SOC FORUM 2023

Успешный опыт создания Центра практической кибербезопасности

Цифровая трансформация Росреестра

ДАНИЛОВ Сергей Николаевич
Начальник управления ИБ

МОСКВА 2023

SOC
FORUM
2023

Данилов Сергей Николаевич

Начальник управления ИБ

Росреестр

SOC FORUM 2023

Цели

- Повышение практической защищенности информационных систем
- Обеспечение процессов обнаружения, предупреждения и ликвидации компьютерных атак
- Развитие ИБ в соответствии с нормативными требованиями

Исключить недопустимые для Росреестра **события** и обеспечить устойчивою работу ведомства в случае любой кибератаки

Выполненные задачи

1. Проанализированы сценарии недопустимых для Росреестра событий
2. Проведена практическая проверка реализации недопустимых событий
3. Проанализирована инфраструктура и сформировано целевое состояние ИБ Росреестра
4. Разработаны технический проект Центра и программа развития ИБ Росреестра на 2022-2025 гг.

6
Недопустимых событий

13
Целевых и ключевых ИС подлежащих защите

17
Проектов по развитию ИБ Росреестра

План развития

2021/25гг.

Начало пути и системные проблемы в ИБ

SOC FORUM 2023

СОТРУДНИКИ

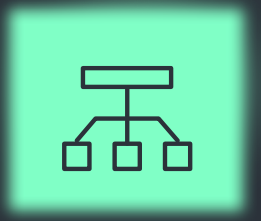
не понимают основ информационной безопасности

ОБЕСПЕЧЕНИЕ ИБ

сводится к формализму и бумажной безопасности

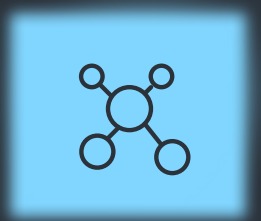
КОМАНДА РЕАГИРОВАНИЯ

отсутствует



ИНФРАСТРУКТУРА

построена без учета информационной безопасности



КЛЮЧЕВЫЕ СИСТЕМЫ

разработаны без учета информационной безопасности

ПОСТАВЩИКИ УСЛУГ

не могут обеспечить оперативную скорость исполнения настроек безопасности

SOC FORUM 2023

Недопустимые события

Нарушение работы ключевых информационных систем

Подмена сведений в реестрах и фондах данных

Полная или частичная утрата данных

Блокировка рабочих станций и серверов сотрудников

Утечки конфиденциальной информации и ПДн

Нелегальное использование ресурсов Росреестра

Информационные системы

13

целевых и ключевых ИС подлежащих защите

+ унаследованные системы (архивные ИС)

+ перспективные разработки

+ используемые сторонние ИС

SOC FORUM 2023

Текущие результаты в направлении Центра

Развернута **инфраструктура ИБ и внедрены базовые процессы,** обеспечивающее **мониторинг** и исключение недопустимых событий Росреестра

Базовые процессы

Мониторинг событий ИБ	**Реагирование** на инциденты ИБ
Управление активами	**Управление** уязвимостями

Технологии

- Secret Net Studio
- Сертифицированная ОС
- Kaspersky Endpoint Security
- MaxPatrol SIEM
- MaxPatrol VM
- MaxPatrol O2
- PT NAD
- vGate
- PT AF
- PT XDR
- PT Sandbox
- Континент

Дальнейшие улучшения

- Расширение области действия Центра на перспективные целевые информационные системы, масштабирование Центра на территориальные управления Росреестра
- Включение требований по результативной ИБ в нормативные документы ведомства и обеспечение их выполнения с последующей практической проверкой
- Определение и исключение недопустимых событий ИБ при проектировании новых и модернизации существующих информационных систем
- Внедрение дополнительных технологий (IDM, DLP, PAM) и развитие процессов ИБ

SOC FORUM 2023

Текущие результаты мониторинга Центра

Развернутый мониторинг позволяет видеть
и анализировать события информационной безопасности

Еженедельно около

30 **тысяч событий в секунду** анализируются средствами мониторинга

Автоматически регистрируются более

45 **тысяч событий подозрительной активности** в неделю

Из них около **115 инцидентов** в неделю, требующих реагирования со стороны специалистов ведомства

Контролируется безопасность **20 тыс. ИТ-активов** в информационной инфраструктуре Росреестра

Работа мониторинга позволила специалистам Росреестра выявить и отреагировать на случаи:

- Превышений служебных полномочий
- Установок и использования хакерского ПО
- Попыток несанкционированного доступа
- Действий способных привести к утечке парольной информации
- Атак на сетевую инфраструктуру (сканирование)
- Атак через попытки подбора парольных данных
- Атак через попытки эксплуатации уязвимости на серверах
- Использования запрещённых сервисов
- Атак на прикладное ПО

Развитие направления Центра

SOC FORUM 2023

Расширение области покрытия мониторинга
и исключение всех недопустимых событий

Процессы

Мониторинг событий ИБ

Реагирование на инциденты ИБ

Управление активами

Управление уязвимостями

\+

Защита от целенаправленных атак

Управление недопустимыми событиями

\+ **контроль**

Контроль эффективности Центра

Контроль безопасных конфигураций

Верификация недопустимых событий и **Киберучения**

Технологии

Расширение сенсоров и зоны покрытия

- DLP
- IDM
- PAM

\+

Настройки безопасной конфигурации

- ИТ-инфраструктуры
- Целевых и ключевых систем

\+

Безопасная разработка ПО

Расширение области действия Центра

\+ Все целевые информационные системы

\+ Неизолированные ключевые информационные системы

\+ Полный сетевой периметр Росреестра

Основные вехи

SOC FORUM 2023

2021

Мониторинг и исключение выборочных недопустимых событий в ограниченной пилотной зоне

2 из 13 ИС
4 из 7 сенсоров

2022

Расширение зоны мониторинга и перечня исключенных недопустимых событий

9 из 13 ИС
5 из 7 сенсоров
1 из 2 метапродуктов

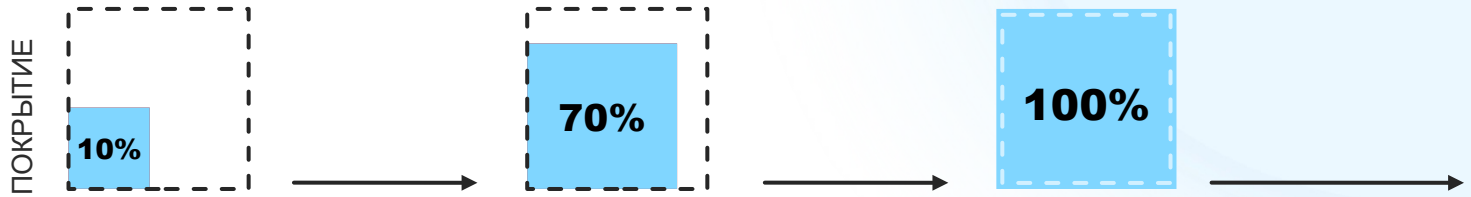
2023

Полное покрытие мониторингом инфраструктуры Росреестра и исключение всех недопустимых событий

ВСЕ ИС
ВСЕ сенсоры
ВСЕ метапродукты

2024

Автоматизация исключения недопустимых событий и проверка результата на киберучениях



- \+ Донастройка ИТ и ИБ систем
- \+ Подготовка и проведение киберучений
- \+ Продолжение покрытия мониторингом управлений Росреестра

! Участие в роли защитников в кибербитве Standoff

SOC FORUM 2023

РОСРЕЕСТР обеспечивает защищенность цифровых сервисов

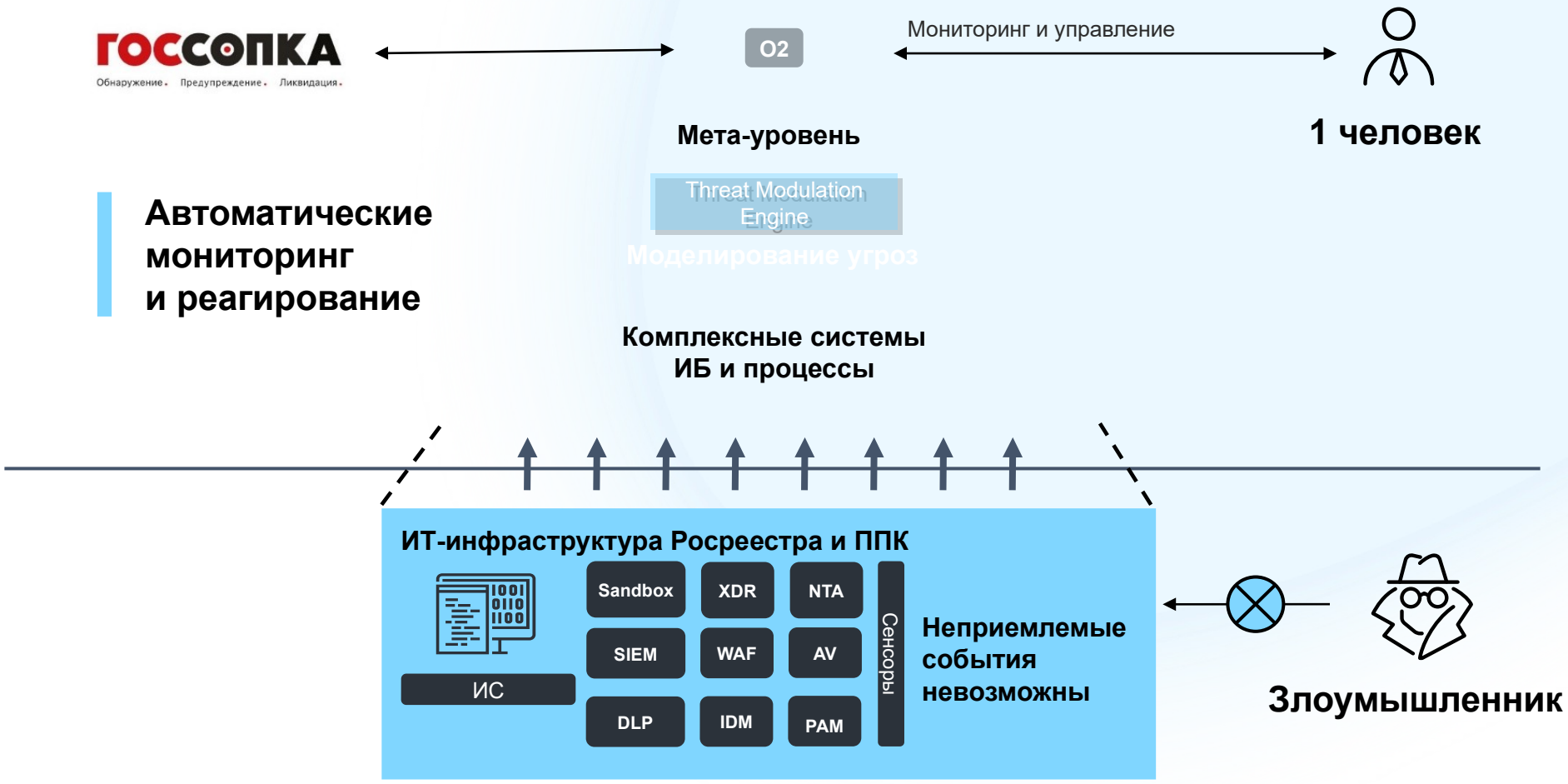
Центр делает возможным достижение стратегических целей и цифровую трансформацию Росреестра **без киберкатастроф**

Результаты

- Невозможность утечек персональных данных
- Функционирование ведомства не прерывается из-за хакерских атак
- Невозможность утечек персональных данных
- Функционирование ведомства не прерывается из-за хакерских атак

Исключить недопустимые для Росреестра события и обеспечить устойчивую работу в случае любой кибератаки

Целевая архитектура безопасности центра. 2024 год



Как предотвратить наступление недопустимого?

SOC FORUM 2023

- **Применять риск-ориентированный подход для построения эффективной системы защиты**
- Провести обновление и следить за актуальностью программного обеспечения
- Проверять хранение ключевой информации на рабочих станция, применять сложные пароли сотрудникам и пользователям сайтов
- Проводить регулярные тестирования на проникновение и анализ защищенности систем

- утверждение недопустимых событий
- построение центра противодействие киберугрозам, деятельность которого направлена на предотвращение недопустимых событий
- проведение киберучений для оценки эффективности центра противодействие киберугрозам и разработки программы его улучшения

SOC FORUM 2023

Спасибо!