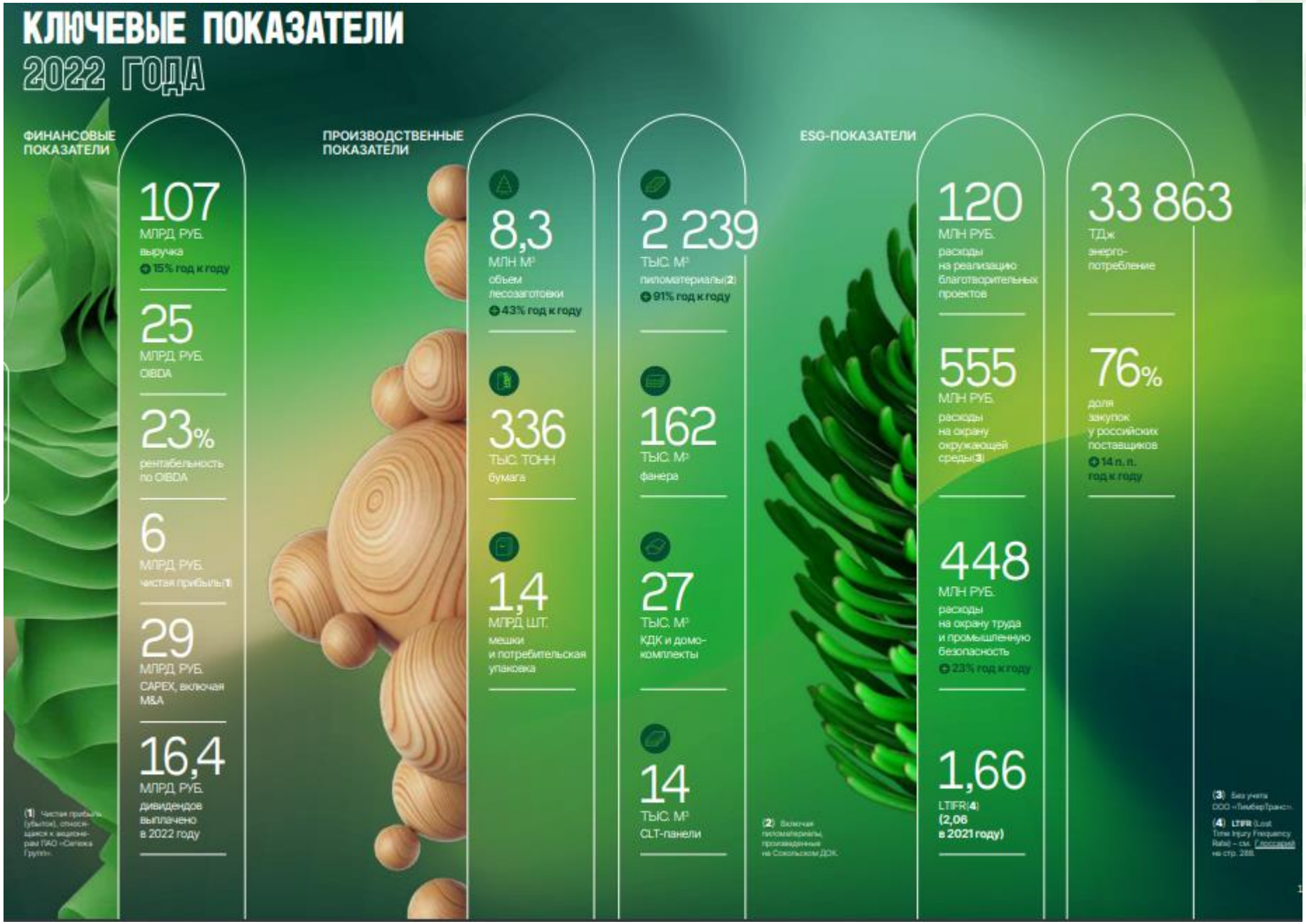
ПРАКТИЧЕСКИЕ, ОТРАСЛЕВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ВНЕШНЕГО SOC ПРОВАЙДЕРА В ДЕРЕВООБРАБАТЫВАЮЩЕЙ ОТРАСЛИ

Максим Королев
Сегежа Групп

Сегежа Групп - в цифрах 1/2



Сегежа Групп - в цифрах 2/2

1-е МЕСТО в России по производству мешочной бумаги(1)

1-е МЕСТО в России по производству бумажных мешков(1)

2-е МЕСТО в мире по производству бумаги для многослойных мешков(1)

Segezha Group уделяет особое внимание повышению уровня обеспеченности лесным сырьем из собственных источников: в 2022 году 93% потребностей Компании в древесине было покрыто за счет собственных ресурсов. Это дает возможность эффективно контролировать себестоимость производства, снижать зависимость от цен на лесное сырье и успешно конкурировать с другими производителями на российском и мировом рынках.

Компания активно внедряет ESG-принципы в свой бизнес. Segezha Group является участником Глобального договора Организации Объединенных Наций (United Nations Global Compact) – инициативы ООН в сфере корпоративной социальной ответственности и устойчивого развития. Кроме того, с целью увеличения вклада российских лесов в глобальную борьбу с изменением климата, а также улучшения их продуктивности во всех лесных активах Группы внедряются принципы устойчивого лесопользования на основе научно подтвержденной интенсивной модели.

С 2021 года Segezha Group является публичной компанией. Ценные бумаги Компании включены в котировальный список Московской биржи первого уровня.

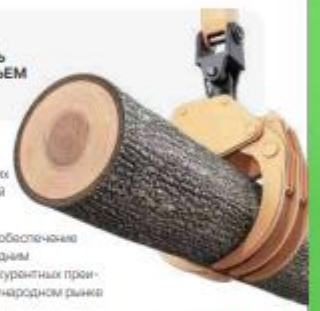
(1) Оценка Fisher International.

Segezha Group работает с лесными ресурсами – полностью возобновляемым сырьем

01 **ВЫСОКАЯ ДОБАВЛЕННАЯ СТОИМОСТЬ**

- Продукция глубокой переработки
- Максимизация использования сырья
- Низкая себестоимость

02 **ОБЕСПЕЧЕННОСТЬ ДРЕВЕСНЫМ СЫРЬЕМ**



- Segezha Group – один из крупнейших лесопользователей в мире
- Собственное лесообеспечение на 93% является одним из важнейших конкурентных преимуществ на международном рынке

03 **ПРИВЕРЖЕННОСТЬ ПРИНЦИПАМ УСТОЙЧИВОГО РАЗВИТИЯ**

- Полностью возобновляемое сырье
- Сертификация продукции
- Лесовосстановление
- Социальные инвестиции

(2) **Источник:** https://www.timber-online.net.
(3) **Источники:** внутренние исследования Segezha Group, данные WhatWood. Данные представлены с учетом мощности Галичского фанерного комбината.
(4) **Источник:** внутренние исследования Segezha Group.

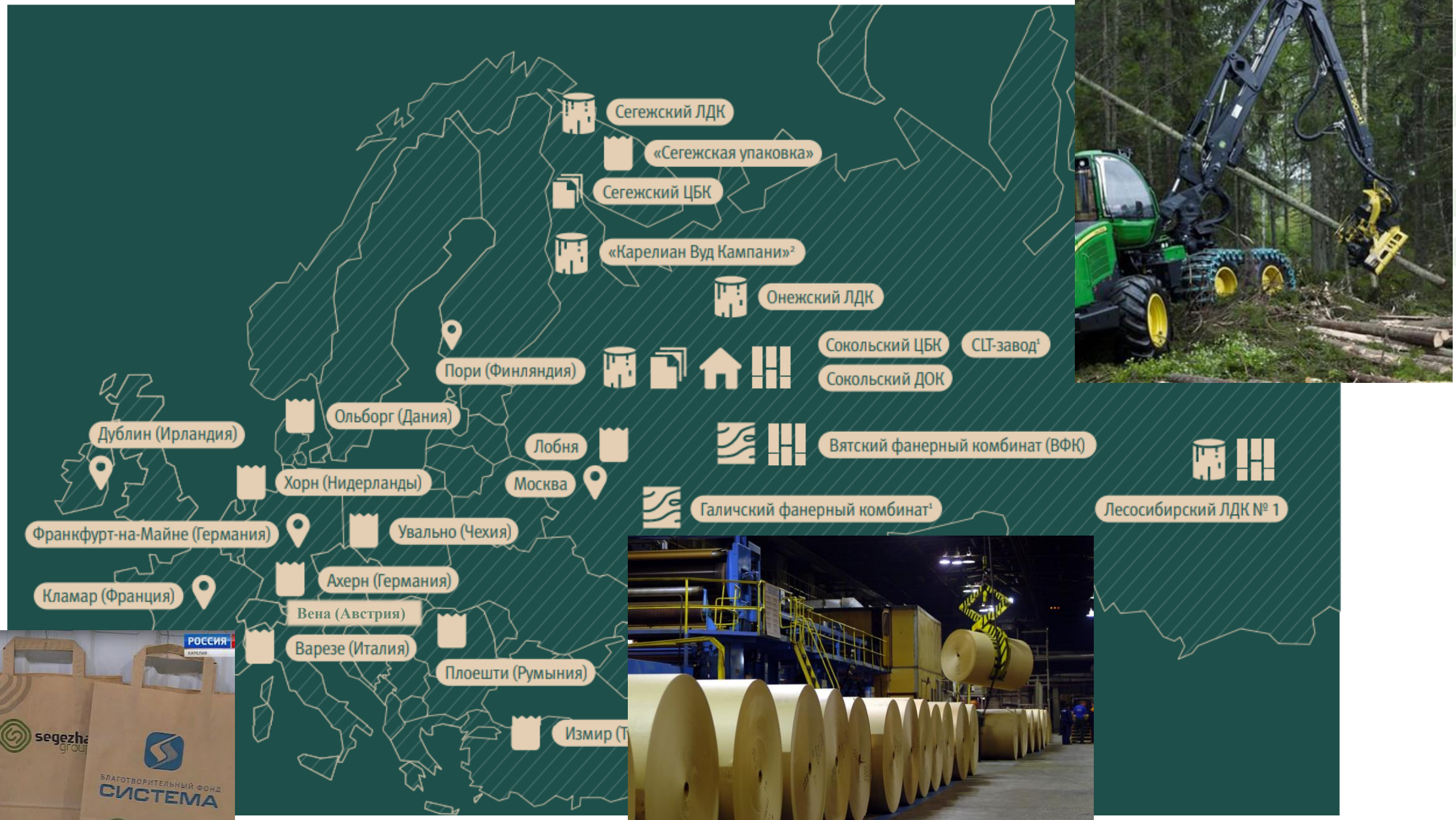
9-е МЕСТО в Европе по производству хвойных пиломатериалов(2)

3-е МЕСТО в мире по производственным мощностям березовой фанеры(3)

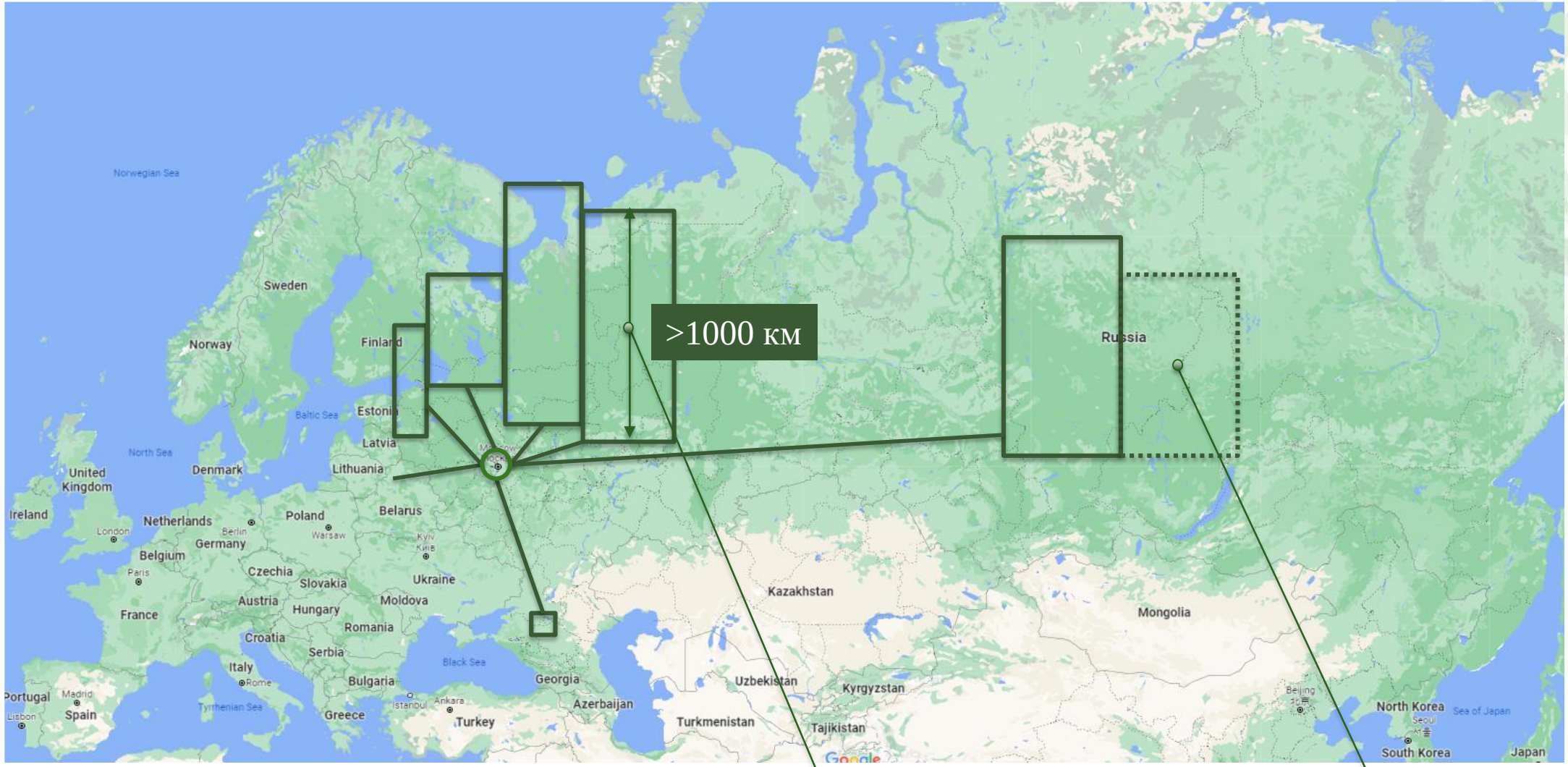
1-е МЕСТО в России по мощности производства КДК и домокомплектов из клееного бруса(4)

1-е МЕСТО в России по производству CLT-панелей(4)

Сегежа Групп - география производства



Отраслевая специфика обеспечения ИБ Сегежа Групп



Огромные расстояния
Плохие дороги

Низкая защищенность приобретаемых активов

SOC. Начало

1. Интенсификация сделок M&A, рост информационных активов

2. Тотальная цифровизация

3. Роботизация

4. Облачные вычисления

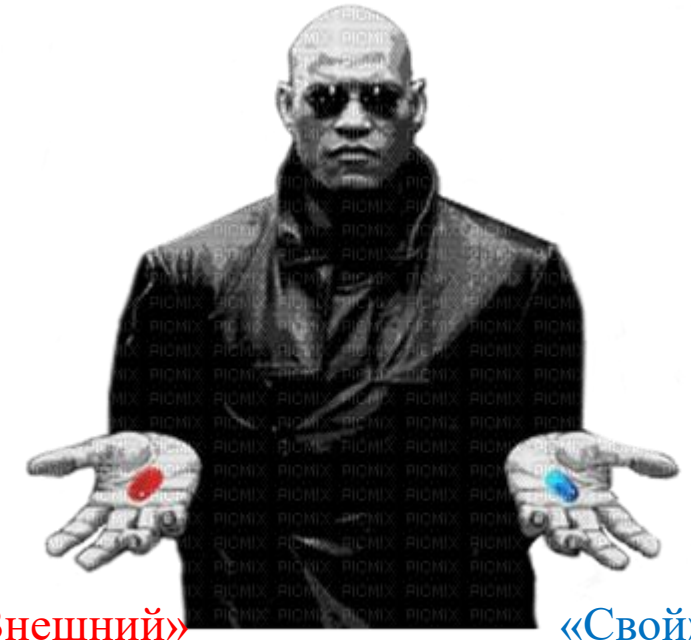
5. Covid-19 с уходом работников на удаленный режим работы

НО

Если все идет хорошо … значит вы чего-то не знаете

(интерпретация следствия из второго закона Чизхолма)

SOC. Выбор пути



«Внешний» SOC

- В «сестринской» компании МТС создан и успешно функционирует коммерческий SOC

«Свой» SIEM

- покупка SIEM
- поиск и удержание специалистов
- создание круглосуточного диспетчерского центра

Что потребовалось сделать нам (заказчику)

1. Инвентаризация активов, сетевой инфраструктуры Сегежа Групп

2. Определение критичных источников событий

3. Подготовка инфраструктуры:

3.1 Настройка защищённого канала между SOC МТС и Сегежа Групп

3.2 Установка сервера сбора и нормализации событий (инструкция предоставлена SOC МТС)

3.3 Развернуть несколько WEC-серверов для сбора журналов безопасности (расчет количества и параметров предоставлен SOC МТС)

3.4 Настройка источников событий (инструкции предоставлены SOC МТС)

Welcome to the Real World …

Что мы получили сразу после подключения к SOC МТС (из коробки)

1. Формирование инцидентов ИБ на основании «базового» набора правил корреляции. Необходимость произвести профилирование правил корреляции (срок - около 1 месяца)
2. Контроль процессов информационной безопасности (добавление пользователя в привилегированную группу AD, контроль использования не персонифицированных УЗ и т.д.)
3. Выявление существующей вредоносной активности в инфраструктуре Сегежа Групп
4. Сканирование сервисов внешнего периметра (в т.ч. «подключение по RDP»)
5. Доступность ретроспективного анализа событий (подключения по VPN, интерактивные входы пользователей, установка служб и т.д.)
6. Контроль источников событий (мониторинг доступности)
7. Диспетчеризацию событий информационной безопасности компании в режиме 24/7 с четко прописанным SLA
8. Помощь со стороны SOC МТС в расследовании инцидентов
9. Предоставление отчётов. Ежедневные оперативные отчеты и ежемесячные аналитические отчеты
10. Раннее получение информации о новых критичных уязвимостях, требующих немедленного реагирования

Развитие сервиса SOC в первый год эксплуатации

1. Настройка кастомных правил
    1.1. интерактивный вход технологической учётной записи
    1.2. атрибут «Не истекает срок действия пароля» – Включён
    1.3. включение или исключение пользователя из критичных групп
    1.4. удаление учетной записи в течении 24 часов после создания

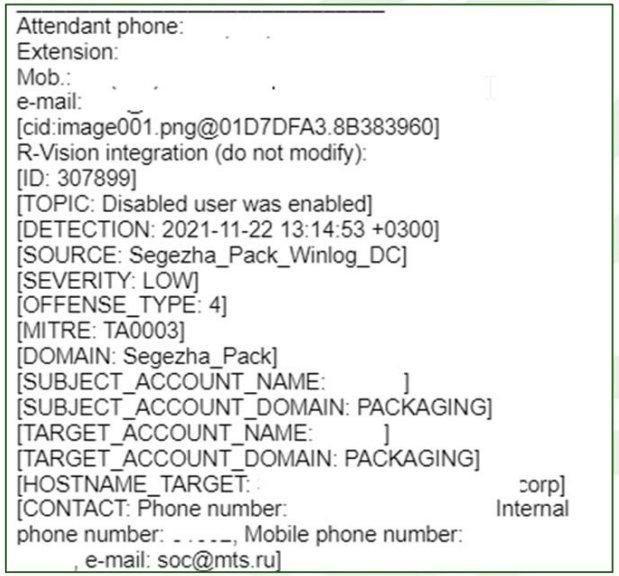
2. Интеграция с IRP R-Vision через почтовое взаимодействие. Тегирование писем

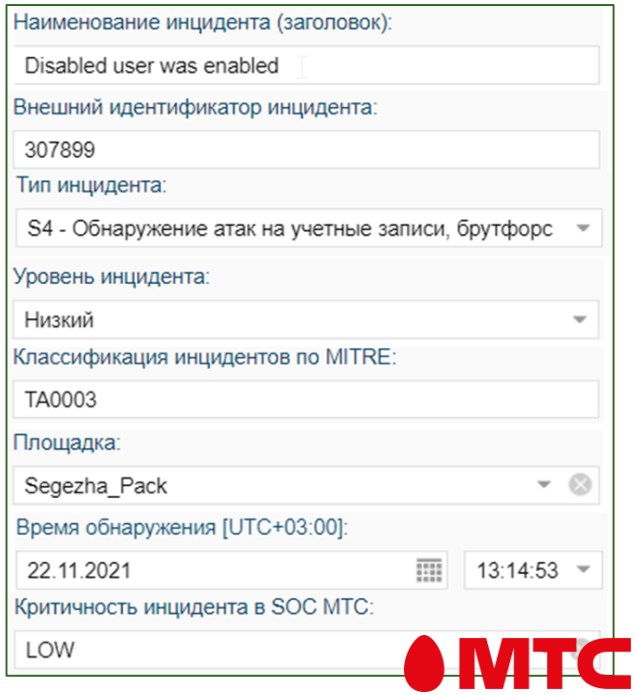
3. Фильтрация «мусорных» событий до попадания их на корреляцию для уменьшения входного EPS. Это фильтрация на WEC, выборочные запросы к базам данных

4. Подключение PT NAD. На этапе пилотирования подключение к SOC MTC. Реагирование на инциденты через дежурную смену. Совместное изучение нового источника. Облегчение интеграции решения

5. Включение рекомендаций в части проверки жесткого диска

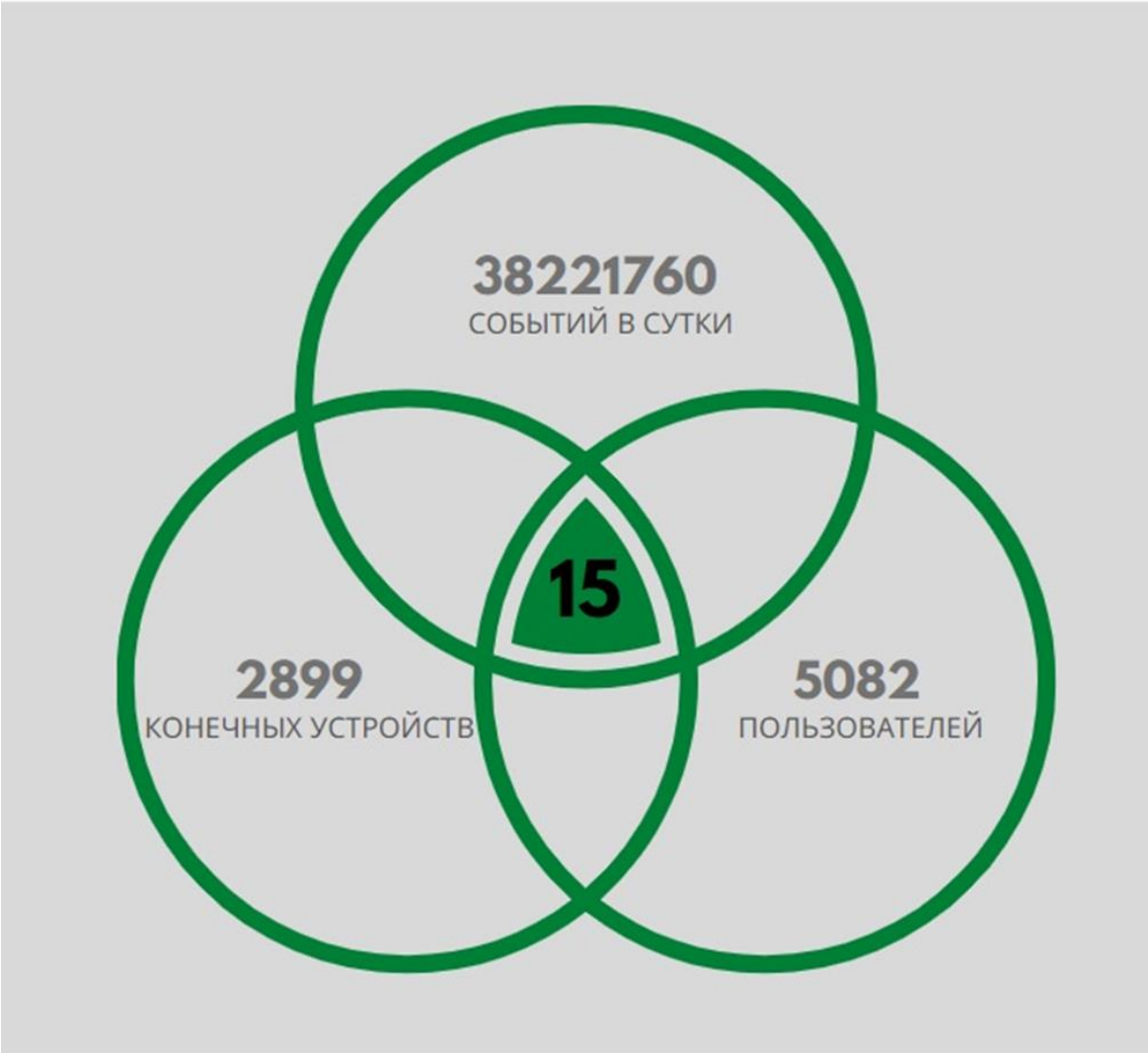
6. Подключение западных активов. Отдельная инфраструктура со своими уникальными типами источников. Взаимодействие происходит на английском языке с учетом часового пояса

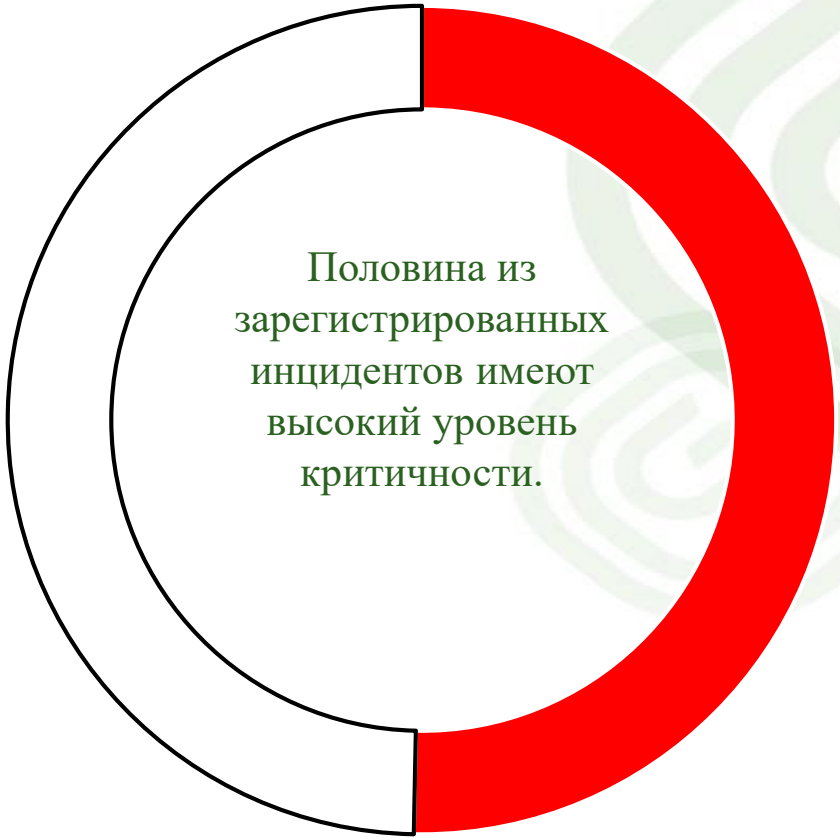




Немного цифр

ИНЦИДЕНТОВ В СУТКИ



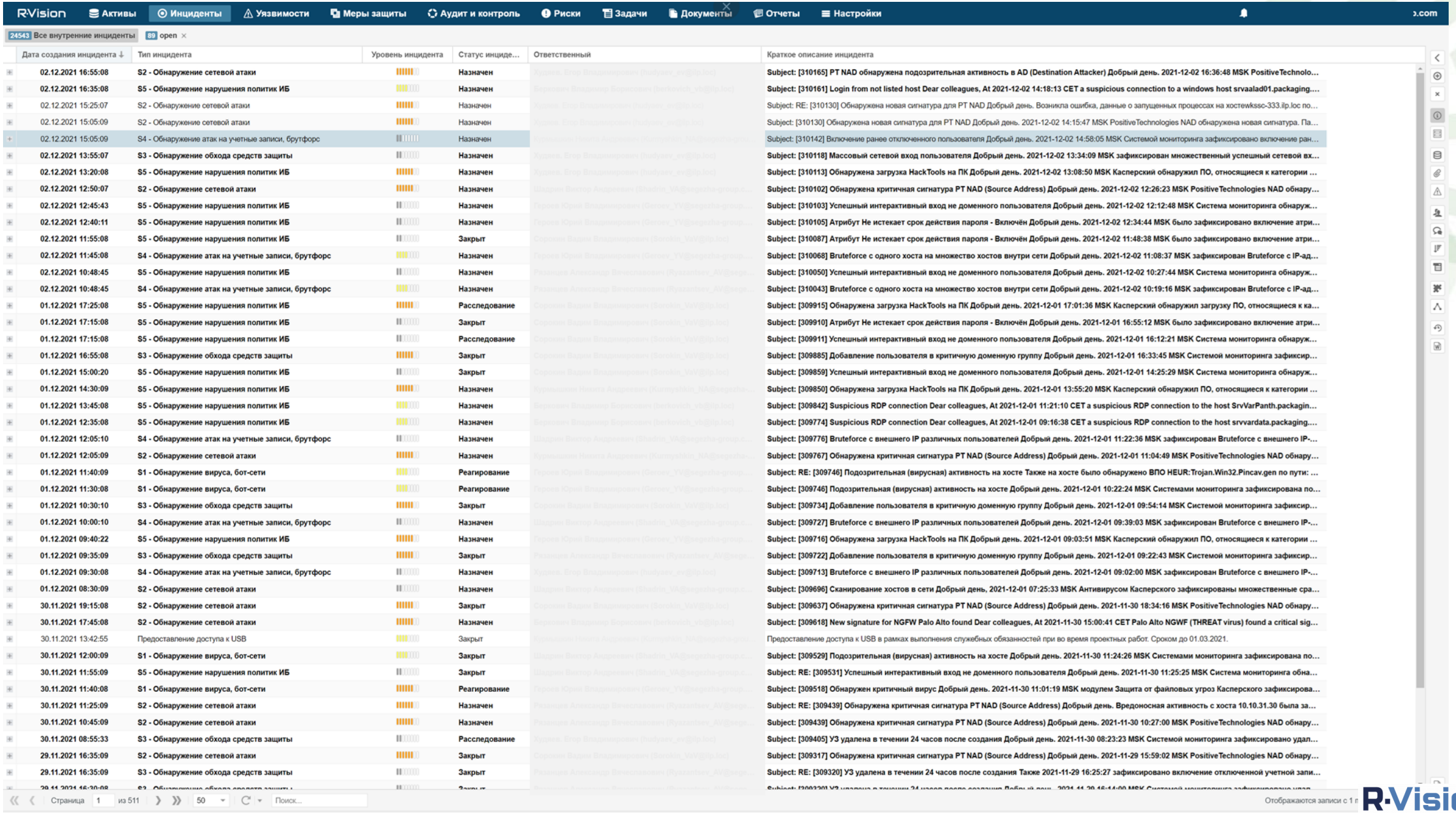


Средняя скорость информирования

~14 мин

с соблюдением SLA

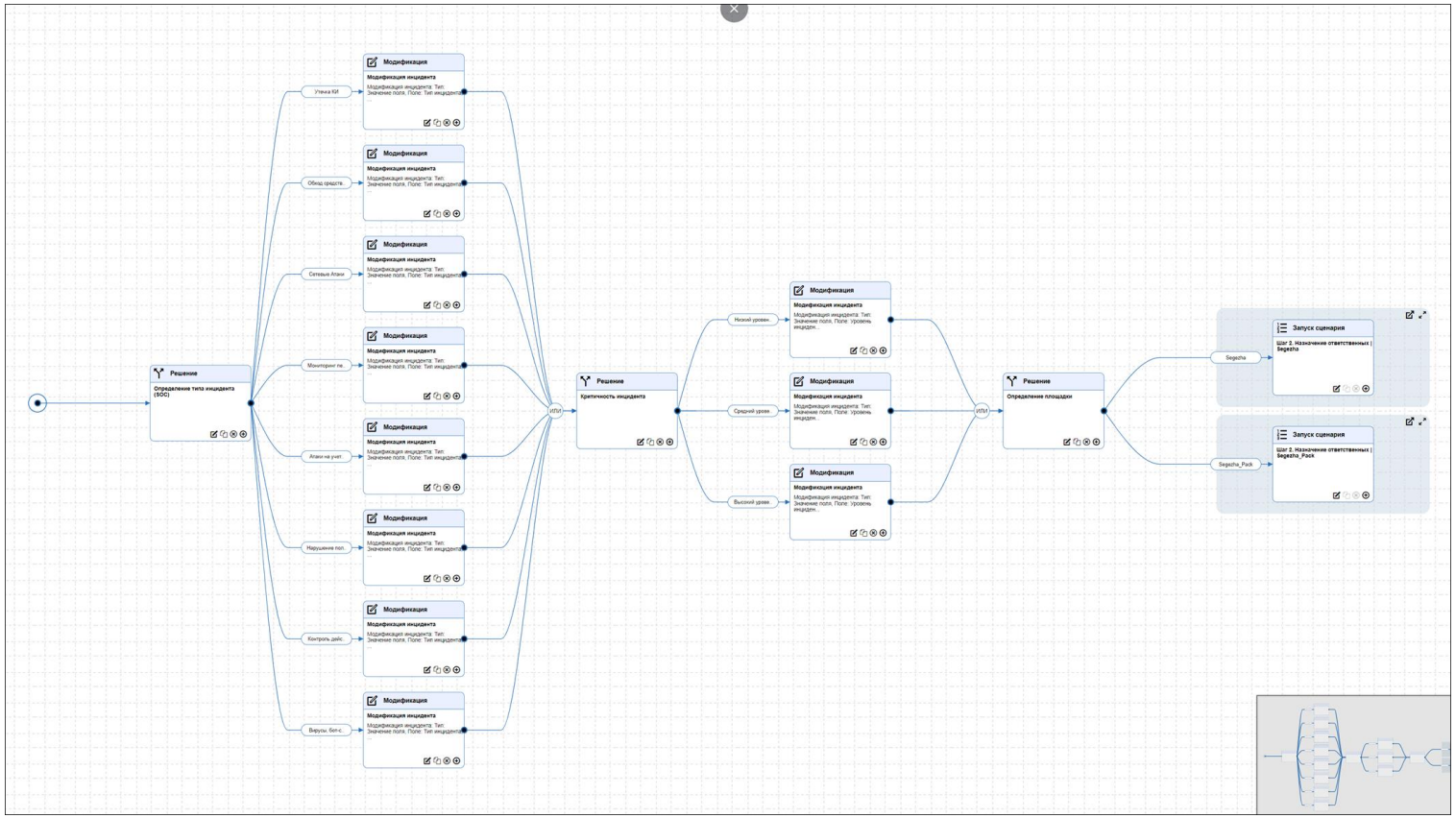
Инциденты ИБ



Дашборд SOC MTS

Сценарии реагирования. Эскалация инцидентов

1. Автоматическая предобработка инцидента (определение региона, назначение ответственного)
2. Направление уведомлений в группы реагирования (почта, telegram)
3. Обогащение инцидента данными инвентаризации и контекстом из внешних систем
4. Приоритезация инцидента исходя из потенциального ущерба



R-Vision

Сценарии реагирования. Результаты

1. В разы сокращено время реагирования на инциденты ИБ и их расследование

2. Реализована автоматическая регистрация и распределение инцидентов, единое пространство для работы аналитиков ускорило работу и сократило количество ошибок

3. Запущены коннекторы к разным системам с обогащением карточек инцидентов, сбором свидетельства и реагированием в автоматизированном режиме:

   - проверка состояния учетной записи (заблокирована, истек срок действия ученой записи, истек пароль)
   - блокировка учетной записи Active Directory
   - запуск задачи проверки хоста антивирусом
   - проверка внешнего IP-адреса в базе Alienvault
   - проверка хэша файла в VirusTotal

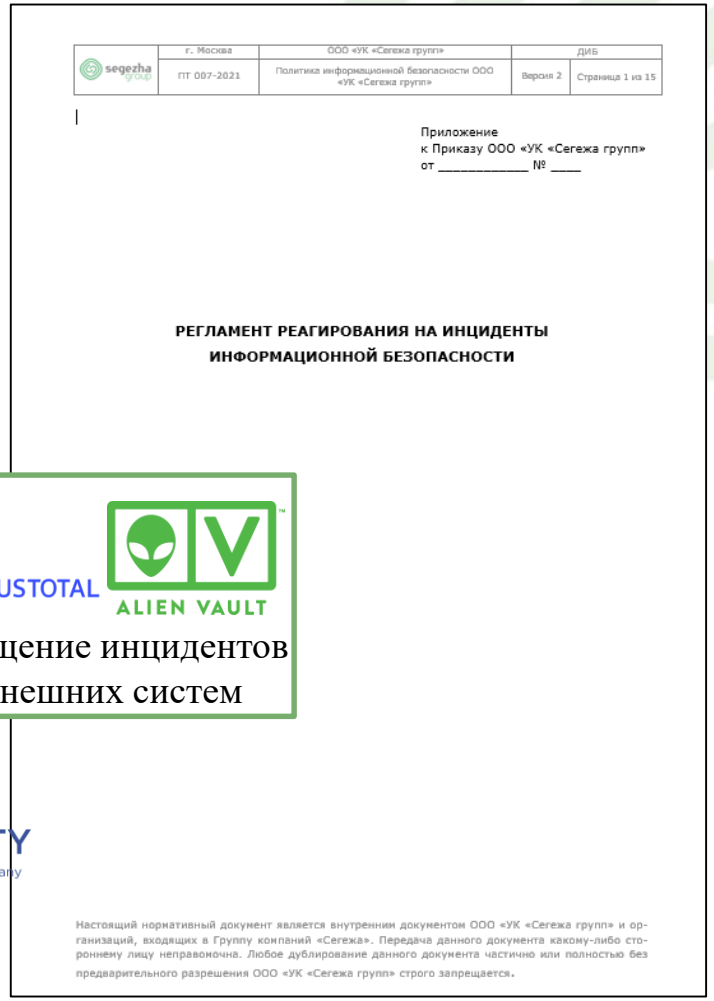
4. Визуализация операционной деятельности (графики, диаграммы) предоставляет возможность для удобного мониторинга и анализа данных

Реагирование на инциденты ИБ

SOC МТС

Команда реагирования Сегежа Групп ИБ+ИТ

Security Operations Center (SOC) • Центр реагирования на инциденты ИБ • R·Vision IRP



РЕГЛАМЕНТ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Приложение к Приказу ООО «УК «Сегежа групп» от _____ № ____

Настоящий нормативный документ является внутренним документом ООО «УК «Сегежа групп» и организаций, входящих в Группу компаний «Сегежа». Передача данного документа какому-либо стороннему лицу неправомочна. Любое дублирование данного документа частично или полностью без предварительного разрешения ООО «УК «Сегежа групп» строго запрещается.

VIRUSTOTAL ALIEN VAULT

Обогащение инцидентов из внешних систем

INFOSECURITY a Softline company

Настройка файрволов

Журналы безопасности ПК и серверов

Журналы антивируса

paloalto NETWORKS

Журналы файрволов

PT Network Attack Discovery

Журнал анализатора сетевого трафика

Active Directory

Kaspersky Security Center

Активное реагирование

Эффективность работы связки SOC МТС + IRP + Команда реагирования Сегежа Групп
Реальные кейсы

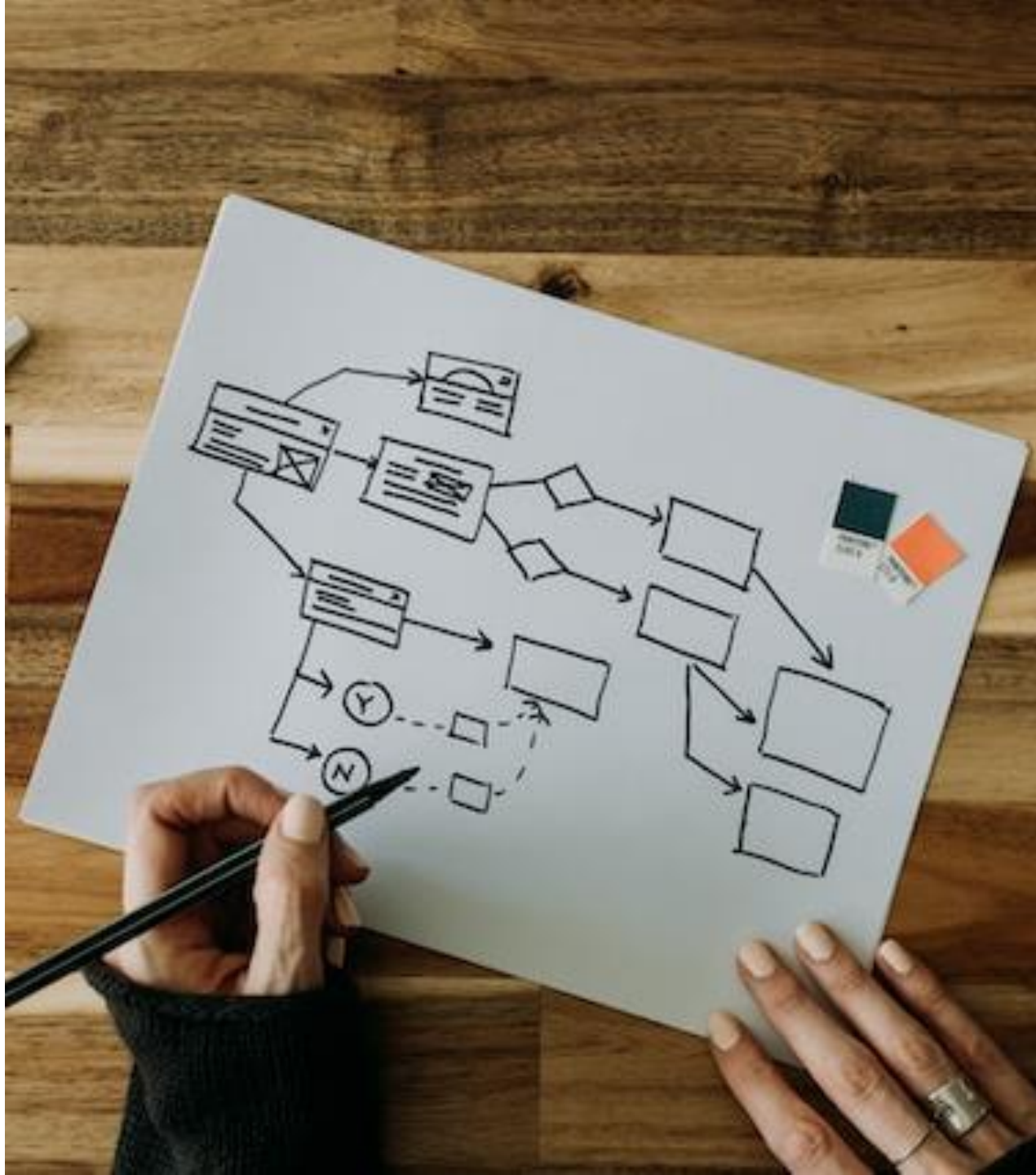
В ноябре 2020 года была детектирована вирусная активность по сигнатуре «ETERNALBLUE (WannaCry, Petya)», исходящая с домашнего компьютера сотрудника, работающего удаленно. В результате своевременной реакции угроза была нейтрализована.

В феврале 2021 года были детектированы множественные вирусные атаки исходящие из г. Лесосибирск. В результате расследования была обнаружена врезка в кабель UTP, ведущая к точке доступа Wi-Fi, через которую работники цеха выходили в Интернет с личных зараженных устройств

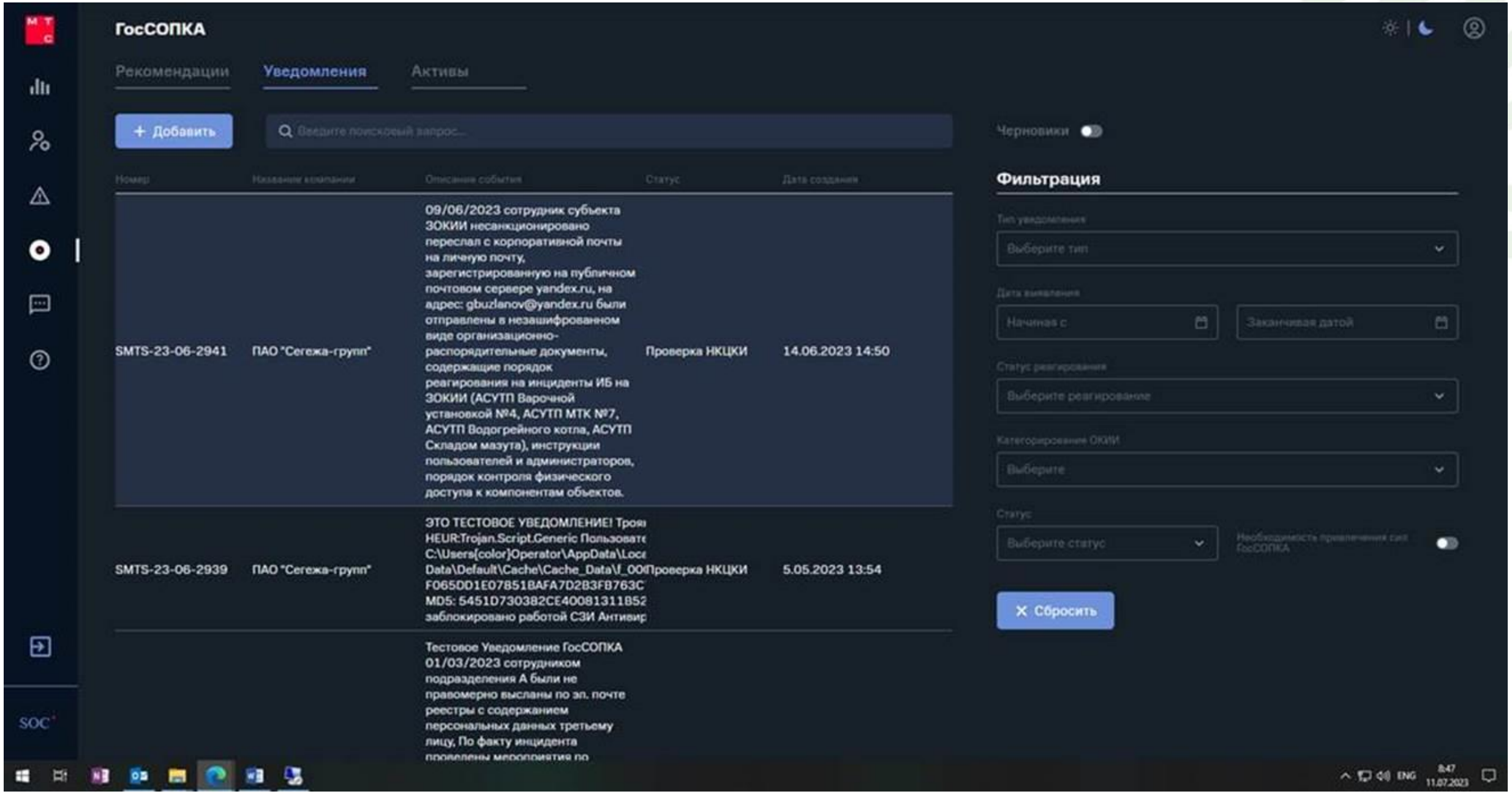
В рамках проведения пентеста в конце 2020 года и киберучений в конце 2021 года все критичные действия атакующей стороны были детектированы SOC со своевременным оповещением команды реагирования

Дальнейшее развитие SOC 2021-2023

1. Подключение англоговорящих администраторов ИТ западных активов холдинга к IRP R-Vision
2. Интеграция систем обеспечения информационной безопасности АСУТП (в первую очередь КИИ) в процесс Управления инцидентами Сегежа
3. Подключение в SOC приобретаемых активов (в т.ч. недавно приобретенных активов в Западной Сибири)
4. Подключение в SOC дополнительных источников (Linux, логи уровня приложений: CRM, ERP и т.д.)
5. Постоянная разработка новых правил корреляции
6. Постоянная доработка плейбуков IRP (разбиение на подтипы, подключение новых СЗИ к IRP, усложнение логики)



Работа с НКЦКИ через SOC



Ваши вопросы