# Зачем деревообрабатывающей отрасли нужен SOC: история сотрудничества и развития ИБ

Никита Курмышкин · Руководитель направления защиты ИТ-инфраструктуры Segezha Group

# Несколько слов о нас

**Финансовые показатели 2022 г.**

**106,8 млрд ₽**
Выручка

**24,7 млрд ₽**
OIBDA

**Segezha Group сегодня – это**

**23**
офиса в РФ

**>20 тыс.**
сотрудников

Segezha Group – уникальный российский лесопромышленный холдинг с полным циклом собственной лесозаготовки и специализацией на выпуске широкой линейки высокотехнологичной продукции. Мы представлены на рынках 80+ стран

## ПРОИЗВОДСТВЕННАЯ БАЗА

**23.3 млн м³**
Расчетная лесосека 2022


**Производственные активы в 10 регионах РФ**

**Проблематика:**

- геораспределенность >1000 км, проблемы с логистикой
- низкая защищенность приобретаемых активов

SEGEZHA GROUP

# Почему мы выбрали внешний SOC

## В КОМПАНИИ:

- Была зарубежная, некорректно настроенная SIEM-система
- 10 000+ ложноположительных срабатываний в день
- Нехватка специалистов ИБ / их дефицит на рынке
- Существовала необходимость управления инцидентами

## ЧТО НАМ БЫЛО НУЖНО?

01 Надежный SOC с полной поддержкой

02 Высокая скорость подключения

03 Гибкие условия тарификации

04 Финансовая выгода: экономия на штате специалистов и мощностях => перенаправление освободившихся ресурсов на развитие ИБ

05 Взаимодействие с НКЦКИ

SEGEZHA GROUP

# Почему МТС RED SOC

- Успешно функционирует в АФК «Система»
- Обладает командой квалифицированных экспертов и вычислительными мощностями
- Быстрое подключение ИТ-системы Segezha group
- Имеет необходимые лицензии и сертификаты для взаимодействия с регулятором
- Обеспечивает мониторинг событий ИБ, реагирование на инциденты и помогает их расследовать

SEGEZHA GROUP

# Как мы подключались к SOC

- Провели инвентаризацию активов и сетевой инфраструктуры
- Определили критичные источники событий
- Подготовили инфраструктуру →

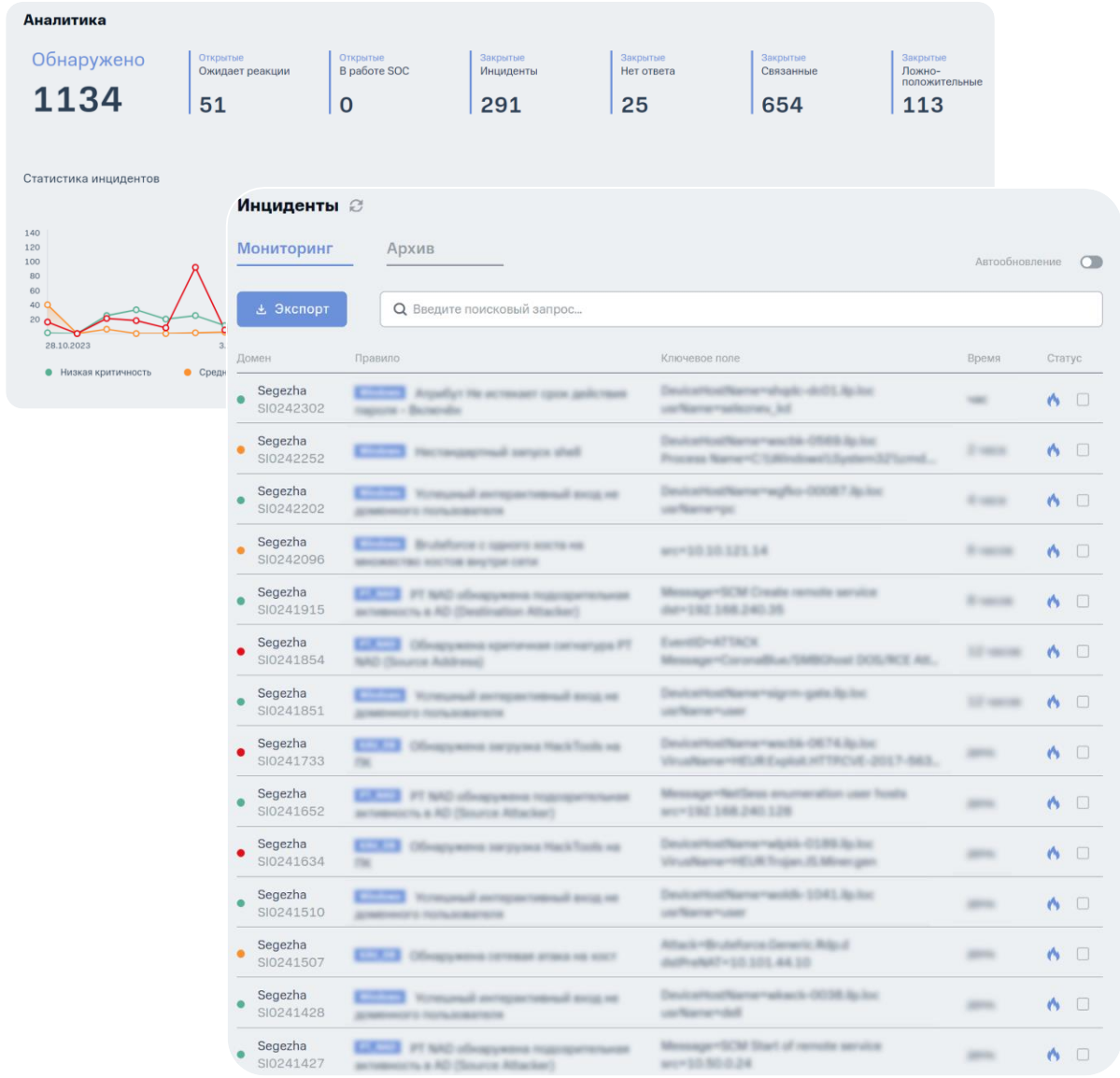
1. настроили защищенный канал между SOC и Segezha group
2. установили серверы сбора и нормализации событий
3. развернули web-серверы для сбора журналов безопасности
4. настроили источники событий

**ИНСТРУКЦИИ И РАСЧЕТЫ БЫЛИ ПРЕДОСТАВЛЕНЫ ПРОВАЙДЕРОМ**

SEGEZHA GROUP

# Что мы получили сразу?

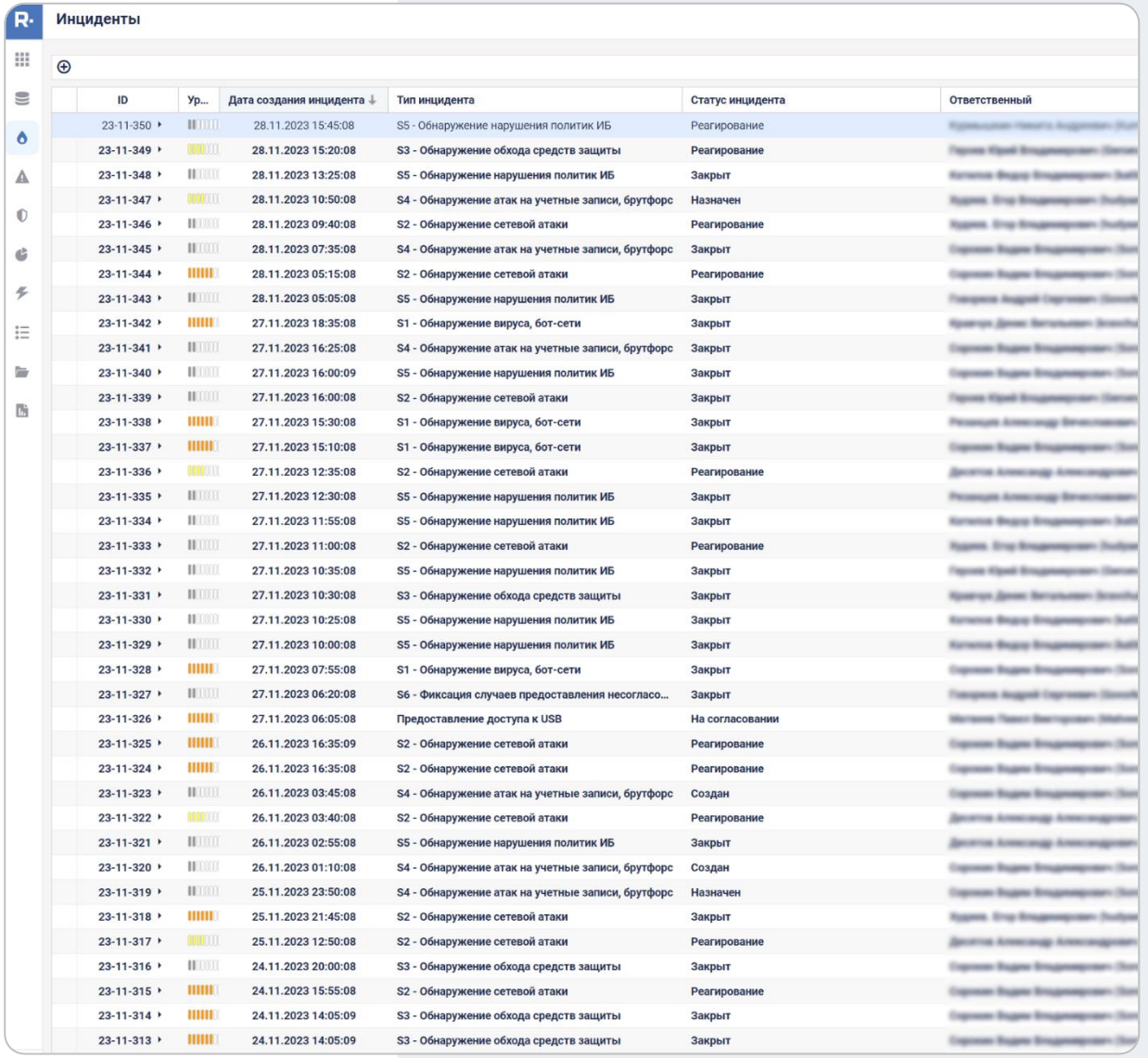
- Формирование перечня инцидентов на основании набора правил корреляции и их дальнейшее профилирование
- Контроль процессов ИБ
- Выявление существующей вредоносной активности
- Сканирование сервисов внешнего периметра
- Ретроспективный анализ
- Мониторинг событий ИБ 24/7
- Помощь со стороны МТС RED в расследовании инцидентов
- Наглядные отчеты
- Раннее уведомление о новых критичных уязвимостях, требующих реагирования
- Подключение к ГосСОПКА



SEGEZHA GROUP

# Как мы развили сервис за первый год

- Настроили кастомные правила, включая интерактивный вход технологической учетной записи
- Интегрировались с IRP R-Vision
- Отфильтровали «мусорные события» с помощью WEC
- Подключили PT NAD
- Включили рекомендации в части проверки жесткого диска

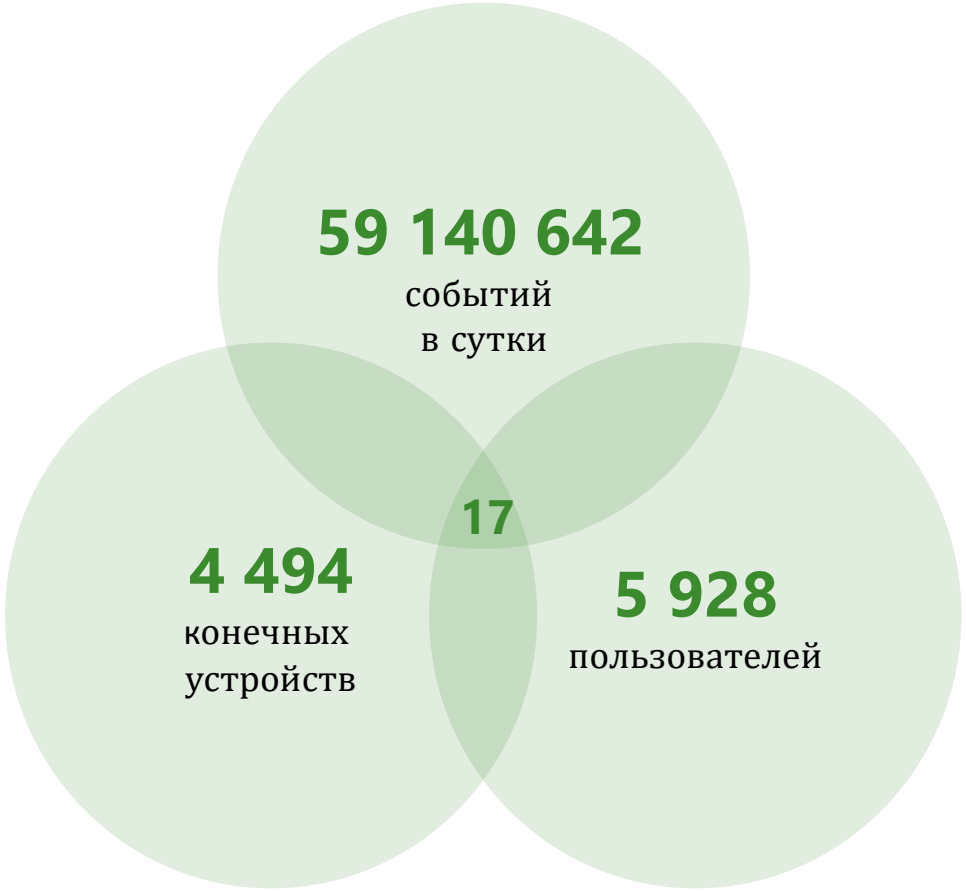


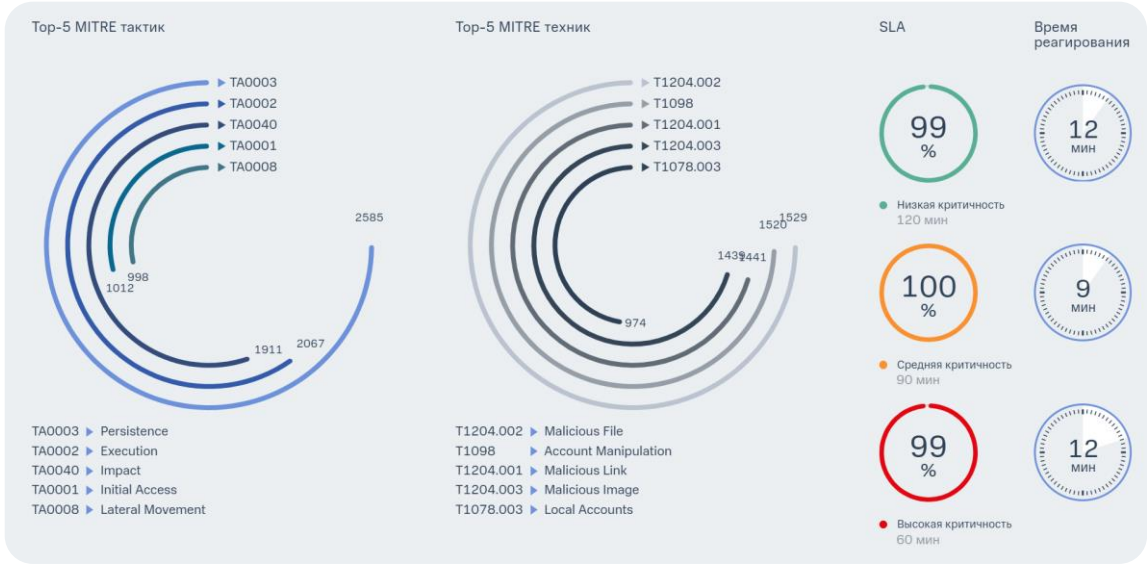

| ID | Ур... | Дата создания инцидента | Тип инцидента | Статус инцидента | Ответственный |
|---|---|---|---|---|---|
| 23-11-350 | | 28.11.2023 15:45:08 | S5 - Обнаружение нарушения политик ИБ | Реагирование | |
| 23-11-349 | | 28.11.2023 15:20:08 | S3 - Обнаружение обхода средств защиты | Реагирование | |
| 23-11-348 | | 28.11.2023 13:25:08 | S5 - Обнаружение нарушения политик ИБ | Закрыт | |
| 23-11-347 | | 28.11.2023 10:50:08 | S4 - Обнаружение атак на учетные записи, брутфорс | Назначен | |
| 23-11-346 | | 28.11.2023 09:40:08 | S2 - Обнаружение сетевой атаки | Реагирование | |
| 23-11-345 | | 28.11.2023 07:35:08 | S4 - Обнаружение атак на учетные записи, брутфорс | Закрыт | |
| 23-11-344 | | 28.11.2023 05:15:08 | S2 - Обнаружение сетевой атаки | Реагирование | |
| 23-11-343 | | 28.11.2023 05:05:08 | S5 - Обнаружение нарушения политик ИБ | Закрыт | |
| 23-11-342 | | 27.11.2023 18:35:08 | S1 - Обнаружение вируса, бот-сети | Закрыт | |
| 23-11-341 | | 27.11.2023 16:25:08 | S4 - Обнаружение атак на учетные записи, брутфорс | Закрыт | |
| 23-11-340 | | 27.11.2023 16:00:09 | S5 - Обнаружение нарушения политик ИБ | Закрыт | |
| 23-11-339 | | 27.11.2023 16:00:08 | S2 - Обнаружение сетевой атаки | Закрыт | |
| 23-11-338 | | 27.11.2023 15:30:08 | S1 - Обнаружение вируса, бот-сети | Закрыт | |
| 23-11-337 | | 27.11.2023 15:10:08 | S1 - Обнаружение вируса, бот-сети | Закрыт | |
| 23-11-336 | | 27.11.2023 12:35:08 | S2 - Обнаружение сетевой атаки | Реагирование | |
| 23-11-335 | | 27.11.2023 12:30:08 | S5 - Обнаружение нарушения политик ИБ | Закрыт | |
| 23-11-334 | | 27.11.2023 11:55:08 | S5 - Обнаружение нарушения политик ИБ | Закрыт | |
| 23-11-333 | | 27.11.2023 11:00:08 | S2 - Обнаружение сетевой атаки | Реагирование | |
| 23-11-332 | | 27.11.2023 10:35:08 | S5 - Обнаружение нарушения политик ИБ | Закрыт | |
| 23-11-331 | | 27.11.2023 10:30:08 | S3 - Обнаружение обхода средств защиты | Закрыт | |
| 23-11-330 | | 27.11.2023 10:25:08 | S5 - Обнаружение нарушения политик ИБ | Закрыт | |
| 23-11-329 | | 27.11.2023 10:00:08 | S5 - Обнаружение нарушения политик ИБ | Закрыт | |
| 23-11-328 | | 27.11.2023 07:55:08 | S1 - Обнаружение вируса, бот-сети | Закрыт | |
| 23-11-327 | | 27.11.2023 06:20:08 | S6 - Фиксация случаев предоставления несогласо... | Закрыт | |
| 23-11-326 | | 27.11.2023 06:05:08 | Предоставление доступа к USB | На согласовании | |
| 23-11-325 | | 26.11.2023 16:35:09 | S2 - Обнаружение сетевой атаки | Реагирование | |
| 23-11-324 | | 26.11.2023 16:35:08 | S2 - Обнаружение сетевой атаки | Реагирование | |
| 23-11-323 | | 26.11.2023 03:45:08 | S4 - Обнаружение атак на учетные записи, брутфорс | Создан | |
| 23-11-322 | | 26.11.2023 03:40:08 | S2 - Обнаружение сетевой атаки | Реагирование | |
| 23-11-321 | | 26.11.2023 02:55:08 | S5 - Обнаружение нарушения политик ИБ | Закрыт | |
| 23-11-320 | | 26.11.2023 01:10:08 | S4 - Обнаружение атак на учетные записи, брутфорс | Создан | |
| 23-11-319 | | 25.11.2023 23:50:08 | S4 - Обнаружение атак на учетные записи, брутфорс | Назначен | |
| 23-11-318 | | 25.11.2023 21:45:08 | S2 - Обнаружение сетевой атаки | Закрыт | |
| 23-11-317 | | 25.11.2023 12:50:08 | S2 - Обнаружение сетевой атаки | Реагирование | |
| 23-11-316 | | 24.11.2023 20:00:08 | S3 - Обнаружение обхода средств защиты | Закрыт | |
| 23-11-315 | | 24.11.2023 15:55:08 | S2 - Обнаружение сетевой атаки | Реагирование | |
| 23-11-314 | | 24.11.2023 14:05:09 | S3 - Обнаружение обхода средств защиты | Закрыт | |
| 23-11-313 | | 24.11.2023 14:05:09 | S3 - Обнаружение обхода средств защиты | Закрыт | |

SEGEZHA GROUP

# А оно «вам» надо?

**Инцидентов в сутки**




**50%**

зарегистрированных инцидентов имеют высокий уровень критичности

**~14 мин.**

Средняя скорость информирования с соблюдением SLA

SEGEZHA GROUP

# Что сейчас?

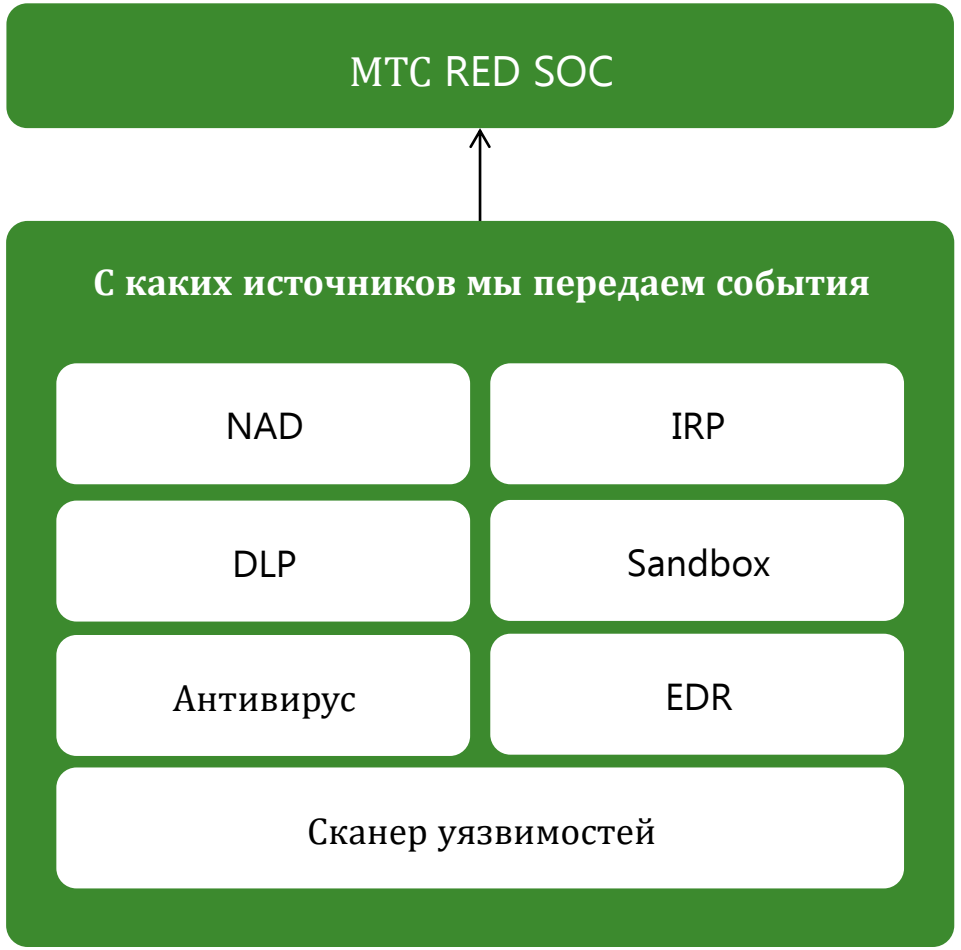
Интеграция систем обеспечения ИБ АСУ ТП (в первую очередь КИИ) в процесс управления инцидентами

Подключение к SOC приобретаемых активов

Подключение к SOC дополнительных источников (Linux, логи с оборудования и т.д.)

Постоянная разработка новых правил корреляции

Постоянная доработка плейбуков IRP (разбивка на подтипы, подключение новых СЗИ к IRP, усложнение логики)




**7000+** рабочих станций сотрудников и серверов

# Спасибо!

Никита Курмышкин · Руководитель направления защиты ИТ-инфраструктуры Segezha Group