



Ритейл 2026

Единый контур ИБ в ритейле



Контекст

Распределённая инфраструктура и множество источников данных



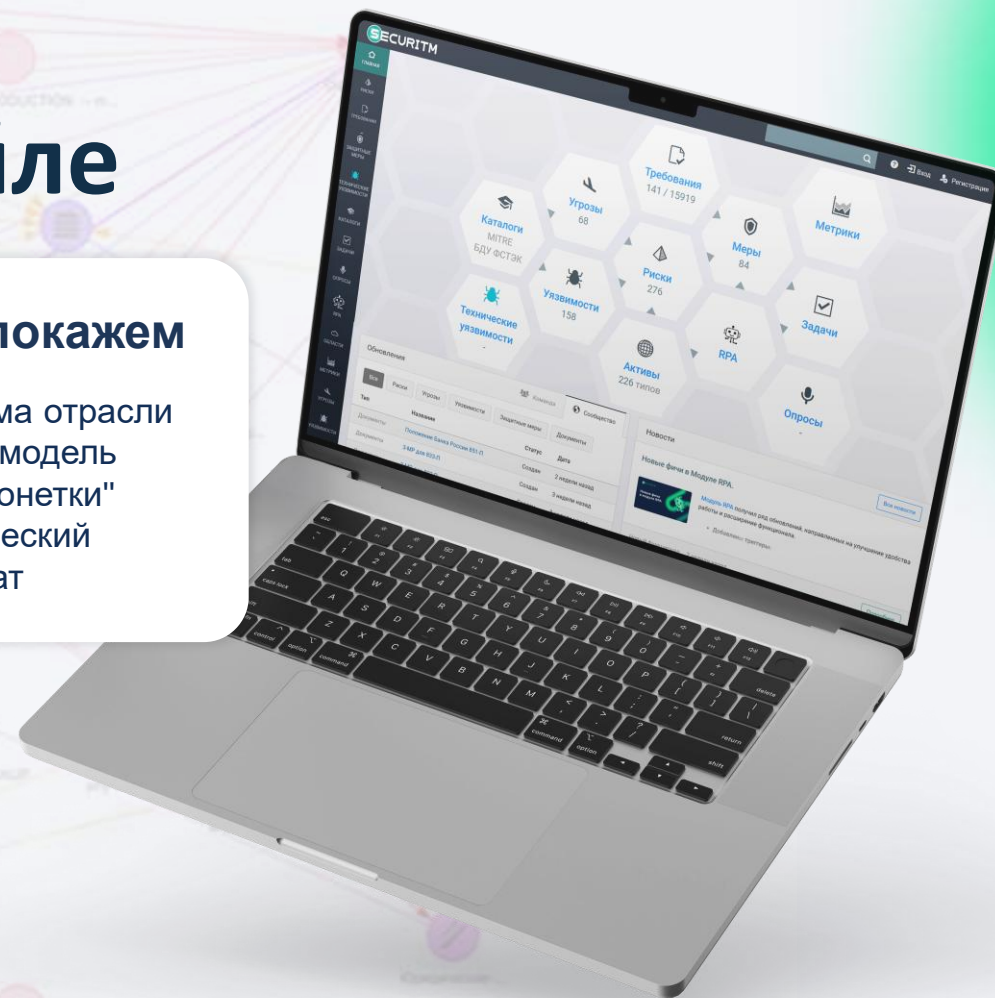
Фокус

- Активы
- Риски
- Требования
- Уязвимости



Что покажем

- Проблема отрасли
- Единая модель
- Кейс "Монетки"
- Практический результат



Активы • Риски • Требования • VM



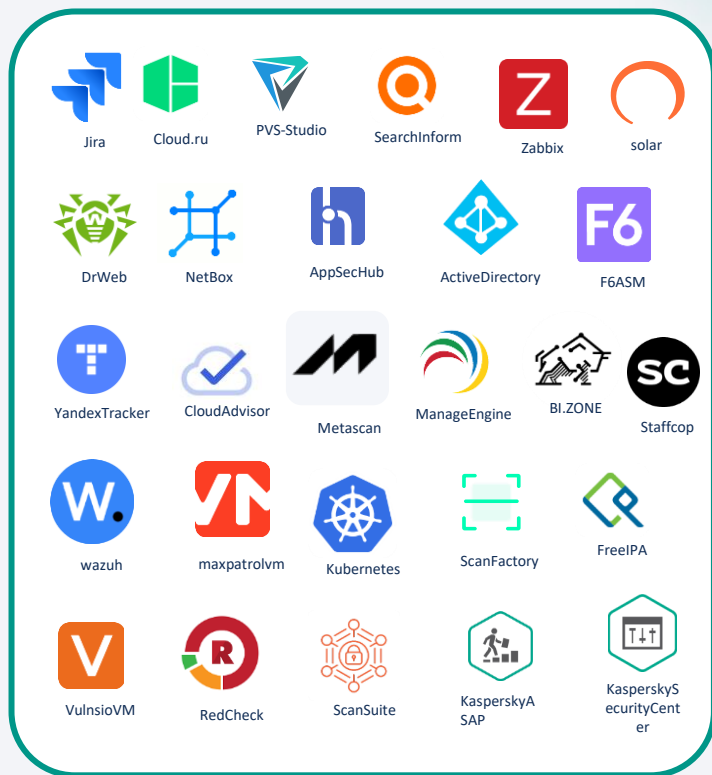
Максим Шаманаев
SECURITM

securitm.ru

**В ритейле ИБ - это умение соединять технологии,
риски, людей и бизнес-цели.**



Прямые интеграции

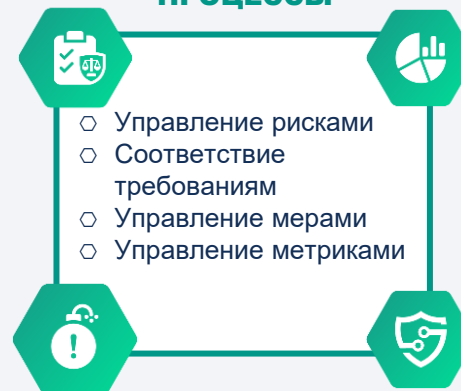


- API
- Импорт файлов csv / xls / cer/crt
- Сетевые хранилища

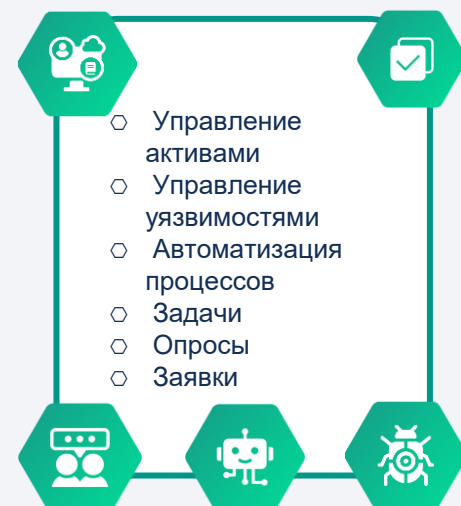
ВНЕШНИЕ/
ВНУТРЕННИЕ
ТРЕБОВАНИЯ ПО ИБ



СТРАТЕГИЧЕСКИЕ
ПРОЦЕССЫ



ОПЕРАЦИОННЫЕ
ПРОЦЕССЫ



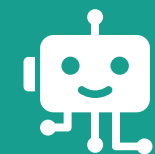
АНАЛИЗ



ОТЧЕТНОСТЬ



АВТОМАТИЗАЦИЯ





повышает эффективность службы ИБ



Меры

Учет организационных и технических мероприятий



Задачи

Таск-менеджер для операционной работы



Требования

Соответствие требованиям регуляtorики и стандартов по ИБ



Риски

Управление ИБ на базе риск-ориентированного подхода



Каталоги

БДУ ФСТЭК, MITRE ATT&CK



Активы

Учет и управление любыми типами активов



RPA

Robotic process automation - автоматизация задач



Метрики

Конструктор метрик для процессов ИБ



Уязвимости

Агрегатор отчетов от сканеров безопасности



Опросы

Сбор сведений с работников и контрагентов, Service Desk



Области

Централизованный контроль и адаптация процессов



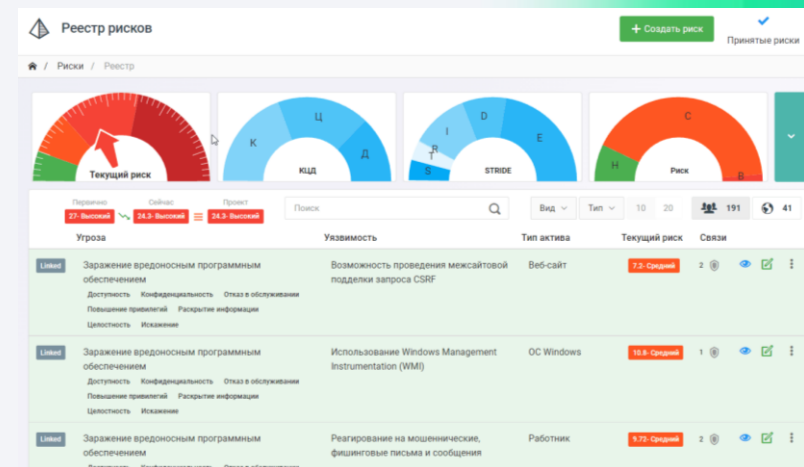
AI

Ассистент для ускорения анализа и приоритизации



Конструктор документов

Конструктор документов с готовыми шаблонами



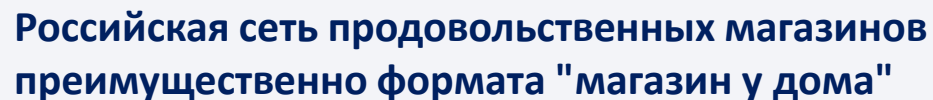
**БЕСПЛАТНАЯ
COMMUNITY-ВЕРСИЯ
SECURITM**



**> 6000
ПОЛЬЗОВАТЕЛЕЙ В
COMMUNITY-ВЕРСИИ**



**ОТКРЫТАЯ ЦЕНА
ПОНЯТНЫЕ ТАРИФЫ**



44 000 активов
в распределённой
инфраструктуре



- LDAP
- AB3
- ИТ-мониторинг
- VM



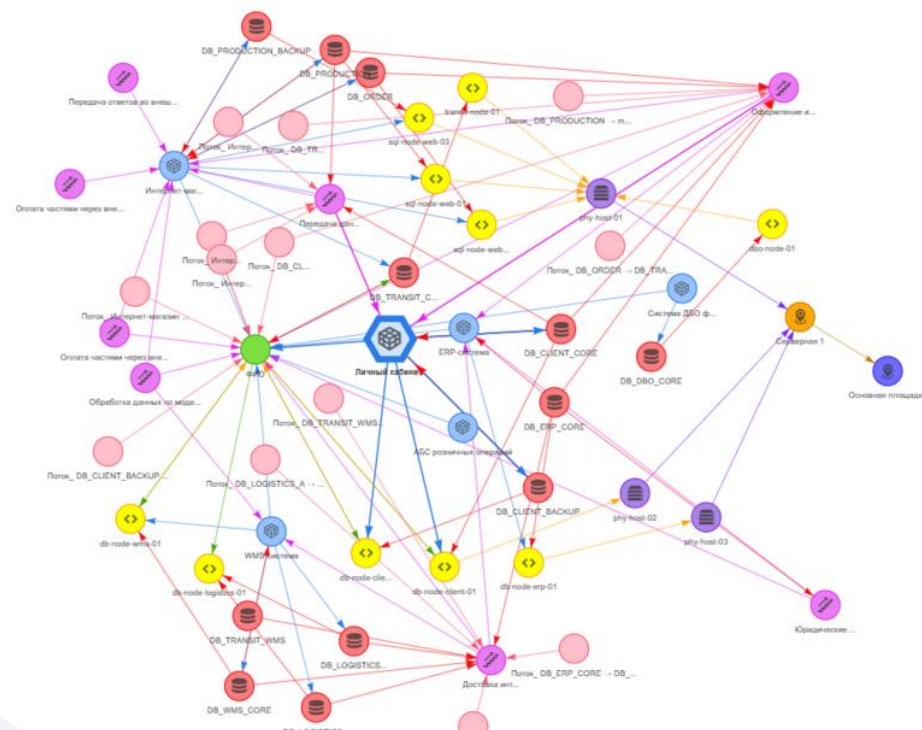
- Риски
- Соответствие
- Технические уязвимости
- ИСПДн
- КИИ



активы, владельцы
и контроль исполнения
связаны в одной модели

Пример связанной модели

Демонстрационные данные





Актив: актив - точка сборки контекста

Информационная
система

Демонстрационные
данные



Технические данные

система, размещение,
узлы и связи



Бизнес- контекст

владелец, процессы,
назначение и критичность



Что меняется

Одна карточка связывает
инфраструктуру, ПДн, риски
и применимые требования.



Результат

понятно, что затронуто
и кто отвечает

Активы / Система / Информационная система персона... / Личный кабинет клиента

Личный кабинет клиента

Информационная система персональных данных, в нескольких местах расположения
Клиентский контур личного кабинета / мобильного приложения.

Приоритет: 2. Средний

Динамические типы активов: Информационная система персональных данных

Владелец:

Администратор:

Области: Клиентские сервисы

Персональные данные

Категории ПДн	Иные
Категории субъектов ПДн	
Категории субъектов ПДн	
Уровень защищенности ПДн	УЗЗ
Действия, совершаемые с ПДн	сбор; запись; хранение; уточнение (обновление, изменение); использование; удаление
Состав документов, предоставляемых субъектами ПДн	
Условия окончания обработки ПДн	
Осуществляется трансграничная передача ПДн	Нет
Срок обработки (хранения) ПДн	

Содержание (2)

- Оформление интернет-заказа (Процесс обработки персональных данных)
- Передача данных во внешний маркетинговый сервис (Процесс обработки персональных данных)

Размещение (2)

- db-node-client-02 (Операционная система)
- db-node-client-01 (Операционная система)
- phy-host-02 (Физический сервер)
- Серверная 1 (Серверное помещение)
- Основная площадка (Площадка)



VM: Уязвимость получает контекст и приоритет



VM



Актив



Информационная
система

Демонстрационные
данные



Источник

данные VM и сканеров
безопасности



Связь

- хост
- система
- владелец



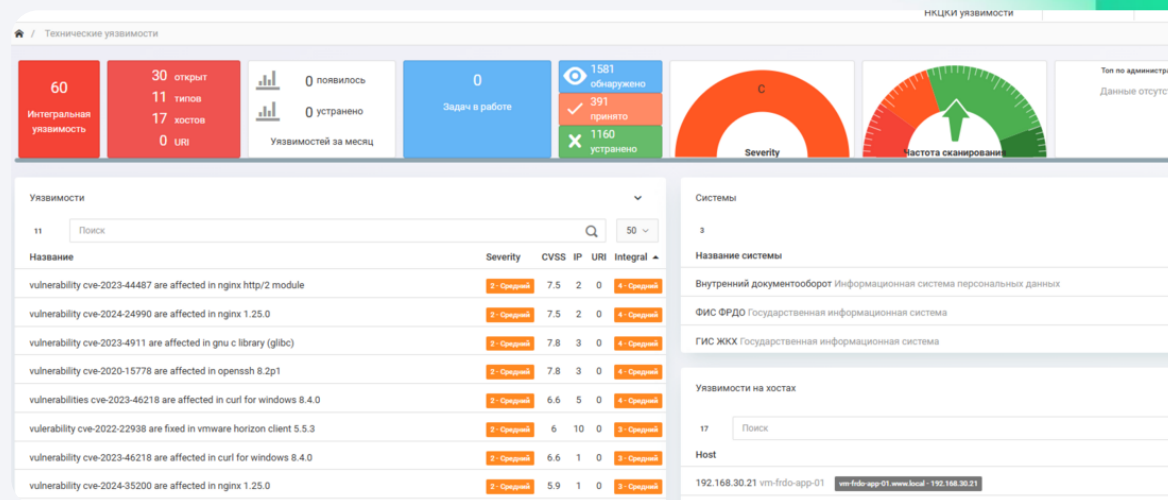
Действие

Приоритет зависит
не только от CVSS, но
и от критичности
связанного актива.



Результат

видно, что исправлять
первым





RPA: Автоматизация превращает состояние в действие



Мера



Задача



свидетельство



Условие

событие, срок
или изменение объекта



Задача

ответственный, срок
и инструкция



Свидетельство

Результат выполнения
возвращается в защитную
меру и общий контроль.



Результат

контроль не заканчивается
уведомлением

Изменение защитной меры

Общее

Цепочка мер

☒ Задачи

Риски

Требования

Ресурсы

Созда

Установка антивирусной защиты рабочих станций - сбор свидетельств

Включе

Периодичность

0 0 ***

Инструкция

Требуется собрать свидетельства для определения работоспособности системы АВЗ.



Шаблон функционирует исправно. Последняя задача, созданная по шаблону, еще не завершена.



Контроль. Руководитель видит приоритеты, а не тысячи строк

Дашборд

Демонстрационные
данные



Показатели

активы, меры, инциденты
и контрольные процедуры



Детализация

до объекта, владельца
и ответственного



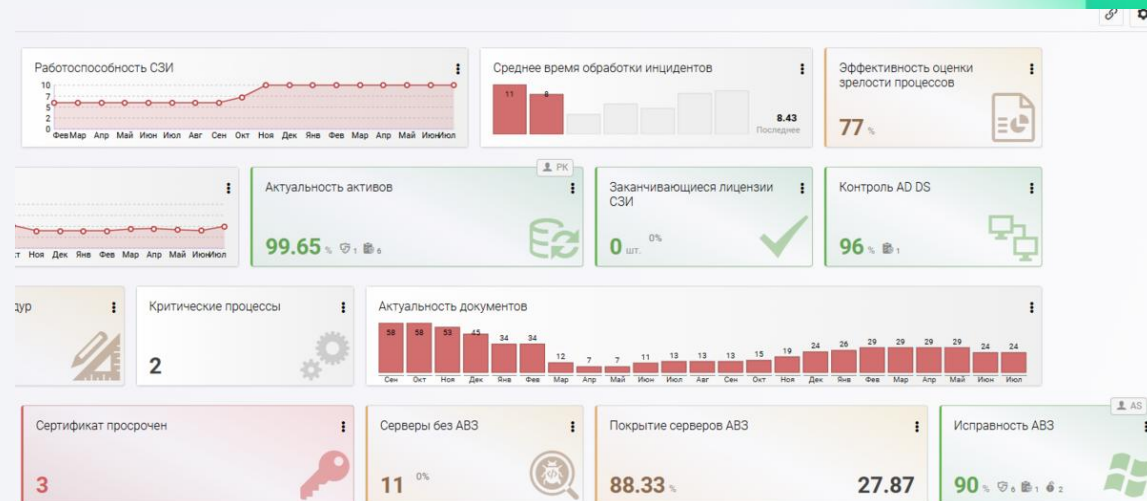
Управление

Результат выполнения
возвращается в защитную
меру и общий контроль.



Результат

единая картина
без ручной сборки отчёта

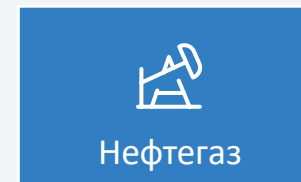
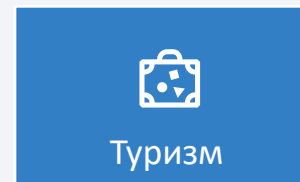
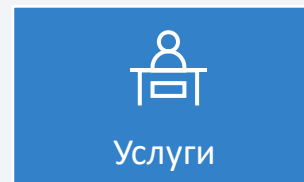
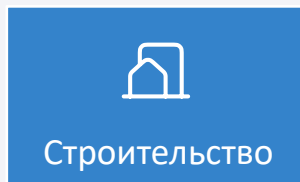
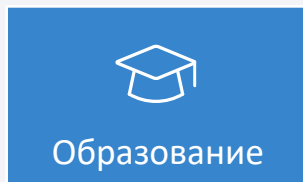
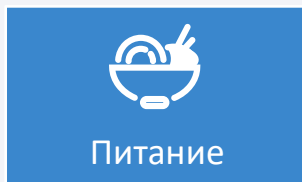
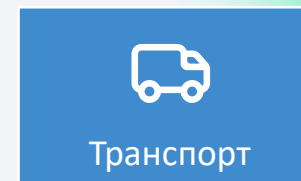
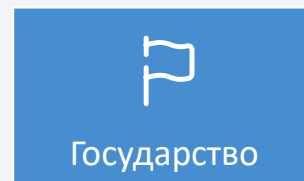
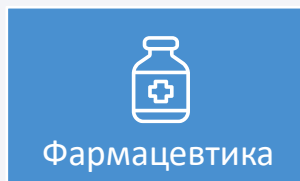
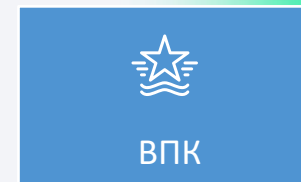
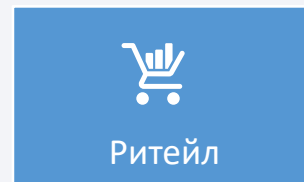
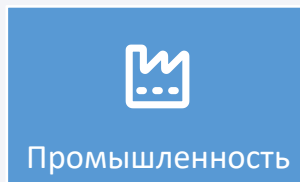
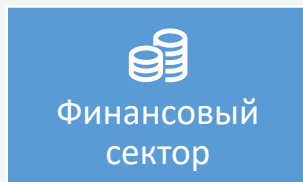


SECURITM - стандарт управления процессами ИБ

ЭТО ПОДТВЕРЖДАЮТ

 **> 100**
ЗАКАЗЧИКОВ

 **> 6000**
ПОЛЬЗОВАТЕЛЕЙ
В COMMUNITY-ВЕРСИИ



КОМИТЕТ
ПО ИНФОРМАТИЗАЦИИ
И СВЯЗИ САНКТ-ПЕТЕРБУРГА





service.securitm.ru



@SECURITM



max.ru/id7820074059_biz

✉ info@securitm.ru
☎ 8 800 300 37 64
🌐 securitm.ru



**СПАСИБО
ЗА ВНИМАНИЕ!**