R-Vision

Автоматизация процесса VM в крупном промышленном холдинге и обеспечение контроля устранения уязвимостей

История успеха

Заказчик

Крупный промышленный холдинг с распределённой ИТ-инфраструктурой по всей стране.

Основное направление деятельности — разработка и производство высокопрочных сталей и сплавов.

Отрасль

Промышленность

Проект в цифрах

6
филиалов

25 000
хостов

Задачи

В 2024 году к R-Vision обратился крупный промышленный холдинг с запросом на внедрение системы управления уязвимостями. Цель — автоматизировать и централизовать процесс VM в 6 филиалах, каждый из которых — крупный завод. В инфраструктуре холдинга около 25 000 хостов: серверы, сетевое оборудование, рабочие станции и другие устройства. Управлением ИБ занимается центральная команда из 12 специалистов, которые работают совместно с ИТ-администраторами в каждом филиале.

До внедрения R-Vision VM управление уязвимостями преимущественно велось в «ручном» режиме с использованием сканера стороннего вендора. Сканер собирал данные с нескольких тысяч хостов в каждом филиале и передавал их специалистам по ИБ. Данные обрабатывались вручную, приоритизировались и передавались в ИТ-департамент. После устранения уязвимостей проводилось повторное сканирование, результаты вручную сопоставлялись с предыдущими отчётами. Процесс был трудозатратным и уязвимым для ошибок, вызванных человеческим фактором, что снижало эффективность контроля безопасности.

Команда ИБ понимала, что нужен инструмент для автоматизации и централизации процесса. После тестирования нескольких решений выбрали R-Vision VM — систему, которая показала стабильную работу и соответствие требованиям организации. Она обеспечивает полный цикл управления уязвимостями: от выявления до автоматического контроля устранения.

Карточка проекта

Заказчик

Крупный промышленный холдинг с распределённой ИТ-инфраструктурой, включающей 6 филиалов по всей стране.

Основное направление деятельности — разработка и производство высокопрочных сталей и сплавов.

Задачи

Централизовать и автоматизировать процесс выявления, приоритизации и устранения уязвимостей в масштабах всей ИТ-инфраструктуры холдинга

Решение

R-Vision VM - система автоматизации процесса управления уязвимостями со встроенным модулем сканирования

Результаты

Централизованный и автоматизированный процесс VM

Высокая скорость и точность работы с уязвимостями

Снижение времени на рутинные операции до 90%

Ход проекта

Основная цель проекта — централизовать и автоматизировать процесс выявления, приоритизации и устранения уязвимостей в масштабах всей ИТ-инфраструктуры холдинга.

Для этого потребовалось выстроить несколько ключевых процессов, охватывающих все этапы управления уязвимостями (Vulnerability Management):

- Интеграция системы R-Vision VM со всеми ИТ и ИБ-системами холдинга;
- Сбор и анализ данных о каждом активе во всех филиалах при помощи сканера R-Vision;
- Настройка регулярного и оперативного сканирования ИТ-инфраструктуры на уязвимости с использованием встроенного сканера R-Vision VM;
- Приоритизация уязвимостей на основе их критичности и значимости активов;
- Двусторонняя интеграция с системой Service Desk (Jira), позволяющая автоматически создавать и передавать задачи на устранение уязвимостей;
- Контроль выполнения задач и автоматическая проверка устранения уязвимостей.

В ходе проекта особое внимание уделили интеграции R-Vision VM с существующими ИТ- и ИБ-системами холдинга, включая CMDB (собственная разработка заказчика), Kaspersky Security Center, Microsoft Active Directory и Microsoft SCCM (System Center Configuration Manager). Это позволило получить полную картину по всем активам и уязвимостям — как в центральном офисе, так и в филиалах.

Собранные данные использовались для автоматического формирования ресурсно-сервисной модели активов, где учитывались различные факторы: тип оборудования, ОС, прикладное ПО, физическое расположение, состояние поддержки и уровень критичности для бизнес-процессов. Это позволило оценить влияние каждого актива на ключевые бизнес-процессы, что стало основой для последующей точной приоритизации уязвимостей.

Карточка проекта

Заказчик

Крупный промышленный холдинг с распределённой ИТ-инфраструктурой, включающей 6 филиалов по всей стране.

Основное направление деятельности — разработка и производство высокопрочных сталей и сплавов.

Задачи

Централизовать и автоматизировать процесс выявления, приоритизации и устранения уязвимостей в масштабах всей ИТ-инфраструктуры холдинга

Решение

R-Vision VM - система автоматизации процесса управления уязвимостями со встроенным модулем сканирования

Результаты

Централизованный и автоматизированный процесс VM

Высокая скорость и точность работы с уязвимостями

Снижение времени на рутинные операции до 90%

Результат

Внедрение R-Vision VM помогло холдингу построить централизованный и автоматизированный процесс управления уязвимостями, повысить скорость и точность работы с уязвимостями, а также обеспечить полный контроль над их устранением.

О проекте из первых уст

Нашей задачей было не просто внедрить продукт, а адаптировать его под сложную распределённую инфраструктуру заказчика.

При внедрении мы учли множество факторов, таких как архитектура решения, текущие требования и уже работающие процедуры по управлению уязвимостями, а также имеющиеся ограничения, чтобы обеспечить точную приоритизацию, автоматизацию устранения и минимизацию ручных операций.

Андрей Селиванов,
руководитель продукта R-Vision VM

R-Vision – разработчик систем цифровизации и кибербезопасности. С 2011 года компания создаёт технологии, которые помогают организациям эффективно противостоять киберугрозам, поддерживать надёжность ИТ-инфраструктуры и обеспечивать цифровую трансформацию.

Технологии R-Vision используются в крупнейших банках,государственных организациях, нефтегазовой отрасли, энергетике, металлургии, промышленности и компаниях других отраслей.

sales@rvision.ru
+7 (499) 755 55 70
t.me/rvision_pro
vk.ru/rvision_ru