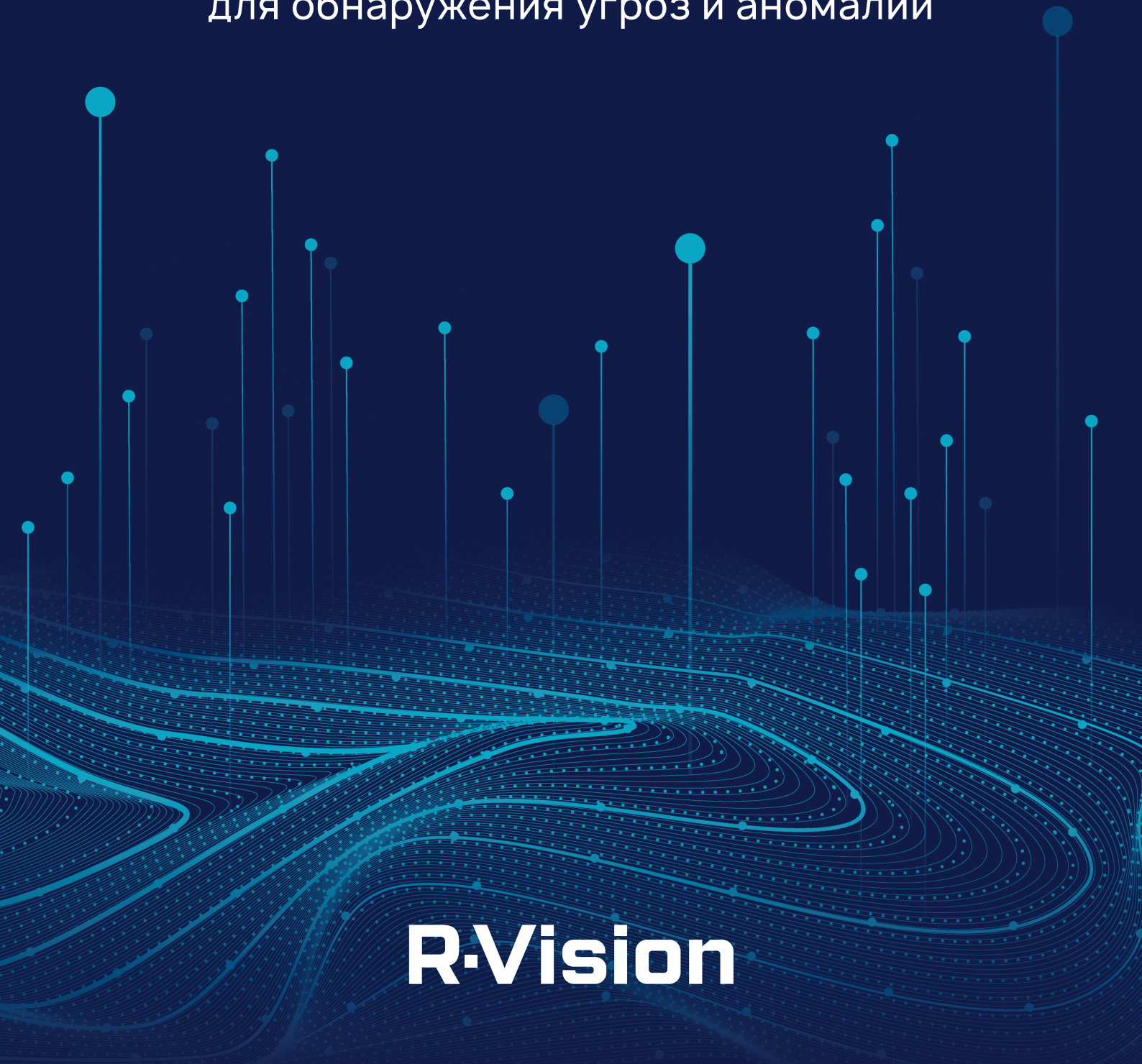
R-Vision User and Entity Behavior Analytics

Продвинутая аналитика
для обнаружения угроз и аномалий



R·Vision

R-Vision User and Entity Behavior Analytics (UEBA) — программный продукт, который осуществляет непрерывный мониторинг событий безопасности, анализируя данные из различных источников, включая системы Log Management, SIEM и конечные устройства.

Аналитические инструменты R-Vision UEBA позволяют своевременно выявить признаки начинающейся атаки, приоритизировать угрозы и проанализировать всю цепочку аномальных событий.

Задачи	Решение
Выявить аномалии, которые неочевидны для классических правил детектирования SIEM-систем	Применение встроенных в UEBA алгоритмов, которые используют методы статистического анализа и машинного обучения (ML) для выявления аномалий и угроз в потоке событий
Проанализировать нелегитимные действия связанные с конкретным объектом	Инструменты анализа, заложенные в продукт, изучают поведение объектов (пользователь, учетная запись, оборудование), формирует профили нормального поведения и фиксирует 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

При совместной работе с R-Vision Endpoint позволяет получать:

- ✓ События с большего количества источников информации, в том числе с Linux-систем
- ✓ Информацию о поведении пользователей и АРМ
- ✓ Широкий перечень телеметрии с конечных устройств

Контроль состояния безопасности объектов

Работа R-Vision UEBA основана на объектно-центричном подходе, по которому все события анализируются в отношении конкретных объектов: пользователей, рабочих станций, файлов, учетных записей, сервисов и т.д.

Изучая поведение объектов, R-Vision UEBA формирует профили нормального поведения и фиксирует подозрительную активность в случае отклонений.

Инструменты анализа R-Vision UEBA

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

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

- ✓ запуск процессов и приложений
- ✓ события авторизации
- ✓ доступ к файлам
- ✓ определение DGA и look-a-like доменов
- ✓ почтовый трафик
- ✓ смену учетной записи
- ✓ подключения VPN
- ✓ действия пользователей и групп безопасности

Технология адаптивной корреляции событий

R-Vision UEBA автоматически совершенствует встроенную аналитику по выявлению аномалий. При появлении новых источников и моделей данных инструменты анализа адаптируются в автоматическом режиме и не требуют донастройки.

R-Vision UEBA использует универсальный формат данных для анализа, что обеспечивает гибкость в работе аналитических инструментов.

Динамическая оценка угроз и аномалий

Система динамической оценки угроз и аномалий рассчитывает рейтинг опасности контролируемых объектов. При обнаружении подозрительной активности рейтинг объекта увеличивается, и в случае превышения допустимого уровня аналитик получит оповещение. Это позволяет приоритизировать угрозы и своевременно 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 значительно упрощает анализ инцидентов и выявление проблем в защите для устранения.

R-Vision

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

sales@rvision.ru

+7 (499) 322 80 40

Дайджест информационной безопасности:
rvision.ru/blog

t.me/rvision_pro

/rvision_ru

/RVisionPro