АйТи БАСТИОН

ПАК
контроль подрядчиков
данные
контроль
РАМ
отказоустойчивость
Цифровой профиль пользователя
СКДПУ НТ
односторонняя передача
КИИ
контроль удаленной работы
SSO
удаленный доступ
уровень доверия
API
аналитика
детектор аномалий
отчеты
Синоним
SIEM
ICAP
безопасная передача данных
контроль данных
DLP
масштабирование
AstraLinux
поведенческий анализ
АСУ ТП
контроль администраторов
однонаправленный шлюз

ФСТЭК России РД НДВ-4

Реестр отечественного ПО

МО РФ РД НДВ-2

info@it-bastion.com www.it-bastion.com +7 (499) 322-36-67

DLP и интеграция бизнес-сценариев.

Сложные сценарии и перспективы развития контроля

Компания «АйТи БАСТИОН»

- Разработчик:
  - **СКДПУ НТ** – Система контроля действий поставщиков ИТ-услуг
  - **Синоним** – Безопасный шлюз передачи данных между сетями

- **100+** крупных заказчиков и успешно реализованных проектов

Заказчики

ОАК

НОРНИКЕЛЬ

ВЭБ РФ

ГАЗПРОМ ЭНЕРГОХОЛДИНГ

ОСК ОБЪЕДИНЕННАЯ СУДОСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ

РОСНЕФТЬ

РусГидро

ПРАВИТЕЛЬСТВО МОСКВЫ

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

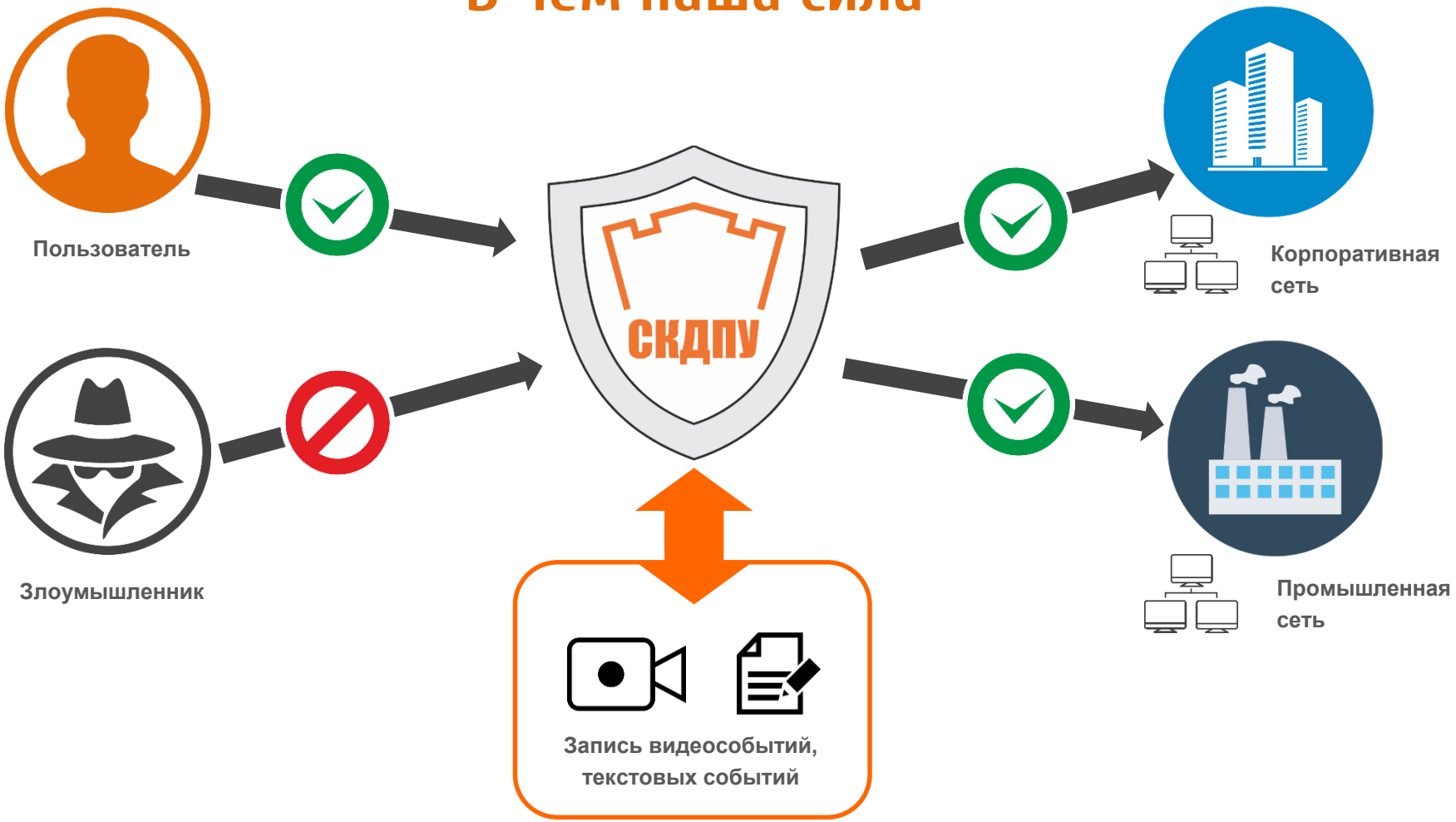
РОСЭНЕРГОАТОМ РОСАТОМ

ВОЕНТЕЛЕКОМ

Ростех

Северсталь

В чём наша сила



Решаемые задачи

Контроль действий
Предоставление доступа в соответствии с политиками доступа

Удаленный доступ
Обеспечение безопасного подключения внешних сотрудников и аутсорс-организаций

Безопасное внедрение
Отсутствие агентов, отсутствие необходимости изменения архитектуры, интеграция с различными решениями

Соответствие требованиям
Соответствие требованиям регуляторов

DLP

Несколько важных сценариев

–

«Контроль контролёра»

–

Когда страшно ставить агент DLP

–

DLP в АСУ ТП сетях

Контроль контролёра

Риски сценария:

- Доступ к критической информации в «одних руках» и одной «корзине»
- Знание архитектуры решения и способы её обхода

Снижение рисков:

- Обслуживание DLP под контролем средствами PAM
- Контроль подключений
- Запись действий
- Доказательная база изменений политик

Когда страшно ставить агент DLP

Опасения заказчика:

- Эффективно, но «дорого» и «сложно»
- Выше вероятность проблем в эксплуатации
- Необходимость работоспособности выше, чем потенциальные риски
- Требуется контроль файлов, так как они могут содержать защищаемую информацию

Реализованная схема:

- РАМ как система доступа к части инфраструктуры
- Доступ как для внешних, так и внутренних сотрудников
- Файлы, передаваемые через РАМ, до передачи отправляются на проверку в DLP для принятия решения
- Штатный контроль со стороны DLP сохранен

DLP в АСУ ТП сетях

Базовая концепция:

- Агентам – «нет»
- Пассивный сбор информации – «да»
- Доступ нужен, профилирование нужно, работа с утечками нужна

Расширение концепции:

- Контроль подключений средствами РАМ
- РАМ усилен контролем контента
- Расширение профиля пользователя за счет информации о сессиях через РАМ
- Проверка файлов, проходящих через РАМ, средствами DLP и AV

Интеграции и развитие

В чем задача?

- В людях
- В количестве людей
- В качестве работы с информацией по людям
- И в количестве людей, которые работают с этой информацией

Системы ИБ

+

Интеграции

Используя сильные стороны друг друга

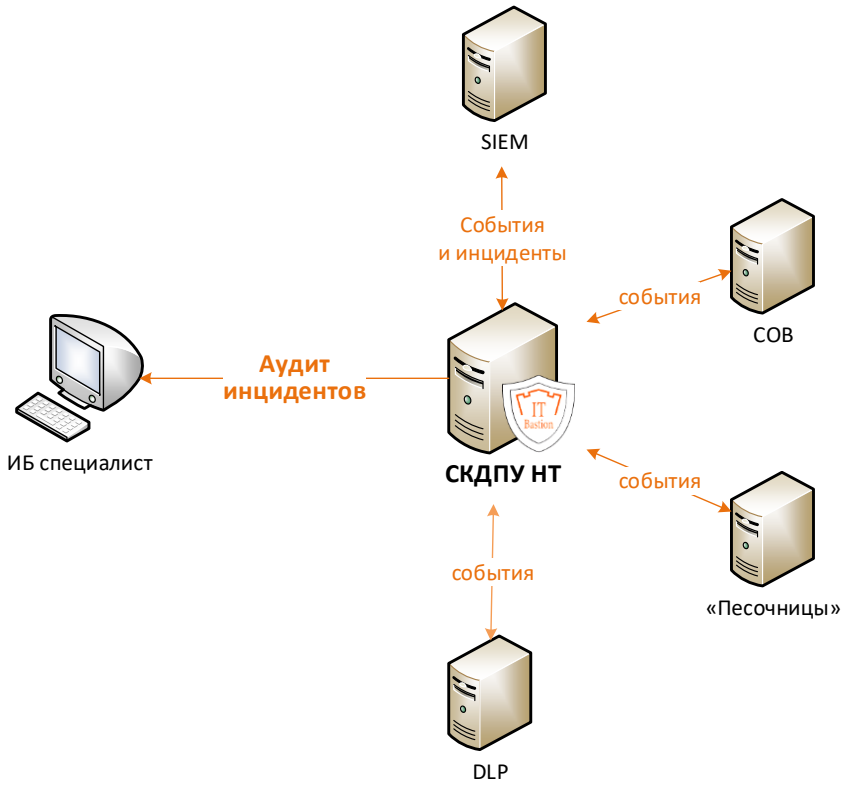
В чем решение

- Защита одного решения другим
- Наполнение профильной информацией, характерной для конкретной системы
- Снижение рисков, повышение эффективности
- Снижение нагрузки на контролёров за счет автоматизации

Интеграция сценариев взаимодействия в контуре

- DLP
- PAM
- SIEM
- СОВ
- AV
- Sandbox

Интеграции в контуре ИБ и ИТ



kaspersky INFOWATCH® PT POSITIVE TECHNOLOGIES RUSIEM

Вместе интересней

Мы заинтересованы в реальных задачах бизнеса

и готовы к сотрудничеству!

Спасибо за внимание!

Руководитель технического центра
ООО "АйТи Бастион"
Константин Родин
k.rodin@it-bastion.com

Какие задачи решает СКДПУ НТ

- **Контроль доступа** к информационной инфраструктуре в реальном времени;
- **Создание доказательной базы** для ретроспективного аудита и анализа сбоев или инцидентов ИБ;
- Контроль соблюдения корпоративной **политики ИБ**;
- **Контроль действий подрядчиков**, потенциально влекущих за собой утечку информации и различные атаки;
- **Контроль за исполнением условий SLA** подрядчиками;
- Соблюдение **требований регуляторов**;
- **Ведение отчётности:** быстрый доступ к аналитике, отчётам и потенциальным инцидентам в рамках инфраструктуры*.

* -- возможность расширения функциональности системы

Спасибо за внимание, ещё раз!

Руководитель технического центра
ООО "АйТи Бастион"
Константин Родин
k.rodin@it-bastion.com