией между узлами одной сети или разными сетями, предотвращая распространение киберугроз и вредоносного взаимодействия между ними.



www.it-bastion.com

ПЕРЕДАЧА ДАННЫХ

Передача данных между изначально ИЗОЛИРОВАННЫМИ системами со встроенной защитой транспортного уровня

- TCP, UDP, в т.ч. Однонаправленная
- Независимые политики для двух контуров
- Физическая блокировка передачи данных
- Скорость до 1 Гб/с

ПЕРЕДАЧА ФАЙЛОВ

Передача файлов между изначально ИЗОЛИРОВАННЫМИ системами проверкой этих файлов на соответствие политикам передачи

- SFTP
- Проверка корректности размера и маски файлов и других параметров
- Внешняя валидация по ICAP (DLP, Sandbox, AV и др.)
- Автоматизация процесса доставки файлов

КОМБИНИРОВАННЫЙ РЕЖИМ

СИНОНИКС

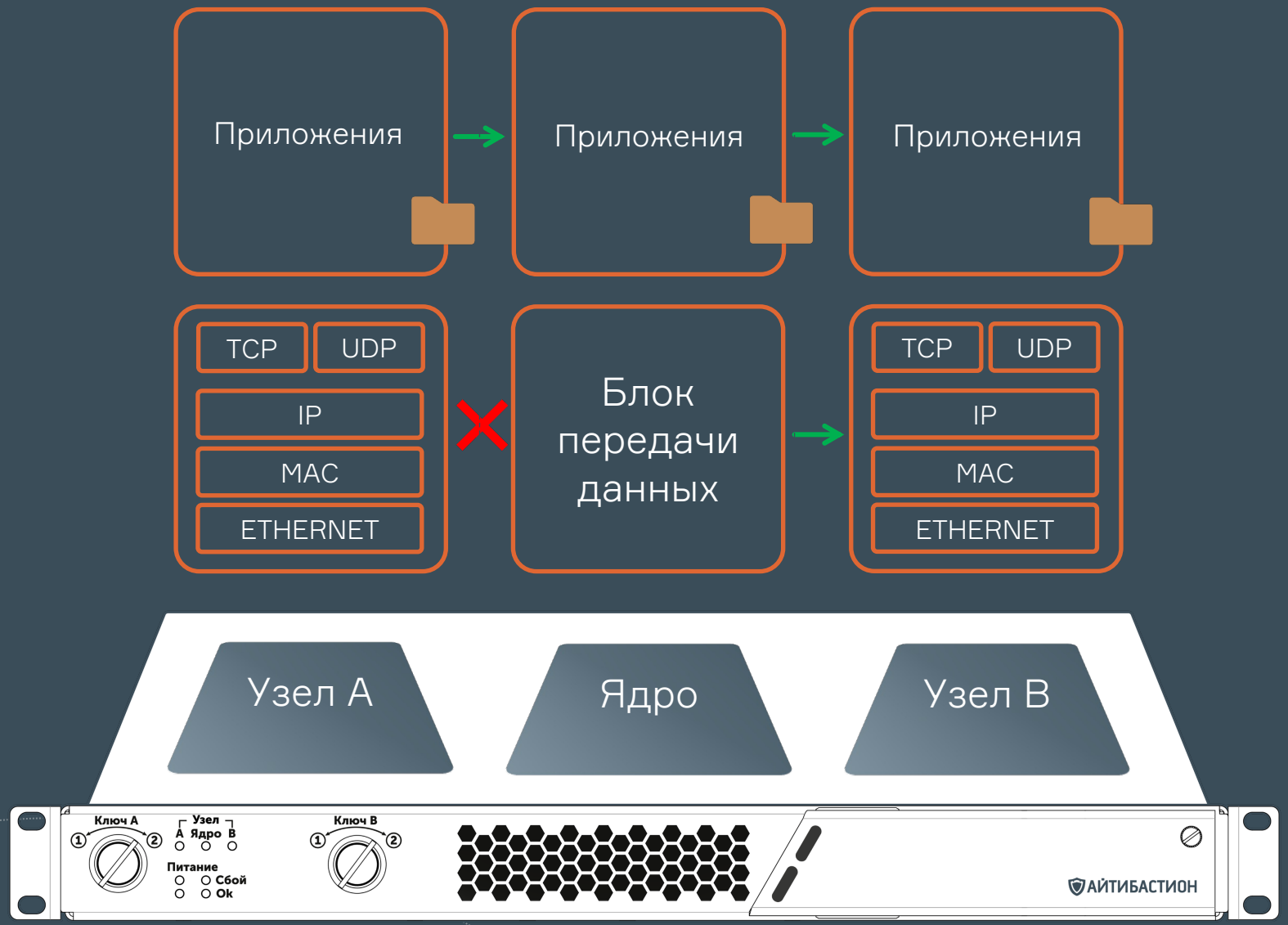
АЙТИБАСТИОН

- Системы остаются невидимыми друг для друга.
- Ограничивает количество взаимодействующих систем.
- Проверка сертификата.
- Согласование правил между сетями.
- Дополнительная физическая блокировка.
- Работа на 1 - 4 уровнях семиуровневой модели OSI.

www.it-bastion.com

СИНОНИКС
АРХИТЕКТУРА

АЙТИБАСТИОН

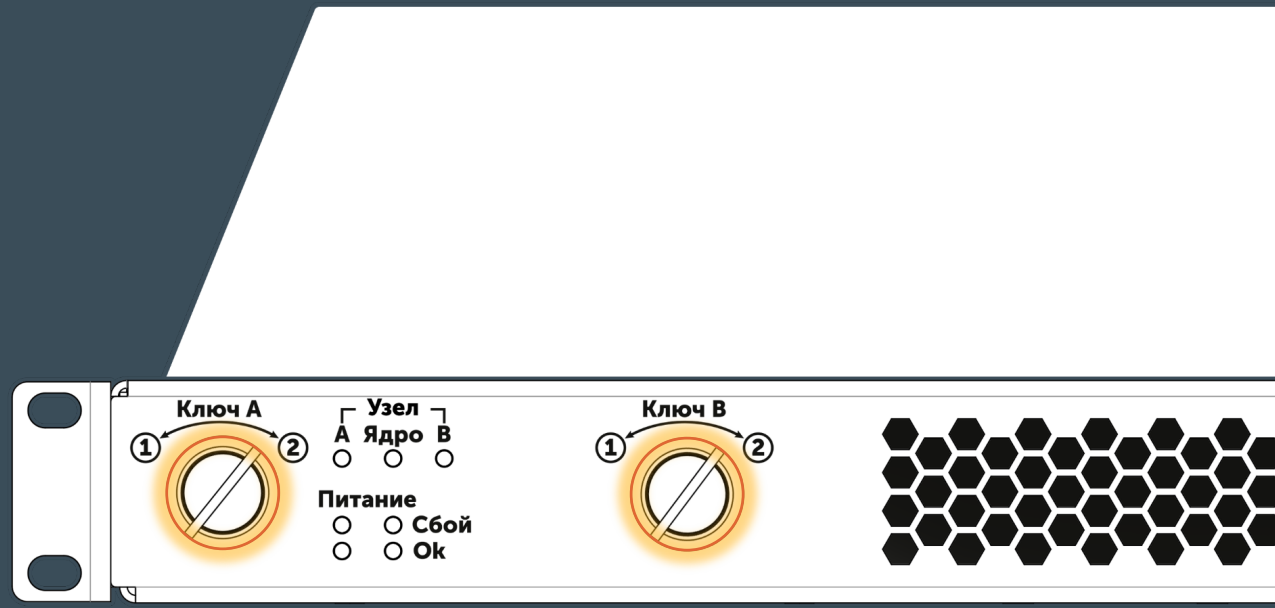


СИНОНИКС
АРХИТЕКТУРА

АЙТИБАСТИОН

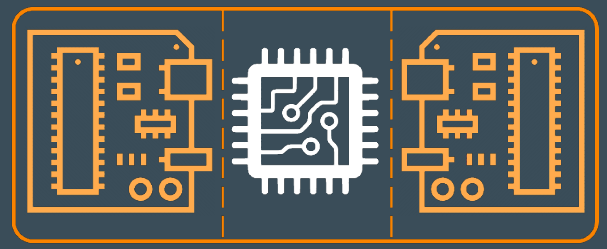
Дополнительный физический контроль

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



АЙТИБАСТИОН

Внешние, внутренние специалисты

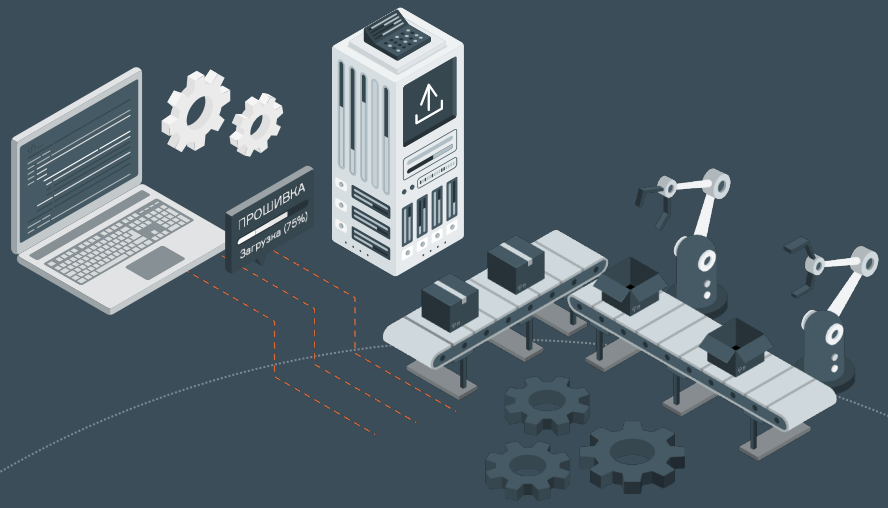


www.it-bastion.com

СИНОНИКС

АЙТИБАСТИОН

- Передача актуальных обновлений
- Передача фалов конфигураций
- Подключение по протоколам удаленного доступа
- Проверка файлов в sandbox

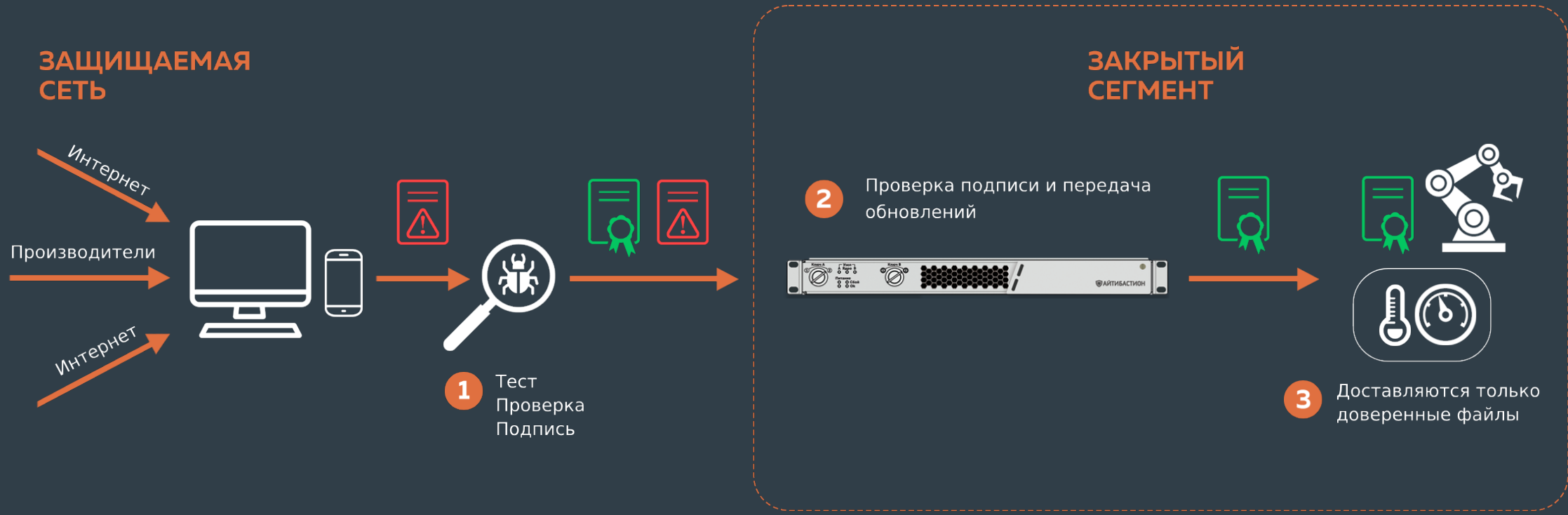


- Получение телеметрии
- Отправка событий безопасности в SOC
- Сбор данных бизнес-процессов

www.it-bastion.com

ПРАКТИЧЕСКИЙ СЦЕНАРИЙ

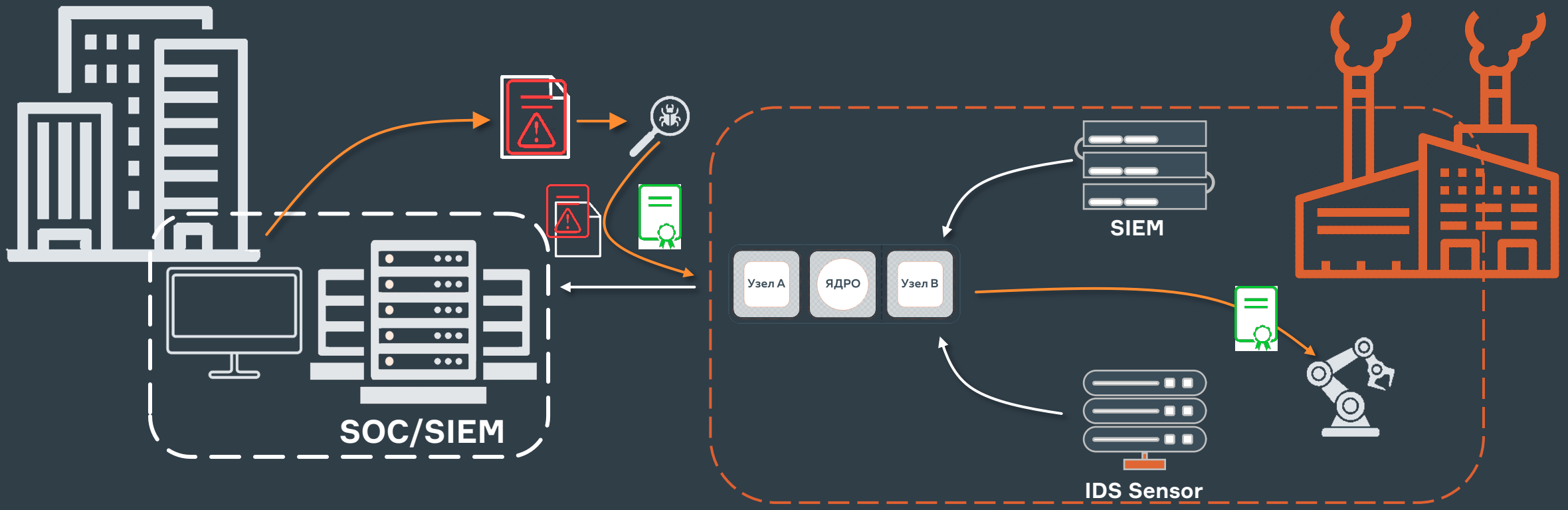
АЙТИБАСТИОН



www.it-bastion.com

ПРАКТИЧЕСКИЙ СЦЕНАРИЙ

АЙТИБАСТИОН



Передача событий в SOC или корп. SIEM данных от IDS Sensor и SIEM Collector

Передача обновлений и прошивок в закрытый сегмент с фиксацией фактов передачи в SOC или корп. SIEM

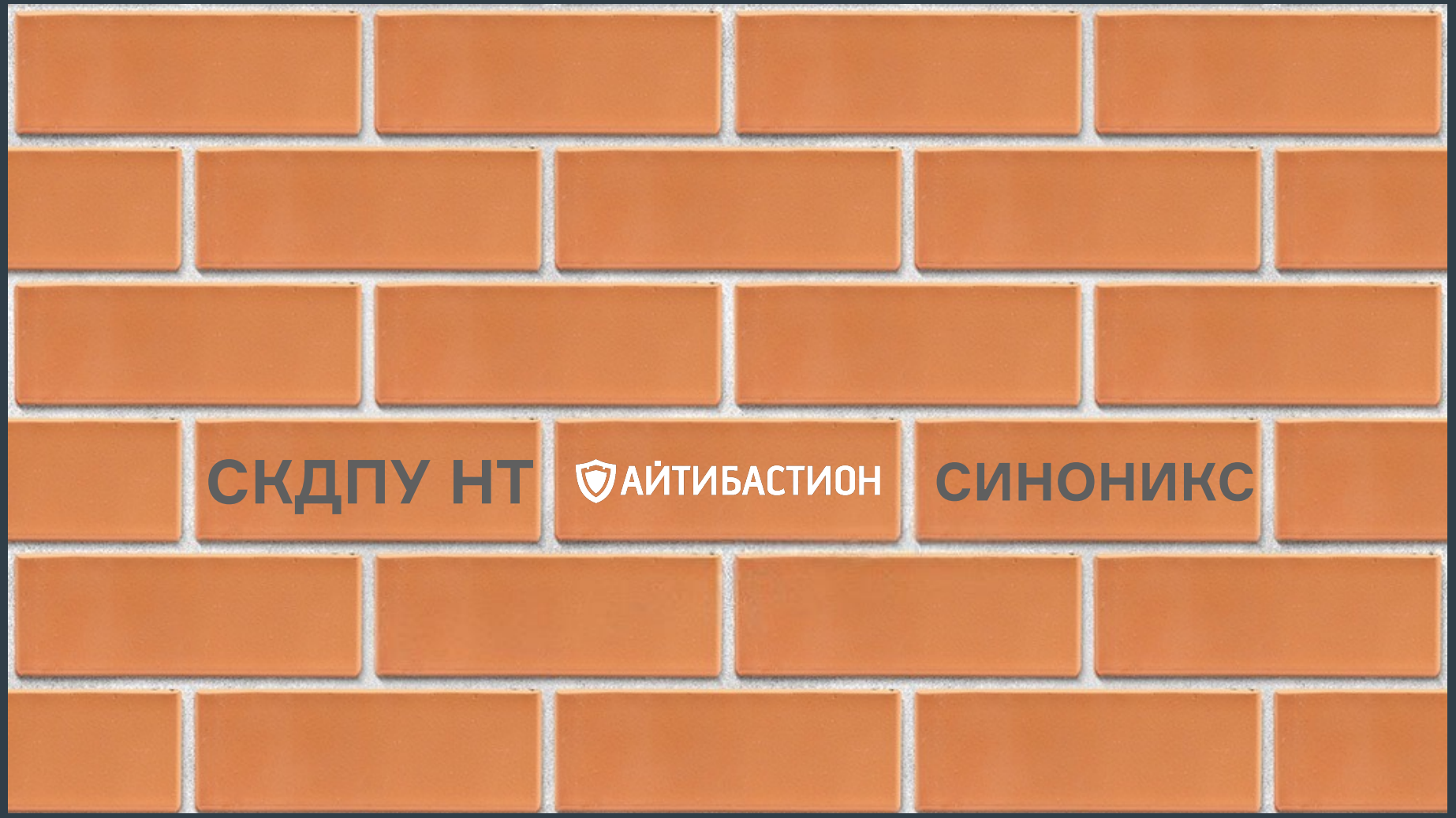
ПРАКТИЧЕСКИЙ СЦЕНАРИЙ

АЙТИБАСТИОН

```
SynOS-B> transport show slots
transport set slot 1 protocol tcp mode exchange ip 192.168.0.5 port 443
transport set slot 2 protocol tcp mode exchange ip 192.168.0.5 port 3389
transport set slot 3 protocol tcp mode exchange ip 192.168.0.5 port 22
transport diode set slot 4 protocol udp mode collect ip 192.168.0.100 port 514
```


```
SynOS-A> transport show slots
transport set slot 1 protocol tcp mode collect ip 10.1.0.34 port 443
transport set slot 2 protocol tcp mode collect ip 10.1.0.34 port 75
transport set slot 3 protocol tcp mode collect ip 10.1.0.34 port 22
transport diode set slot 4 protocol udp mode exchange ip 10.0.128.75 port 515
```

ПОСТРОЕНИЕ ИБ ИНФРАСТРУКТУРЫ
КОМПЛЕКСНЫЙ ПОДХОД



АЙТИБАСТИОН

Благодарю за внимание!

ШИРИКАЛОВ АЛЕКСЕЙ

a.shirikalov@it-bastion.com

+7 499 322 3667

it-bastion.com