АЙТИБАСТИОН

ИНСТРУМЕНТЫ ОБНАРУЖЕНИЯ КОМПРОМЕТАЦИИ И АНОМАЛЬНОГО ПОВЕДЕНИЯ СОТРУДНИКОВ СРЕДСТВАМИ PAM-СИСТЕМ

www.it-bastion.com

«ЭТО БАЗА»
ТРЕМЯ «КРУЖОЧКАМИ»

АЙТИБАСТИОН

СТАРАЯ «БАЗА»,
КОТОРОЙ УЖЕ МАЛО

АЙТИБАСТИОН

«ФИКСИРУЕМ, КТО И КУДА ЗАШЕЛ»

«ПИШЕМ ВСЯКОЕ»

«СТАРАЕМСЯ МЕНЯТЬ ПАРОЛИ»

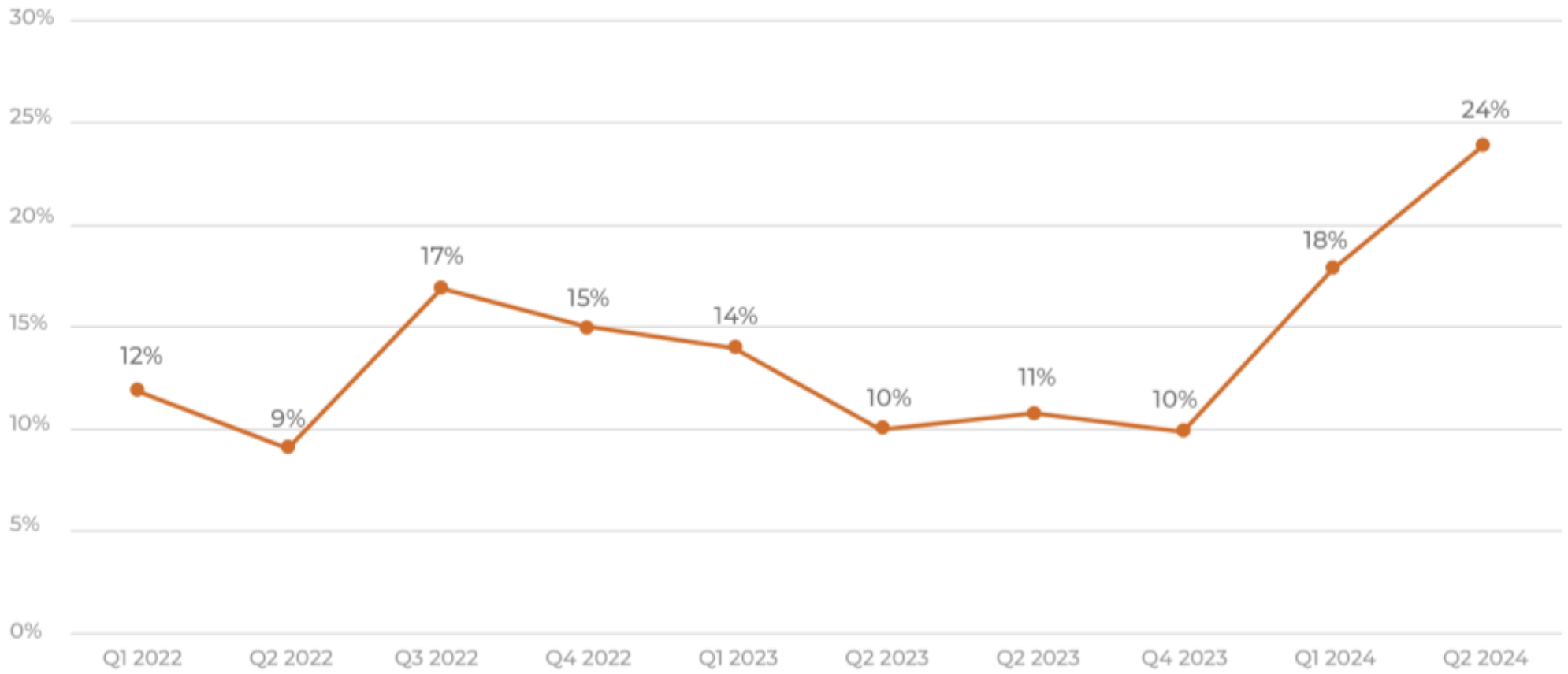
www.it-bastion.com

Достаточно ли этого

Смотря для чего

РОСТ ЧИСЛА УТЕЧЕК ДАННЫХ
ПОЧЕМУ ЭТО ПРОИСХОДИТ?

АЙТИБАСТИОН



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

РЕАЛЬНЫЕ ЗАДАЧИ И ВОЗМОЖНОСТИ
РАМ-ПЛАТФОРМ В 2024 ГОДУ

РЕАЛИИ СОВРЕМЕННЫХ РАМ-СИСТЕМ

АЙТИБАСТИОН

Следование концепции Zero trust

Следование концепции Just-in-time

Создание и ведение профилирования пользователей

Анализ всех действий в разрезе «пользователь — цель — действие», машинное обучение и математические модели

Предобработка, анализ и детектирование аномального поведения пользователей

На основе профилирования и событий

Возможности реагирования на инциденты в рамках системы

Обработка информации и её выдача в виде понятных отчётов

От оперативных до сводных, в том числе для руководителей

Поддержка REST API

Для загрузки и выгрузки данных, для управления

Возможности интеграции с другими решениями

www.it-bastion.com

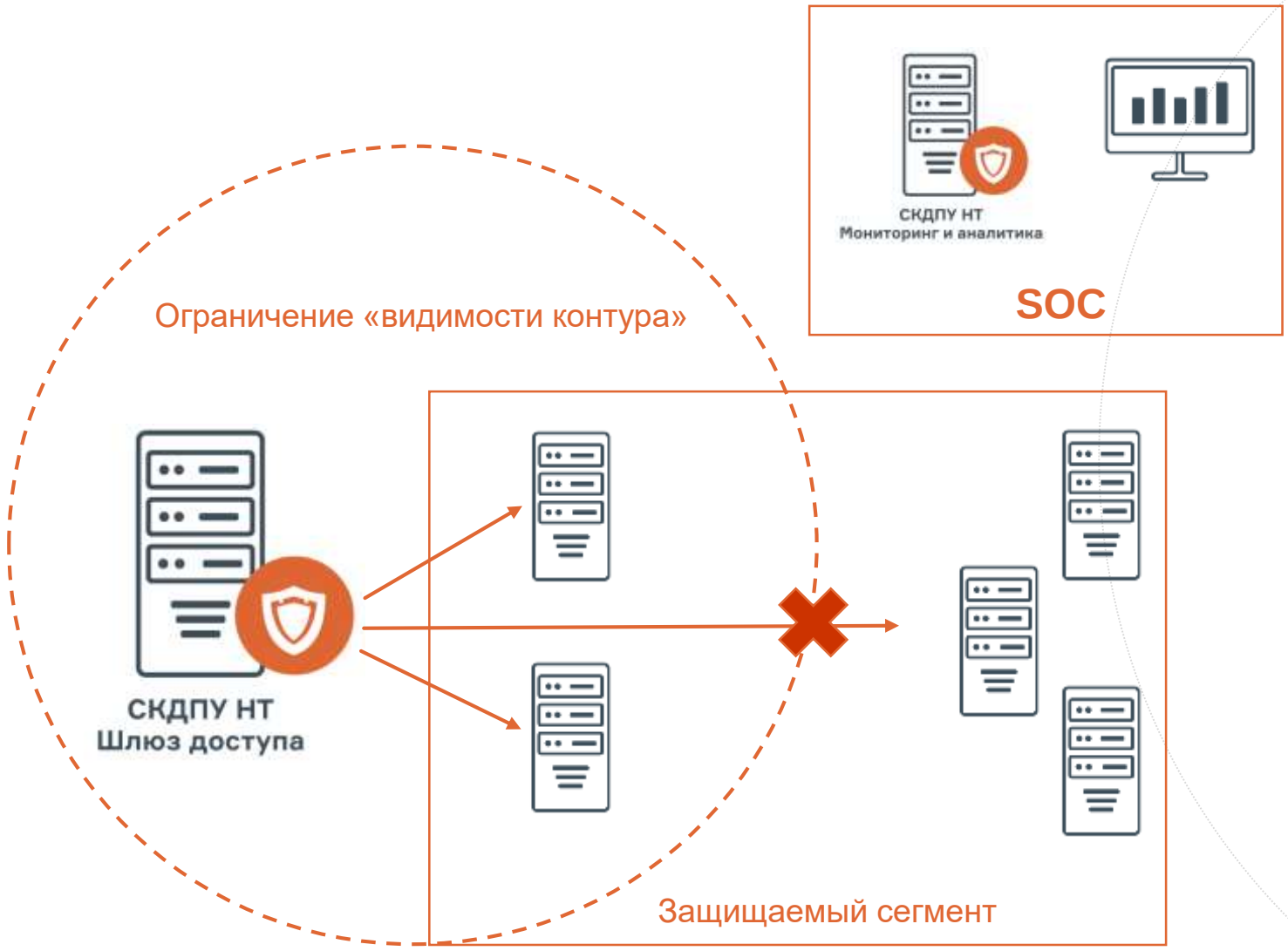
PAM NG*

* шутка

ПРОСТО СОВРЕМЕННАЯ
РАМ-ПЛАТФОРМА

- Детализированная информация с конечных машин
- Контроль действий на конечных машинах
- Контроль перемещения внутри сети
- Аналитика и реагирование собственными силами
- Разделение систем по принципу

«не жалко в поле» и «критичное внутри»



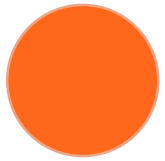
СЛОВАМИ БЕЗ КАРТИНОК
ОЧЕНЬ МНОГО СЛОВ

АЙТИБАСТИОН

- **Идентификация и аутентификация** пользователей с расширенным набором прав
- **Мониторинг** деятельности административных аккаунтов
- **Сбор статистики,** ведение журнала
- **Анализ аномальной активности,** выявление действий, которые могут нести угрозу ИБ
- Организация защищённого **хранилища учётных записей**
- Предоставление **единой точки входа** с разными механиками
- Адаптивное **понижение разрешений** до уровня, достаточного для выполнения задачи
- **Блокировка использования неизменяемых логинов** и паролей в сторонних приложениях
- Уход от бесконтрольного использования разделяемых учётных записей (root, admin)

НАША СТАТИСТИКА
СКОРОСТИ РАССЛЕДОВАНИЯ

АЙТИБАСТИОН



Стандартными методами

С аналитикой СКДПУ НТ

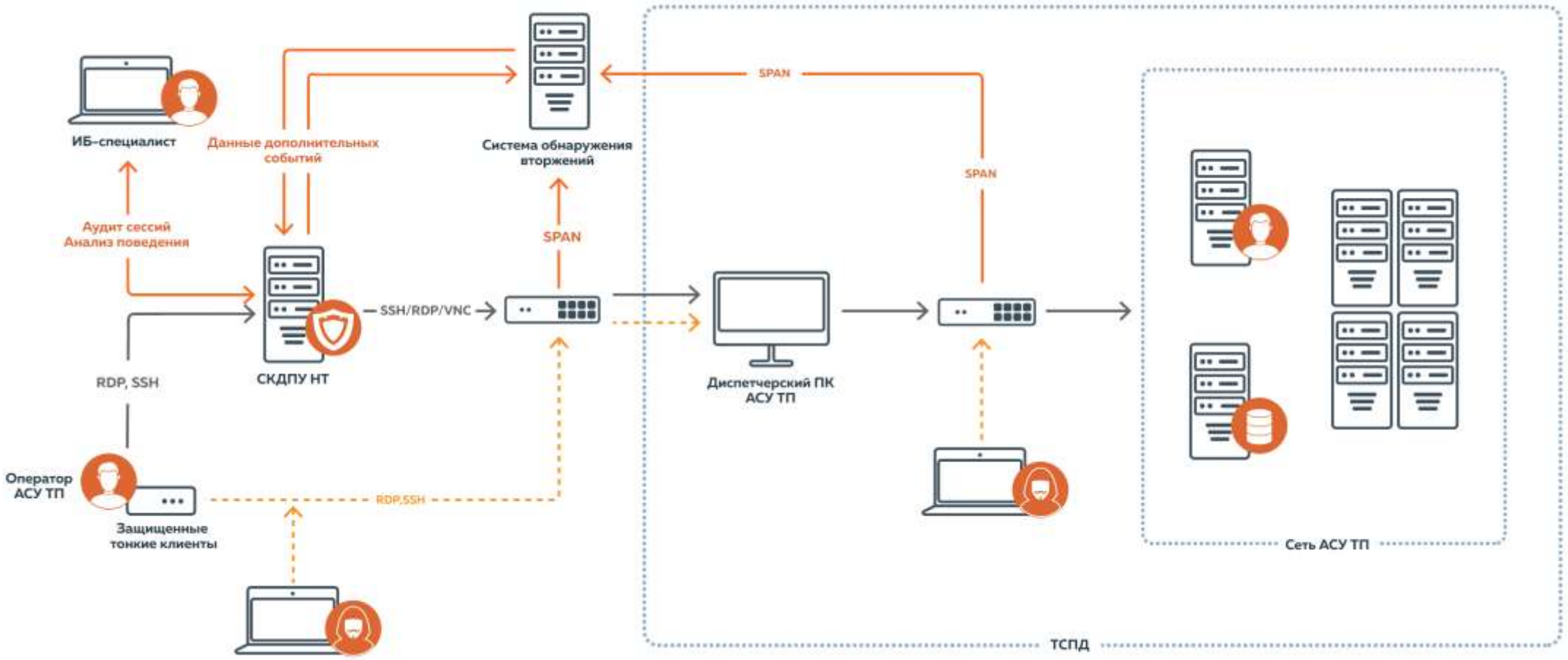
ВОЗМОЖНОСТИ
МЕЖВЕНДОРНЫХ ВЗАИМОДЕЙСТВИЙ

АЙТИБАСТИОН

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

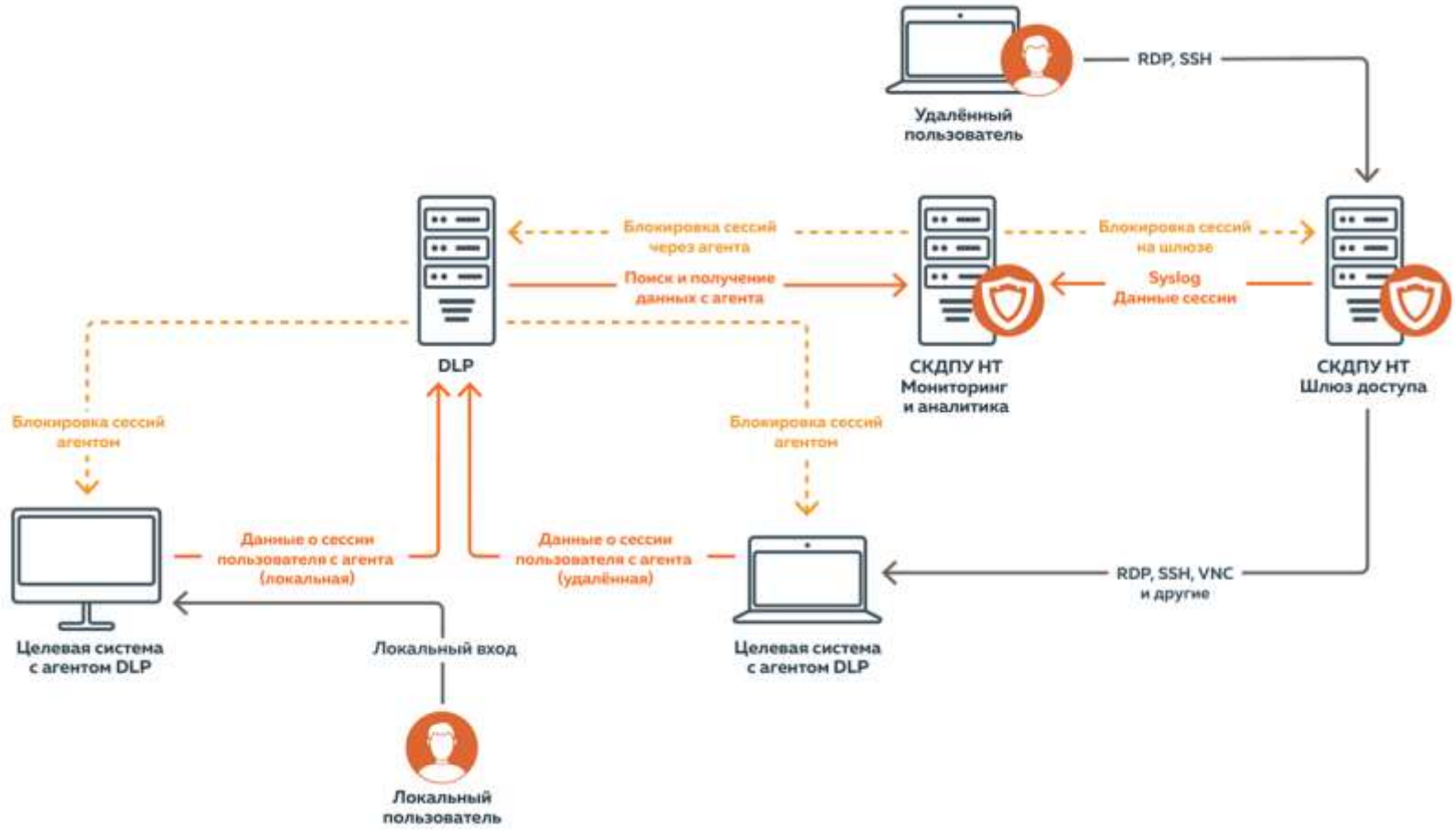
АЙТИБАСТИОН

Идентификация **нелегитимных сессий** администрирования в сети АСУ ТП. Определение подключений **в обход** комплекса СКДПУ НТ и **реагирование** на это событие созданием инцидента ИБ



DLP-система*

Сценарии **взаимного обогащения событиями** и использование обеих систем для **увеличения зоны покрытия контроля доступа** пользователей в рамках инфраструктуры: отсутствие DLP-агента на целевой системе (обогащение DLP событиями из PAM) или подключения в обход PAM (обогащение PAM событиями из DLP)

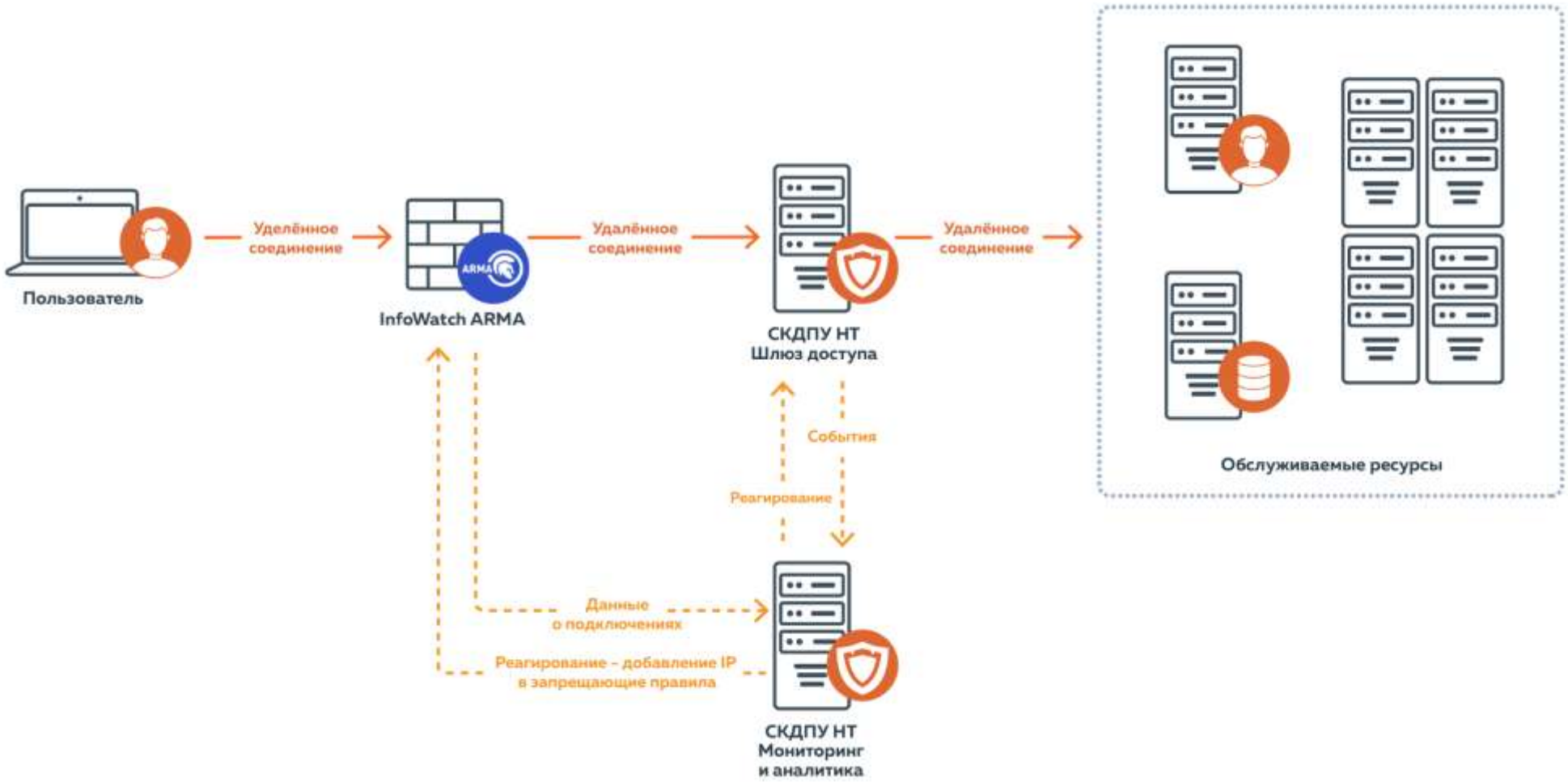


*в работе

ИНТЕГРАЦИЯ С МЭ
РЕАГИРОВАНИЕ НА АНОМАЛЬНОЕ ПОВЕДЕНИЕ

АЙТИБАСТИОН

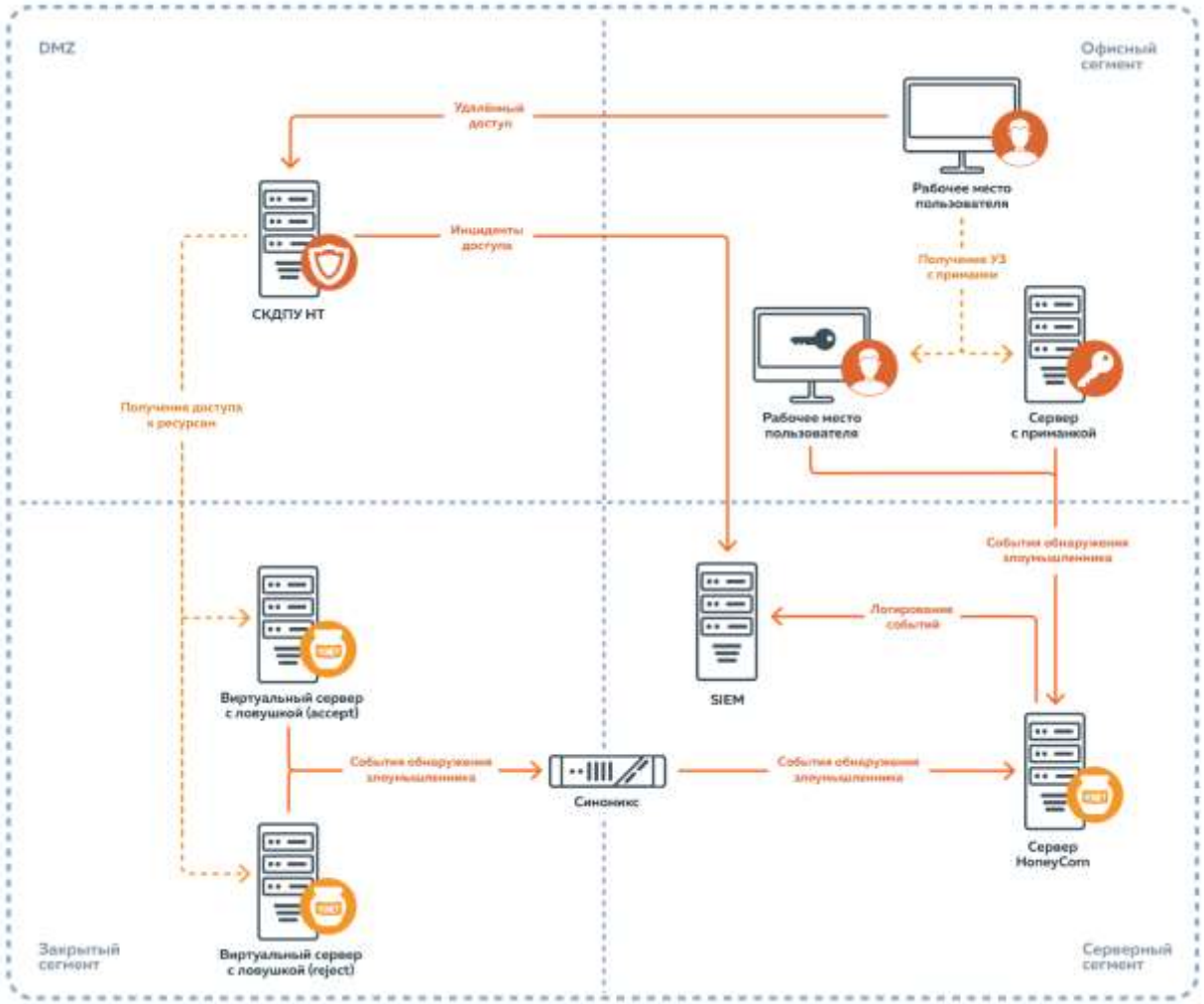
Реагирование на возникающие в ходе работы пользователя инциденты и возможность его **блокировки**



КОНТРОЛИРУЕМЫЙ ВЗЛОМ (HoneyCorn)

АЙТИБАСТИОН

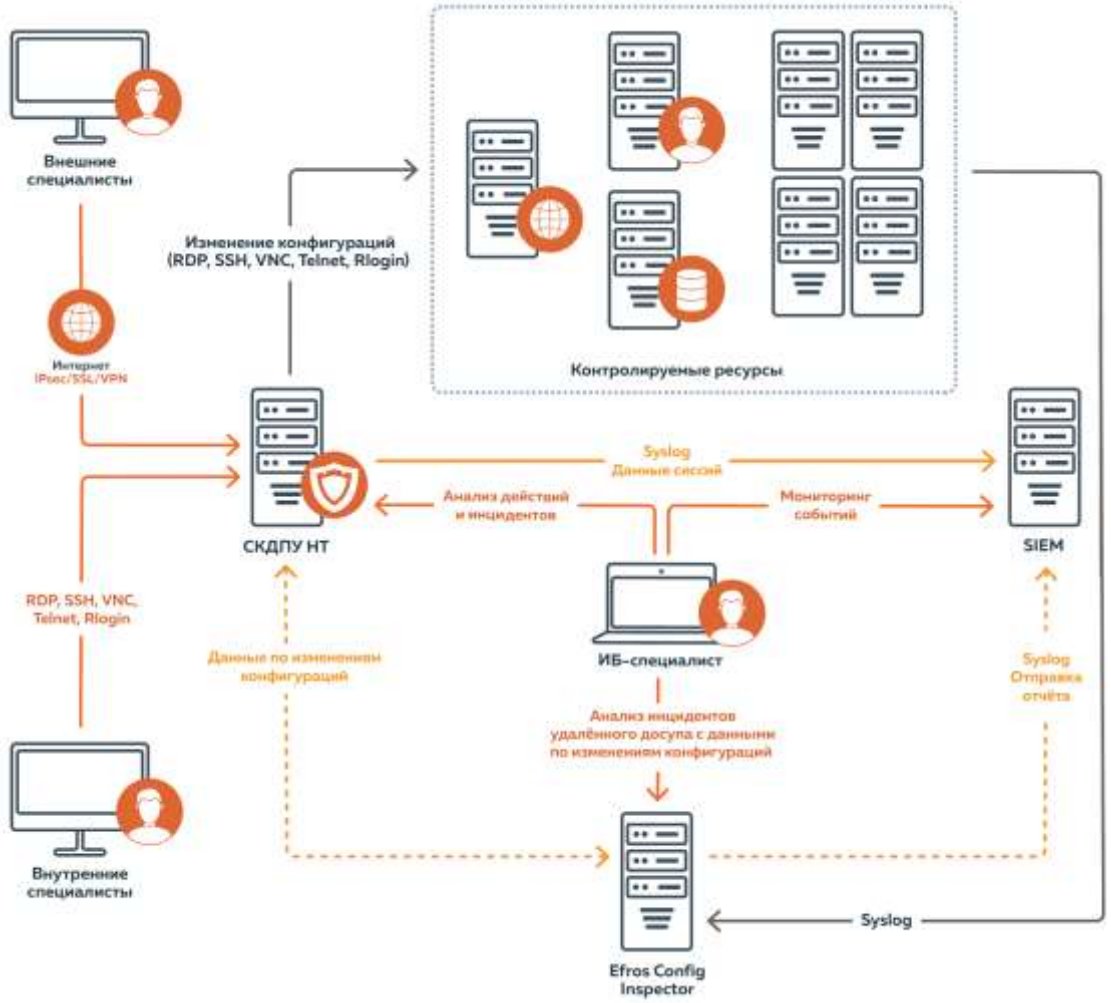
Интеграция СКДПУ НТ в систему ловушек HoneyCorn. Расширение системы идентификации **компрометации сети, анализ действий нарушителей и отслеживание вектора атаки**



СИСТЕМА КОНТРОЛЯ КОНФИГУРАЦИЙ

АЙТИБАСТИОН

Интеграционный **обмен информацией** и точное определение **источника изменений конфигурации** целевого оборудования в рамках сессий удаленного доступа



Спасибо за внимание!

АЙТИБАСТИОН

Константин Родин
Руководитель отдела развития продуктов

k.rodin@it-bastion.com

+7 916 560 50 66

it-bastion.com