R-Vision

Крупный машиностроительный холдинг выстроил централизованный процесс управления уязвимостями на десятках тысяч активов с помощью R-Vision VM

История успеха



Заказчик
Крупный машиностроительный холдинг

Год основания
2002 год

Отрасль
Транспортное машиностроение

Количество сотрудников
›100 000

География
›30 стран

Производственная инфраструктура
›260 площадок

Задачи

ИТ-инфраструктура холдинга включает в себя более 30 000 активов и обьединяет офисные и производственные сегменты. Среда географически распределена, дочерние предприятия отличаются по качеству каналов связи и особенностям локальной инфраструктуры, а в едином контуре управления уязвимостями работают более 20 организаций со своими активами и зонами ответственности.

До внедрения R-Vision VM в компании уже использовались инструменты сканирования уязвимостей. Проверки проводились регулярно, результаты формировались в отчёты и передавались ИТ-подразделениям. Однако по мере роста масштаба и зрелости процессов существующего подхода стало недостаточно.

Основными ограничениями были:

- Существующие ограничения используемого решения не давали единой картины состояния инфраструктуры;
- Отсутствие единых правил работы с уязвимостями;
- Требование повысить своевременность и стабильность сканирования;
- Необходимость централизованного контроля актуальности обновлений;
- Высокая трудозатратность при обслуживании предыдущего VM-решения.

При таком масштабе задача заключалась уже не только в том, чтобы обнаружить отдельную уязвимость. Центральной команде было важно в любой момент понимать реальное состояние безопасности инфраструктуры в целом — какие активы существуют, где они расположены, насколько регулярно и своевременно они проверяются, и кто отвечает за устранение выявленных проблем.

Дополнительным катализатором пересмотра подхода стал инцидент в конце 2024 года, который наглядно показал необходимость более системного контроля. Команда пересмотрела требования к процессу Vulnerability Management и сделала акцент на централизованной видимости, контроле обновлений, масштабируемости и автоматизации.

Карточка проекта

Задачи

- Централизовать управление уязвимостями в распределённой инфраструктуре.
- Обеспечить единую видимость активов и их состояния по всем подключённым организациям и площадкам.
- Организовать своевременное и стабильное сканирование около 30 000 активов.
- Обеспечить контроль актуальности обновлений и критичных уязвимостей.
- Разграничить доступ организаций к собственным активам и результатам сканирования.
- Автоматизировать распределение активов, регулярное сканирование и формирование отчётности.
- Снизить объём ручных операций и нагрузку на центральную ИБ-команду.
- Формализовать взаимодействие между ИТ и ИБ и закрепить единый процесс управления уязвимостями.

Решение

R-Vision VM

Ход проекта

Одним из ключевых требований к новой системе стала возможность централизованно управлять распределённой инфраструктурой, сохраняя самостоятельность отдельных организаций.

Ключевыми требованиями к решению стали:

- Централизованная видимость: возможность получать единую картину активов, уязвимостей и результатов сканирования по подключённым организациям и площадкам.
- Мультитенантность и разграничение доступа: каждая организация должна видеть только свои активы и задачи, в то время как центральная команда сохраняет возможность контролировать процесс в целом.
- Стабильность и масштабируемость: система должна регулярно сканировать десятки тысяч активов и не требовать пропорционального увеличения ресурсов на сопровождение.
- Автоматизация: возможность минимизировать ручное распределение активов, запуск проверок и подготовку отчётности.
- Удобство работы: решение должно быть понятно как центральной команде ИБ, так и ИТ-специалистам на производственных площадках и не требовать сложного обучения.

Внедрение R-Vision VM началось с пилотного проекта на небольшой тестовой зоне из нескольких серверов. Уже в течение двух недель периметр был расширен на весь серверный сегмент, а после успешного пилота система перешла в промышленную эксплуатацию и начала масштабироваться на производственные площадки.

Для работы нескольких организаций в единой системе были разграничены зоны ответственности и права доступа (мультитенантная модель): каждая организация получила возможность работать со своими активами и результатами сканирования, при этом центральная команда сохранила общую картину и контроль процесса.

Карточка проекта

Результаты

- Централизовали управление уязвимостями: получили единую картину активов и уязвимостей по распределённой инфраструктуре.
- Настроили мультитенантную модель: более 20 организаций работают в едином контуре, каждая - со своими активами, задачами и результатами сканирования.
- Автоматизировали регулярные процессы: сканирование, распределение новых активов, отчётность и контроль актуальности обновлений.
- Выявили скрытые проблемы инфраструктуры: ранее неизвестные активы и ошибки конфигурации сетевого оборудования.
- Снизили ручную нагрузку и формализовали Vulnerability Management: закрепили единые правила работы и взаимодействие ИТ- и ИБ-подразделений.

Ход проекта

К работе с платформой начали подключать администраторов производственных площадок. Это позволило распределить ответственность между центральным подразделением и локальными командами, сохранив единый подход к управлению уязвимостями.

Одним из важных направлений стала автоматизация работы с активами. Для новых устройств были настроены правила автоматического распределения между организациями и группами, что сократило количество ручных операций при развитии и изменении инфраструктуры.

Также команда настроила необходимую форму отчётности с учётом внутренних требований. Отчёты по результатам сканирования регулярно направляются ИБ- и ИТ-подразделениям организаций, участвующих в процессе.

Сканирование выполняется с разной периодичностью в зависимости от типа проверки и критичности инфраструктуры.

Так сформировался повторяемый цикл работы: обнаружение активов, сканирование, анализ результатов, передача информации ответственным подразделениям, устранение и последующий контроль.

Параллельно техническое внедрение стало основой для развития самого процесса Vulnerability Management. Опыт эксплуатации предыдущих решений и работа с R-Vision VM позволили команде систематизировать практику и закрепить взаимодействие между ИТ и ИБ в единых регламентах.

Команда машиностроительного холдинга также отмечает взаимодействие со специалистами R-Vision на этапах внедрения и эксплуатации: возникающие вопросы и критичные для заказчика доработки передаются продуктовой команде, а пожелания по развитию функциональности учитываются при дальнейшей работе над платформой.

История Успеха

Проект в цифрах

~30 000
активов

~20
организаций в едином контуре управления уязвимостями



Ключевые результаты

Централизованная видимость: команда получила единую картину состояния активов и уязвимостей по подключённым организациям и площадкам.

Мультитенантная модель: около 20 организаций работают в единой системе, при этом каждая видит только собственные активы, задачи и результаты сканирования.

Стабильное регулярное сканирование: проверки выполняются по расписанию с периодичностью от недели до месяца в зависимости от типа сканирования и критичности инфраструктуры.

Контроль актуальности обновлений: команда может системно отслеживать состояние активов и своевременно выявлять системы, требующие установки обновлений.

Автоматизация работы с активами: вновь обнаруженные активы автоматически распределяются между организациями и группами на основании заданных правил.

Сокращение рутинной нагрузки: автоматизированы регулярные сканирования, распределение активов и формирование отчётности, что сделало процесс более прозрачным и снизило объём ручной работы.

Выявление ранее неизвестных активов: в ходе инвентаризации были обнаружены неучтённые системы, в том числе активы, оставшиеся после завершённых проектов.

Выявление и устранение ошибок конфигурации: система помогла обнаружить некорректные настройки сетевого оборудования, после чего конфигурация была скорректирована.

Формализация процесса Vulnerability Management: команда систематизировала накопленный опыт, сформировала единые правила работы с уязвимостями и закрепила взаимодействие между ИТ- и ИБ-подразделениями.

Основа для дальнейшего развития: команда продолжает развивать процесс, в том числе настраивает собственную формулу приоритизации уязвимостей с учётом контекста инфраструктуры.

История успеха

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

О проекте из первых уст

Для нас было важно не просто заменить один инструмент сканирования другим, а выстроить полноценный процесс управления уязвимостями. При масштабе в десятки тысяч активов и распределённой инфраструктуре критичны централизованная видимость, понятное распределение ответственности и стабильность работы системы.

R-Vision VM позволил объединить организации в едином контуре и при этом разграничить доступ к активам и результатам сканирования. Центральная команда получила общую картину состояния инфраструктуры, а локальные специалисты - возможность самостоятельно работать со своей зоной ответственности.

В результате мы смогли автоматизировать значительную часть рутинных операций, формализовать взаимодействие между ИТ и ИБ и перейти от отдельных проверок к системному управлению уязвимостями.

Отдельно хочется отметить взаимодействие с командой R-Vision. Специалисты сопровождают нас как на этапе внедрения, так и в процессе эксплуатации, оперативно реагируют на возникающие вопросы, а наши предложения учитываются в развитии продукта.

Представитель заказчика,
Руководитель SOC

