SECURITY VISION SPC

ФУНДАМЕНТ ЗРЕЛОЙ КИБЕРБЕЗОПАСНОСТИ

Роман ДУШКОВ
эксперт, Security Vision

Валерий ГОРБАЧЁВ
руководитель группы внедрения систем мониторинга АО «ДиалогНаука»

В современной корпоративной среде автоматизированное управление конфигурациями безопасности и контроль соответствия перестали быть исключительно вопросом выполнения требований регуляторов. Продукты класса SPC (Security Profile Compliance) превратились в фундаментальный элемент зрелой стратегии кибербезопасности.

Некорректные конфигурации ИТ-активов являются одним из наиболее распространённых и опасных векторов атак, открывая злоумышленникам доступ к критически важным системам, а непрерывный и автоматизированный контроль за состоянием конфигураций становится стратегическим процессом проактивного снижения поверхности атаки и минимизации рисков.

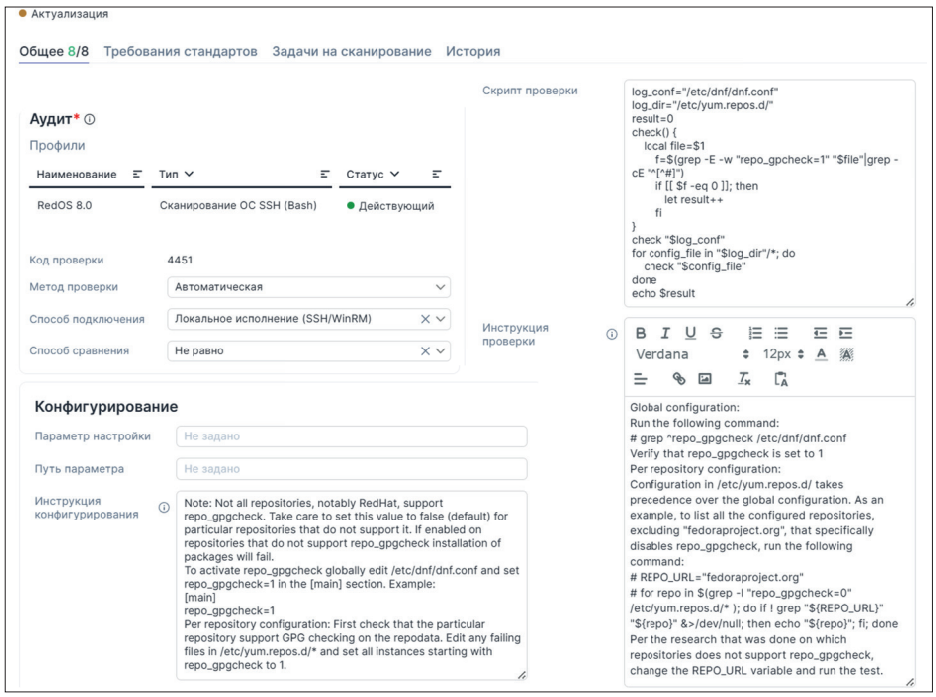

Рисунок 1. Настройки и автоматизация аудита конфигураций

ЦЕЛИ И ОСОБЕННОСТИ АРХИТЕКТУРЫ

Внедрение Security Vision SPC подразумевает централизацию функции контроля соответствия в рамках одновременно GRC-подразделения, команды, отвечающей за автоматизацию процессов ИБ и директоров по информационной безопасности.

Модуль контроля параметров безопасности не является изолированным продуктом и представляет собой решение, которое наследует все сильные стороны базовой платформы Security Vision. Его польза проистекает из синергии с другими модулями: для управления активами и инвентаризацией (AM), уязвимостями (VM) со сканером (VS), инцидентами (SOAR) и SGRC. Эффективный контроль соответствия невозможен без полного, точного и постоянно актуализируемого реестра ИТ-активов: способность платформы обнаруживать, инвентаризировать и работать в разнообразных технических средах является её ключевой характеристикой (рис. 1).

Решение сочетает методы сканирования с использованием агентов и без них, а также проводит проверки как с использованием предварительно подготовленных УЗ, так и без них. Микросервисная архитектура позволяет организациям масштабировать отдельные компоненты (на-

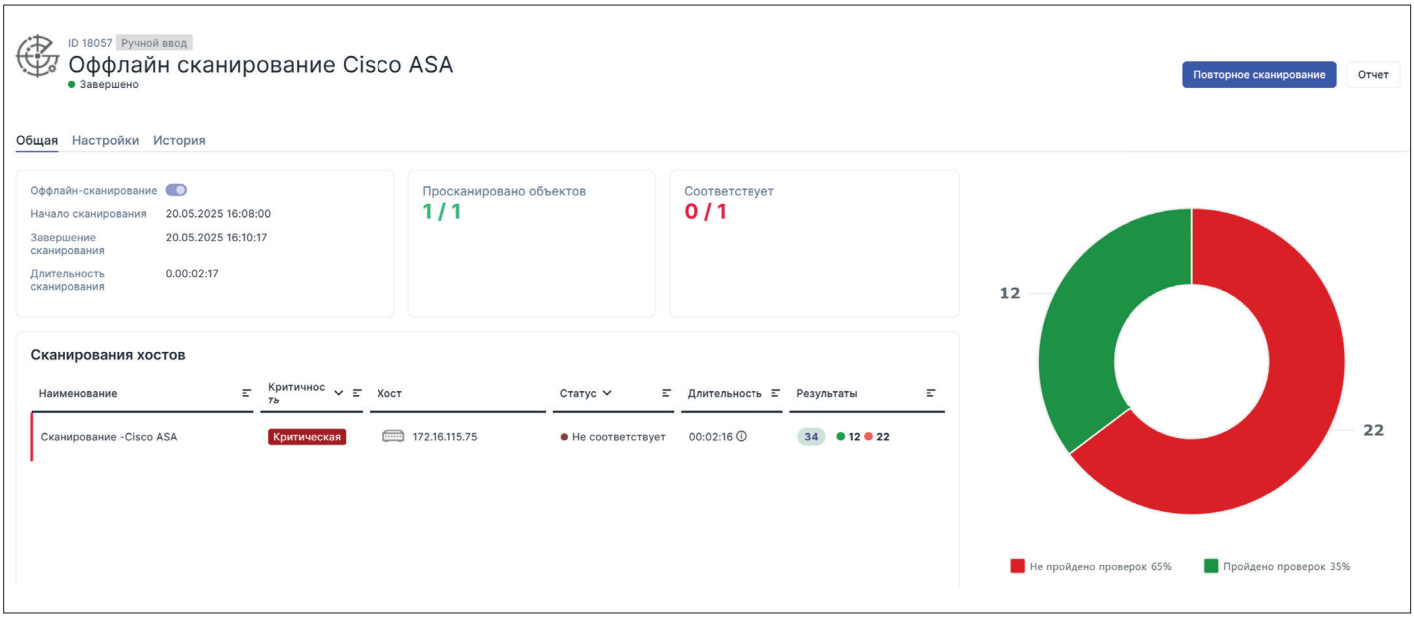

Рисунок 2. Результаты офлайн-сканирования

пример, сервис коннекторов для интеграции с внешними системами) по мере роста нагрузки и появления новых задач, что обеспечивает гибкость развёртывания и высокую отказоустойчивость.

ОСОБЕННОСТИ ПРОЦЕССА КОМПЛАЕНСА

Поскольку ни одна технология сканирования не может обеспечить 100% видимости данных, вендоронезависимый подход Security Vision идеально подходит для компаний, где для обогащения данными применяются разрозненные системы от различных поставщиков. Low-code фреймворк-коннекторов позволяет агрегировать данные из внешних систем (служб каталогов, SCCM-, CMDB- и SIEM-систем, и других источников) вне зависимости от поставщика решения и без участия вендоров.

Офлайн-сканер позволяет определять степень соответствия параметров безопасности для любых сетей, включая применение в изолированных средах (рис. 2).

Автоматизация процесса, от обнаружения активов и технологических платформ до приведения к соответствию их настроек, позволяет освободить ресурсы аналитиков и ИТ-специалистов. В случае выявления несоответствия конфигураций активов эталонным значениям значения при помощи коннекторов приводятся к заданным. Ведение профилей технологических платформ (например, операционных систем, СУБД, прикладного ПО), содержащих перечень релевантных проверок, можно проводить как вручную, так и автоматически по расписанию (рис. 3).

Security Vision SPC имеет встроенный движок управления бизнес-процессами (BPM) и позволяет создавать полностью кастомизированные рабочие процессы (для управления жизненным циклом активов, устранения несоответствий, обновления настроек и создания задач). Система может автоматически создавать задачи, назначать ответственных, контролировать SLA и интегрироваться с внешними системами Service Desk, такими как Jira, Naumen SD, Redmine и др.

Системы контроля соответствия регулярно (например, раз в сутки) сканируют хосты и сравнивают их текущую конфигурацию с эталонным «золотым образом».

Отдельным преимуществом является возможность самостоятельно собрать не только «золотой образ», но и требования, проверки, скрипты проверок с выполняемыми командами. Таким образом, сильно расширяются возможности кастомизации и подстройки под используемые в компании стандарты.

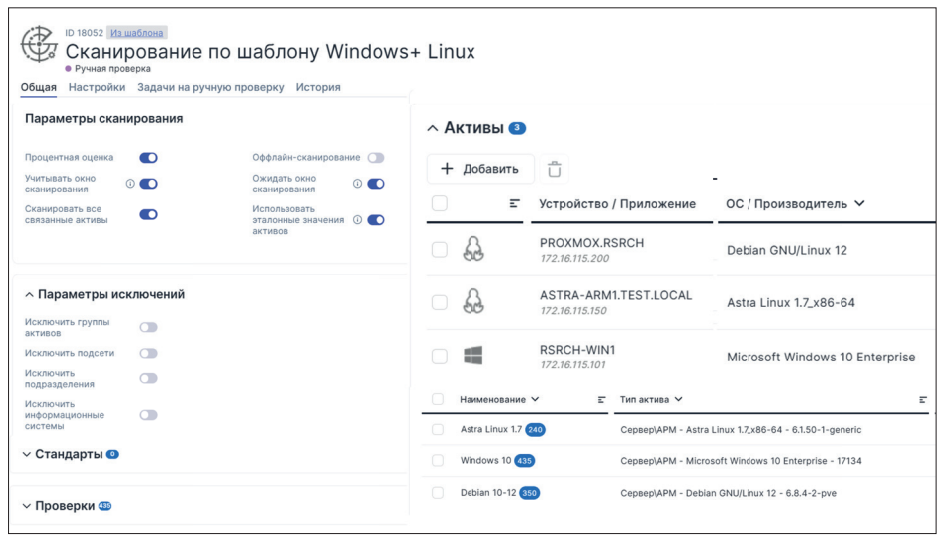

Рисунок 3. Гранулярные настройки контроля соответствия

РЕЗУЛЬТАТЫ И ВЛИЯНИЕ НА БИЗНЕС

Контроль конфигураций и соответствия профилям безопасности напрямую снижает поверхность атаки и повышает общую защищённость, делая системы более предсказуемыми, управляемыми и устойчивыми к взлому. Это достигается за счёт нескольких ключевых механизмов:

- устранение известных векторов атак (харденинг), приведение систем в соответствие с лучшими практиками безопасности (бенчмарками) и внутренними стандартами; этот процесс систематически закрывает распространённые лазейки;
- отключение ненужных служб и портов, потенциальных точек входа для злоумышленника: система находит и отмечает службы, которые не требуются для бизнес-функций, позволяя их отключить (например, если на веб-сервере не используется FTP, соответствующий порт (21) и служба должны быть отключены, что мгновенно убирает все известные уязвимости FTP-серверов из поля зрения атакующего до того, как он сможет их применить);
- проверка прав на выполнение системных команд или изменение критически важных файлов у обычных пользователей мешает горизонтальному перемещению по сети и повышению привилегий после первичного проникновения;
- неиспользуемое программное обеспечение (старые версии библиотек, тестовые утилиты) не обновляется, содержит уязвимости и может быть использовано для проникновения или повышения привилегий в системе. Функционал управления активами идентифицирует такое ПО для последующего (в т.ч. автоматического) удаления;
- выявление несоответствий парольной политике, misконфигураций и/или ошибок в различных файлах конфигов (для самых разных механизмов — от удалённого доступа и повышения привилегий до PAM и прочих);
- системы по умолчанию часто настроены на максимальную функциональность, а не на безопасность, поэтому контроль соответствия способен исправить сотни параметров: от отключения старых протоколов (SSL 3.0, TLS1.0) до установки корректных прав на системные файлы и каталоги.

Контроль соответствия профилям безопасности превращает реактивный подход в проактивный, систематически устраняя слабые места и обеспечивая постоянную видимость реального состояния защищённости ИТ-инфраструктуры (рис. 4).

Любое отклонение (например, открытие нового порта, появление нового пользователя с правами администратора, изменение прав на файл) немедленно фиксируется и отправляется в виде оповещения команде безопасности. Это позволяет быстро обнаружить как случайные ошибочные изменения, так и вредоносную активность, значительно сокращая «окно», в течение которого система остаётся уязвимой.

ЗАКЛЮЧЕНИЕ

В будущем инструменты для работы с уязвимостями и конфигурациями будут включать в себя больше GRC-функций, а GRC-платформы — углублять свои технические возможности оценки. Выбор, сделанный организацией сегодня, определит её траекторию развития в этом меняющемся ландшафте. Он должен быть основан на глубоком понимании собственной организационной культуры, операционной зрелости и долгосрочной стратегии в области кибербезопасности.

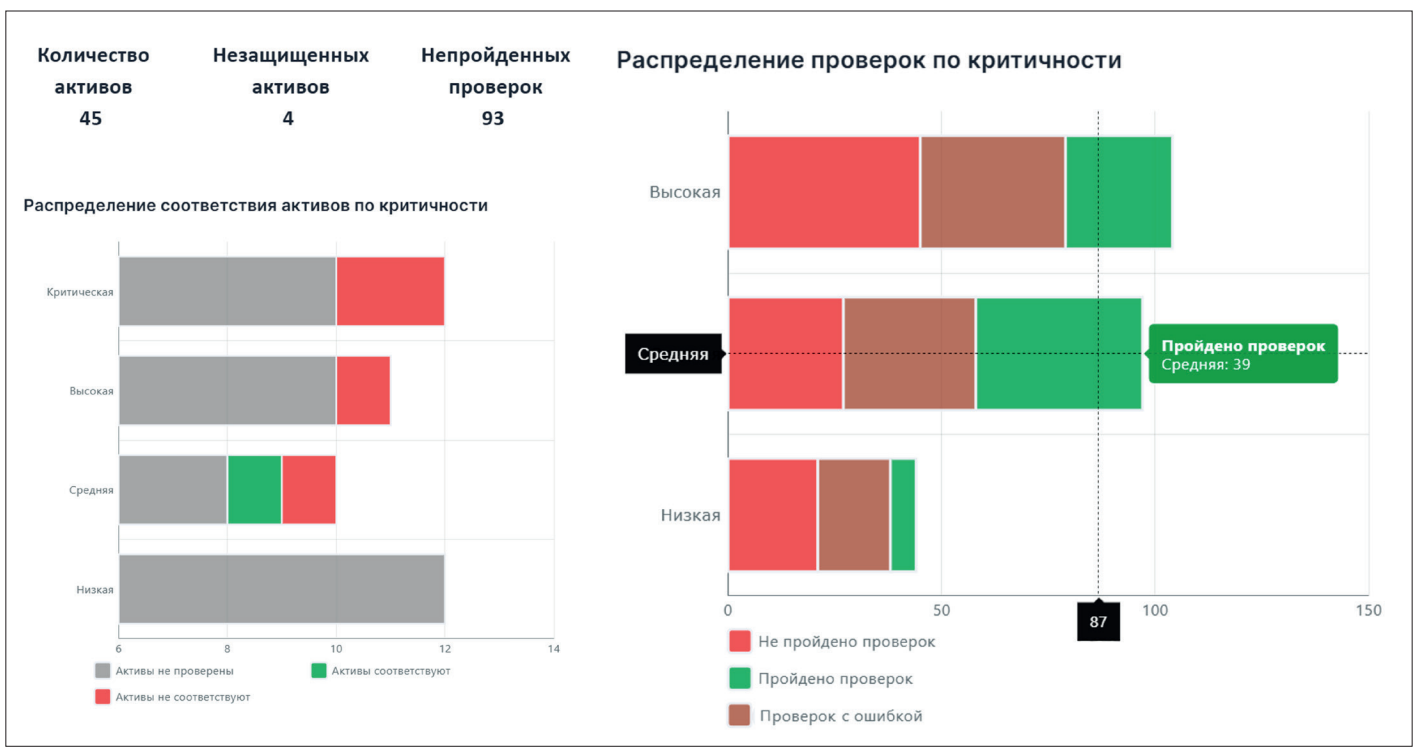

Рисунок 4. Визуализация результатов для ресурсно-сервисной модели компании (выделенный контур)