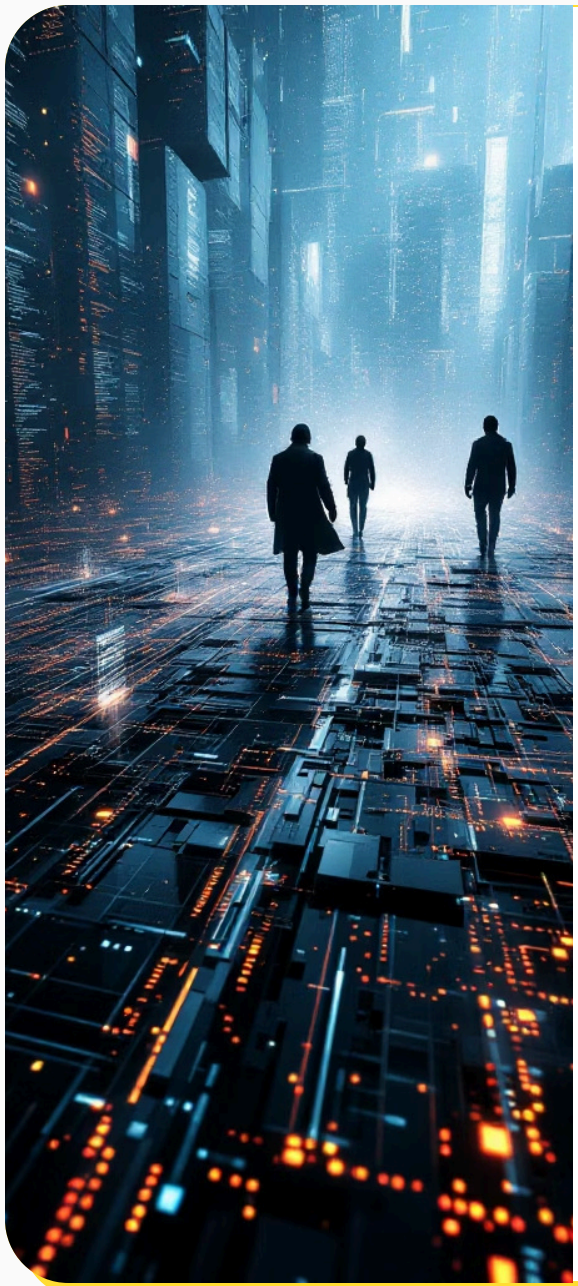
РАЗУМНЫЕ ДЕЛОВЫЕ ТЕХНОЛОГИИ

SIEM-системы:

Центр управления безопасностью вашей IT-инфраструктуры

Что это такое, зачем нужно и обзор российских решений



Почему недостаточно антивируса и фаервола?

Современные киберугрозы требуют комплексного подхода

Сложные атаки развиваются поэтапно, проходя через множество систем и оставляя следы в разных местах. Традиционные средства защиты видят лишь отдельные фрагменты.

Угрозы исходят не только извне — инсайдеры и скомпрометированные учётные записи создают риски изнутри периметра.

Многоступенчатые атаки

APT-атаки растягиваются на недели, используя цепочки эксплойтов

Внутренние угрозы

Инсайдеры и скомпрометированные аккаунты внутри сети

Разрозненные логи

Серверы, сеть, приложения генерируют данные в разных форматах

Что такое SIEM?

Security Information and Event Management — система управления информацией и событиями безопасности.

> Это централизованный мозг безопасности: умная сигнализация и видеонаблюдение для всей ИТ-инфраструктуры, которая видит полную картину происходящего.

Сбор данных

Централизация логов из всех источников

Анализ событий

Корреляция и выявление аномалий

Реагирование

Оповещения и автоматизация ответа

Как работает SIEM?

Три ключевых этапа превращают хаос разрозненных данных в структурированную защиту

Сбор & Нормализация

Агенты собирают логи из всех систем — серверов, сетевого оборудования, приложений, БД. Данные приводятся к единому формату для дальнейшей обработки.

Корреляция & Анализ

Движок корреляции применяет правила и ML-алгоритмы для поиска связей между событиями. Обнаруживает паттерны атак, аномальное поведение и индикаторы компрометации.

Реагирование & Отчётность

Система генерирует инциденты, отправляет оповещения, создаёт отчёты для регуляторов. Интеграция с SOAR позволяет автоматизировать ответные действия.

Зачем вам нужна SIEM?

Ключевые преимущества для вашей организации

Обнаружение сложных угроз

Выявление APT-атак и многоступенчатых кампаний, которые невозможно заметить точечными средствами защиты. Корреляция событий показывает полную картину атаки.

Оперативное реагирование

Сокращение MTTR (Mean Time To Response) с часов до минут. Автоматические оповещения и интеграция с системами реагирования ускоряют ответ на инциденты.

Соответствие требованиям

Выполнение требований ФСТЭК, 152-ФЗ, приказов ФСБ. Автоматическая генерация отчётов для регуляторов и внутренних аудитов безопасности.

Расследование инцидентов

Полная история событий для форензики. Возможность «отмотать назад» и проследить цепочку действий злоумышленника от точки входа до конечной цели.

Единая картина безопасности

Видимость всей ИТ-инфраструктуры в одной консоли. Понимание текущего уровня защищённости и проблемных зон, требующих внимания.

Проактивная защита

Threat Intelligence и обновляемые правила корреляции позволяют опережать известные векторы атак и адаптироваться к новым угрозам.

Российский рынок SIEM

Отечественные решения, соответствующие требованиям регуляторов и обеспечивающие технологическую независимость

Гарда SIEM

Гарда Технологии — быстрое развертывание и удобный интерфейс для оперативного мониторинга безопасности.

Киберпротект TDS

Киберпротект — эффективное выявление угроз с акцентом на анализ сетевого трафика и поведенческую аналитику.

MaxPatrol SIEM

Positive Technologies — фокус на обнаружении сложных целевых атак и глубоком расследовании инцидентов.

R-Vision SIEM

R-Vision — решение для мониторинга и управления событиями безопасности объектов КИИ (критической информационной инфраструктуры).

UserGate Security Platform

UserGate — единая платформа, объединяющая SIEM, NGFW и EDR для сокращения сложности инфраструктуры.

Все решения включены в Реестр отечественного ПО и имеют сертификаты ФСТЭК и ФСБ для работы с конфиденциальной информацией.

Сравнительный анализ

Функциональность и интеграция

Система	Достоинства	Недостатки
MaxPatrol SIEM	Лидер рынка с 15+ лет опыта. Глубокая экспертиза, более 500 готовых интеграций. Полное соответствие ГОСТ и требованиям регуляторов. Мощные возможности корреляции.	Высокая стоимость владения. Требует квалифицированной команды для настройки и эксплуатации. Длительное внедрение в крупных инфраструктурах.
UserGate Security Platform	Удобство «всё в одной коробке» — NGFW + SIEM. Тесная интеграция компонентов. Простота внедрения и эксплуатации. Хорошее соотношение цена/качество.	Меньше готовых парсеров для узкоспециализированного ПО. Ограниченные возможности для очень крупных enterprise-инфраструктур.
Киберпротект TDS	Мощный UEBA и поведенческий анализ на базе ML/AI. Современная архитектура, высокая производительность. Автоматизация расследований.	Относительно молодая платформа на рынке. Меньше референсов и кейсов внедрения по сравнению с лидерами.

Сравнительный анализ

Целевая аудитория и масштабируемость

Система	Достоинства	Недостатки
R-Vision SIEM	Гибкая ценовая политика, подходит для СМБ-сегмента. Модульная архитектура. Быстрое внедрение. Хорошая техподдержка и обучение.	Возможности для очень крупных распределённых инфраструктур ограничены. Меньше готовых интеграций с зарубежными системами.
Гарда SIEM	Простота освоения, низкий порог входа. Интуитивный интерфейс. Подходит для организаций без выделенного SOC. Доступная стоимость.	Ограниченная сложность правил корреляции. Базовые возможности автоматизации. Не подходит для advanced use cases.

Важно: Выбор решения зависит от масштаба инфраструктуры, бюджета, наличия квалифицированной команды и специфических требований вашей отрасли.

Критерии выбора SIEM

Ключевые вопросы для принятия решения

Бюджет и TCO

Стоимость лицензий, внедрения, обучения и ежегодной поддержки. Включая затраты на железо и штатных специалистов для эксплуатации системы.

Масштаб инфраструктуры

Объём логов в день (EPS — Events Per Second, GB per day). Количество источников данных. Требования к производительности и времени хранения данных.

Компетенции команды

Наличие в команде специалистов ИБ с опытом работы с SIEM, их готовность к обучению или возможность привлечения внешнего SOC-провайдера.

Регуляторные требования

Какие требования необходимо выполнить: ФСТЭК (152-ФЗ, 187-ФЗ), приказы ФСБ, отраслевые стандарты (ЦБ, ОРПД). Необходимость сертификации.

Дополнительные факторы

- **Интеграция с существующими системами**
- **Скорость и сложность внедрения**
- **Качество техподдержки вендора**
- **Roadmap развития продукта**

SIEM — не роскошь, а необходимость

Краеугольный камень SOC

SIEM — основа современного Security Operations Center, обеспечивающая видимость и контроль над безопасностью.

Зрелый российский рынок

Отечественные решения покрывают весь спектр задач — от СМБ до крупного enterprise, с полным соответствием требованиям регуляторов.

Индивидуальный подход

Выбор системы зависит от конкретных требований, масштаба, бюджета и компетенций команды. Универсального решения не существует.

Инвестиция в устойчивость

Главная цель внедрения — повышение киберустойчивости организации и способности противостоять современным угрозам.

> Вопрос не в том, нужна ли вам SIEM, а в том, какое решение подходит именно вашей организации.

РАЗУМНЫЕ ДЕЛОВЫЕ ТЕХНОЛОГИИ

Next Steps / Контакты

> Готовы подобрать SIEM-решение, которое идеально соответствует масштабу вашей инфраструктуры и требованиям регуляторов. Обсудим ваши задачи?

Контактное лицо: Дорошенко Алексей Алексеевич

Должность: Директор проектного офиса

Alexey.Doroshenko@rdtex.ru