R-Vision TDP

Имитация ИТ-инфраструктуры для обнаружения кибератак

R-Vision Threat Deception Platform

R-Vision TDP (Threat Deception Platform) – 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 даёт возможность ИБ-специалистам остановить развитие атаки.

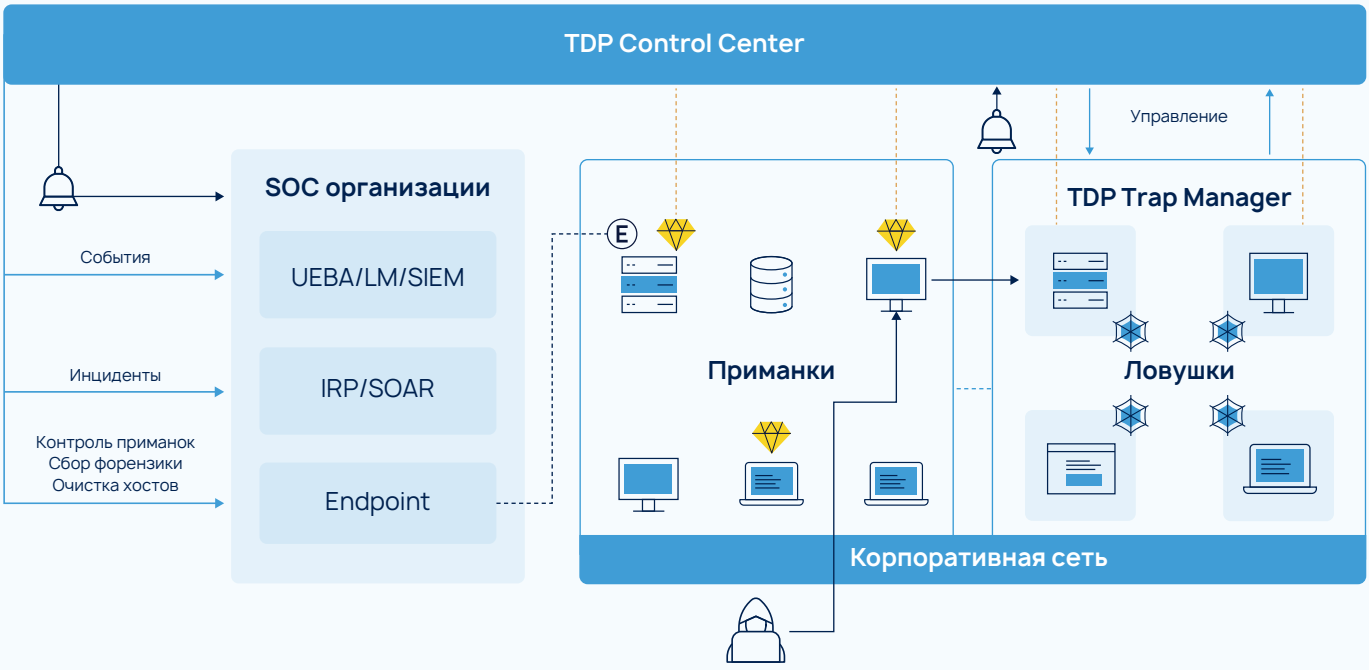
Реалистичность для хакера: каждая приманка ведёт в уникальную ловушку

Широкий перечень видов ловушек и приманок, включая АСУТП и специфические

Безагентское и агентское размещение приманок

Сервер управления работает **на Linux, поддержка российских ОС**

Задачи	Решения
Обнаружить и замедлить развитие сложных атак (APT и 0-day), недетектируемых другими средствами	Сеть взаимосвязанных ловушек и приманок позволяет выявить злоумышленника на этапе горизонтального перемещения после обхода им традиционных средств защиты и систем обнаружения
Предотвратить намеренную или случайную утечку конфиденциальных данных через сотрудников организации	Ловушки, эмулирующие реальные ИТ-активы, не участвуют в рабочих процессах, любое взаимодействие с ними является инцидентом и требует расследования
Выявить слабые места в инфраструктуре и защитить высококритичные активы	Приманки, ведущие в ловушки, автоматически размещаются в инфраструктуре, отвлекают атакующего от ценных активов и позволяют анализировать его действия в контексте конкретной организации



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 её 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 учётных 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 для обнаружения угроз и аномалий R-Vision UEBA, 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 SOAR, и автоматизировать процесс реагирования за счёт 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.

Ключевые элементы R-Vision TDP

Приманки

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

- Учётные 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
- Промышленные контроллеры, базы данных
- Серверы
- Сервисы и т.д.

R-Vision

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.

R-Vision TDP зарегистрирован в Реестре отечественного ПО и сертифицирован ФСТЭК России по 4 уровню доверия.

rvision.ru
sales@rvision.ru
+7 (499) 322 80 40
t.me/rvision_pro
vk.ru/rvision_ru
youtube.com/@rvision_ru
rvision.ru