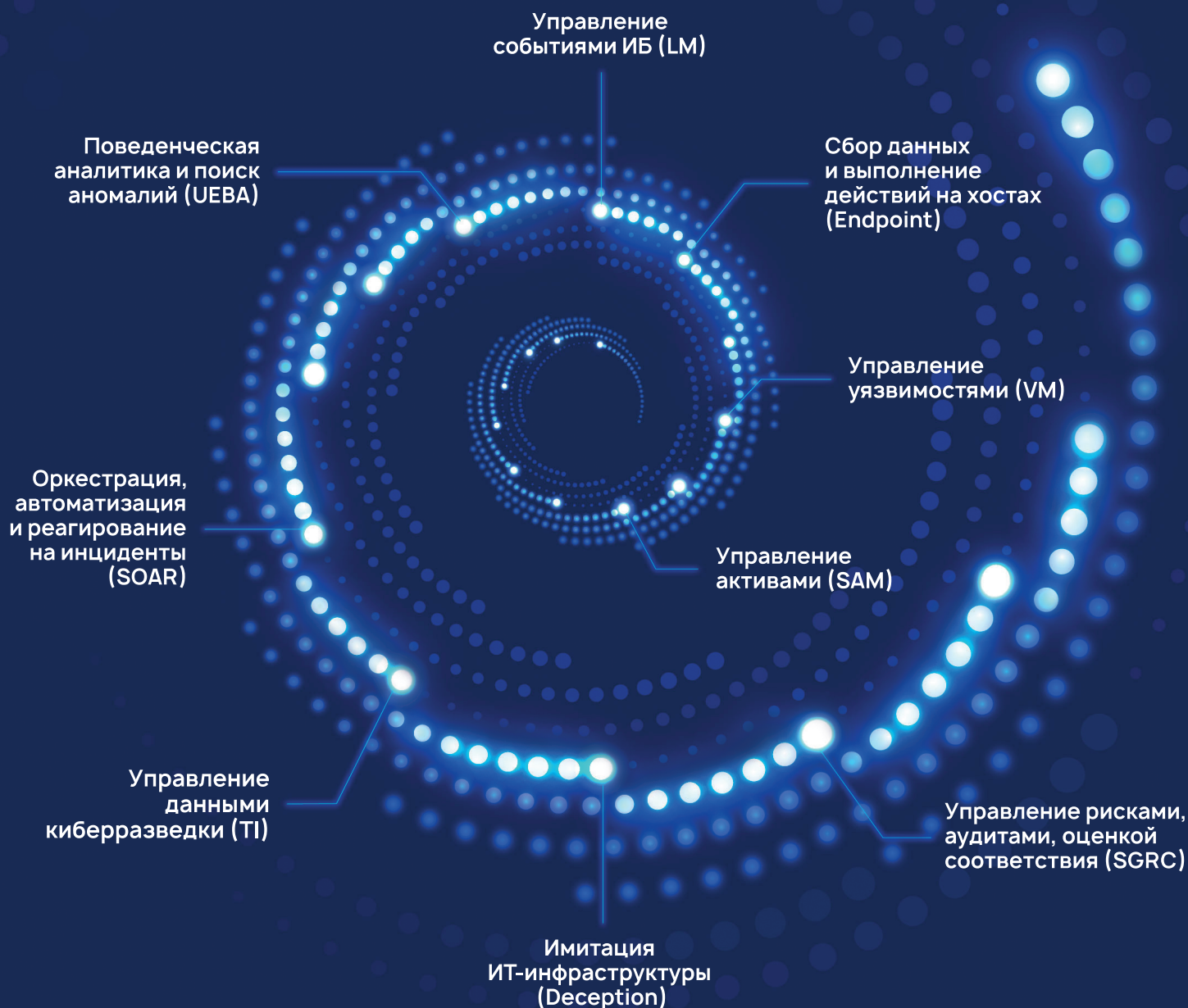


R-Vision EVO

Экосистема технологий для эволюции SOC



R-Vision

Экосистема R-Vision EVO — это комплекс взаимосвязанных технологий, компонентов и выстроенных между ними процессов, которые позволяют компаниям построить Security Operation Center и развивать его до необходимого уровня зрелости. Технологии R-Vision EVO помогают эволюционировать всем SOC, вне зависимости от их первоначального масштаба и отрасли.

Технологии экосистемы и их функционал



Vulnerability Management (VM) автоматизирует процесс управления уязвимостями, агрегирует данные по уязвимостям и приоритизирует их обработку на основании автоматически рассчитанного рейтинга. Рейтинг динамический и может быть адаптирован под конкретную организацию.



Deception имитирует элементы инфраструктуры, детектирует присутствие злоумышленника в сети, замедляет его горизонтальное перемещение и дает возможность своевременно остановить развитие атаки.



Log Management (LM) организует процесс сбора, обработки, хранения событий ИБ со всех элементов инфраструктуры, а также предоставляет возможность извлечения и анализа собранной информации.



Endpoint собирает ИБ и ИТ-события с конечных точек, инвентаризирует данные об активах, позволяет оперативно реагировать на инциденты на хостах, а также автоматически проводить аудит соответствия стандартам ИБ.



Security Orchestration, Automation, Response (SOAR) автоматизирует процесс управления инцидентами ИБ, агрегирует данные по инцидентам, автоматически запускает сценарии реагирования, а также управляет другими системами через механизм оркестрации.



Security Governance, Risk management, Compliance (SGRC) формирует процессы менеджмента ИБ в соответствии с лучшими практиками и стандартами, позволяет контролировать все ИБ-процессы и принимать обоснованные решения по развитию системы ИБ в организации.



User and Entity Behavior Analytics (UEBA) детектирует нарушения в состоянии ИТ и ИБ-систем и подозрительную активность объектов, применяя инструменты ML-анализа, в том числе осуществляет динамическую оценку угроз и аномалий.



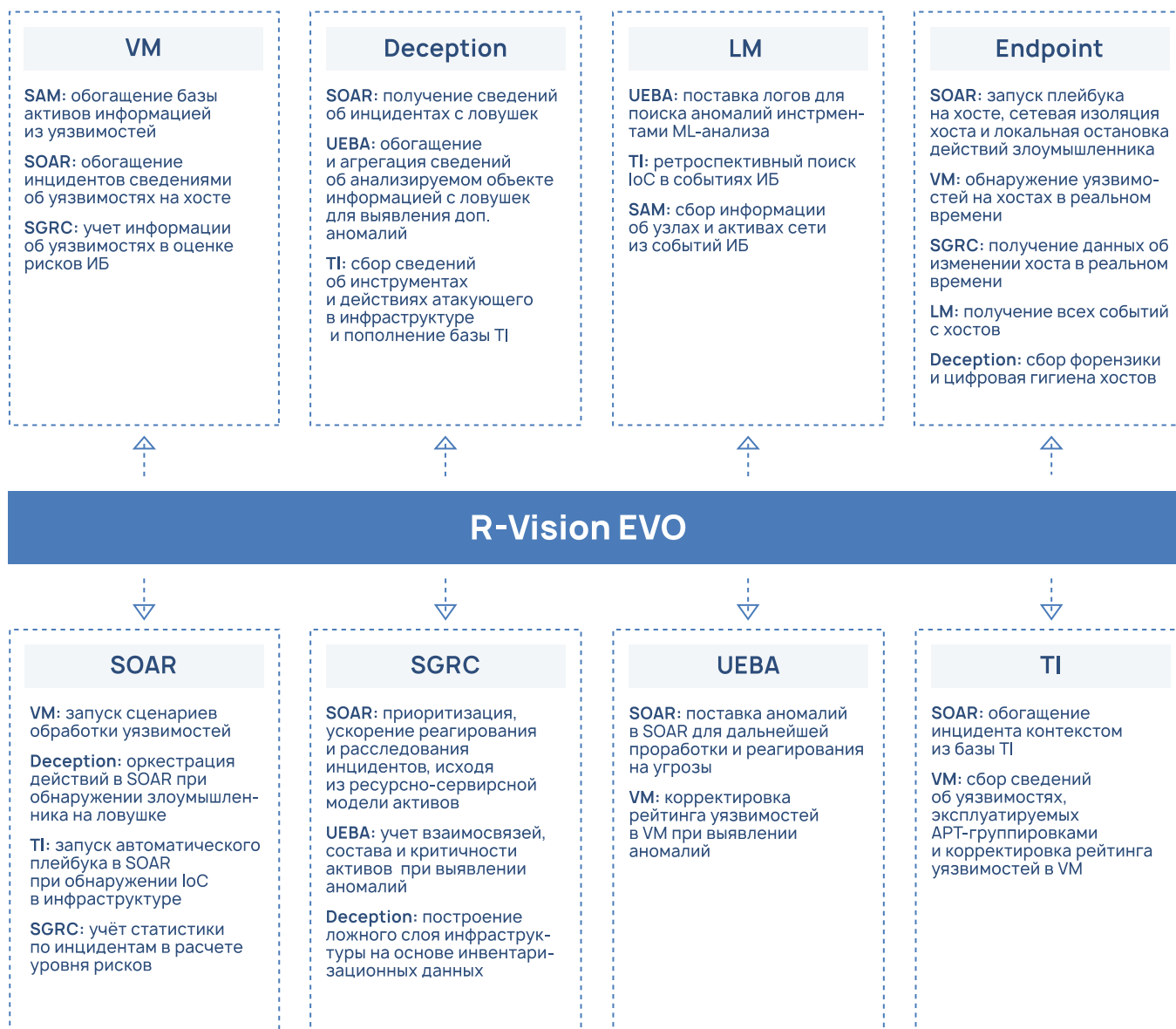
Threat Intelligence (TI) обеспечивает сбор, нормализацию и обогащение IoCs из различных источников, автоматизирует процесс управления данными киберразведки, позволяет передавать обработанную информацию напрямую на СЗИ, а также осуществлять поиск и обнаружение IoCs в инфраструктуре.



Security Asset Management (SAM) выстраивает процесс управления активами организации, автоматизирует построение ресурсно-сервисной модели и сбор всеобъемлющей инвентаризационной информации, контролирует установленные обновления.

Взаимодействие компонентов экосистемы

Технологии R-Vision EVO обогащаются дополнительным функционалом при совместном использовании с другими элементами экосистемы



Преимущества использования экосистемы R-Vision EVO

- Решение задач на стыке технологий и компонентов экосистемы
- Возможность поэтапного наращивания и расширения функционала экосистемы по мере роста потребностей Вашего SOC
- Наличие встроенных единых интеграционных механизмов, конфигураций, ролевых моделей и других функций
- Формирование долгосрочного плана развития SOC и построения эффективной защиты
- Достижение быстрых результатов за счет опыта и экспертизы вендора
- Экспертная поддержка на каждом этапе внедрения технологий экосистемы



О компании

R-Vision – разработчик систем кибербезопасности. Компания с 2011 года создает технологии, 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.

 rvision.ru

 t.me/rvision_pro

 sales@rvision.ru

 [/rvision_ru](https://vk.com/rvision_ru)

 +7 (499) 322 80 40

 [/RVisionPro](https://www.youtube.com/RVisionPro)

Дайджест информационной безопасности: rvision.ru/blog

