



UserGate

SIEM

Способы реагирования
на инциденты информационной
безопасности





UserGate SIEM

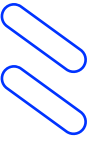
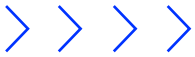
Способы реагирования на инциденты информационной безопасности

Каждый день компании и организации сталкиваются с угрозами, возникающими в цифровом пространстве. Любой из киберинцидентов может нести риск финансовых потерь, серьёзного ущерба для инфраструктуры или даже полной остановки бизнеса. Чтобы обеспечить надёжную защиту своих клиентов, компания **UserGate** разработала первый в России **экосистемный SIEM** с функциональностью IRP/SOAR.

UserGate SIEM — не просто система мониторинга событий информационной безопасности, а единый командный центр, оснащённый встроенными механизмами реагирования и способный эффективно работать в любых гибридных инфраструктурах. Вы можете осуществлять отражение атак в автоматическом режиме или взять управление на себя, выполняя все необходимые действия вручную из веб-интерфейса системы.

С помощью **UserGate SIEM** в арсенале вашей службы ИБ появятся различные варианты реагирования, которые позволят обнаружить и нейтрализовать злоумышленников до их перехода к активным действиям.

- **Блокировка подозрительного IP-адреса**
В цифровом мире каждый подозрительный IP — это незваный гость. UserGate SIEM распознаёт нарушителя по неестественному поведению (аномальной активности) и посылает сигнал межсетевому экрану следующего поколения UserGate NGFW. Адрес злоумышленника вносится в чёрный список, а путь в вашу сеть для него автоматически закрывается.
- **Удаление VPN пользователя из группы**
Представьте, что VPN-группа — это закрытый клуб с пропусками. Когда UserGate SIEM распознаёт множественные неудачные попытки входа, пользователь исключается из группы на NGFW, и доступ в корпоративную сеть для него прекращается.
- **Уведомление о критическом событии**
Иногда автоматике нужна помощь человеческого разума. При срабатывании критичного правила UserGate SIEM отправляет сигнал аналитику через e-mail, SMS, Telegram или webhook. Это позволяет эксперту вручную разобраться в ситуации, имея на руках все данные об инциденте.
- **Отзыв сертификата или токена доступа**
Если учётные данные скомпрометированы, недостаточно просто заблокировать аккаунт. UserGate SIEM аннулирует связанные сертификаты и токены, лишая злоумышленника доступа изнутри.
- **Отключение USB-портов на хосте**
Чтобы предотвратить утечку данных или заражение через физические носители, UserGate SIEM может дистанционно «запечатать» USB-порты на конечном устройстве. Это как удалённое перекрытие канала, по которому может проникнуть угроза.
- **Изоляция заражённого хоста**
Как только антивирус или EDR обнаруживают вредоносное ПО, срабатывает протокол изоляции и устройство автоматически отрезается от всех сетевых коммуникаций (например, через UserGate Client). Заблокировать вредонос можно централизованно через UserGate NGFW или же точно, — отправив команду на сетевое оборудование для мгновенного обновления ACL.
- **Остановка подозрительного процесса**
Обнаружив процесс с аномальным поведением (например, шифрование файлов), UserGate SIEM реагирует в связке с UserGate Client и завершает его. Критерии аномальности вы задаёте сами, прописывая их в детектирующей логике правил корреляции.
- **Обогащение инцидента информацией**
Обнаружив следы злоумышленника с помощью индикаторов компрометации (IoC), UserGate SIEM не останавливается на этом. Система автоматически дополняет карточку инцидента свежими данными из внешних источников (фидов), рисуя более полную картину атаки.
- **Откат изменений в конфигурации**
При несанкционированном изменении критичных файлов UserGate SIEM может автоматически запускать реакцию на восстановление этих файлов до исходного состояния.
- **Сброс сессии пользователя**
Обнаружив подозрительные действия, UserGate SIEM может принудительно сбрасывать пароли для учётных записей.



■ Автоматический сбор артефактов для расследования

Как только на хосте замечена anomальная активность, UserGate SIEM запускает своего «цифрового аналитика» — специальный скрипт. Он оперативно собирает все улики: логи, дампы памяти и другие данные, необходимые для последующего анализа инцидента.

■ Сетевая изоляция хоста

При первых признаках компрометации хост помещается в «карантинную зону». UserGate SIEM отдаёт команду на его полную изоляцию от сети, чтобы эксперты могли проанализировать инцидент без риска для остальной инфраструктуры.

■ Обязательный сброс пароля для учётной записи

В случае утечки или компрометации пароля UserGate SIEM действует на опережение: система принудительно сбрасывает пароль для учётной записи, вынуждая пользователя создать новый и одновременно лишая злоумышленника доступа.

■ Принудительная остановка службы/демона

Обнаружив вредоносную службу, UserGate SIEM не просто её останавливает, но одновременно блокирует попытки прописаться в автозагрузку. Это позволяет нейтрализовать саму угрозу и механизм её повторного проникновения.

■ Блокировка доменов

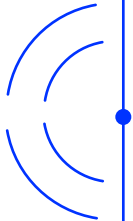
Вредоносный домен — это штаб-квартира злоумышленника в Интернете. UserGate SIEM может отправить команду на его блокировку на уровне межсетевого экрана и перекрыть канал управления атакой или скачивания вредоносного кода.

■ Обрыв VPN-сессии

Если активность VPN-пользователя вызывает подозрения, UserGate SIEM обрывает его защищённый туннель, не давая потенциальному злоумышленнику действовать извне.

■ Квотирование трафика

Если хост начинает генерировать подозрительно большой объём трафика (возможно, участвуя в DDoS-атаке), UserGate SIEM действует гибко. Вместо полного отключения система через SNMP или API даёт команду коммутатору ограничить ширину канала (пропускную способность) для этого устройства, минимизируя ущерб, но при этом сохраняя работоспособность.



Выводы:

Приведённые сценарии можно дорабатывать под особенности вашей инфраструктуры и используемые источники событий, настраивая комплексные механизмы реагирования.

Действуя как единый центр управления, который координирует все элементы защиты — от межсетевых экранов и EDR до клиентских агентов и систем аутентификации, — **UserGate SIEM** запускает чёткий набор действий, ведущий к ликвидации угрозы.

Согласованная работа всех средств защиты и масштабируемая автоматизация позволит команде ИБ не просто фиксировать инциденты, а управлять ими, автоматизируя рутинные процессы и концентрируясь на сложных комплексных атаках.

UserGate SIEM превращает сбор и анализ событий безопасности в управляемый и предсказуемый процесс, обеспечивая надёжный иммунитет вашей ИТ-инфраструктуры против современных киберугроз.

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:

