R-Vision CERS

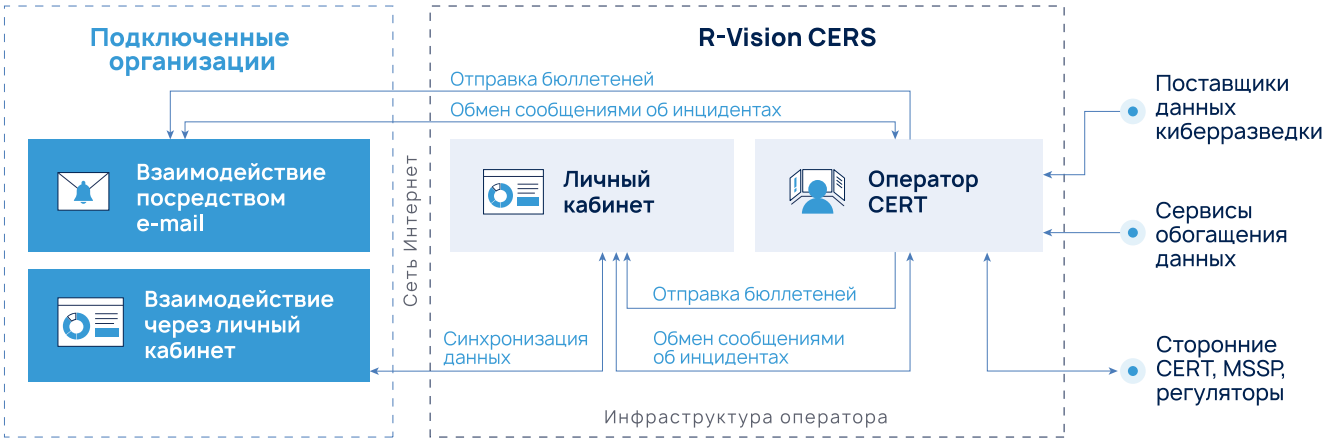
Построение центра реагирования
на компьютерные инциденты и киберугрозы

R-Vision

R-Vision CERS (Computer Emergency Response System) представляет собой программный комплекс, который позволяет создать центр мониторинга и реагирования на компьютерные инциденты (CERT/CSIRT) с интегрированными функциями обработки данных о киберугрозах.

С помощью R-Vision CERS можно реализовать как территориальный/государственный центр мониторинга и реагирования на компьютерные инциденты, так и ведомственный/ корпоративный центр, услугами которого могут пользоваться подведомственные организации/дочерние организации.

Оператор CERT получает готовый инструмент для обработки и анализа данных по компьютерным инцидентам и угрозам, осуществления информационного обмена с подключенными организациями (участниками) и оперативного информирования.



Функциональные возможности

Агрегация информации об инцидентах и киберугрозах

Программный комплекс R-Vision CERS агрегирует информацию об инцидентах и уязвимостях, поступающую от подключенных организаций, а также сведения об угрозах, полученные из внешних источников. Все поступающие сообщения об индикаторах вредоносной активности обрабатываются в соответствии с настроенными правилами и обогащаются дополнительным контекстом.

Создание личного кабинета подключенной организации

В системе предусмотрена возможность создания Личного Кабинета (ЛК) для подключаемой организации с целью оперативного обмена данными и визуализации метрик. Готовый инструмент обладает рядом функциональных возможностей, среди которых:

- отправка сообщений об инцидентах
- просмотр сводной статистики по инцидентам
- взаимодействие со специалистами оператора
- получение бюллетеней с информацией об угрозах от оператора

Передача сведений об активах организации в CERT

В ЛК организации могут вести базу информационных активов с указанием атрибутов для их идентификации. Оператору CERT могут передаваться сведения о различных типах информационных активов, как предустановленных, так и пользовательских, актуальных для той или иной отрасли подключенных организаций.

Информационный обмен с участниками

В R-Vision CERS регистрируются все обращения, поступающие от подключенных организаций, и поддерживается обмен сведениями, связанными с инцидентами.

Автоматизация реагирования на компьютерные инциденты

R-Vision CERS позволяет автоматизировать процесс обработки инцидентов, включая информирование участников о релевантных угрозах и уязвимостях и обмен данными с внешними CERT/CSIRT/SOC.

Встроенные сценарии реагирования позволяют оперативно обрабатывать входящую информацию, оповещать участников о новых угрозах и уязвимостях и направлять рекомендации для эффективного реагирования на инциденты.

Формирование информационных бюллетеней и информирование

В R-Vision CERS предусмотрена возможность формирования собственных информационных бюллетеней об угрозах на основе обработанных и проанализированных данных, полученных с помощью TI-компонента из внешних систем, а также созданных аналитиками CERT, и информирования участников.

Выстраивание взаимодействия с внешними центрами реагирования на компьютерные инциденты

Поддержка различных механизмов интеграции в R-Vision CERS позволяет реализовать информационный обмен с внешними центрами реагирования (CERT/CSIRT/SOC), MSS-провайдерами, включая зарубежные.

Предоставление статистических данных и отчетность

Специалисты центра мониторинга и команды подключенных к центру организаций с помощью системы R-Vision CERS могут формировать различные отчеты и графики:

- информация по собранным и обработанным инцидентам
- данные по собранным информационным активам
- отчет/график по выполнению SLA
- детальная статистика по работе ответственных за выявление инцидентов, обрабатываемых в центре
- отчеты для руководства
- иные пользовательские отчеты и графики

Преимущества R-Vision CERS

- **Центр экспертизы и знаний,** аккумулирующий сведения об угрозах, уязвимостях, методах и средствах злоумышленников, способах противодействия.
- **Наличие TI (Threat Intelligence)компонента**, обеспечивающего анализ и обработку данных киберразведки и применение полученной информации в процессах CERT.
- **Глобальный контроль и анализ информации** по инцидентам и киберугрозам в масштабе территории/государства, отрасли, группы организаций и применение знаний об угрозах на основе данных киберразведки.
- **Единая система** для обработки больших обьемов данных и организации работы команды CERT.
- **Позволяет выстроить информационный обмен** и связанные процессы по угрозам и уязвимостям внутри отрасли или ряда организаций.
- **Повышение уровня осведомленности об актуальных угрозах** за счет оперативного распространения проанализированной аналитиками CERT релевантной информации об угрозах на группу компаний, отрасль, регион и, как следствие, уровня защищенности для всех подключенных организаций.

R-Vision

О компании

R-Vision – российский разработчик систем кибербезопасности. Компания с 2011 года создает технологии, которые помогают организациям эффективно противостоять актуальным киберугрозам и обеспечивать надежное управление информационной безопасностью.

Технологии R-Vision применяются в государственных учреждениях, финансовой сфере, телекоммуникациях, а также в нефтегазовой, энергетической и металлургической отраслях промышленности в России и странах СНГ.

rvision.ru

sales@rvision.ru

+7 (499) 322 80 40

t.me/rvision_pro

vk.ru/rvision_ru

youtube.com/@rvision_ru