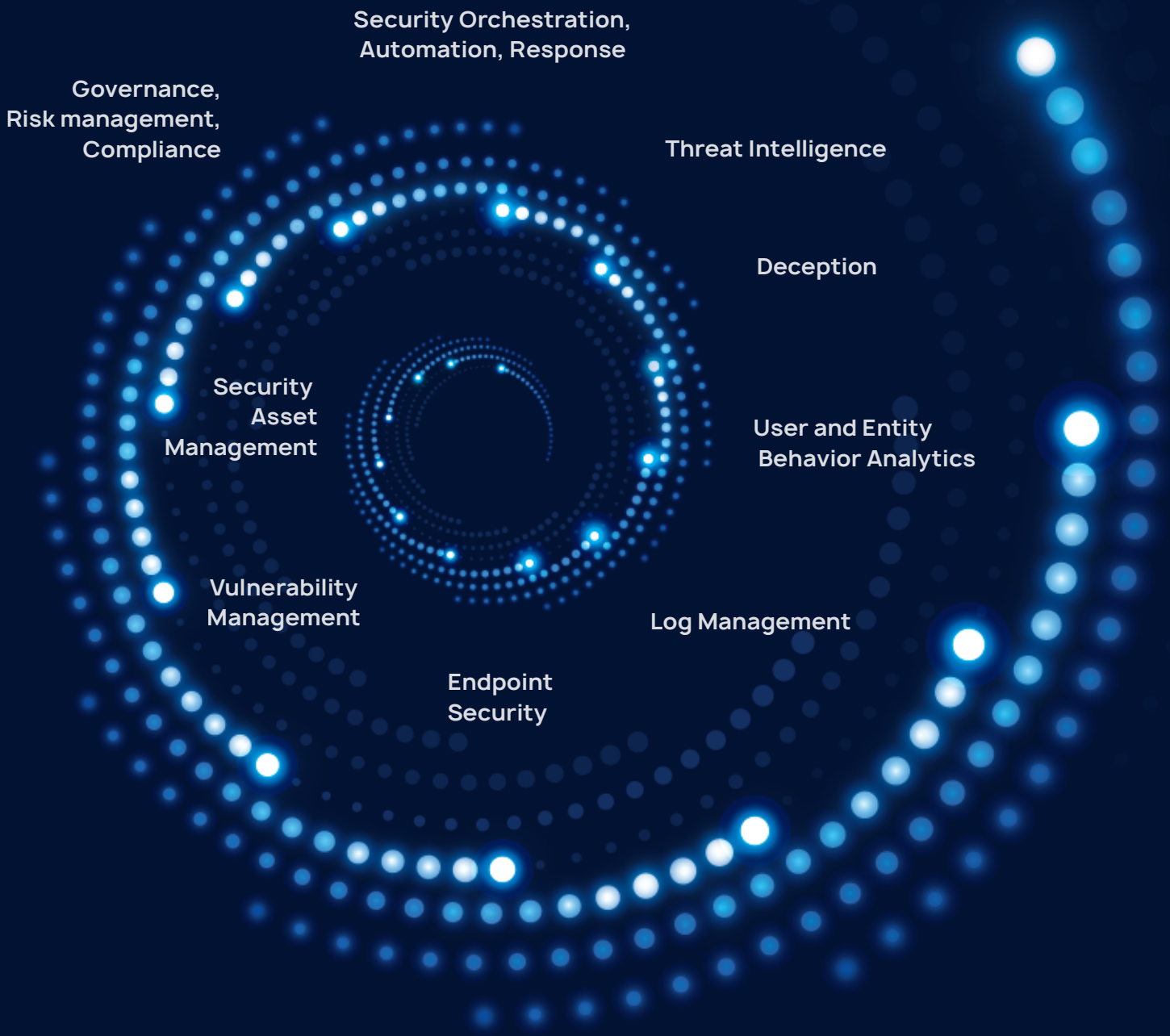
# Экосистема R-Vision EVO

## Технологии эволюции SOC




R-Vision

**Экосистема R-Vision** — 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, входящие в экосистему R-Vision EVO

- Security Asset Management (SAM);
- Vulnerability Management (VM);
- Endpoint Security (ES);
- Log Management (LM);
- User and Entity Behavior Analytics (UEBA);
- Security Orchestration, Automation, Response (SOAR);
- Threat Intelligence (TI);
- Deception;
- Governance, Risk management, Compliance (SGRC).

## Основные функциональные возможности

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

**Vulnerability Management** 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.

**Endpoint Security** собирает и инвентаризирует информацию о событиях ИБ с конечных точек и дополняет PCM инвентаризационной информацией, а также агрегирует события и позволяет реагировать на инциденты для ликвидации последствий атаки на хостах.

**Log Management** собирает события со всех элементов инфраструктуры, а также позволяет выстроить процесс сбора, нормализации и хранения событий ИБ и предоставляет возможность анализа собранной информации.

**User and Entity Behavior Analytics** детектирует нарушения в состоянии ИТ и ИБ-систем, подозрительную активность объектов и осуществляет динамическую оценку угроз и аномалий.

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

**Threat Intelligence** автоматизирует процесс управления данными киберразведки, обеспечивает сбор, нормализацию и обогащение IoC, передачу обработанных данных напрямую на СЗИ, а также осуществляет поиск и обнаружение IoC в инфраструктуре.

**Deception** имитирует элементы инфраструктуры, за счет чего осуществляется детектирование присутствия злоумышленника, замедление его продвижение внутри сети, и дает возможность своевременно остановить атаку.

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

## Дополнительный функционал

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

### UEBA

**SOAR:** поставка аномалий в SOAR для дальнейшей проработки и реагирования на угрозы

**VM:** корректировка рейтинга уязвимостей в VM при выявлении аномалий

### Deception

**UEBA:** обогащение и агрегация сведений об анализируемом объекте информацией с ловушек для выявления доп. аномалий

**TI:** сбор сведений об инструментах и действиях атакующего в отношении инфраструктуры и пополнение базы TI

### Endpoint Security

**SOAR:** запуск плейбука на хосте, сетевая изоляция хоста и локальное предотвращение действий злоумышленника, остановка вредоносного процесса

**VM:** обнаружение уязвимостей на хостах в реальном времени

**SAM:** получение данных об изменении хоста в реальном времени без доп. сканирования

### LM

**UEBA:** LM приоритетный поставщик логов для поиска аномалий программными экспертами UEBA

**TI:** ретроспективный поиск IoC в событиях ИБ

**SAM:** сбор информации об узлах и активах сети из событий ИБ

## R-Vision EVO

### SAM

**UEBA:** учет взаимосвязей, состава, критичности активов PCM* при выявлении аномалий

**SOAR:** приоритизация, ускорение реагирования и расследования инцидентов, исходя из PCM* активов

**SGRC:** учет взаимосвязей, состава, критичности активов PCM* для проведения оценки рисков в SGRC, учет объектов КИИ для проведения аудитов

**Deception:** построение ложного слоя инфраструктуры на основе инвентаризационных данных

### VM

**SAM:** обогащение базы активов информацией из уязвимостей

**SOAR:** обогащение инцидентов сведениями об уязвимостях на хосте

**SGRC:** учет информации об уязвимостях в оценке рисков ИБ

### SOAR

**VM:** запуск сценариев обработки уязвимостей

**Deception:** оркестрация действий для своевременной локализации злоумышленника на ловушке и сбора информации для предотвращения его продвижения

**TI:** запуск автоматического плейбука в SOAR при обнаружении IoC в инфраструктуре

**SGRC:** учёт статистики по инцидентам в расчете уровня рисков

### TI

**SOAR:** обогащение инцидента контекстом из базы TI

**VM:** сбор сведений об уязвимостях, эксплуатируемых APT-группировками и корректировка рейтинга уязвимостей в VM

***PCM - ресурсно-сервисная модель**

## 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
- Достижения быстрых результатов за счет опыта и экспертизы вендора

R-Vision

## О компании

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


rvision.ru

t.me/rvision_pro

sales@rvision.ru

/rvision_ru

+7 (499) 322 80 40

/RVisionPro


Дайджест информационной безопасности: **rvision.ru/blog**