R-Vision

Как Домклик ускорил время решения инцидентов на 80% и усилил работу SOC с R-Vision SIEM и R-Vision UEBA

История успеха

Заказчик

Домклик

Домклик - сервис для поиска, покупки, продажи, аренды недвижимости и безопасного проведения сделок с жильём

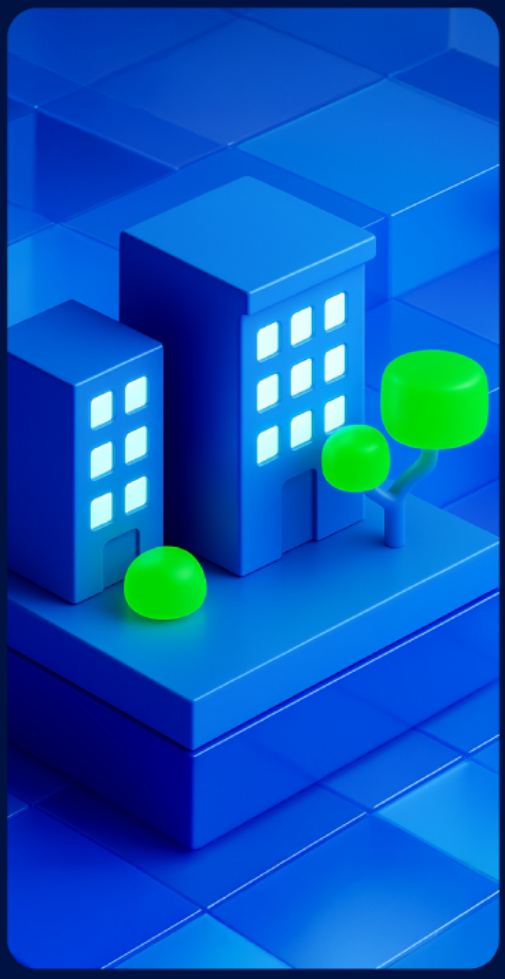
Отрасль
ИТ

Сотрудников
1 000+

Клиентов
730+ тысяч

Задачи

- **Обеспечение непрерывности бизнеса:** гарантировать стабильную и безопасную работу цифровых сервисов компании для более чем 20 млн активных пользователей в месяц.
- **Снижение зависимости от внешних факторов:** выстроить архитектуру ИБ, устойчивую к изменению регуляторных требований, рыночных условий и внешних атак.
- **Выявление и нейтрализация сложных угроз:** обеспечить возможность обнаружения и анализа продвинутых атак (APT, инсайдерские сценарии, таргетированные атаки на бизнес-приложения).
- **Развитие внутренних компетенций:** сформировать в компании центр экспертизы по SIEM/UEBA, подготовить специалистов к самостоятельной разработке правил корреляции и сценариев реагирования, заложив основу для дальнейшего роста SOC.



Ход проекта

Домклик внедрил комплексное решение R-Vision SIEM и R-Vision UEBA, обеспечив централизованное управление событиями безопасности, их анализ и корреляцию в режиме реального времени.

Гибридное решение позволяет собирать логи с серверов, рабочих станций, сетевых устройств и бизнес-приложений, проводить нормализацию и обогащение данных, а также автоматически выявлять аномалии с помощью продвинутой поведенческой аналитики на базе алгоритмов машинного обучения. Подключение бизнес-систем осуществлялось по степени критичности обрабатываемых данных: в первую очередь были интегрированы системы, содержащие наибольшие объёмы клиентских данных.

С учётом особенностей инфраструктуры был разработан кастомизированный сервис интеграции с DLP-системой Домклик, обеспечивающий корректный и стабильный сбор событий и их передачу в R-Vision SIEM. Сервис закрыл критически важный интеграционный сценарий и позволил обеспечить полноту данных в системе мониторинга.

История успеха

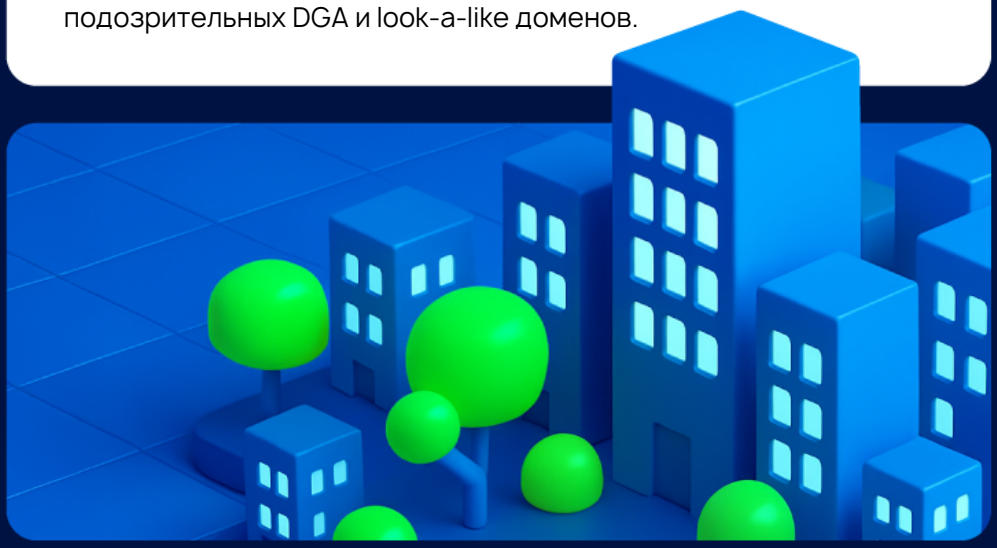
Проект в цифрах

На 60%
сократилось среднее время реагирования

На 80%
уменьшилось среднее время решения инцидента

Дополнительно была реализована интеграция R-Vision SIEM с Telegram-ботом, благодаря чему команда безопасности Домклик получила возможность в режиме реального времени получать уведомления о срабатываниях и оперативно реагировать на инциденты.

Параллельно решение R-Vision UEBA обеспечило детальный анализ событий авторизации, попыток перебора паролей, управления учетными записями и группами безопасности, запусков процессов и приложений, мониторинг почтового трафика, а также выявление подозрительных DGA и look-a-like доменов.



~72kEPS

R-Vision SIEM стабильно обрабатывает в пиковой нагрузке — это в 5 раз выше плановых проектных мощностей

Результат

На текущий момент все события анализируются с использованием сложных корреляционных правил и продвинутой поведенческой аналитики, что позволяет SOC работать проактивно, а не только реагировать на угрозы. Время выявления инцидентов сократилось на 60% и время реагирования — на 80%.

SIEM-система демонстрирует стабильную работу под нагрузкой ~ 72к EPS, при ресурсах на коллекторе CPU - 16 ядер и RAM 8 ГБ (по RAM не использовалось и половины, CPU ~ 80-85%).

Также команда R-Vision провела для Домклик расширенное обучение по работе с функционалом решения. В результате команда Домкли» существенно повысила уровень компетенций и перешла к самостоятельной разработке правил корреляции и нормализации для R-Vision SIEM, заложив тем самым основу для дальнейшего совершенствования SOC в компании.

История успеха

Карточка проекта

Заказчик

Домклик

Задачи

Гарантировать стабильную и безопасную работу цифровых сервисов компании

Выстроить архитектуру ИБ, устойчивую к внешним изменениям

Обеспечить возможность обнаружения и анализа продвинутых атак

Сформировать в компании центр экспертизы и подготовить специалистов к самостоятельной работе, заложив основу для дальнейшего роста SOC

Решение

R-Vision SIEM, R-Vision UEBA

Результаты

Открыты новые инциденты, которые ранее были вне доступа

Время выявления инцидентов сократилось на 60%, время реагирования — на 80%

Все события теперь анализируются с использованием сложных корреляционных правил и продвинутой поведенческой аналитики

Сформированы устойчивые компетенции по самостоятельному созданию и адаптации корреляционных правил и схем нормализации данных командой Домклик

О проекте из первых уст

С самого начала мы смотрели на данный проект как на развитие нашей архитектуры безопасности. Нам было важно получить более глубокую связность данных, повысить точность выявления и сделать реагирование более осмысленным.

Сегодня команда использует сложные корреляции как естественную часть ежедневной работы и понимает, как развивать системы дальше. Мы стали действовать быстрее и увереннее, а сам SOC стал устойчивее к изменениям и новым сценариям атак.

Домклик

Андрей Лагоденко,
исполнительный директор – начальник управления кибербезопасности «Домклик»

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