R-Vision UEBA

Модуль продвинутой аналитики для обнаружения угроз и аномалий

R-Vision User and Entity Behavior Analytics

R-Vision UEBA (User and Entity Behavior Analytics) осуществляет непрерывный мониторинг событий безопасности, анализируя данные из различных источников, включая системы лог-менеджмента, SIEM и конечные устройства, и регистрирует подозрительные изменения.

Задачи	Решения
Обнаружить скрытые угрозы, которые невозможно выявить с помощью стандартных правил корреляции SIEM	Встроенные алгоритмы, использующие методы статистического анализа и машинного обучения (ML), выявляют аномалии и угрозы в потоке событий
Проанализировать нелегитимные действия, связанные с конкретным объектом	Инструменты анализа изучают действия объектов, формируют профили нормального поведения и фиксируют любую подозрительную активность, связанную с объектом
Оперативно получить полный контекст по объекту при расследовании инцидента	Средства визуализации отображают всю активность по объекту и связанные с ним сущности, помогают провести детальный анализ событий и понять причины возникновения аномалии

Глубинная аналитика и автоматизация реагирования

R-Vision UEBA + R-Vision SIEM

R-Vision UEBA расширяет возможности R-Vision SIEM, позволяя выявлять неизвестные атаки и скрытые угрозы.

R-Vision UEBA + R-Vision SOAR

R-Vision UEBA работает в связке с R-Vision SOAR для реагирования на выявленные инциденты и предотвращения угроз.

Контроль состояния безопасности объектов

R-Vision UEBA использует объектно-центричный подход, анализируя события в контексте конкретных объектов — пользователей, рабочих станций, файлов, учётных записей и сервисов. Система формирует профили нормального поведения и фиксирует подозрительную активность в случае отклонений.

Инструменты анализа R-Vision UEBA

Простые правила - базовый инструмент анализа событий ИБ. Аналитику достаточно задать набор критериев, после чего события, удовлетворяющие указанным критериям, будут маркироваться как подозрительные.

Программные эксперты - встроенные алгоритмы, которые используют методы статистического анализа и машинного обучения для выявления аномалий и угроз в потоке событий. Они позволяют в автоматическом режиме детектировать:

- запуск процессов и приложений
- события авторизации
- доступ к файлам
- перебор паролей
- определение DGA и look-a-like доменов
- почтовый трафик
- смену учётной записи
- подключения VPN
- действия пользователей
- управление группами безопасности

Технология адаптивной корреляции событий

R-Vision UEBA автоматически совершенствует встроенную аналитику аномалий: при появлении новых источников и моделей данных инструменты адаптируются без ручной донастройки. Благодаря универсальному формату данных система сохраняет гибкость в работе аналитических инструментов.

Динамическая оценка угроз и аномалий

Система динамической оценки угроз и аномалий рассчитывает рейтинг опасности контролируемых объектов. При выявлении подозрительной активности рейтинг объекта повышается, и при превышении допустимого порога аналитик получает оповещение. Это позволяет приоритизировать угрозы и оперативно реагировать на значимые отклонения.

Визуализация последовательности событий в таймлайне

Подробная информация о подозрительной активности объектов сохраняется в виде таймлайна — временной шкалы, на которой отмечаются аномалии, выстраивается последовательность событий и контекст. Таймлайн помогает в расследовании инцидента, значительно упрощает анализ и выявление проблем в защите.

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 UEBA зарегистрирован в Реестре отечественного ПО.

rvision.ru

sales@rvision.ru

+7 (499) 755 55 70

t.me/rvision_pro

vk.ru/rvision_ru

youtube.com/@rvision_ru

rvision.ru