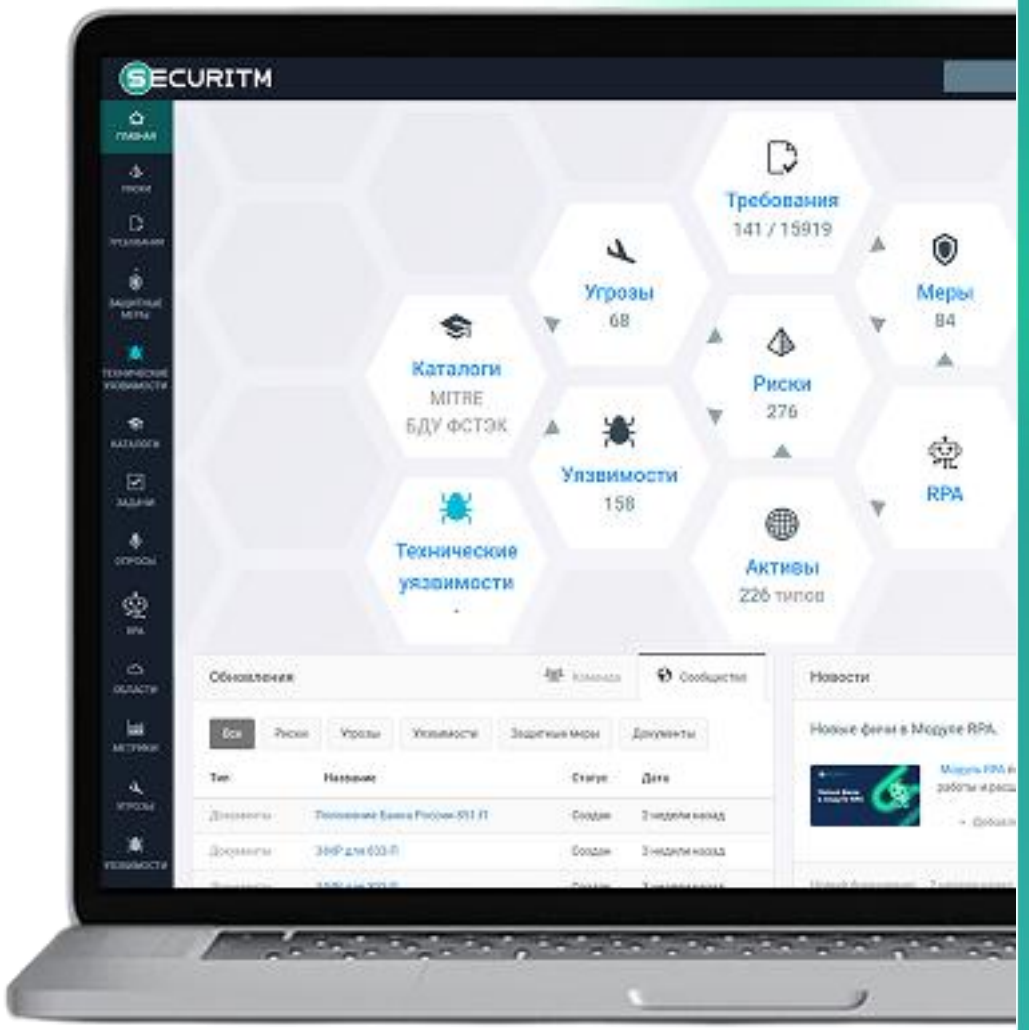
SECURITM

Система управления информационной безопасностью

SGRC AM VM IRP SOAR RPA BI AI CMDB Service Desk



securitm.ru

ООО «СЕКЪЮРИТМ»

Разработчик одноименного ПО класса SGRC / IRP / ITAM / VM/ ASOC

Сервис управления информационной безопасностью SECURITM

ФСТЭК России

Sk Сколково

- Появились в 2020 году
- Аккредитованная ИТ компания
- Есть лицензии ФСТЭК России:
  - на ТЗКИ
  - на разработку СрЗКИ
- Участник Сколково

Минцифры России

В реестре отечественного ПО

ФСТЭК России

Сертификат соответствия ФСТЭК России по 4 уровню доверия. № 5019 от 25.12.2025 в реестре сертифицированных средств защиты информации

РАЗРАБОТАНО БЕЗОПАСНИКАМИ ДЛЯ БЕЗОПАСНИКОВ

Основной мотивацией создания сервиса стала практическая потребность в доступном и эффективном едином решении, которое позволяло бы удобно и оперативно взаимодействовать со всеми аспектами защиты, управления уязвимостями и контроля состояния систем в режиме единого окна.

Развитие системы защиты в организации

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 все еще происходят
- нанося финансовый и репутационный ущерб;
- Регуляторы продолжают выявлять несоответствия;
- Процессы ведутся в разрозненных таблицах Excel
- и неспециализированных системах, что приводит к путанице данных, отсутствию данных в реальном времени и простой путанице в большом потоке информации.

Основные тренды в отрасли:

- Усиление регуляторных требований
- Технологический суверенитет объектов КИИ
- Рост ответственности за утечки
- Персональная ответственность руководителей за ИБ объектов КИИ*

на **25%** в среднем **увеличивается количество атак** на инфраструктуры компаний в год*

~60% компаний отмечают, что кибершпионаж и утечка конфиденциальной информации являются ключевыми проблемами бизнеса*

20-25% Нехватка квалифицированных кадров от текущей численности сотрудников ИБ*

* Б1. НА ЗАЩИТЕ ЦИФРОВОЙ ЭКОНОМИКИ: РЫНОК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

SECURITM повышает эффективность службы ИБ

Меры
Учет организационных и технических мероприятий

Задачи
Таск-менеджер для операционной работы

Требования
Соответствие требованиям регуляторики 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

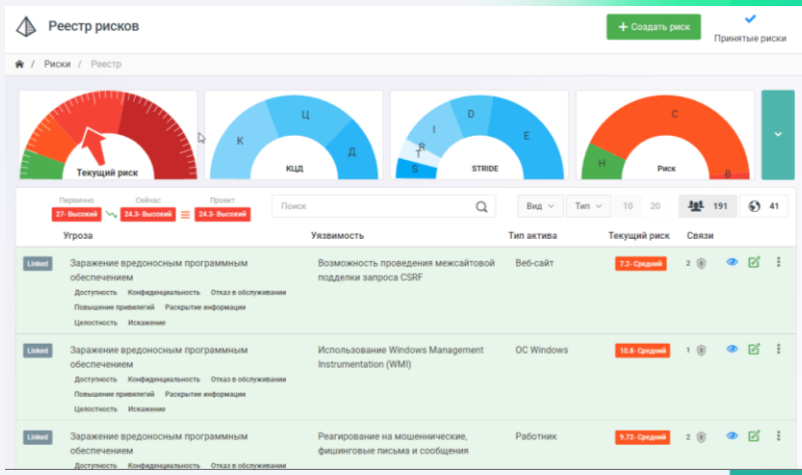
Уязвимости
Агрегатор отчетов от сканеров безопасности

Опросы
Сбор сведений с работников и контрагентов, Service Desk

Области
Централизованный контроль и адаптация процессов

AI
Ассистент для ускорения анализа и приоритезации

Конструктор документов
Конструктор документов с готовыми шаблонами



БЕСПЛАТНАЯ COMMUNITY-ВЕРСИЯ SECURITM

> 4000 ПОЛЬЗОВАТЕЛЕЙ В COMMUNITY-ВЕРСИИ

ОТКРЫТАЯ ЦЕНА ПОНЯТНЫЕ ТАРИФЫ

Модули SECURITM

Конструктор документов
Документация для объектов ПДн, КИИ, ГИС, банковских систем и других направлений.

Единая система показателей по ИБ
Конструктор организационных и технических показателей, формируемых от СЗИ, ИТ и опросов, дашборды руководителя, влияние метрик на риски и compliance.

Искусственный интеллект
Обогащение модулей SECURITM рекомендациями от ИИ

Планирование и контроль работ по ИБ
Управление проектами в привязке к требованиям и рискам безопасности.

Анкетирование и Service Desk
Сбор данных от сотрудников и контрагентов - оценка соответствия, актуализация активов, ознакомления и обучение, сбор обратной связи и заявок.

Контроль соответствия требованиям
Ручная и автоматическая оценка соответствия по 130+ стандартам, проведение аудитов, чеклисты и бэнчмарки.

Помогает управлять ИБ в крупных организациях
Обеспечивает централизованный контроль и адаптацию процессов под нужды дочерних структур.

Управление рисками ИБ и ИТ
Реестры и планы обработки рисков, интеграция с БДУ и MITRE, ручная и автоматическая оценка.

Единый таск-менеджер для ИБ-команды
Все что нужно для идеального управления задачами + полная интеграция в процессы ИБ.

БДУ ФСТЭК, MITRE ATT&CK, CVE, НКЦКИ

Управление техническими уязвимостями
Агрегация данных от сканеров инфраструктуры, периметра, кода, контейнеров и веб-приложений. Обогащение из БДУ и НКЦКИ, приоритезация по ФСТЭК, ручное и автоматическое управление процессом VM.

Учет и управление активами
Создание единой цифровой модели: ИТ-активы, СЗИ, документация, заявки и инциденты. Интеграция с СЗИ/ИТ системами, контроль изменений, кастомизация форм и автоматизации.

Автоматизация рутинных задач
Настройка сценариев реагирования и автоматизированных операций.

УПРАВЛЕНИЕ АКТИВАМИ

Модуль активов (АМ) — это единая цифровая модель компании, объединяющая всё, что имеет ценность: IT-инфраструктуру, ПО, данные, людей и процессы. SECURITM помогает собрать и актуализировать информацию об активах, связывая их с владельцами и процессами ИБ. Активы становятся живым элементом системы безопасности, а не просто реестром.

Проблема

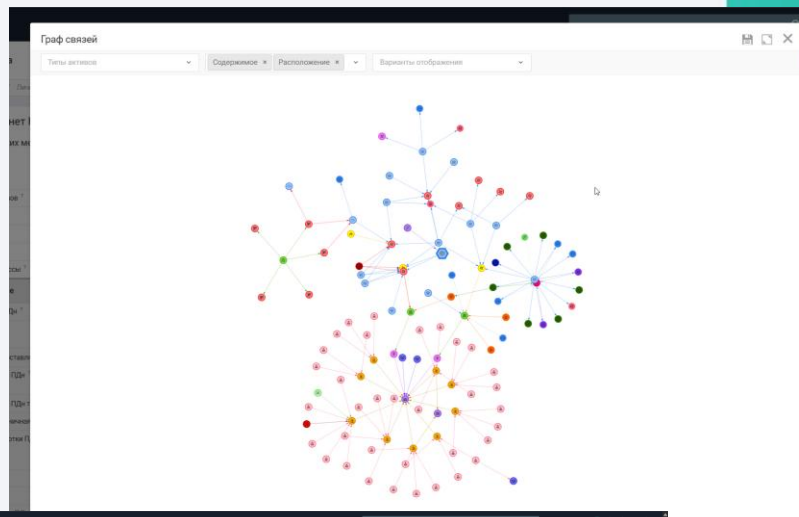
Не понимая что защищать - невозможно построить эффективную систему защиты. Нужно учитывать активы, но

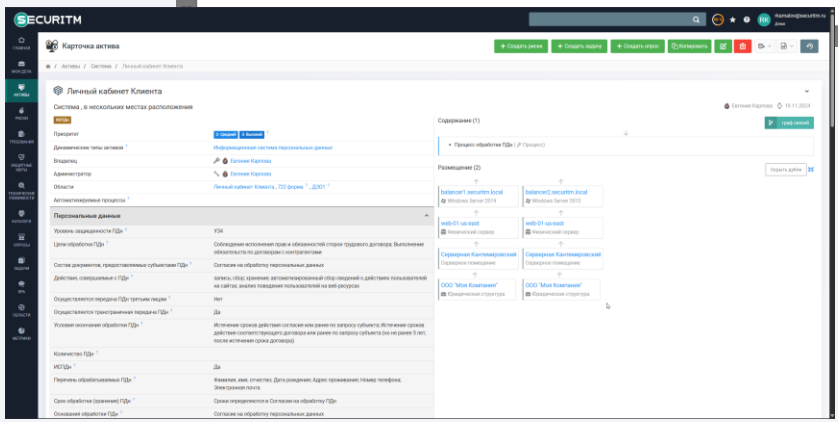
- **Активы разные**
  Серверы, ПО, СЗИ, ЭП, люди, информация, процессы – все это активы, подлежащие учету
- **Активы связаны**
  и без понимания взаимосвязей невозможно оценить их приоритеты
- **Активы быстро меняются**
  а реестры в Excel моментально устаревают
- **Активы кому-то принадлежат**
  и без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

УПРАВЛЕНИЕ ТРЕБОВАНИЯМИ

Модуль Compliance помогает системно подходить к соответствию требованиям, устраняя дублирование и ручной труд. Система автоматически объединяет пересекающиеся требования, актуализирует нормативную базу и позволяет проводить как ручные, так и автоматические проверки.

Проблема

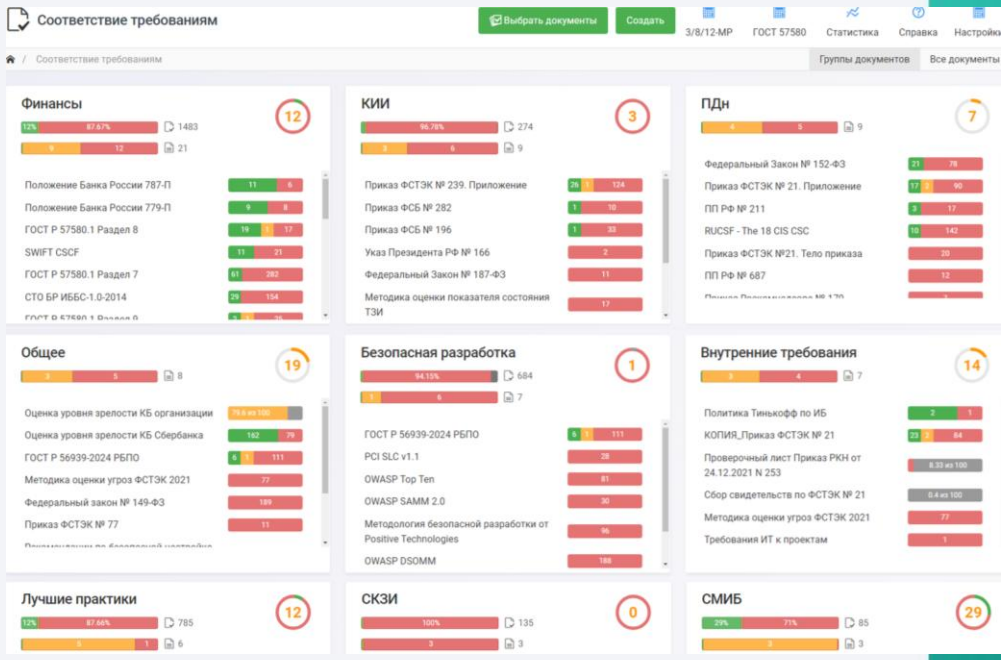
Управление соответствием требованиям превращается в трудоёмкий процесс:

- Повторяющиеся требования из разных нормативных документов и стандартов
- Высокие трудозатраты на подготовку к каждому аудиту
- Нет чётких инструкций по исполнению требований на практике
- Разрозненность информации о статусе соответствия требованиям

Решение

От хаоса к структурному управлению требованиями:

- База из 130+ стандартов и нормативных документов
- Автоматическая корреляция требований и устранение дублей
- Возможность добавления внутренних регламентов и политик компании
- Ручная и автоматическая оценка соответствия требованиям
- Контроль изменений законодательства и регулярная актуализация требований
- Связь модуля с активами, рисками, инцидентами и уязвимостями



Результат

Минимум ручной работы, максимум прозрачности:

- Аудиты проходят в 3 раза быстрее благодаря автоматизации
- Экономия времени за счёт устранения повторных операций
- Все требования собраны в одной актуальной системе
- Снижение трудозатрат на 20–40% за счет устранения повторяющейся работы
- Подтверждение соответствия без ручного сбора документов
- Интеграция комплаенса в единую систему управления ИБ

УПРАВЛЕНИЕ РИСКАМИ

Модуль RM (Risk Management) помогает эффективно управлять рисками, обеспечивая автоматическую приоритизацию, связь с активами и мерами защиты. SECURITM позволяет быстро оценивать риски на основе угроз и уязвимостей, упрощая процессы анализа, планирования и отчетности, а также обеспечивая прозрачность для бизнеса и аудиторов.

Проблема

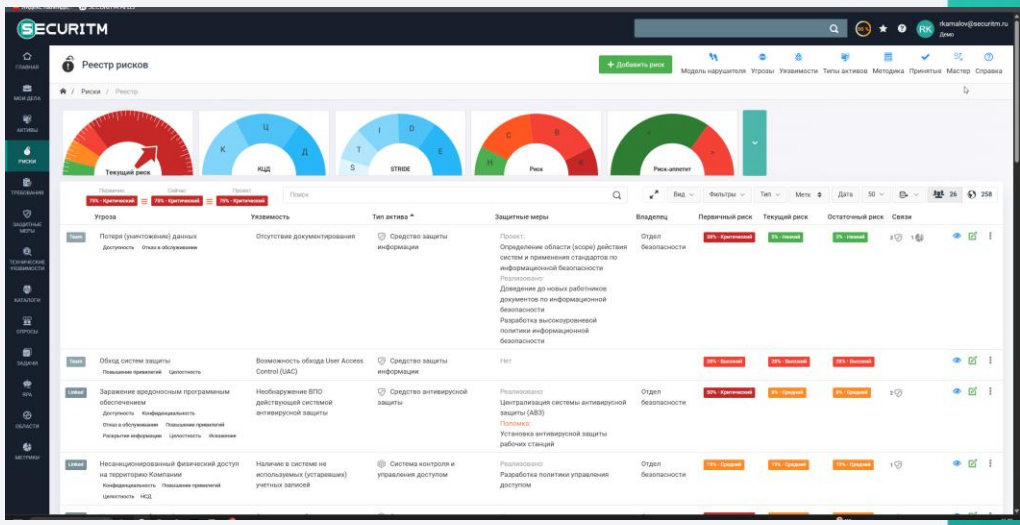
Управление рисками остаётся неструктурированным и трудоёмким:

- Нет методологии — риски фиксируются вручную, без единого подхода
- Данные фрагментированы — риски не связаны с активами и уязвимостями
- Сложно оценить влияние рисков на бизнес и операционные процессы
- Невозможно обосновать приоритеты управления и бюджет на ИБ

Решение

SECURITM делает управление рисками системным и управляемым:

- Готовая база рисков, адаптирующаяся под инфраструктуру компании
- Обогащение рисков через MITRE ATT&CK и БДУ ФСТЭК
- Автоматическая идентификация и оценка критичности риска
- Связь рисков с защитными мерами и формирование плана реагирования
- Динамический расчет и переоценка риска
- Отчётность и контрольный след для руководства и аудиторов



Результат

Управление рисками становится простым и эффективным:

- Быстрый запуск управления рисками без сложной настройки
- Автоматизация анализа рисков и избавление от рутины
- Связь рисков с активами, угрозами и мерами защиты
- Приоритизация — система показывает, что закрывать в первую очередь
- Прозрачность для бизнеса: риски описаны в понятных терминах

УПРАВЛЕНИЕ МЕРАМИ

Модуль защитных мер помогает системно управлять мерами безопасности, связывая их с рисками, активами и задачами. SECURITM помогает оценивать эффективность внедрённых мер и позволяет планировать ресурсы, отчёты и внедрение с учётом приоритетов и рисков

Проблема

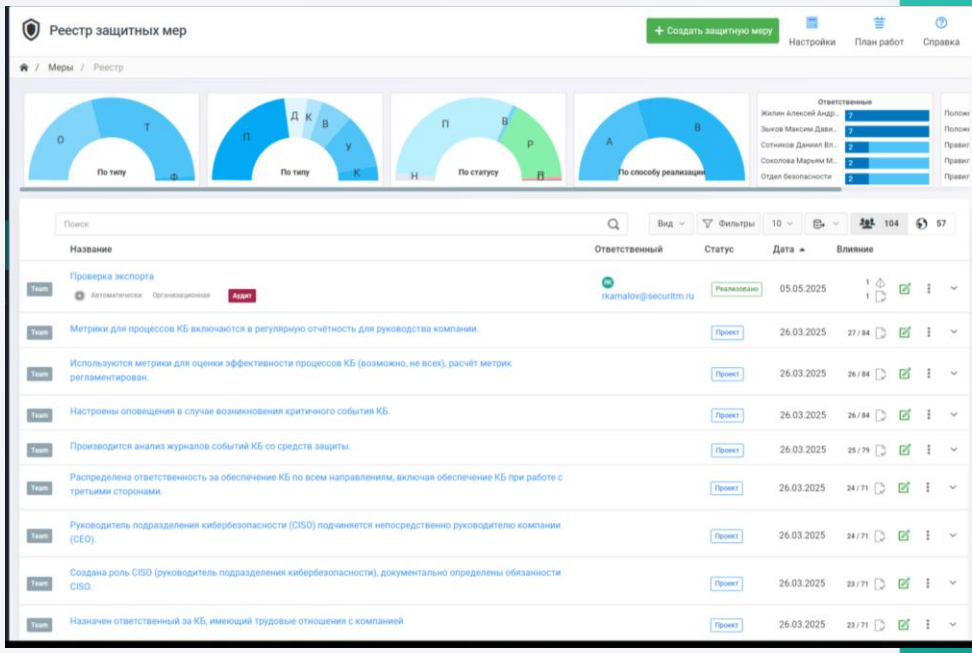
Управление защитными мерами затруднено:

- Отсутствие учёта и статуса внедрения мер безопасности
- Нет приоритизации — сложно определить критичные зоны
- Разрозненные данные — нет единого представления о реализованных задачах и закрытых рисках
- Отсутствие связи с другими процессами ИБ — меры не интегрированы с активами, рисками и задачами

Решение

SECURITM упрощает управление защитными мерами:

- Единый учёт всех мер безопасности: каталог мероприятий и привязка к активам
- Оценка эффективности: система показывает какие меры снижают риски
- Связь с процессами ИБ: каждая мера привязана к активам, задачам и рискам
- Отслеживание внедрения с учётом бюджета, сроков и ответственных
- Автоматическая отчётность: формирование планов и отчётов по ИБ



Результат

С модулем защитных мер в SECURITM компании могут:

- Контролировать все меры безопасности — связь с рисками и активами
- Повышать эффективность — направлять ресурсы на важные меры, а не на формальные
- Системно управлять безопасностью — видеть, какие меры реально снижают риски и выполняют требования

УПРАВЛЕНИЕ МЕТРИКАМИ

Модуль KPM (Key Performance Metrics) помогает эффективно управлять метриками ИБ, связывая их с рисками, комплаенсом и защитными мерами. SECURITM предоставляет гибкие дашборды, автоматическую аналитику и актуальные данные в реальном времени, что позволяет быстро принимать обоснованные решения и контролировать состояние безопасности компании.

Проблема

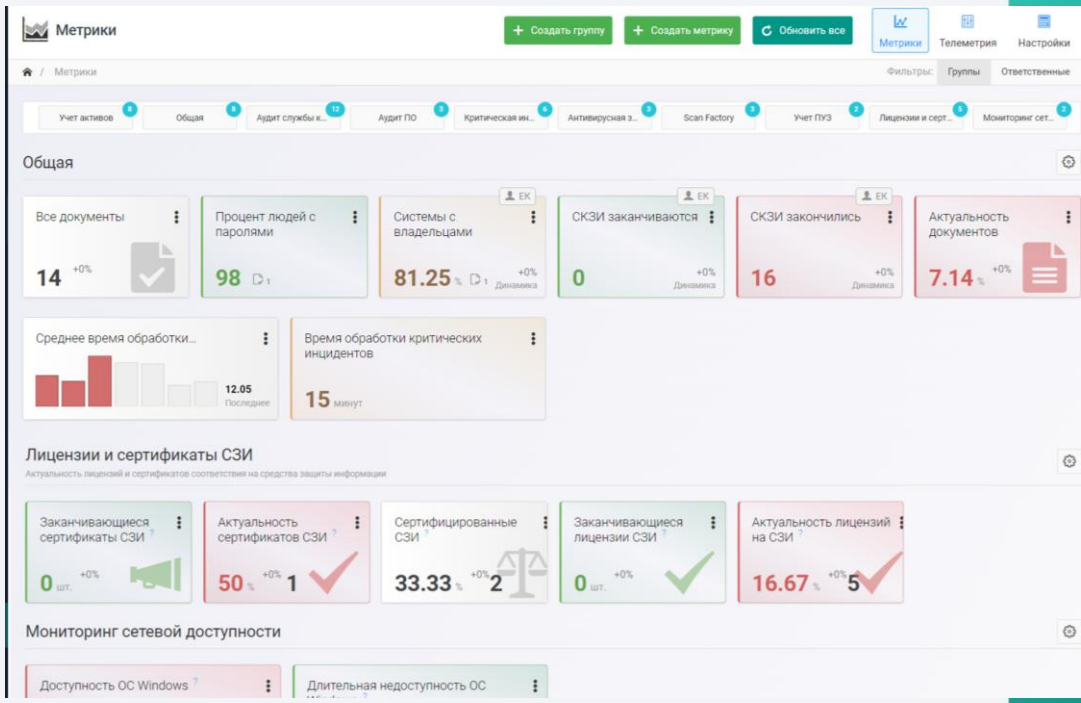
Для эффективного управления ИБ нужны актуальные и понятные метрики, но:

- Нет единой точки контроля — метрики разбросаны по системам
- Отсутствует связь метрик с процессами ИБ — визуализация без действия
- Статичные дашборды — нет гибких настроек
- Ручной сбор данных и отчётность — требует времени и усилий
- Без автоматизации сложно оперативно запускать процессы

Решение

SECURITM упрощает управление метриками ИБ:

- Гибкие дашборды под задачи службы ИБ
- Готовые пресеты и кастомные метрики
- Единая точка контроля всех метрик
- Метрики для принятия решений в рисках и комплаенсе
- Актуальные данные в реальном времени



Результат

С модулем метрик в SECURITM компании могут:

- Гибко настраивать мониторинг ИБ-процессов
- Связывать метрики с процессами ИБ: рисками, мерами и комплаенсом
- Контролировать состояние ИБ в реальном времени
- Принимать решения на основе влияния метрик на бизнес
- Сократить время на отчетность за счёт автоматической аналитики

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

Модуль VM (Vulnerability Management) помогает выстроить системный процесс работы с уязвимостями — от сбора данных из сканеров до приоритизации, контроля устранения и формирования метрик. SECURITM объединяет все источники, выделяет действительно критичные проблемы и связывает уязвимости с рисками, активами и задачами.

Проблема

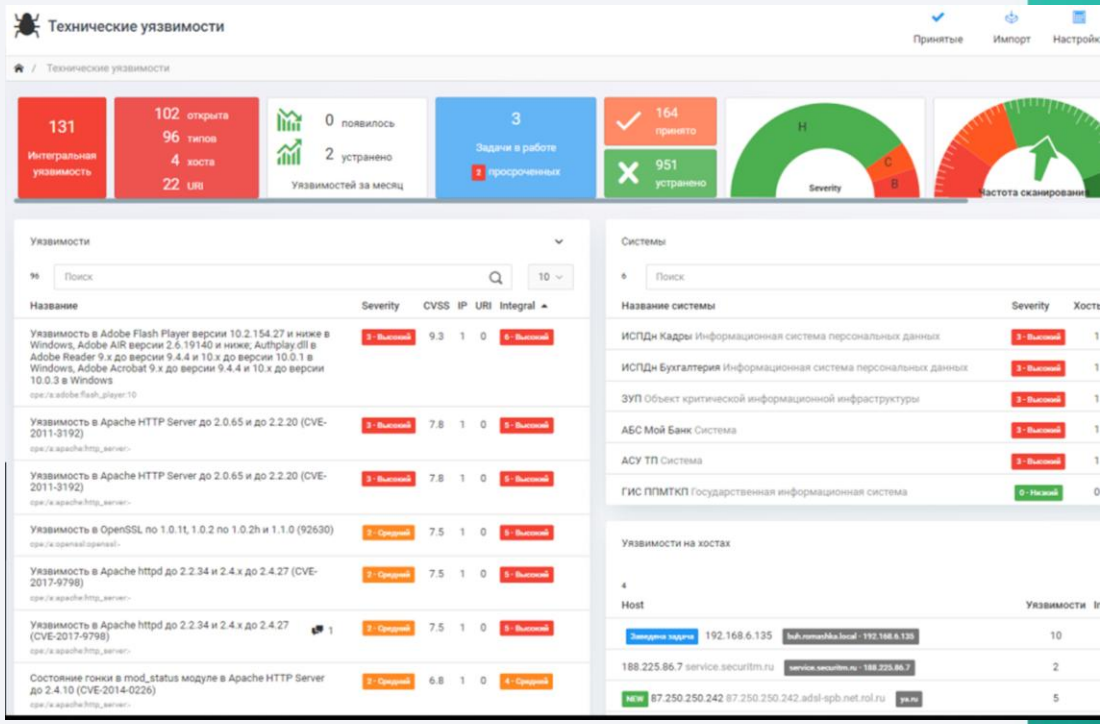
Сканеры находят уязвимости, но это не решает проблему:

- Нет приоритизации — какие из тысяч уязвимостей реально угрожают бизнесу
- Избыточные отчёты — сотни страниц без выделения критичных проблем
- Уязвимости не связаны с активами
- Нет контроля устранения — сложно отследить, что действительно решено
- Отсутствует единая система управления уязвимостями и их обработкой

Решение

SECURITM превращает данные из сканеров в управляемый процесс:

- Автоматическая приоритизация с учётом критичности уязвимости
- Статус уязвимостей в модуле метрик
- Контрольный след: логирование изменений и фиксация решений
- Интеграция с MaxPatrol VM, ScanFactory, Kaspersky и другими сканерами
- Корреляция с CVE, БДУ ФСТЭК и НКЦКИ для качественной приоритезации
- Единое окно для всех типов сканеров на рынке



Результат

Управление уязвимостями становится точным и системным:

- Фокус на критичных уязвимостях, а не на общем объёме
- Экономия времени за счёт автоматической обработки отчётов
- Прозрачный контроль устранения и статус каждой уязвимости
- Управление исключениями и фиксация принятых рисков
- Метрики и отчёты для оценки эффективности работы ИБ
- Связь с управлением рисками и комплаенсом в единой системе

УПРАВЛЕНИЕ ЗАДАЧАМИ

Модуль задач помогает эффективно управлять процессами ИБ, связывая задачи с активами, рисками, уязвимостями, а также комплаенсом. SECURITM автоматизирует контроль сроков, отслеживание исполнения и формирование отчётов, обеспечивая прозрачность и системность в работе службы ИБ.

Проблема

Задачи ИБ становятся неэффективными без полной картины:

- Нет контекста — задачи существуют отдельно от процессов ИБ, без учета вовлечённых активов
- Нет связи с активами и рисками — нет понимания, какие данные затронуты
- Разрозненное управление — задачи ведутся в разных системах

Решение

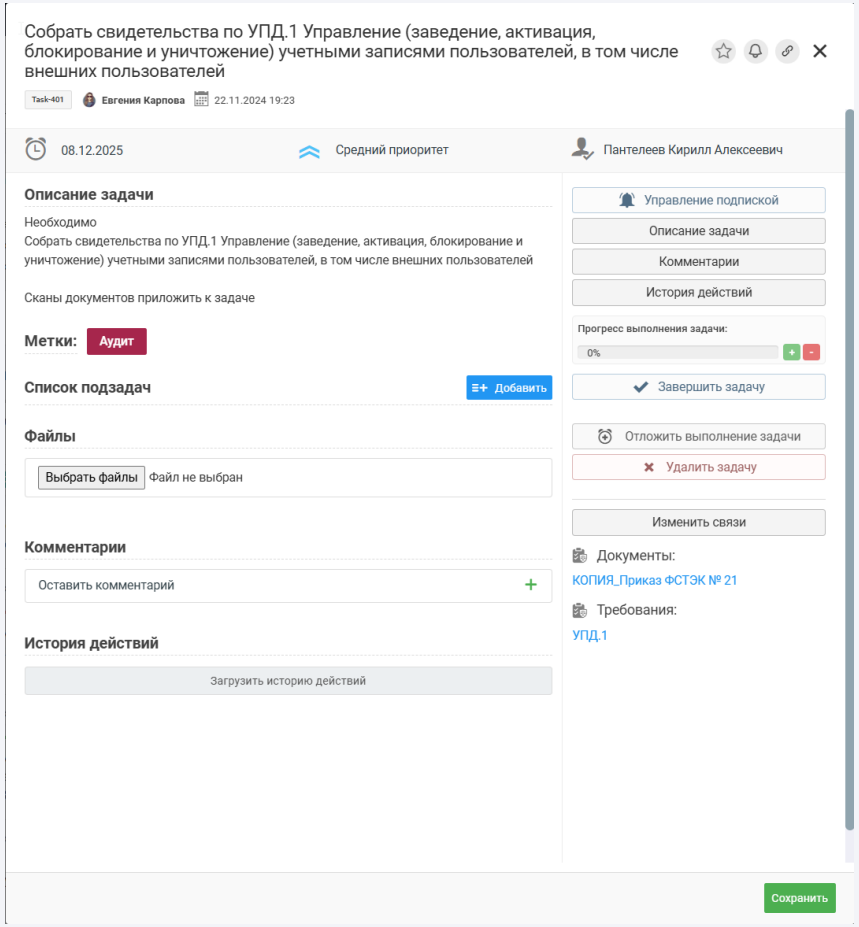
SECURITM оптимизирует управление задачами ИБ:

- Связь задач с контекстом — привязка к активам, рискам и уязвимостям
- Контроль сроков и исполнения — автоматические напоминания и назначение ответственных
- Отчётность без ручного сбора — автоматическая фиксация изменений и метрик
- Замена традиционных инструментов — все задачи в одной системе

Результат

С модулем задач в SECURITM компании могут:

- Контролировать все процессы ИБ — задачи всегда связаны с актуальными активами
- Обеспечить прозрачность и ответственность — чёткое распределение задач и контроль исполнения
- Систематизировать управление процессами — интеграция с другими модулями позволяет управлять задачами эффективно



УПРАВЛЕНИЕ АВТОМАТИЗАЦИЯМИ

Модуль RPA/SOAR автоматизирует рутинные процессы ИБ, снижая нагрузку на команду и ускоряя выполнение задач. SECURITM позволяет настраивать гибкие сценарии реагирования, интегрируя их с событиями в системе и стандартизируя действия.

Проблема

Автоматизация процессов ИБ — ключ к эффективности, но:

- Много рутинных задач — специалисты тратят часы на выполнение повторяющихся задач
- Отсутствие сквозных процессов — нет единого сценария от события до действия
- Реагирование на инциденты вручную — базовые действия требуют много времени и усилий
- Нет стандартизированных сценариев реагирования — каждый процесс создаётся вручную

Решение

SECURITM упрощает автоматизацию процессов ИБ:

- Многоуровневые триггеры для запуска процессов по различным событиям
- Сценарии реагирования (плейбуки) для стандартизации действий
- Поддержка интеграций и скриптов для адаптации под специфические процессы
- Контроль изменений в инфраструктуре с автоматическим запуском действий

Результат

С модулем RPA в SECURITM компании могут:

- Снизить нагрузку на команду ИБ — автоматизация рутинных задач освобождает время для стратегических вопросов
- Повысить согласованность действий — стандартизированные плейбуки сокращают риски ошибок
- Обеспечить гибкость автоматизации — настройка сценариев под любые события

УПРАВЛЕНИЕ ОПРОСАМИ

Модуль опросов помогает автоматизировать сбор данных и актуализировать информацию по ИБ. С помощью модуля появляется возможность стандартизировать процесс оценки соответствия, ускорить аудит и сбор обратной связи от сотрудников и контрагентов.

Проблема

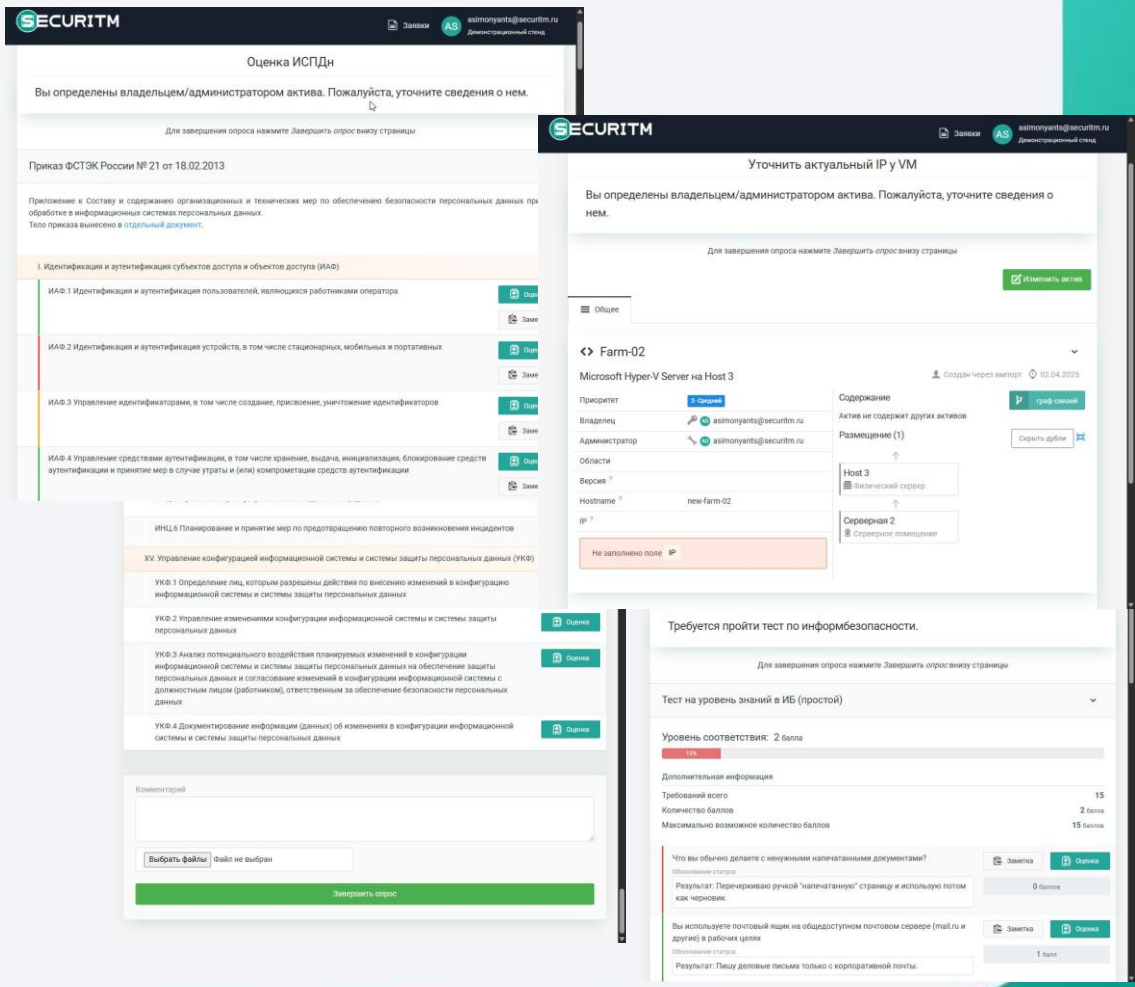
Сбор важной информации затруднен:

- Отсутствие единого механизма оценки соответствия
- Сложно поддерживать актуальность данных без обратной связи
- Трудности в аудите внешних сторон из-за ручной обработки
- Отсутствие механизма сбора обратной связи от сотрудников и контрагентов

Решение

SECURITM помогает собирать данные:

- Опросы для оценки соответствия: чек-листы для сотрудников и подрядчиков
- Аудит внешних сторон: оценка соответствия требованиям
- Актуализация данных: обновление информации об активах и системах
- Ознакомление с требованиями: доведение норм ИБ до сотрудников
- Service Desk: обработка запросов от сотрудников и контрагентов



Результат

С модулем опросов компании могут:

- Автоматизировать оценку соответствия — быстро собирать отчёты
- Стандартизировать аудит — ускорить проверки ИБ
- Поддерживать актуальность данных — обновлять информацию об активах
- Собирать обратную связь — получать потребности сотрудников и контрагентов
- Сократить время на коммуникацию — автоматизация взаимодействия
- Обеспечить прозрачность — вся информация сохраняется для аудита

КАТАЛОГИ

Модуль каталогов – это единый источник достоверной информации об угрозах, уязвимостях и методах атак. Модуль агрегирует данные из международных и российских баз (CVE, БДУ ФСТЭК, НКЦКИ, MITRE ATT&CK), автоматически обновляя и связывая их с активами, уязвимостями и рисками в системе. Это помогает службе ИБ быстро получать контекст, оценивать значимость угроз и принимать обоснованные решения без ручного поиска информации.

Проблема

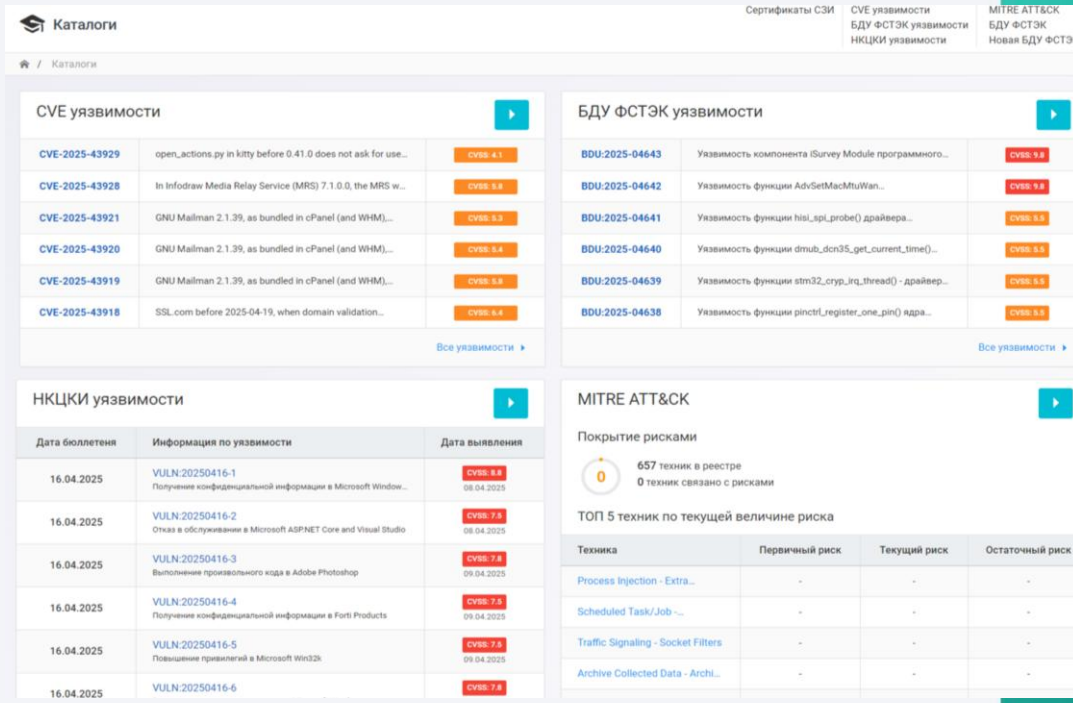
Управление ИБ в крупных компаниях сталкивается с вызовами:

- Уязвимости в отчетах сканеров часто идут без контекста — сложно быстро оценить их опасность и приоритет.
- Большинство команд тратят время на ручной поиск информации в разных источниках: CVE, БДУ ФСТЭК, MITRE ATT&CK и др.ИБ-команды — отсутствие прозрачности и единых стандартов между подразделениями
- Отсутствие единого источника данных мешает быстро реагировать на угрозы и связывать их с рисками.

Решение

SECURITM упрощает управление ИБ в крупных компаниях:

- SECURITM агрегирует данные из всех ключевых каталогов (CVE, БДУ ФСТЭК, НКЦКИ, MITRE ATT&CK) в одной системе.
- Автоматическая корреляция с рисками, уязвимостями и активами позволяет оперативно принимать решения.
- Сервис обновляет данные каталогов, отображает приоритеты (CVSS и др.) и обеспечивает контекст для каждой записи.



Результат

С модулем каталогов компании:

- Экономия времени на анализ — все данные по угрозам, уязвимостям и техникам атак в одном месте.
- Повышение качества оценки рисков и принятия решений.
- Устранение ручной рутины и рост зрелости процессов ИБ.

УПРАВЛЕНИЕ ОБЛАСТЯМИ

Модуль областей помогает управлять ИБ в крупных организациях, обеспечивая централизованный контроль и адаптацию процессов под нужды дочерних структур. SECURITM помогает стандартизировать подход к управлению ИБ, сохраняя гибкость для разных подразделений и команд.

Проблема

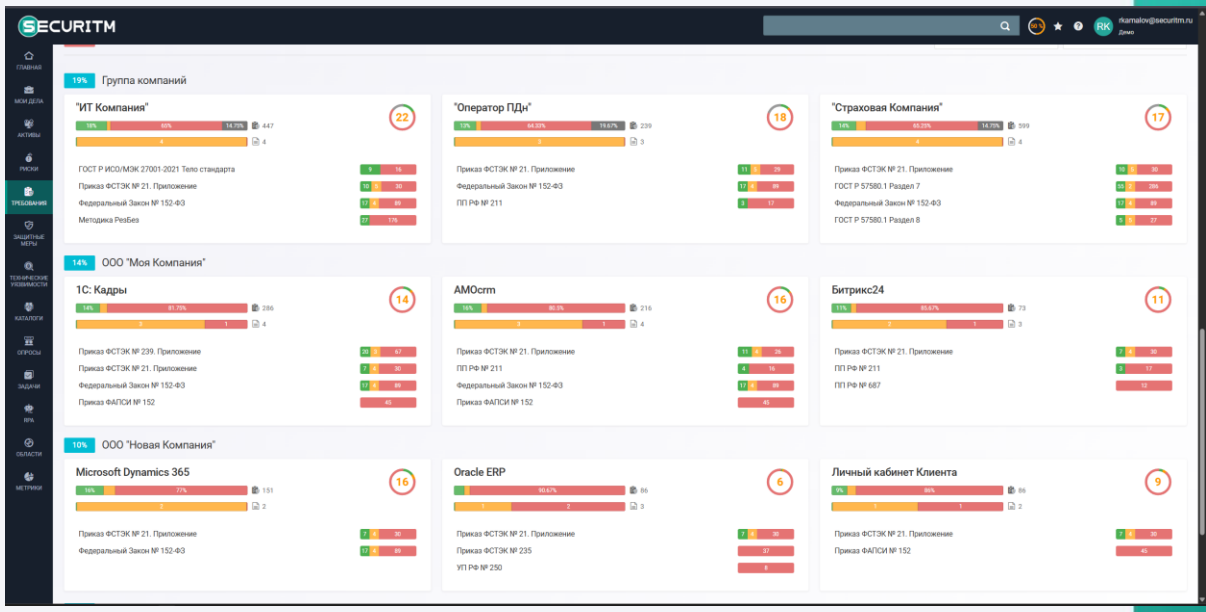
Управление ИБ в крупных компаниях сталкивается с вызовами:

- Нет централизованного контроля для всей инфраструктуры — сложность в стандартизации подходов и требований на уровне всей компании
- Изолированные ИБ-команды — отсутствие прозрачности и единых стандартов между подразделениями
- Разрозненности процессов — разные подходы к ИБ в дочерних организациях приводят к несоответствию требованиям

Решение

SECURITM упрощает управление ИБ в крупных компаниях:

- Контроль ИБ во всех бизнес-структурах из одной точки
- Прозрачность процессов с разграничением данных и задач
- Единые стандарты безопасности для всей компании
- Гибкость и масштабируемость под сложные, многоуровневые структуры



Результат

С модулем областей компании:

- Управляют ИБ во всех дочерних организациях из одной точки
- Контролируют соответствие требованиям благодаря единому подходу
- Обеспечивают прозрачность структурных подразделений
- Адаптируют процессы под специфику каждой команды

Интеграции

SECURITM объединяет и структурирует данные из ваших СЗИ и ИТ систем

SECURITM

API

Прямые интеграции

- Jira
- Cloud.ru
- PVS-Studio
- SearchInform
- ManageEngine
- DrWeb
- NetBox
- AppSecHub
- ActiveDirectory
- ScanFactory
- YandexTracker
- CloudAdvisor
- Metascan
- Kubernetes
- maxpatrolvm
- ScanSuite
- BI.ZONE
- VulnsioVM
- wazuh
- RedCheck
- FreeIPA
- solar
- KasperskyASAP
- Kaspersky Security Center
- Zabbix
- Staffcop
- F6ASM

Импорт отчетов

- Nessus vulnerability scanner
- NMAP.ORG
- XSpider
- Greenbone OpenVAS
- ManageEngine
- MaxPatrol VM
- MaxPatrol 8

Прямые интеграции

Jira
Cloud.ru
PVS-Studio
SearchInform
Zabbix
solar
DrWeb
NetBox
AppSecHub
ActiveDirectory
F6ASM
YandexTracker
CloudAdvisor
Metascan
ManageEngine
BI.ZONE
Staffcop
wazuh
maxpatrolvm
Kubernetes
ScanFactory
FreeIPA
VulnsioVM
RedCheck
ScanSuite
KasperskyASAP
KasperskySecurityCenter

API

Импорт файлов
csv / xls / cer/crt

Сетевые хранилища

ВНЕШНИЕ/
ВНУТРЕННИЕ
ТРЕБОВАНИЯ ПО ИБ

ЛЮДИ

СТРАТЕГИЧЕСКИЕ ПРОЦЕССЫ

- Управление рисками
- Соответствие требованиям
- Управление мерами
- Управление метриками

ОПЕРАЦИОННЫЕ ПРОЦЕССЫ

- Управление активами #ITAM
- Управление уязвимостями #VM
- Автоматизация процессов #RPA
- Задачи
- Опросы
- Заявки

АНАЛИЗ

ОТЧЕТНОСТЬ

АВТОМАТИЗАЦИЯ

...

SGRC

Security, Governance, Risk and Compliance / Контроль соответствия требованиям и управление рисками

AM

Asset Management / Управление активами

VM

Vulnerability Management / Управление уязвимостями

BI

Business Intelligence / Анализ данных

SOAR

Security Orchestration, Automation and Response / Автоматизация и координация процессов реагирования на инциденты

SECURITM SUPER APP

IRP

Incident Response Platform / Управление инцидентами

RPA

Robotic Process Automation / Автоматизация рутинных процессов

CMDB

Configuration Management Database / База данных управления конфигурациями

Service desk

Управление заявками

ITAM

IT Asset Management / Управление ИТ активами

SECURITM

- ЭКОНОМИТ ВРЕМЯ
- ЭКОНОМИТ ДЕНЬГИ КОМПАНИЙ
- ОБЕСПЕЧИВАЕТ ПРОЗРАЧНОСТЬ ПРОЦЕССОВ
- ОБЕСПЕЧИВАЕТ ПОВЫШЕНИЕ УРОВНЯ ЗАЩИТЫ

Ключевая особенность SECURITM — практическая направленность: продукт помогает организациям перейти от формального выполнения требований к реальному управлению безопасностью, обеспечивая прозрачность процессов, экономию ресурсов и повышение уровня защиты.

Для компаний SECURITM обеспечивает непрерывность работы и снижение затрат на устранение инцидентов безопасности, так как:

- позволяет сократить до 40% утечек и нарушений за счёт повышения эффективности процессов и устранения человеческого фактора в ИБ;
- увольнения и отпуска в службе ИБ не приводят к деградации системы ИБ;
- все работы по ИБ прозрачны и понятны благодаря отчётам и метрикам;
- проводится оценка обоснованности затрат на закупки по ИБ.

Службам ИБ SECURITM позволяет:

- уйти от разрозненных таблиц Excel и неспециализированных систем;
- ввести контроль и учет ИСПДн, КИИ, ГИС и любых связанных активов, объединяя их в цифровые модели;
- автоматизировать до 90% рутинных процессов и операций;
- сократить до 70% времени на сбор информации с работников и контрагентов;
- проводить автоматическую оценку и контроль соответствия требованиям любых регуляторов и стандартов;
- интегрироваться с корпоративными системами;
- запустить риск-ориентированный подход с нуля за 5 минут.

SECURITM - это стандарт управления процессами ИБ

это подтверждают

>100 заказчиков

>4000 пользователей

в Community-версии

- Финансовый сектор
- Промышленность
- Ритейл
- ТЭК
- ВПК
- Здравоохранение
- Фармацевтика
- Государство
- ИТ
- Транспорт
- Металлургия
- Питание
- Образование
- Строительство
- Услуги
- Туризм
- Нефтегаз

лента

ЕВРАЗ

Полисан

inSales

КОМИТЕТ ПО ИНФОРМАТИЗАЦИИ И СВЯЗИ САНКТ-ПЕТЕРБУРГА

Центр Внедрения ПРОТЕК

banki.ru

СБЕР РЕШЕНИЯ

Пусть о нас расскажут наши клиенты

ЕВРАЗ

Андрей Нуйкин

Руководитель службы информационной безопасности компании «Евраз»

«Если у компании десятки тысяч пользователей и тысячи серверов, работать в Excel становится проблематично»

Тимур Гараев

руководитель департамента информационной безопасности Банки.ру

«Когда вам кажется, что в плане безопасности все уже сделано, откройте Секъюритм и увидите, какие существуют риски»

banki.ru

Пусть о нас расскажут наши клиенты

РЕГИОН
ГРУППА КОМПАНИЙ

Александр Суслов

ИК Регион

«Решение действительно удобное. Логика системы легла на нашу структуру — ничего не пришлось доделывать. Всё, что нужно, уже было внутри, и сразу начало работать. Это сэкономило время и позволило сразу включиться в работу без лишней настройки.»

Александр Самаркин

ЦВ Протек

«Мы создали свой план защитных мер, оформили его как перечень регулярных мероприятий и связали с модулем RPA. Раньше всё это лежало в Excel-таблицах, которые были согласованы с комитетом по ИБ. Сейчас всё приходит автоматом, не надо лезть в таблицы — просто приходит уведомление, что пора делать. Это сильно упростило процессы.»

Центр Внедрения
ПРОТЕК

Сравнение версий продукта

	Community	SaaS	On-premise
Размещение данных	**облако**	**облако**	**локально**
Лицензия	➖	**1 год**	**бессрочная**
Количество объектов в различных модулях	**до 100**	**10к+**	**10к+**
Интеграции с ИТ и ИБ системами (Active Directory, Kaspersky Security Center, MaxPatrol, Zabbix, Kubernetes и т.д., более 30)	➖	**частично**	✅
Доменная авторизация	➖	➖	✅
Кастомизация интерфейса и WhiteLabel	➖	**частично**	✅
Техническая поддержка	**справка**	**базовая, доступна расширенная**	**базовая, доступна расширенная**
Обучение	**справка**	✅	✅
Функциональные доработки системы	➖	✅	✅
Стоимость	**Бесплатно**	**От 315 тыс. рублей**	**От 900 тыс. рублей**

Варианты технической поддержки

	Базовая	Расширенная
Прием заявок по **почте**	✅	✅
Прием заявок **через портал**	✅	✅
Персональный чат в Telegram	➖	✅
Закрепленный инженер поддержки	➖	✅
Персональные консультации по ВКС	➖	✅ **до 4 в месяц**
График работы	**5/9**	**5/9**
Скорость реакции	**До 8 часов**	**До 2 часов**
Срок устранения неисправностей **в зависимости от приоритета заявки**		
Критический 	**до 8 часов**	**до 4 часов**
Высокий 	**до 2 дней**	**до 8 часов**
Средний 	**до 2 недель**	**до 5 дней**
Низкий	**до 4 недель**	**до 2 недель**

SECURITM – система управления процессами ИБ, доступный любой службе безопасности, вне зависимости от ее штата, бюджета и уровня зрелости.

8 800 300 37 64

info@securitm.ru

securitm.ru

t.me/securitm