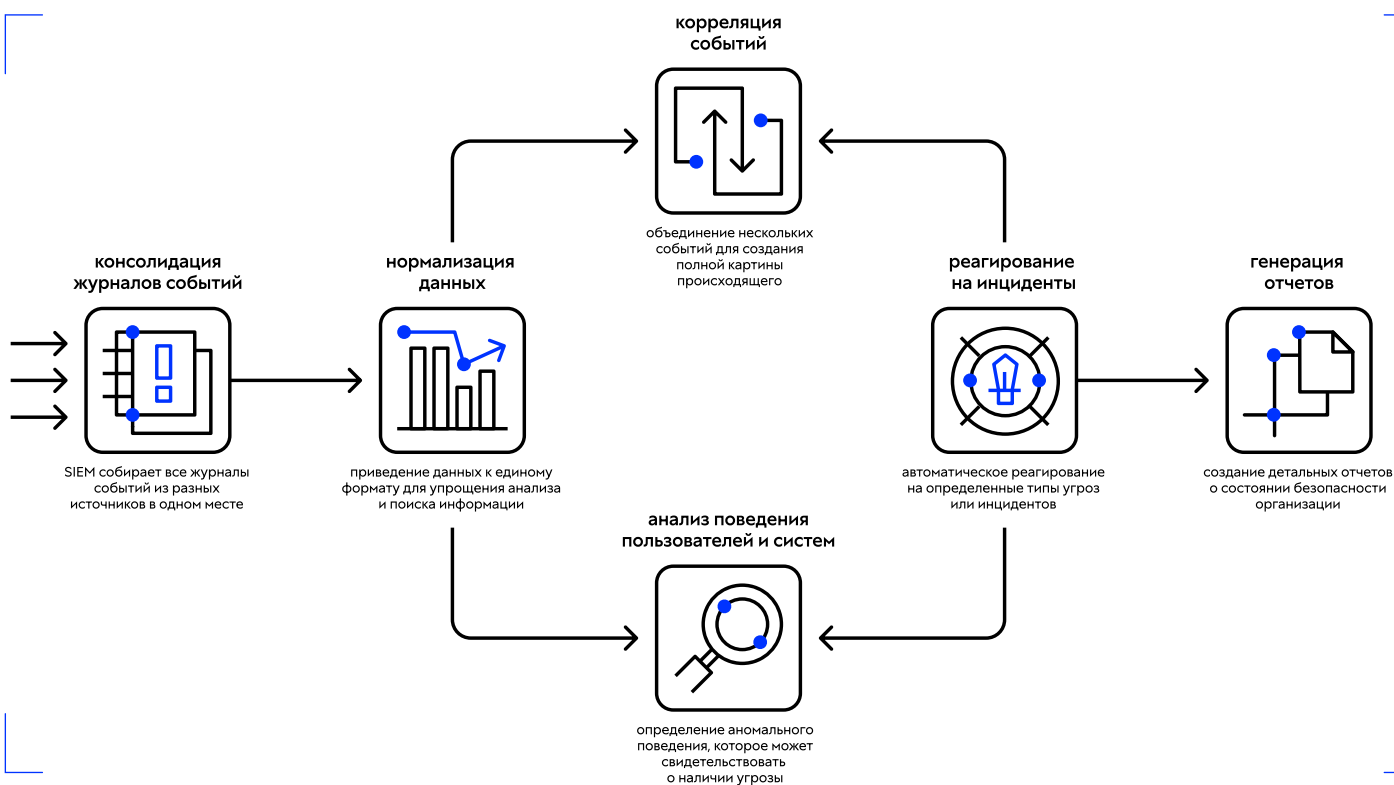


UserGate SIEM

Система управления событиями информационной безопасности с функциональностью IRP/SOAR

UserGate SIEM позволит обнаружить атаки на ИТ-инфраструктуру, обеспечит оперативное реагирование на инциденты информационной безопасности и предоставит данные для принятия мер по предотвращению их повторения.

Как функционирует UserGate SIEM



UserGate SIEM поможет:

- Снизить риски финансовых и репутационных потерь
- Улучшить видимость событий безопасности
- Оптимизировать затраты на ИБ
- Сократить расходы на сбор и хранение логов
- Выстроить внутренние регламенты компании по реагированию на инциденты
- Выполнить требования регуляторов
- Автоматизировать рутинные процессы и снизить нагрузку на команду ИБ
- Непрерывно улучшать защищенность и устойчивость бизнес-процессов компании

Преимущества UserGate SIEM



Пользовательские правила нормализации

- UserGate SIEM нормализует логи, независимо от того, из какого источника, продукта или версии продукта они поступили. При необходимости пользователь может задать свои правила нормализации.

Экспертиза UserGate от команды uFactor

- Наличие собственной экспертизы гарантирует, что правила корреляции регулярно обновляются и работают в соответствии с актуальными тенденциями противодействия киберугрозам.

IRP/SOAR

- Функциональность IRP/SOAR обеспечивает реагирование напрямую из SIEM-системы в автоматическом или ручном режимах. Нет необходимости переключаться между интерфейсами разных ИБ-продуктов: работа с инцидентом происходит в режиме «единого окна».

XDR

- Использование UserGate Client в качестве EDR-решения для защиты конечных устройств позволяет собирать не только логи, но и телеметрию с устройств внутри периметра и от удаленных пользователей. Интеграция UserGate EDR с UserGate SIEM позволяет реализовать расширенный мониторинг и реагирование по принципу построения систем безопасности класса XDR.

TI

- Функциональность TI (Threat Intelligence) позволит наполнять «карточку» инцидента, обогащать ее информацией из внутренних и внешних источников и находить недостающие взаимосвязи событий. Анализ собранной информации позволит вовремя предотвращать угрозы и прогнозировать вероятные нежелательные события.

Экосистемный подход и открытость

- UserGate SIEM — это самостоятельная SIEM-система, которая может полноценно взаимодействовать с любыми источниками событий в инфраструктуре заказчика. В то же время экосистемный подход UserGate к безопасности делает UserGate SIEM более функциональным и гибким. Являясь частью экосистемы безопасности UserGate SIEM, решение обеспечивает расширенное логирование.

Простота установки и использования

- Первый запуск UserGate SIEM занимает не более 15 минут. Решение эксплуатируется без привлечения дополнительных высокооплачиваемых специалистов. Простой язык создания правил корреляции не требует наличия специальных знаний у штатных сотрудников службы ИБ.

Операционная система UserGate

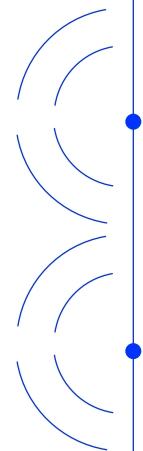
- Собственная ОС UserGate устраняет сложности, связанные с поиском, выбором и поддержкой сторонней операционной системы, необходимой для работы SIEM-решения.

Взаимодействие с ГосСОПКА

- Автоматизированное взаимодействие с ГосСОПКА объектов КИИ и других подключенных организаций существенно экономит ресурсы внутренней службы ИБ. Отправка инцидентов происходит в ручном или автоматическом режиме.

Работа в гибридных инфраструктурах

- Возможность выбрать наиболее удобный вариант развертывания SIEM-системы в вашей инфраструктуре (программно-аппаратный комплекс, виртуальное исполнение или работа в публичных облаках) открывает большое количество сценариев встраивания функций безопасности UserGate в вашу ИТ-архитектуру.



Взять на тест UserGate SIEM



Контактная информация:

Телефон: 8 800 500-40-32
Клиентам: sales@usergate.com
Партнерам: partner@usergate.com
Маркетинг: marketing@usergate.com

© ООО «Юзергейт», 2025.
Все права защищены.

Полезные ресурсы UserGate:

