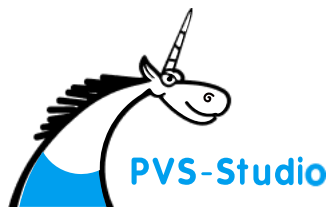


Внедрение процессов безопасной разработки

Практическая интеграция PVS-Studio и Securitm



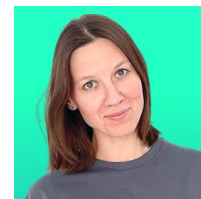
Антон Третьяков

Разработчик, Tools&DevOps



Евгения Карпова

Инженер отдела
внедрения и поддержки



Евгения Карпова

Инженер отдела внедрения и поддержки

- 🛡 Провожу внедрения и пилотные проекты с заказчиками
- 🛡 Отвечаю за качественный клиентский сервис





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



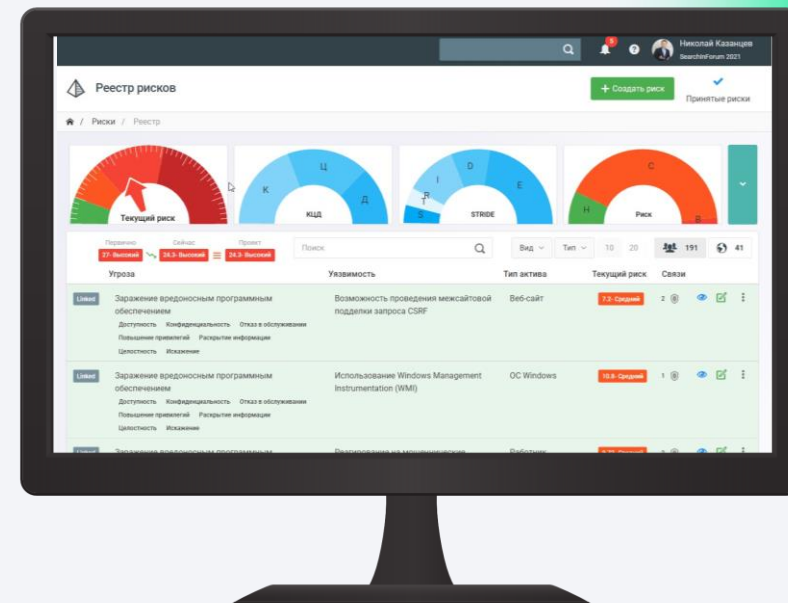
Уязвимости

Агрегатор отчетов от сканеров безопасности



Опросы

Сбор сведений с работников и контрагентов, Service Desk



БЕСПЛАТНАЯ
COMMUNITY-ВЕРСИЯ
SECURITM



> 3000
ПОЛЬЗОВАТЕЛЕЙ
В SAAS-ВЕРСИИ



ОТКРЫТАЯ ЦЕНА
ПОНЯТНЫЕ ТАРИФЫ

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?

*Vulnerability management

Решение

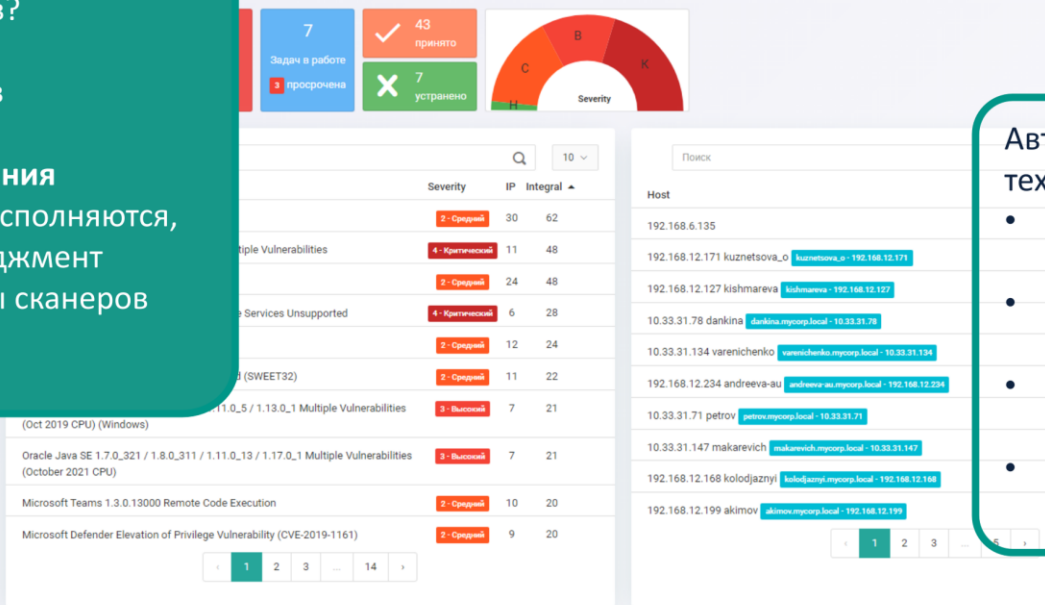
Управление техническими уязвимостями в SECURITM:

- **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





**МЕНЬШЕ СЛОВ,
БОЛЬШЕ ПРАКТИКИ**

#ДЕМО

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 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



SECURITM_2025



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



service.securitm.ru



📍 @SECURITM