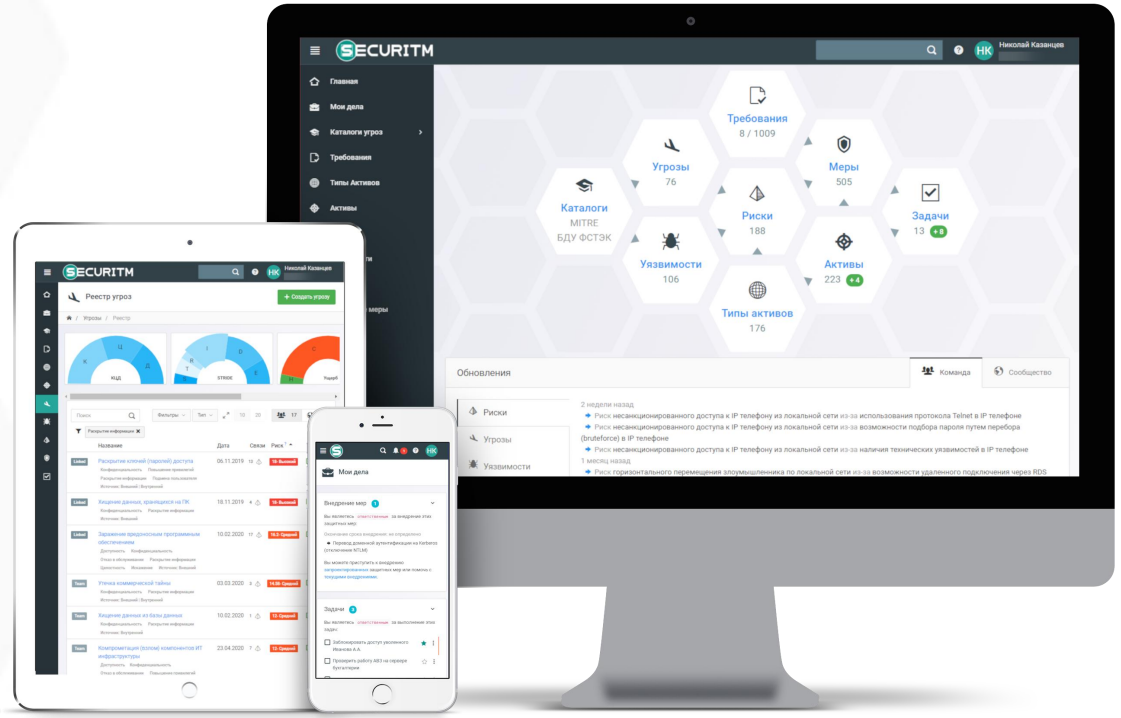
# Сервис управления информационной безопасностью

для корпоративных служб информационной безопасности

B2B SaaS / ПО




securitm.ru

# Чем больше инвестиций в безопасность – тем меньше эффективность

Развитие системы защиты

Рост количества процессов, рутины и ошибок

Деградация системы защиты

**> 40%** утечек и нарушений происходят из-за **низкой эффективности процессов** в службе безопасности*

**С развитием системы защиты приходят проблемы:**

- Высокая **зависимость** от человеческого фактора
- Непрозрачность **инвестиций** в безопасность
- Нехватка и дороговизна **кадров**
- Высокие операционные затраты на **рутину**

**При этом старые проблемы никуда не уходят:**

- **Инциденты** безопасности продолжают происходить нанося финансовый и репутационный ущерб
- Регуляторы продолжают выявлять **несоответствия**

* Исследования vc.ru и tadviser.ru

# SECURITM решает проблему деградации систем защиты

**SECURITM** – это система класса **SGRC** (Security Governance, Risk and Compliance), которая помогает службам информационной безопасности средних/крупных компаний автоматизировать свои процессы управления безопасностью на единой платформе.

*SECURITM - это Jira для служб безопасности*

## ФУНКЦИОНАЛ

- ✓ Управление **рисками** безопасности
- ✓ Контроль **соответствия** требованиям (Compliance)
- ✓ Управление **активами** (ITAM)
- ✓ Планирование, **задачи** и процессы
- ✓ Управление **уязвимостями** (VM)
- ✓ Проведение **опросов**
- ✓ Автоматизация (RPA)

## ВЫГОДЫ

- ✓ **Отсутствие зависимости** от человеческого фактора благодаря цифровизации знаний и процессов
- ✓ **Минимизация затрат** на безопасность за счет обоснованного распределения ресурсов
- ✓ **Снижение ручного труда** службы безопасности через автоматизацию рутинных операций
- ✓ **Повышение защищенности** компании благодаря правильной оценке рисков безопасности

Для продаж – CRM, для производства – ERP, **для безопасности – SECURITM**

# Технологии

## Подходы

- ✓ База Community
- ✓ Социальная платформа
- ✓ Динамические расчеты
- ✓ Авто-операции
- ✓ Универсальные методики
- ✓ Рекомендательная модель

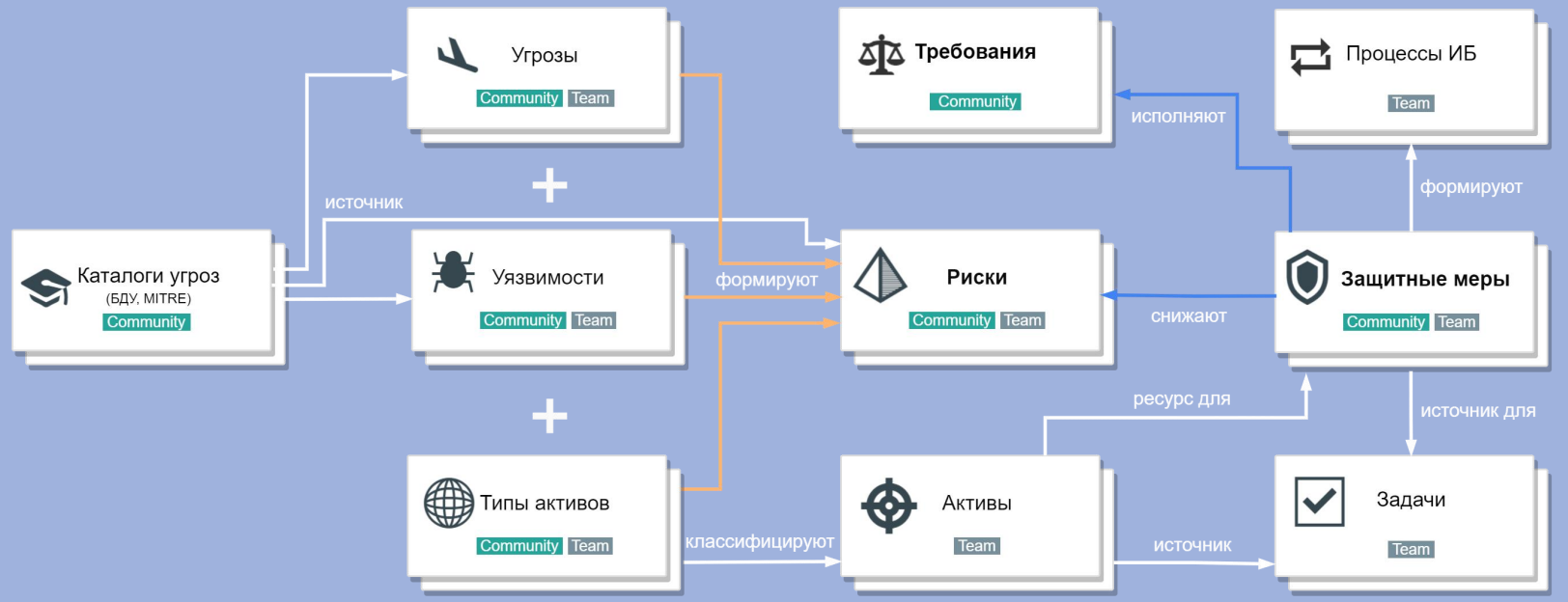
## Интеграции

- ✓ API
- ✓ Active Directory
- ✓ DNS
- ✓ Сканеры безопасности
- ✓ Samba
- ✓ Atlassian Jira
- ✓ Excel/CSV
- ✓ Mail
- ✓ Telegram/Teams
- ✓ ….

Экземпляры системы

SaaS — API — On premise

Функциональные модули




Контейнеры Docker

- СУБД — MySQL/MariaDB
- Web Server — NGINX / Apache
- Application — PHP/JS

Операционная система — Astra Linux / Alt Linux / Ubuntu Server / CentOS

# Риски

## Проблема

Полноценное управление безопасностью требует риск-ориентированного подхода, но

- **Нет методологии/инструмента** - непонятно как управлять рисками
- **Нет данных** - долго и сложно сформировать полный и объективный реестр рисков
- **Нет понимания** - как риски информационной безопасности влияют на цели компании
- **Много рутины** - не хватает времени и сил на поддержание процесса

## Решение

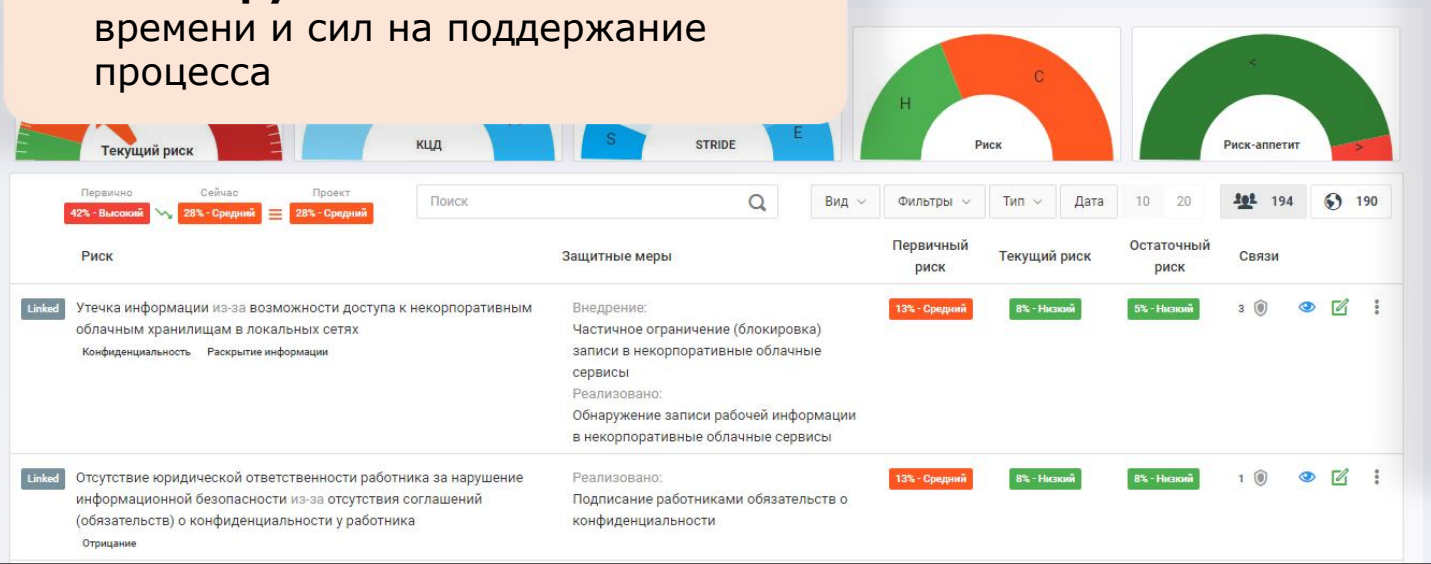
Управление рисками в SECURITM:

- Готовая **база** рисков, подстраивающаяся под активы компании
- Обогащение рисков через **каталоги** MITRE ATT&CK и БДУ ФСТЭК
- **Связь** рисков с активами компании и требованиями комплаенса
- Настраиваемые **методики** оценки
- **Планы** обработки и связь рисков с защитными мерами
- Динамический **расчет** и непрерывная переоценка рисков
- Контрольный **след** и отчетность по всем операциям

## Результат

Автоматизированный процесс управления рисками ИБ, позволяющий:

- **Запустить** управление рисками и получить первые результаты за 5 минут
- **Экономить** время и отказаться от рутинных операций
- Сэкономить и **обосновать** бюджет на информационную безопасность
- **Понять** причины и установить приоритеты в работе службы безопасности
- **Говорить** с бизнесом на одном языке



# Compliance

**Проблема**

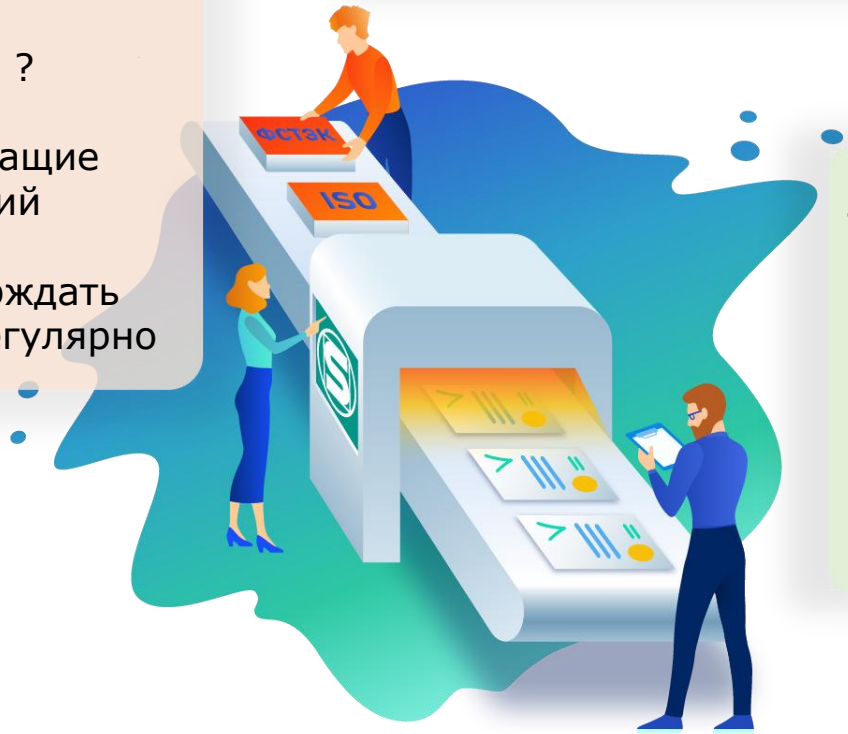
Исполнение требований регуляторов, стандартов, бизнеса и контрагентов - основа информационной безопасности, но

- **Требований много**
  и документы дублируют друг друга, приходится делать одинаковую работу для разных документов
- **Нет конкретики**
  как исполнять требования ?
- **Нет смысла**
  Не понятны причины, лежащие в основе многих требований
- **Много рутины**
  Контролировать и подтверждать соответствие требуется регулярно

**Решение**

Управление внешними и внутренними требованиями в SECURITM:

- Готовая **база нормативных актов** отечественных и международных регуляторов, стандартов и лучших практик
- Готовая **связь одинаковых требований** из разных документов
- Возможность **добавления собственных документов** и требований
- Ручная или автоматическая **оценка исполнения требований**
- Приоритезация требований через **риски** безопасности компании
- Непрерывная переоценка уровня соответствия
- Контрольный **след** по всем операциям




**Результат**

Автоматизированный процесс управления требованиями ИБ, позволяющий:

- Непрерывно **контролировать** соответствие множеству требований и документов
- **Подтвердить** соответствие перед внешними и внутренними аудиторами
- **Экономить** время на повторном контроле и избавиться от дублирующих операций

# Управление активами

## Проблема

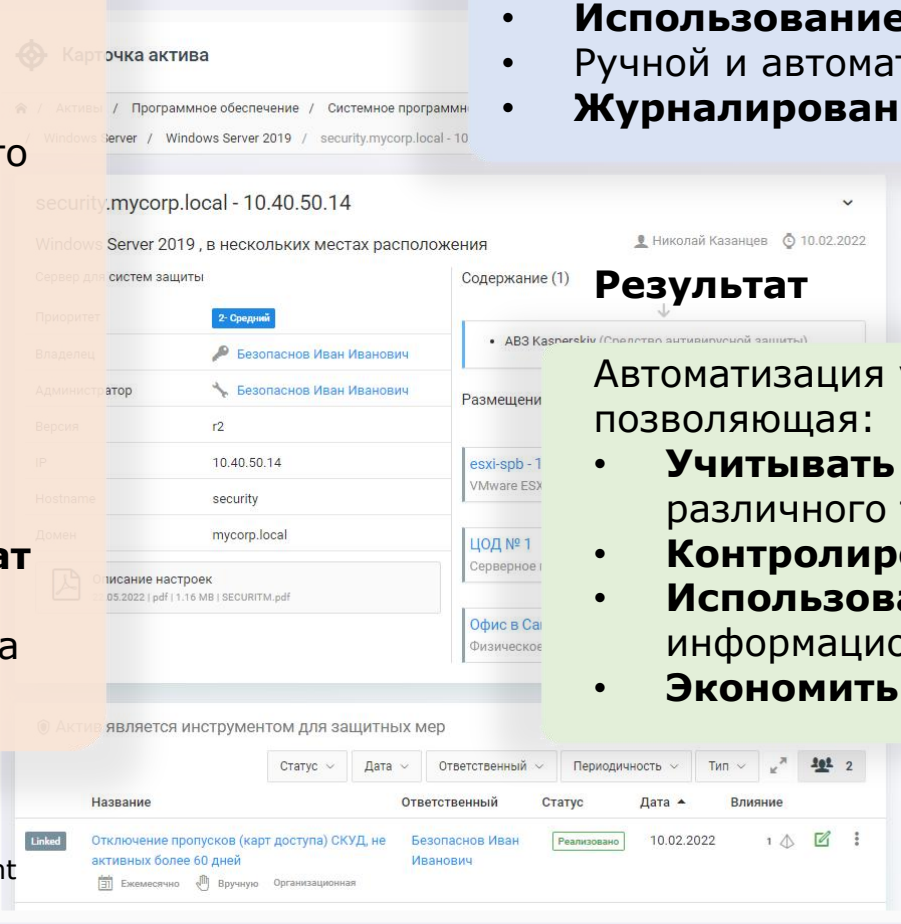
Не понимая что защищать - невозможно построить эффективную систему защиты. Нужно учитывать активы,
но

- **Активы разные**
  Серверы, ПО, СЗИ, ЭП, люди, информация, процессы – все это активы, подлежащие учету
- **Активы связаны**
  и без понимания взаимосвязей невозможно оценить их приоритеты
- **Активы быстро меняются**
  а реестры в Excel моментально устаревают
- **Активы кому-то принадлежат**
  и без понимания кто владелец/администратор актива им невозможно управлять

## Решение

Управление активами в SECURITM:

- **Учет** активов любого типа
- Построение **информационной модели** компании
- Автоматический расчет **приоритетов** и поиск **владельцев/администраторов** через связи активов
- **Поля** в зависимости от типа актива и возможность создавать собственные поля
- **Использование** активов во всех процессах SECURITM
- Ручной и автоматический **импорт** / обновление
- **Журналирование** всех изменений и **архив** активов




## Результат

Автоматизация управления активами, позволяющая:

- **Учитывать** в одном месте активы различного типа
- **Контролировать** жизненный цикл активов
- **Использовать** активы в процессах информационной безопасности
- **Экономить** время при работе с активами

* ITAM – information technology asset management

# Операционная работа

**Проблема**

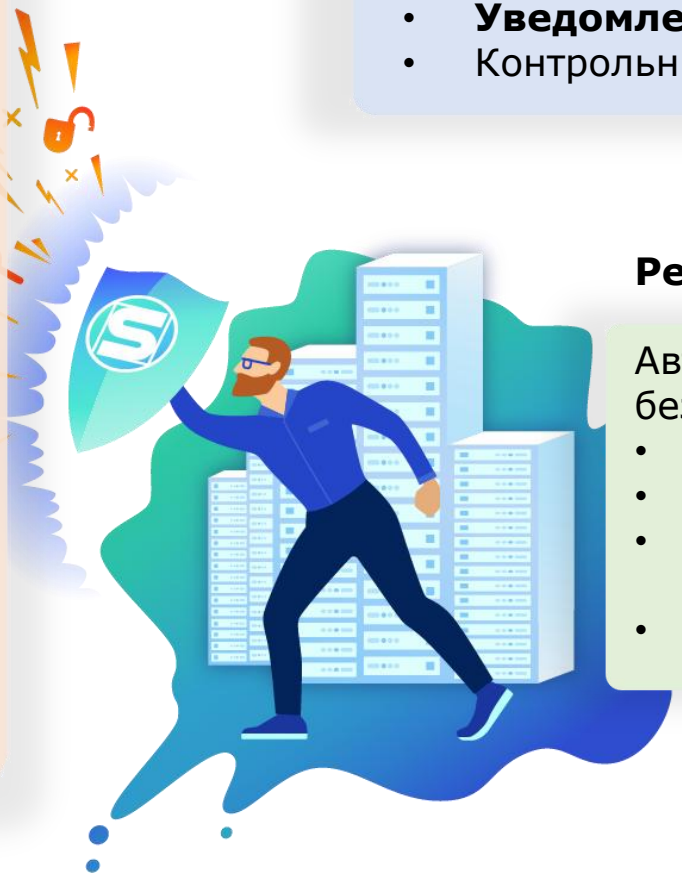
Система информационной безопасности состоит из множества защитных мер, средств защиты, процессов и задач, требующих поддержки,
но

- **Нет контроля**
  Задачи теряются и не исполняются, сроки срываются
- **Нет приоритета**
  Непонятно влияние защитных мер на безопасность компании
- **Нет учета**
  Что и для чего было сделано службой безопасности
- **Нет контекста**
  Отсутствует связь проводимых работ
  с активами, включая людей и информационные системы,
  с рисками и требованиями

**Решение**

Управление процессами и задачами информационной безопасности в SECURITM:

- Учет **защитных мер** на всем их жизненном цикле
- Готовая **база** защитных мер
- Формирование **планов** работ и **отчетов**
- **Таск-менеджер** с привязкой к активам, защитным мерам, рискам и требованиям
- Создание **регулярных** задач по шаблону
- **Уведомления** (mail, Telegram, MS Teams)
- Контрольный **след** по всем операциям



**Результат**

Автоматизация процессов информационной безопасности, позволяющая:

- **Контролировать** все процессы и задачи
- **Оценивать** нагрузку на ответственных лиц
- **Оптимизировать** затраты на поддержание защитных мер
- **Экономить** время работников

# VM*

## Проблема

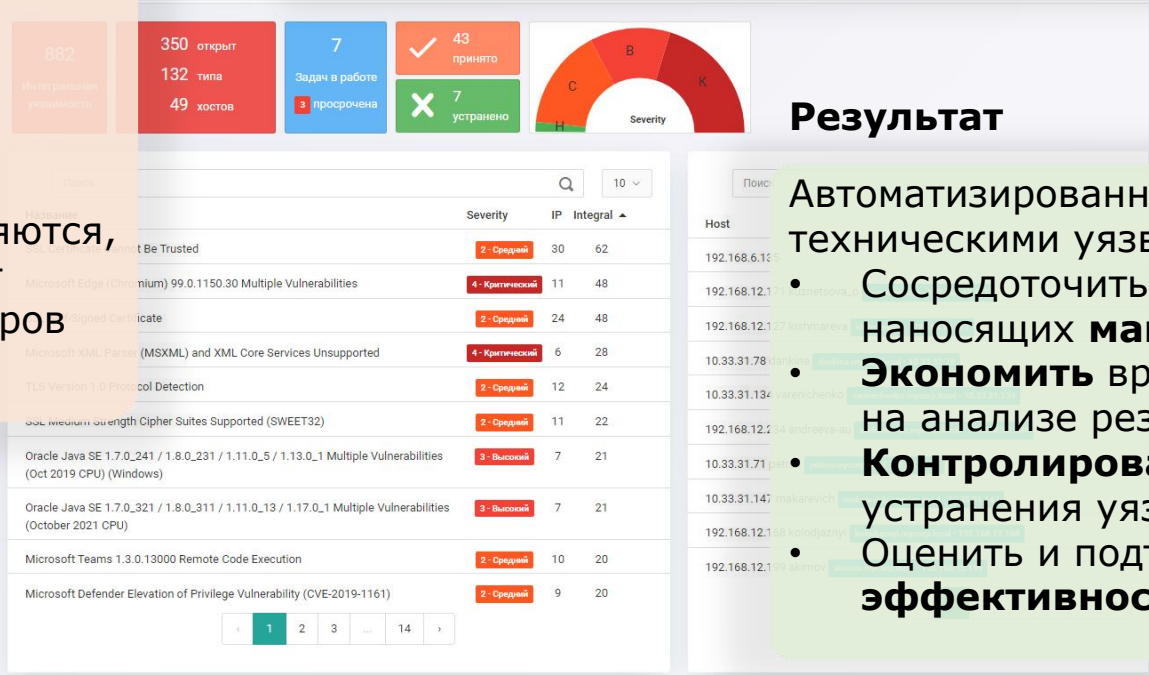
Для поиска технических уязвимостей внедряются сканеры безопасности, но одного сканирования инфраструктуры недостаточно, ведь:

- **Нет приоритета**
  Как оценить уязвимости основываясь на целях бизнеса и критичности активов?
- **Много мусора**
  Сотни страниц отчетов с уязвимостями
- **Нет контроля исполнения**
  Задачи ставятся и не исполняются, как связать таск-менеджмент с результатами работы сканеров безопасности?

## Решение

Управление техническими уязвимостями в SECURITM:

- **Интеграция** с несколькими сканерами уязвимостей одновременно
- Процессы **принятия рисков** (исключений) для уязвимостей
- Автоматическое формирование **задач**, с напоминаниями и контролем исполнения, привязкой к конкретным уязвимостям, группам уязвимостей, активам.
- Механизмы **обсуждения** проблем и ведения базы знаний
- Формирование **метрик** эффективности по процессу
- Контрольный **след** по всем операциям




## Результат

Автоматизированный процесс управления техническими уязвимостями, позволяющий:

- Сосредоточиться на уязвимостях, наносящих **максимальный урон** компании
- **Экономить** время на анализе результатов сканирования
- **Контролировать** процессы устранения уязвимостей
- Оценить и подтвердить **эффективность** процесса

* Vulnerability management

# Кейсы

Одна из компаний группы СБЕРа после ухода с рынка РФ сканеров безопасности (**Nessus, Qualys**) воспользовалась #SECURITM + nmap/vulners восстановив процесс **управления уязвимостями**

Фарм.компания проводит **аудиты безопасности поставщиков** через модуль комплаенса в облачной версии #SECURITM сократив свои временные затраты в несколько раз

Финтех компания провела в #SECURITM комплаенс по ГОСТ 57580, показала результаты на **внешнем аудите** и получила лицензию ЦБ

Крупный строительный холдинг в первую неделю эксплуатации локальной версии перевел в #SECURITM процессы учета **СКЗИ** и **ИТ-активов**

Компания разработчик ПО (входит в ТОП 30 самых дорогих компаний рунета) на пилоте создала в #SECURITM ресурсно-сервисную модель и провела **оценку рисков** по ключевым бизнес-процессам

Заказчик с помощью модулей активов и опросов #SECURITM построил процесс учета и актуализации **процессов обработки персональных данных**,

# Лицензирование

от 0 до 1,3 млн ₽

Калькулятор: https://securitm.ru/#price

SaaS

1. Облачный сервис
2. Выделенный сервер

On premise

3. ПО (лицензия)

+

- ✓ Модуль управления активами (ITAM)
- ✓ Модуль управления рисками
- ✓ Модуль управления соответствием (Compliance)
- ✓ Модуль управления задачами
- ✓ Модуль управления техническими уязвимостями

- Россия, Санкт-Петербург
- Аккредитованная ИТ компания
- В Реестре отечественного ПО
- Резидент Сколково

Новости и обновления:
https://t.me/securitm

8 800 300 37 64 **ПОЗВОНИТЬ**

info@securitm.ru **НАПИСАТЬ**

securitm.ru **ПОПРОБОВАТЬ**