Концепция экосистемы SOC

На базе продуктов R-Vision

Москва, 2022г.

1. Краткое описание линейки продуктов

R-Vision SENSE представляет собой аналитическую платформу кибербезопасности, которая детектирует нарушения в состоянии систем, подозрительную активность объектов и осуществляет динамическую оценку угроз и аномалий.

R-Vision Threat Intelligence Platform (TIP) представляет собой специализированную платформу управления данными киберразведки. Продукт обеспечивает автоматический сбор, нормализацию и обогащение индикаторов компрометации, передачу обработанных данных напрямую на внутренние средства защиты, а также поиск и обнаружение индикаторов во внутренней инфраструктуре организации с помощью сенсоров.

R-Vision Incident Response Platform (IRP) представляет собой платформу класса **SOAR** (Security Orchestration Automation & Response), предназначенную для автоматизации деятельности центров мониторинга и реагирования на инциденты ИБ.

R-Vision Threat Deception Platform (TDP) представляет собой комплекс технологий цифровой имитации элементов ИТ-инфраструктуры класса DDP (Distributed Deception Platform), предназначенный для обнаружения злоумышленников, проникших в корпоративную сеть, замедления их продвижения внутри сети, сбора контекста по средствам и действиям злоумышленника и анализа слабых мест инфраструктуры.

R-Vision Security GRC Platform (SGRC) представляет собой программную платформу для централизованного управления информационной безопасностью. Продукт позволяет автоматизировать:

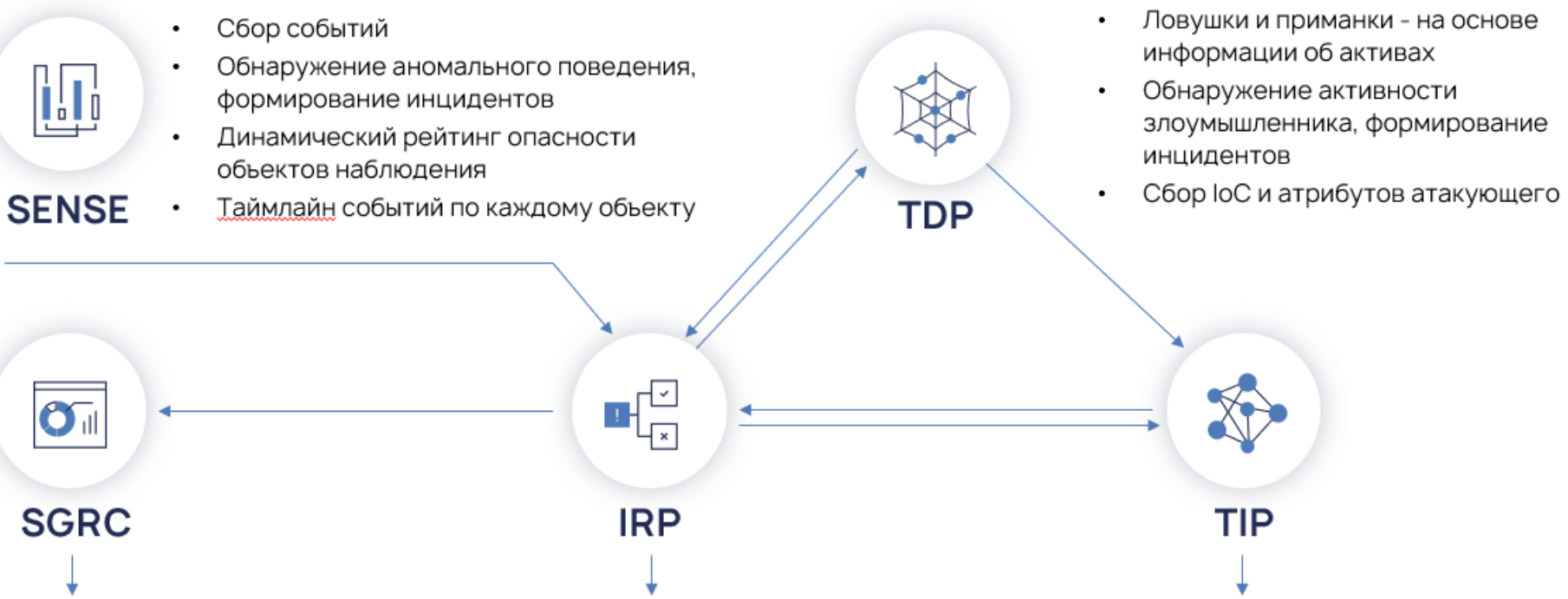
- Контроль и управление информационными активами
- Оценку соответствия требованиям информационной безопасности
- Анализ и управление рисками, моделирование угроз
- Категорирование объектов КИИ
- Мониторинг состояния информационной безопасности

2. Подход в построении SOC

Все компоненты SOC должны обеспечивать максимальную автоматизацию входящих процессов по обеспечению высокого уровня информационной безопасности. Значительно повысить уровень зрелости ИБ поможет внедрение продуктов компании R-Vision, которые обеспечивают интегрированный целостный подход к управлению информационной безопасностью через взаимосвязь стратегии, процессов, технологий и человеческих ресурсов.

R-Vision

Экосистема R-Vision



1. Продукт **R-Vision SENSE** осуществляет непрерывный мониторинг событий безопасности, анализируя данные из различных источников, включая системы лог-менеджмента, SIEM и другие. С помощью функционала самообучения на инфраструктуре Клиента, R-Vision SENSE формирует профили нормального поведения объектов и фиксирует подозрительную активность в случае отклонений.

   Продукт позволит:

   - Значительно снизить количество ложных срабатываний, по сравнению с SIEM-системой.
   - Обнаруживать скрытые угрозы, которые невозможно выявить обычными правилами корреляции.
   - Приоритизировать критичные угрозы и аномалии, сфокусировать внимание на действительно критичных инцидентах.
   - Упростить анализ инцидентов с помощью интуитивно понятного таймлайна.

2. **R-Vision TIP** агрегирует данные об известных мировых и локальных угрозах из различных внешних источников и осуществляет автоматическую обработку полученных сведений.

   Продукт позволит:

   - Проводить анализ взаимосвязей индикаторов, отчетов, вредоносного ПО, уязвимостей.
   - Проводить глубокий анализ индикаторов благодаря автоматическому обогащению из внешних источников.
   - Проводить ретроспективный поиск индикаторов, которые уже присутствуют в инфраструктуре
   - Распространять списки индикаторов на периметровые средства защиты, чтобы всегда держать в актуальном состоянии черные списки.

3. **R-Vision IRP/SOAR** агрегирует сведения об инцидентах из различных источников (SENSE, TIP, SIEM и пр.) и автоматизирует процессы реагирования и расследования на инциденты ИБ, благодаря преднастроенным сценариям реагирования. Значительная часть работы специалиста SOC автоматизируется, что позволяет фокусироваться на восстановлении от последствий инцидента, что в свою очередь приводит к снижению затрат.

   Продукт позволит:

   - Значительно сократить время реагирования на инцидент и возможный ущерб.
   - Координировать и управлять действиями команды реагирования SOC.
   - Управлять процессом расследования инцидентов ИБ с реализацией технических мер реагирования + оркестрацией всех необходимых средств защиты в единую консоль.
   - Автоматизировать процесс управления уязвимостями ИБ.

- Автоматизировать информационный обмен по инцидентам с ГосСОПКА.
- Увидеть детальную картину по информационным ресурсам, активам, процессам.

4. **R-Vision TDP** с помощью набора ловушек и приманок детектирует присутствие киберпреступника, замедляет его продвижение внутри сети, запутывая среди ложных объектов, и дает возможность ИБ-специалистам остановить развитие атаки до того, как она приведет к значимому ущербу. Ловушки размещаются на отдельных серверах Trap Manager, в то время как управление платформой и всей эмулированной инфраструктурой происходит на сервере Control Center, где осуществляется сбор и обработка событий безопасности, обеспечивается взаимодействие с внешними системами, а также управление ловушками, приманками и серверами Trap Manager. Для инфраструктур крупных организаций задача масштабирования легко решается за счёт добавления необходимого количества серверов Trap Manager.

   Продукт позволит:

   - Обнаружить атаки, которые невозможно детектировать другими средствами (APT, 0-day и другие угрозы).
   - Снизить скорость продвижения злоумышленника внутри сети за счет созданного дополнительного слоя инфраструктуры из эмулированных элементов.
   - Выявить слабы места в защите Организации.
   - Собрать информацию об инструментах и действиях атакующего в отношении инфраструктуры Организации.
   - Получить уведомление об атаке до нанесения значительного ущерба.

5. **R-Vision SGRC** помогает выстроить в компании эффективную систему управления информационной безопасностью, обеспечивая своевременное выявление рисков, формирование системы внутренней нормативной документации и облегчая контроль за соблюдением внешних требований.

   Продукт позволит:

   - Сформировать единую многоуровневую базу активов Организации.
   - Обеспечить автоматизацию полного цикла проведения аудитов на соответствие требованиям.
   - Автоматизировать процесс проведения оценки рисков ИБ + моделирование угроз.
   - Осуществлять учет объектов КИИ, процедуру категорирования и формирование полного набора необходимой отчетной документации.
   - Создать объективное представление о состоянии ИБ в Организации.

3. Вывод

Использование продуктов R-Vision в корпоративном SOC обеспечит целостный подход к управлению ИБ на всех этапах и позволит максимально автоматизировать рутинные процедуры специалистов по ИБ.

Формирование полного набора процессов, необходимых для обоснованного стратегического планирования в области управления ИБ, включая планирование расходов на информационную безопасность позволит обеспечить соответствие ИБ лучшему мировому опыту, отраслевым, контрактным, внутрикорпоративным требованиям и целям бизнеса.