



ПРАКТИЧЕСКИЕ, ОТРАСЛЕВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ВНЕШНЕГО SOC ПРОВАЙДЕРА В ДЕРЕВООБРАБАТЫВАЮЩЕЙ ОТРАСЛИ

Максим Королев
Сегежа Групп

КЛЮЧЕВЫЕ ПОКАЗАТЕЛИ 2022 ГОДА

ФИНАНСОВЫЕ ПОКАЗАТЕЛИ

107

МЛРД РУБ.
выручка
↑ 15% год к году

25

МЛРД РУБ.
ОБДА

23%

рентабельность
по ОБДА

6

МЛРД РУБ.
чистая прибыль⁽¹⁾

29

МЛРД РУБ.
SAPEX, включая
M&A

16,4

МЛРД РУБ.
дивидендов
выплачено
в 2022 году

(1) Чистая прибыль (убыток), относящаяся к акционерам ПАО «Сегежа Групп».

ПРОИЗВОДСТВЕННЫЕ ПОКАЗАТЕЛИ



8,3

МЛН М³
объем
лесозаготовки
↑ 43% год к году



336

Тыс. ТОНН
бумага



1,4

МЛРД ШТ.
мешки
и потребительская
упаковка



2 239

Тыс. М³
пиломатериалы⁽²⁾
↑ 91% год к году



162

Тыс. М³
фанера



27

Тыс. М³
КДК и дросто-
комплекты



14

Тыс. М³
CLT-панели



ESG-ПОКАЗАТЕЛИ

120

МЛН РУБ.
расходы
на реализацию
благоприятельных
проектов

555

МЛН РУБ.
расходы
на охрану
окружающей
среды⁽³⁾

448

МЛН РУБ.
расходы
на охрану труда
и промышленную
безопасность
↑ 23% год к году

1,66

LTIFR⁽⁴⁾
(2,06
в 2021 году)

(2) Включая пиломатериалы, произведенные на Соколовском ДСК.

33 863

ТДж
энерго-
потребление

76%

доля
закупок
у российских
поставщиков
↑ 14 п. п.
год к году

(3) Без учета ООО «ЛиберТранск».

(4) LTIFR (Lost Time Injury Frequency Rate) – см. Глоссарий на стр. 288.

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 все 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.

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 лесобеспечение на 93% является одним из важнейших конкурентных преимуществ на международном рынке



03 ПРИВЕРЖЕННОСТЬ ПРИНЦИПАМ УСТОЙЧИВОГО РАЗВИТИЯ

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



9-е

МЕСТО
в Европе
по производству
хвойных
пиломатериалов(2)

3-е

МЕСТО
в мире
по производ-
ственным
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)

(1) Оценка Fisher International.

(2) Источник: <https://www.wood-online.ru/>

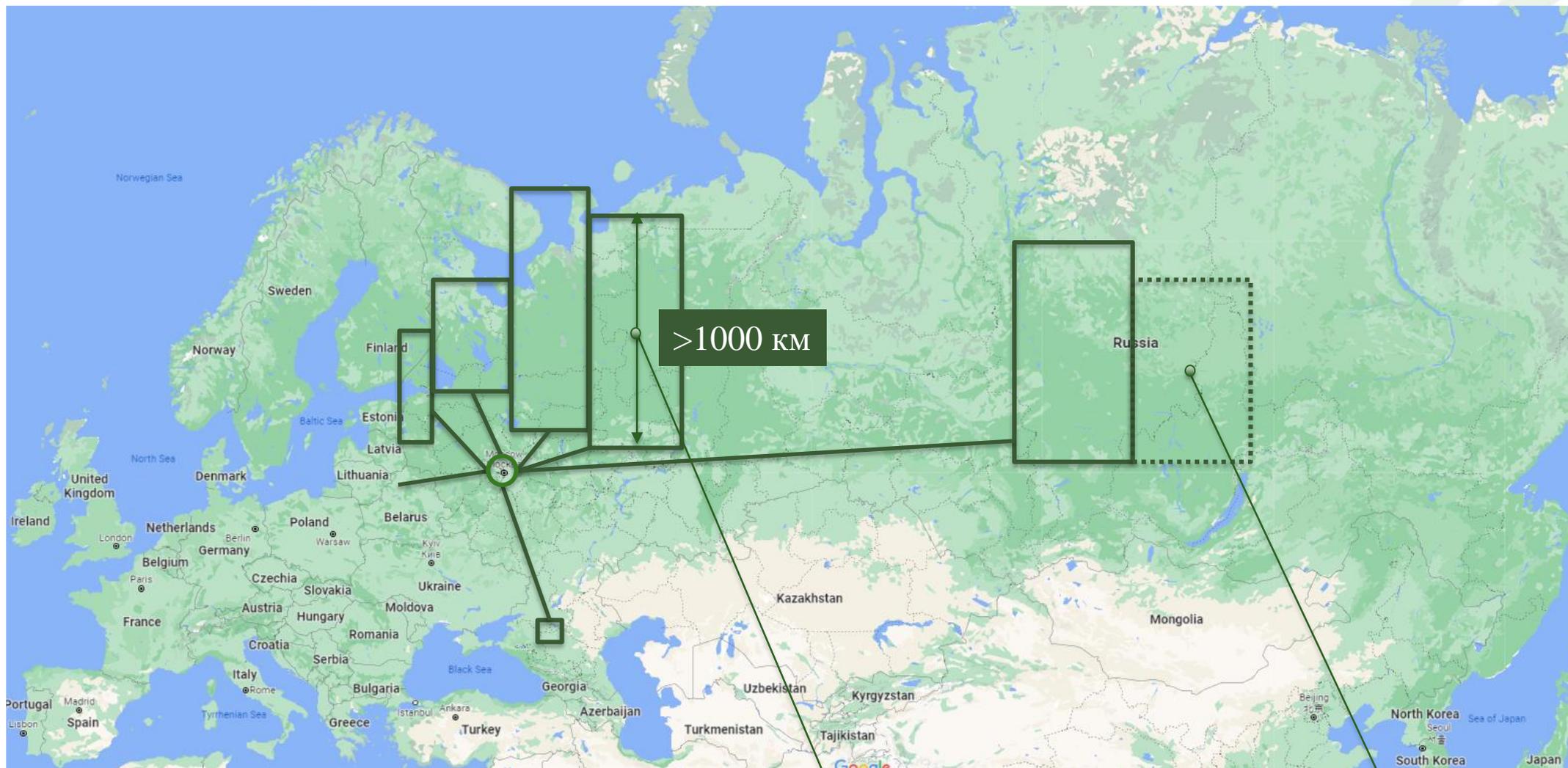
(3) Источник: внутреннее исследование Segezha Group, данные WhatWood. Данные представлены с учетом мощностей Глянского фанерного комбината.

(4) Источник: внутреннее исследование Segezha Group.

Сегежа Групп - география производства



Отраслевая специфика обеспечения ИБ Сегежа Групп



Огромные расстояния
Плохие дороги

Низкая защищенность
приобретаемых
активов



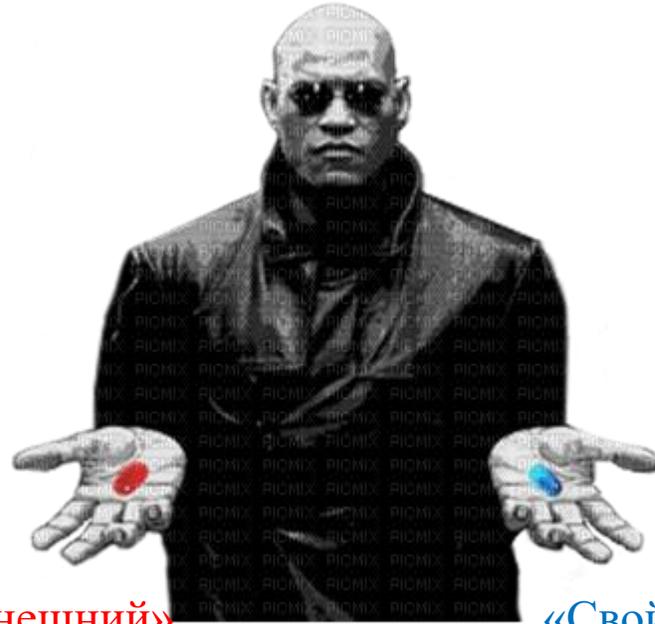
1. Интенсификация сделок M&A, рост информационных активов
2. Тотальная цифровизация
3. Роботизация
4. Облачные вычисления
5. Covid-19 с уходом работников на удаленный режим работы

НО

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

*(интерпретация следствия
из второго закона Чизхолма)*

SOC. Выбор пути



«Внешний»
SOC

«Свой»
SIEM

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

- 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 МТС. 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

```
Attendant phone:
Extension:
Mob.:
e-mail:
[cid:image001.png@01D7DFA3.8B383960]
R-Vision integration (do not modify):
[ID: 307899]
[TOPIIC: Disabled user was enabled]
[DETECTION: 2021-11-22 13:14:53 +0300]
[SOURCE: Segezha_Pack_Winlog_DC]
[SEVERITY: LOW]
[OFFENSE_TYPE: 4]
[MITRE: TA0003]
[DOMAIN: Segezha_Pack]
[SUBJECT_ACCOUNT_NAME: ]
[SUBJECT_ACCOUNT_DOMAIN: PACKAGING]
[TARGET_ACCOUNT_NAME: ]
[TARGET_ACCOUNT_DOMAIN: PACKAGING]
[HOSTNAME_TARGET: ]
[CONTACT: Phone number: , Mobile phone number: , e-mail: soc@mts.ru]
corp
Internal
```



Наименование инцидента (заголовок):
Disabled user was enabled

Внешний идентификатор инцидента:
307899

Тип инцидента:
S4 - Обнаружение атак на учетные записи, брутфорс

Уровень инцидента:
Низкий

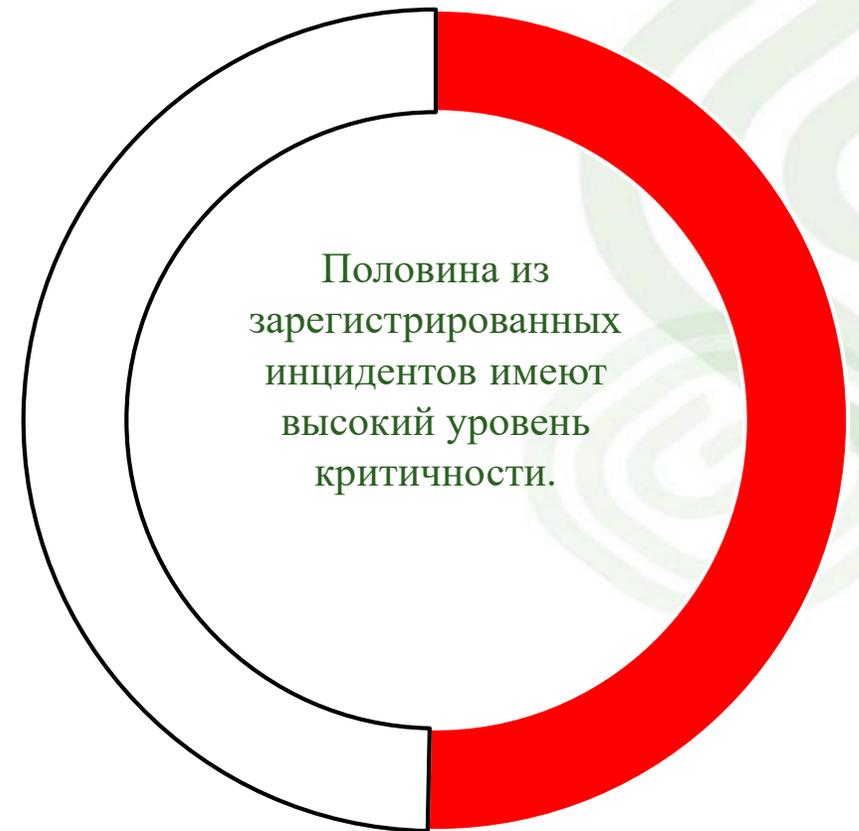
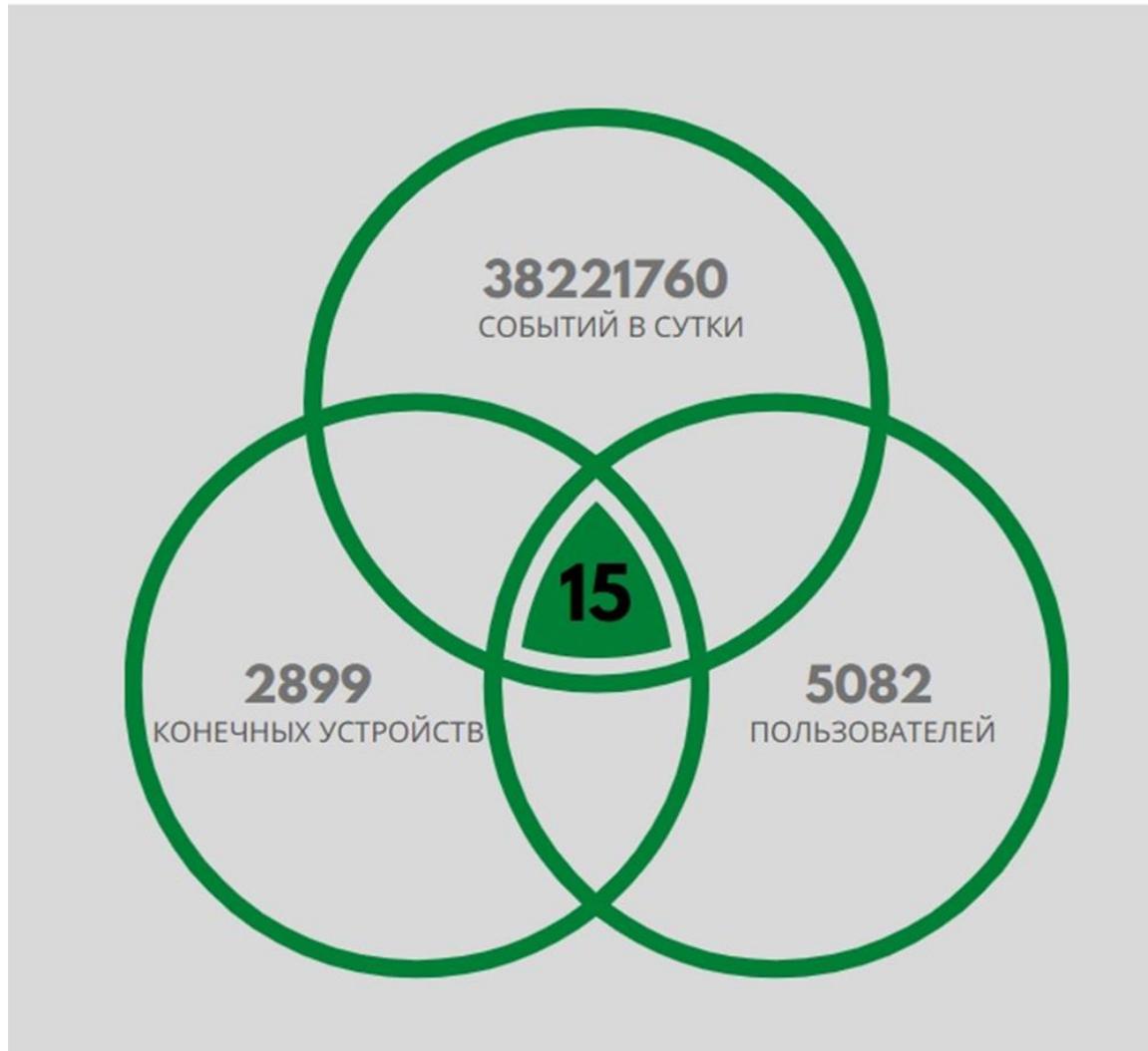
Классификация инцидентов по MITRE:
TA0003

Площадка:
Segezha_Pack

Время обнаружения [UTC+03:00]:
22.11.2021 13:14:53

Критичность инцидента в SOC МТС:
LOW

ИНЦИДЕНТОВ В СУТКИ



Средняя скорость информирования
~14 МИН
с соблюдением SLA

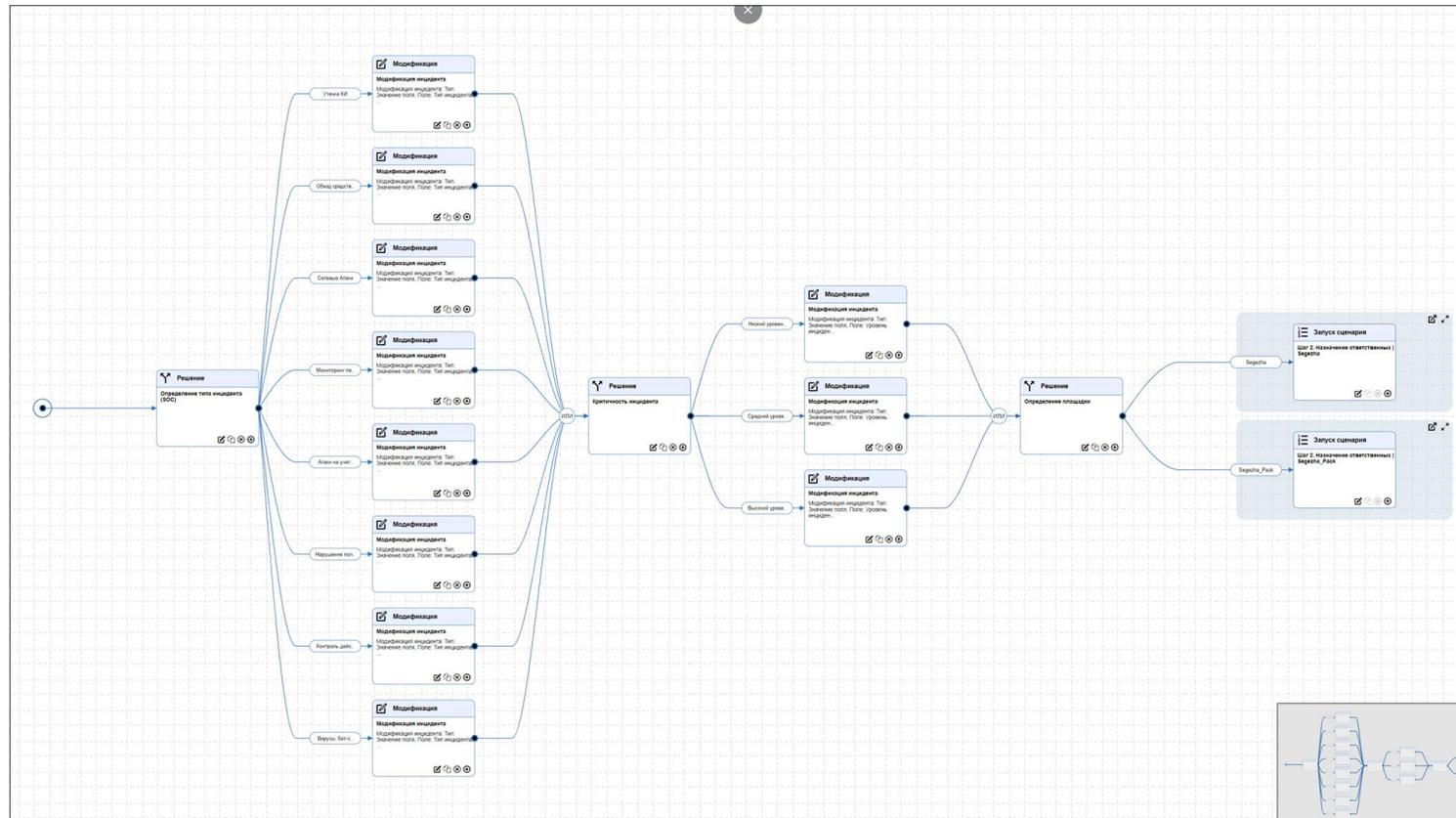
Дата создания инцидента ↓	Тип инцидента	Уровень инцидента	Статус инцидента	Ответственный	Краткое описание инцидента
02.12.2021 16:55:08	S2 - Обнаружение сетевой атаки		Назначен	Хурден Егор Владимирович (Хурден_ЕВ@phd.ru)	Subject: [310165] PT NAD обнаружена подозрительная активность в AD (Destination Attacker) Добрый день. 2021-12-02 16:36:48 MSK PositiveTechnolo...
02.12.2021 16:35:08	S5 - Обнаружение нарушения политик ИБ		Назначен	Воропан Владимир Борисович (Воропан_ВБ@phd.ru)	Subject: [310161] Login from not listed host Dear colleagues, At 2021-12-02 14:18:13 CET a suspicious connection to a windows host srraalad01.packaging...
02.12.2021 15:25:07	S2 - Обнаружение сетевой атаки		Назначен	Хурден Егор Владимирович (Хурден_ЕВ@phd.ru)	Subject: RE: [310130] Обнаружена новая сигнатура для PT NAD Добрый день. Возникла ошибка, данные о запущенных процессах на hostewkss0-333.lpr.loc по...
02.12.2021 15:05:09	S2 - Обнаружение сетевой атаки		Назначен	Хурден Егор Владимирович (Хурден_ЕВ@phd.ru)	Subject: [310130] Обнаружена новая сигнатура для PT NAD Добрый день. 2021-12-02 14:15:47 MSK PositiveTechnologies NAD обнаружена новая сигнатура. Па...
02.12.2021 15:05:09	S4 - Обнаружение атак на учетные записи, брутфорс		Назначен	Хурден Егор Владимирович (Хурден_ЕВ@phd.ru)	Subject: [310142] Включение ранее отключенного пользователя Добрый день. 2021-12-02 14:58:05 MSK Системой мониторинга зафиксировано включение ран...
02.12.2021 13:55:07	S3 - Обнаружение обхода средств защиты		Назначен	Хурден Егор Владимирович (Хурден_ЕВ@phd.ru)	Subject: [310118] Массовый сетевой вход пользователя Добрый день. 2021-12-02 13:34:09 MSK зафиксирован множественный успешный сетевой вх...
02.12.2021 13:20:08	S5 - Обнаружение нарушения политик ИБ		Назначен	Хурден Егор Владимирович (Хурден_ЕВ@phd.ru)	Subject: [310113] Обнаружена загрузка HackTools на ПК Добрый день. 2021-12-02 13:08:50 MSK Касперский обнаружил ПО, относящиеся к категории ...
02.12.2021 12:50:07	S2 - Обнаружение сетевой атаки		Назначен	Щадрин Виктор Андреевич (Щадрин_ВА@phd.ru)	Subject: [310102] Обнаружена критичная сигнатура PT NAD (Source Address) Добрый день. 2021-12-02 12:26:23 MSK PositiveTechnologies NAD обнару...
02.12.2021 12:45:43	S5 - Обнаружение нарушения политик ИБ		Назначен	Герман Юрий Владимирович (Герман_ЮВ@phd.ru)	Subject: [310103] Успешный интерактивный вход не доменного пользователя Добрый день. 2021-12-02 12:12:48 MSK Система мониторинга обнаруж...
02.12.2021 12:40:11	S5 - Обнаружение нарушения политик ИБ		Назначен	Герман Юрий Владимирович (Герман_ЮВ@phd.ru)	Subject: [310105] Атрибут Не истекает срок действия пароля - Включён Добрый день. 2021-12-02 12:34:44 MSK было зафиксировано включение атри...
02.12.2021 11:55:08	S5 - Обнаружение нарушения политик ИБ		Закрыт	Сорокин Вадим Владимирович (Сорокин_ВВ@phd.ru)	Subject: [310087] Атрибут Не истекает срок действия пароля - Включён Добрый день. 2021-12-02 11:48:38 MSK было зафиксировано включение атри...
02.12.2021 11:45:08	S4 - Обнаружение атак на учетные записи, брутфорс		Назначен	Герман Юрий Владимирович (Герман_ЮВ@phd.ru)	Subject: [310068] Bruteforce с одного хоста на множество хостов внутри сети Добрый день. 2021-12-02 11:08:37 MSK зафиксирован Bruteforce с IP-ад...
02.12.2021 10:48:45	S5 - Обнаружение нарушения политик ИБ		Назначен	Рябенко Александр Викторович (Рябенко_АВ@phd.ru)	Subject: [310050] Успешный интерактивный вход не доменного пользователя Добрый день. 2021-12-02 10:27:44 MSK Система мониторинга обнаруж...
02.12.2021 10:48:45	S4 - Обнаружение атак на учетные записи, брутфорс		Назначен	Рябенко Александр Викторович (Рябенко_АВ@phd.ru)	Subject: [310043] Bruteforce с одного хоста на множество хостов внутри сети Добрый день. 2021-12-02 10:19:16 MSK зафиксирован Bruteforce с IP-ад...
01.12.2021 17:25:08	S5 - Обнаружение нарушения политик ИБ		Расследование	Сорокин Вадим Владимирович (Сорокин_ВВ@phd.ru)	Subject: [309915] Обнаружена загрузка HackTools на ПК Добрый день. 2021-12-01 17:01:36 MSK Касперский обнаружил загрузку ПО, относящиеся к ка...
01.12.2021 17:15:08	S5 - Обнаружение нарушения политик ИБ		Закрыт	Сорокин Вадим Владимирович (Сорокин_ВВ@phd.ru)	Subject: [309910] Атрибут Не истекает срок действия пароля - Включён Добрый день. 2021-12-01 16:55:12 MSK было зафиксировано включение атри...
01.12.2021 17:15:08	S5 - Обнаружение нарушения политик ИБ		Расследование	Сорокин Вадим Владимирович (Сорокин_ВВ@phd.ru)	Subject: [309911] Успешный интерактивный вход не доменного пользователя Добрый день. 2021-12-01 16:12:21 MSK Система мониторинга обнаруж...
01.12.2021 16:55:08	S3 - Обнаружение обхода средств защиты		Закрыт	Сорокин Вадим Владимирович (Сорокин_ВВ@phd.ru)	Subject: [309885] Добавление пользователя в критичную доменную группу Добрый день. 2021-12-01 16:33:45 MSK Системой мониторинга зафиксир...
01.12.2021 15:00:20	S5 - Обнаружение нарушения политик ИБ		Закрыт	Сорокин Вадим Владимирович (Сорокин_ВВ@phd.ru)	Subject: [309859] Успешный интерактивный вход не доменного пользователя Добрый день. 2021-12-01 14:25:29 MSK Система мониторинга обнаруж...
01.12.2021 14:30:09	S5 - Обнаружение нарушения политик ИБ		Назначен	Курочкин Никита Андреевич (Курочкин_НА@phd.ru)	Subject: [309850] Обнаружена загрузка HackTools на ПК Добрый день. 2021-12-01 13:55:20 MSK Касперский обнаружил ПО, относящиеся к категории ...
01.12.2021 13:45:08	S5 - Обнаружение нарушения политик ИБ		Назначен	Воропан Владимир Борисович (Воропан_ВБ@phd.ru)	Subject: [309842] Suspicious RDP connection Dear colleagues, At 2021-12-01 11:21:10 CET a suspicious RDP connection to the host SrVArPanth.packagin...
01.12.2021 12:35:08	S5 - Обнаружение нарушения политик ИБ		Назначен	Воропан Владимир Борисович (Воропан_ВБ@phd.ru)	Subject: [309774] Suspicious RDP connection Dear colleagues, At 2021-12-01 09:16:38 CET a suspicious RDP connection to the host srrvdata.packaging...
01.12.2021 12:05:10	S4 - Обнаружение атак на учетные записи, брутфорс		Назначен	Щадрин Виктор Андреевич (Щадрин_ВА@phd.ru)	Subject: [309776] Bruteforce с внешнего IP различных пользователей Добрый день. 2021-12-01 11:22:36 MSK зафиксирован Bruteforce с внешнего IP...
01.12.2021 12:05:09	S2 - Обнаружение сетевой атаки		Назначен	Курочкин Никита Андреевич (Курочкин_НА@phd.ru)	Subject: [309767] Обнаружена критичная сигнатура PT NAD (Source Address) Добрый день. 2021-12-01 11:04:49 MSK PositiveTechnologies NAD обнару...
01.12.2021 11:40:09	S1 - Обнаружение вируса, бот-сети		Реагирование	Герман Юрий Владимирович (Герман_ЮВ@phd.ru)	Subject: RE: [309746] Подозрительная (вирусная) активность на хосте Также на хосте было обнаружено ВПО HEUR:Trojan.Win32.Pincav.gen по пути: ...
01.12.2021 11:30:08	S1 - Обнаружение вируса, бот-сети		Реагирование	Герман Юрий Владимирович (Герман_ЮВ@phd.ru)	Subject: [309746] Подозрительная (вирусная) активность на хосте Добрый день. 2021-12-01 10:22:24 MSK Системой мониторинга зафиксирована по...
01.12.2021 10:30:10	S3 - Обнаружение обхода средств защиты		Закрыт	Сорокин Вадим Владимирович (Сорокин_ВВ@phd.ru)	Subject: [309734] Добавление пользователя в критичную доменную группу Добрый день. 2021-12-01 09:54:14 MSK Системой мониторинга зафиксир...
01.12.2021 10:00:10	S4 - Обнаружение атак на учетные записи, брутфорс		Назначен	Щадрин Виктор Андреевич (Щадрин_ВА@phd.ru)	Subject: [309727] Bruteforce с внешнего IP различных пользователей Добрый день. 2021-12-01 09:39:03 MSK зафиксирован Bruteforce с внешнего IP...
01.12.2021 09:40:22	S5 - Обнаружение нарушения политик ИБ		Назначен	Герман Юрий Владимирович (Герман_ЮВ@phd.ru)	Subject: [309716] Обнаружена загрузка HackTools на ПК Добрый день. 2021-12-01 09:03:51 MSK Касперский обнаружил ПО, относящиеся к категории ...
01.12.2021 09:35:09	S3 - Обнаружение обхода средств защиты		Закрыт	Рябенко Александр Викторович (Рябенко_АВ@phd.ru)	Subject: [309722] Добавление пользователя в критичную доменную группу Добрый день. 2021-12-01 09:22:43 MSK Системой мониторинга зафиксир...
01.12.2021 09:30:08	S4 - Обнаружение атак на учетные записи, брутфорс		Назначен	Хурден Егор Владимирович (Хурден_ЕВ@phd.ru)	Subject: [309713] Bruteforce с внешнего IP различных пользователей Добрый день. 2021-12-01 09:02:00 MSK зафиксирован Bruteforce с внешнего IP...
01.12.2021 08:30:09	S2 - Обнаружение сетевой атаки		Назначен	Щадрин Виктор Андреевич (Щадрин_ВА@phd.ru)	Subject: [309696] Сканирование хостов в сети Добрый день, 2021-12-01 07:25:33 MSK Антивирусом Касперского зафиксированы множественные спра...
30.11.2021 19:15:08	S2 - Обнаружение сетевой атаки		Закрыт	Сорокин Вадим Владимирович (Сорокин_ВВ@phd.ru)	Subject: [309637] Обнаружена критичная сигнатура PT NAD (Source Address) Добрый день. 2021-11-30 18:34:16 MSK PositiveTechnologies NAD обнару...
30.11.2021 17:45:08	S2 - Обнаружение сетевой атаки		Назначен	Воропан Владимир Борисович (Воропан_ВБ@phd.ru)	Subject: [309618] New signature for NGFW Palo Alto found Dear colleagues, At 2021-11-30 15:00:41 CET Palo Alto NGFW (THREAT virus) found a critical sig...
30.11.2021 13:42:55	Предоставление доступа к USB		Закрыт	Курочкин Никита Андреевич (Курочкин_НА@phd.ru)	Предоставление доступа к USB в рамках выполнения служебных обязанностей при во время проектных работ. Сроком до 01.03.2021.
30.11.2021 12:00:09	S1 - Обнаружение вируса, бот-сети		Закрыт	Щадрин Виктор Андреевич (Щадрин_ВА@phd.ru)	Subject: [309529] Подозрительная (вирусная) активность на хосте Добрый день. 2021-11-30 11:24:26 MSK Системой мониторинга зафиксирована по...
30.11.2021 11:55:09	S5 - Обнаружение нарушения политик ИБ		Закрыт	Щадрин Виктор Андреевич (Щадрин_ВА@phd.ru)	Subject: RE: [309531] Успешный интерактивный вход не доменного пользователя Добрый день. 2021-11-30 11:25:25 MSK Система мониторинга обна...
30.11.2021 11:40:08	S1 - Обнаружение вируса, бот-сети		Реагирование	Герман Юрий Владимирович (Герман_ЮВ@phd.ru)	Subject: [309518] Обнаружен критичный вирус Добрый день. 2021-11-30 11:01:19 MSK модулем Защита от файловых угроз Касперского зафиксирова...
30.11.2021 11:25:09	S2 - Обнаружение сетевой атаки		Назначен	Рябенко Александр Викторович (Рябенко_АВ@phd.ru)	Subject: RE: [309439] Обнаружена критичная сигнатура PT NAD (Source Address) Добрый день. Вредоносная активность с хоста 10.10.31.30 была за...
30.11.2021 10:45:09	S2 - Обнаружение сетевой атаки		Назначен	Рябенко Александр Викторович (Рябенко_АВ@phd.ru)	Subject: [309439] Обнаружена критичная сигнатура PT NAD (Source Address) Добрый день. 2021-11-30 10:27:00 MSK PositiveTechnologies NAD обнару...
30.11.2021 08:55:33	S3 - Обнаружение обхода средств защиты		Расследование	Хурден Егор Владимирович (Хурден_ЕВ@phd.ru)	Subject: [309405] УЗ удалена в течении 24 часов после создания Добрый день. 2021-11-30 08:23:23 MSK Системой мониторинга зафиксировано удал...
29.11.2021 16:35:09	S2 - Обнаружение сетевой атаки		Закрыт	Сорокин Вадим Владимирович (Сорокин_ВВ@phd.ru)	Subject: [309317] Обнаружена критичная сигнатура PT NAD (Source Address) Добрый день. 2021-11-29 15:59:02 MSK PositiveTechnologies NAD обнару...
29.11.2021 16:35:09	S3 - Обнаружение обхода средств защиты		Закрыт	Рябенко Александр Викторович (Рябенко_АВ@phd.ru)	Subject: RE: [309320] УЗ удалена в течении 24 часов после создания Также 2021-11-29 16:25:27 зафиксировано включение отключенной учетной запис...
29.11.2021 16:30:08	S2 - Обнаружение обхода средств защиты		Закрыт	Рябенко Александр Викторович (Рябенко_АВ@phd.ru)	Subject: [309320] УЗ удалена в течении 24 часов после создания Добрый день. 2021-11-29 16:14:00 MSK Системой мониторинга зафиксировано вклю...

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



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 MTC



Команда
реагирования
Сегежа Групп
ИБ+ИТ



	г. Москва	ООО «Сегежа групп»	ДИБ	
	ГТ 007-2021	Политика информационной безопасности ООО «УК «Сегежа групп»	Версия 2	Страница 1 из 15

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

**РЕГЛАМЕНТ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Обогащение инцидентов
из внешних систем

Настройка
файрволов

Активное
реагирование

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



Журналы
безопасности
ПК и
серверов



Журналы
антивируса



Журналы
файрволов



Журнал
анализатора
сетового
трафика

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.



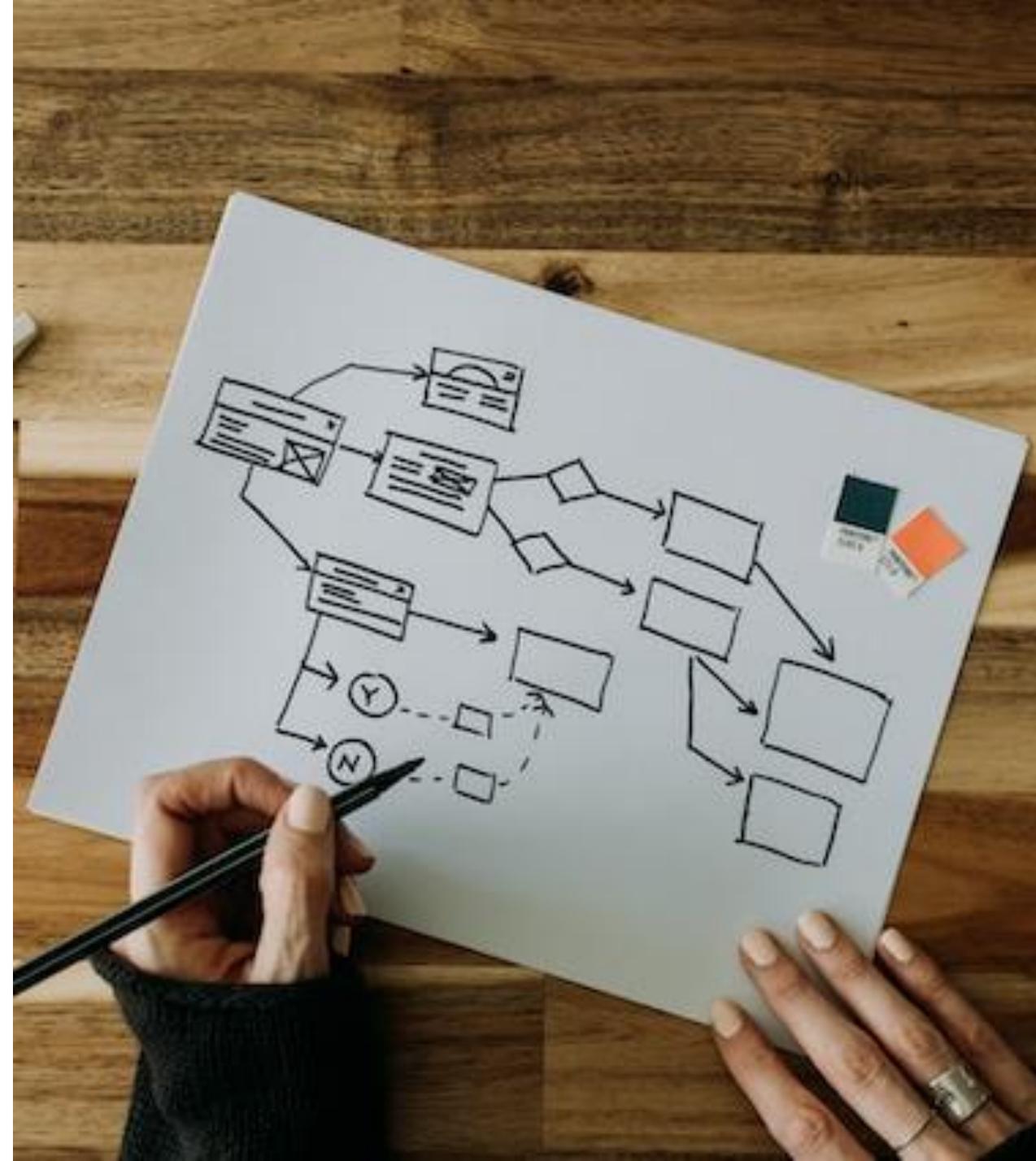
В феврале 2021 года были детектированы множественные вирусные атаки исходящие из г. Лесосибирск. В результате расследования была обнаружена врезка в кабель UTP, ведущая к точке доступа Wi-Fi, через которую работники цеха выходили в Интернет с личных зараженных устройств



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 СОС

The screenshot displays the GosSOPKA web application interface. At the top, there are navigation tabs for "Рекомендации", "Уведомления" (selected), and "Активы". A search bar is present with the placeholder text "Введите поисковый запрос...". Below the search bar is a table of notifications with the following columns: "Номер", "Название компании", "Описание события", "Статус", and "Дата создания".

Номер	Название компании	Описание события	Статус	Дата создания
SMTS-23-06-2941	ПАО "Сережа-групп"	09/06/2023 сотрудник субъекта ЗОКИИ несанкционировано переслал с корпоративной почты на личную почту, зарегистрированную на публичном почтовом сервере yandex.ru, на адрес: gbuzlanov@yandex.ru были отправлены в незашифрованном виде организационно-распорядительные документы, содержащие порядок реагирования на инциденты ИБ на ЗОКИИ (АСУТП Варочной установкой №4, АСУТП МТК №7, АСУТП Водогрейного котла, АСУТП Складом мазута), инструкции пользователей и администраторов, порядок контроля физического доступа к компонентам объектов.	Проверка НКЦКИ	14.06.2023 14:50
SMTS-23-06-2939	ПАО "Сережа-групп"	ЭТО ТЕСТОВОЕ УВЕДОМЛЕНИЕ! Троян HEUR:Trojan.Script.Generic Пользоват C:\Users\color\Operator\AppData\Local Data\Default\Cache\Cache_Data\1_00\F065001E07851BAFA7D283FB763C MD5: 5451D730382CE40081311B52 заблокировано работой СЗИ Антивир	Проверка НКЦКИ	5.05.2023 13:54
		Тестовое Уведомление ГосСОПКА 01/03/2023 сотрудником подразделения А были не правомерно высланы по эл. почте реестры с содержанием персональных данных третьему лицу. По факту инцидента выявлены несоответствия по		

On the right side of the interface, there is a "Фильтрация" (Filtering) panel with the following options:

- Тип уведомления: Выберите тип
- Дата выявления: Начиная с [calendar icon] Заключая датой [calendar icon]
- Статус реагирования: Выберите реагирование
- Категорирование ОКЗМ: Выберите
- Статус: Выберите статус
- Необходимость привнесения сил ГосСОПКА: [toggle switch]

At the bottom of the filtering panel is a "Сбросить" (Reset) button. The bottom of the screen shows a Windows taskbar with the date and time 11.07.2023 8:47.

Ваши вопросы

