R-Vision Threat Deception Platform

Имитация ИТ-инфраструктуры
для обнаружения кибератак

R·Vision

R-Vision Threat Deception Platform представляет собой комплекс технологий цифровой имитации элементов ИТ-инфраструктуры для раннего обнаружения и предотвращения кибератак. С помощью набора ловушек и приманок R-Vision TDP детектирует присутствие злоумышленника, замедляет его продвижение внутри сети и дает возможность ИБ-специалистам остановить развитие атаки.

Платформа зарегистрирована в Реестре отечественного ПО
Запись в реестре №11731 от 15.10.2021

Ключевые элементы R-Vision TDP

Приманки

Информация, представляющая интерес для злоумышленника, которая приведет его в ловушку.

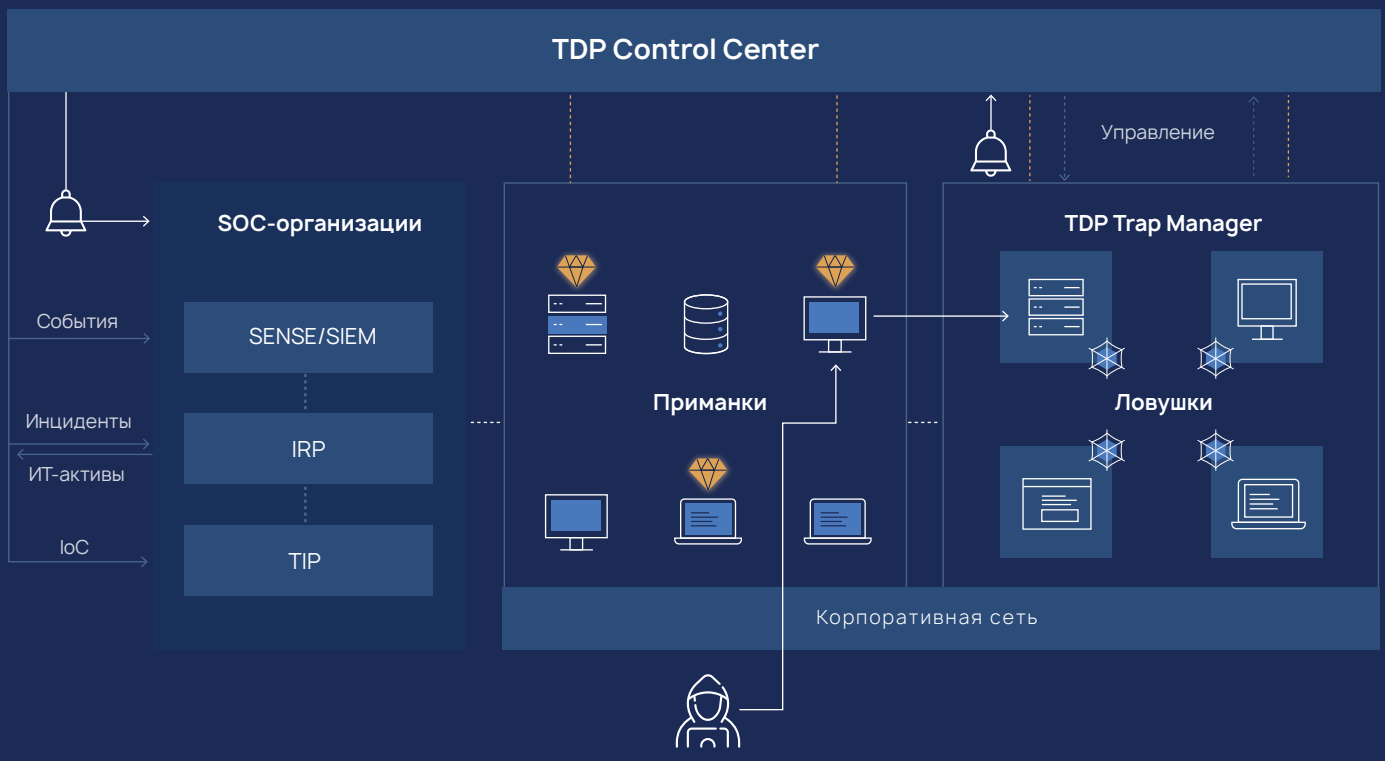
- ✓ Учетные записи
- ✓ Файлы данных
- ✓ История браузера
- ✓ Ключи и т. д.

Ловушки

Ложные узлы сети, позволяющие обнаружить злоумышленника и отвлечь его от настоящих узлов.

- ✓ Рабочие станции
- ✓ Сетевое оборудование
- ✓ Серверы
- ✓ Сервисы и т. д.

Схема работы R-Vision TDP



Функциональные возможности R-Vision TDP

Централизованное управление системой ловушек

R-Vision TDP автоматически разворачивает комплекс ловушек, эмулирующих реальные ИТ-активы организации, и позволяет управлять ими из **единого центра**. С помощью готовых шаблонов ловушек можно быстро воссоздать подразделения организации и воспроизвести специфические системы. Для большей привлекательности и реалистичности эмулированные элементы повторяют параметры реальной сети и особенности ее функционирования.

Автоматическая генерация и расстановка приманок

Для привлечения внимания злоумышленника на ловушках и по узлам реальной инфраструктуры автоматически расставляются приманки, которые генерируются с соблюдением характерных для организации параметров, таких как политика именования учетных записей и рабочих станций, используемое ПО, версии ОС и другие.

Обнаружение злоумышленника и реагирование

R-Vision TDP детектирует события при взаимодействии с ловушками, осуществляет их обработку и направляет оповещение об обнаружении ИБ-специалисту. Эти события можно передать в SIEM-системы или в аналитическую платформу кибербезопасности R-Vision SENSE что позволит собрать всю информацию по взаимодействию с ловушками и предоставить необходимый контекст аналитику SOC. Полученные инциденты можно также передать в системы IRP/SOAR, в том числе в R-Vision IRP, и автоматизировать процесс реагирования за счет предустановленных сценариев.

Сбор данных и атрибутов атакующего

В процессе анализа действий злоумышленника R-Vision TDP собирает атрибуты и индикаторы компрометации, которые могут быть переданы в системы управления данными киберразведки (Threat Intelligence), в том числе в R-Vision TIP. TI-платформа позволит обогатить эти данные, выявить взаимосвязи с другими доступными данными TI, настроить автоматический мониторинг в событиях SIEM, а также экспортировать индикаторы компрометации на средства защиты для блокировки.

Преимущества от использования

- Обнаружение атак, которые невозможно детектировать другими средствами (целенаправленные атаки, угрозы нулевого дня и другие)
- Снижение скорости продвижения злоумышленника внутри сети за счет создания дополнительного слоя из эмулированных элементов
- Возможность предотвращения атак на ранних стадиях до наступления значительного ущерба
- Выявление слабых мест в защите, понимание инструментов и действий атакующего в отношении инфраструктуры организации
- Низкий процент ложных срабатываний

R-Vision

О компании

R-Vision – разработчик систем кибербезопасности. Компания с 2011 года создает продукты и сервисы, которые помогают бизнесу и государственным организациям по всему миру уверенно противостоять актуальным киберугрозам и обеспечивать надежное управление информационной безопасностью.

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

www.rvision.ru

sales@rvision.ru

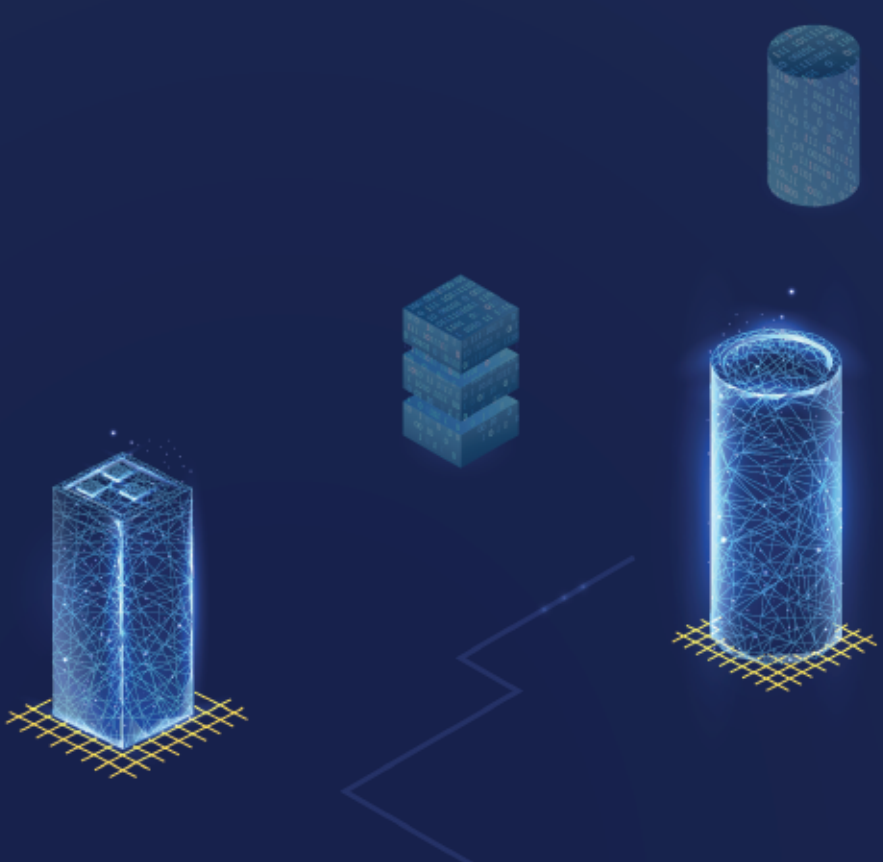
+7 (499) 322 80 40

Дайджест информационной безопасности:
rvision.ru/blog

t.me/rvision_pro

/rvision_ru

/RvisionPro



Sk Участник