UserGate

UserGate SIEM

своевременное обнаружение сложных комплексных атак и оперативное реагирование на них

UserGate SIEM – система управления событиями информационной безопасности от признанного лидера рынка.

Основной задачей SIEM-системы является аккумулирование в себе событий (логов) из различных источников в инфраструктуре заказчика и автоматическое обнаружение инцидентов информационной безопасности за счет правил корреляции в режиме реального времени. А функциональность IRP/SOAR позволит реагировать на инциденты как в ручном, так и в автоматическом режиме.

SIEM поможет:

- Минимизировать финансовые потери из-за простоя бизнес-критических сервисов.
- Снизить риск утечки данных.
- Выполнить требования регулятора.
- Получить качественную экспертизу.
- Облегчить работу сотрудников в режиме постоянного дефицита кадров.
- Обезопасить свою компанию от сложных комплексных атак.
- Своевременно обнаруживать инциденты.
- Оперативно реагировать на инциденты.
- Качественно расследовать инциденты.
- Не допустить повторения инцидентов.

Выявляйте сложные комплексные атаки

Загружайте правила корреляции из нашей базы, написанной экспертами компании, имеющими огромный опыт работы

Создавайте собственные правила корреляции, импортируйте и экспортируйте их, в том числе и в YAML-формате

Будьте всегда на связи благодаря обширным вариантам оповещений о новых сработках правил корреляции

Контролируйте состояние ИБ и ИТ в своей инфраструктуре

Отслеживайте изменения внутренней инфраструктуры

Обогащайте инциденты информацией из внешних сервисов

Держите руку на пульсе используя дашборды, виджеты и отчеты

Соответствуйте требованиям регулятора

Преимущества UserGate SIEM

ЭКОСИСТЕМА
Гибкость взаимодействия с продуктами из экосистемы, расширенное логирование за счет наличия экосистемных продуктов в инфраструктуре. Удобство администрирования, вам не нужно будет строить «зоопарк» из решений различных вендоров.

ЭКСПЕРТИЗА
Наличие собственной экспертизы на базе Центра мониторинга и реагирования компании UserGate (MRC UG). Мы начали развитие нашей экосистемы с NGFW и накопили действительно большую экспертизу, которая помогает в развитии нашей экосистемы в целом и SIEM-системы в частности.

300 ПРАВИЛ КОРРЕЛЯЦИИ
Более 300 правил корреляции, написанных экспертами нашей компании и отсортированных по матрице MITRE ATT&CK для удобства пользователей.

SOC
Открытие собственного SOC на базе продуктов экосистемы UserGate SUMMA, в том числе с использованием UserGate SIEM.

ОТКРЫТОСТЬ
Полноценная SIEM-система, которая может работать и в инфраструктуре, где нет других продуктов из экосистемы UserGate SUMMA.

TI
Возможность обогащения инцидента информацией из внешних сервисов, например, вы можете проверить адрес на предмет его чистоты на внешних базах данных, как платных, так и бесплатных.

IRP/SOAR
Возможности реагирования прямо из SIEM-системы. Как в автоматическом, так и в ручном режиме. При этом вам не нужно будет переключаться между различными продуктами ИБ, вся работа с инцидентом будет происходить в едином окне.

EDR
Благодаря UserGate Client вы сможете собирать не только логи, но и телеметрию, причем как с устройств внутри периметра, так и от удаленных пользователей.

НОРМАЛИЗАЦИЯ
Возможность создавать свои правила нормализации. От того, как качественно вы выполните нормализацию, будет зависеть качество и скорость работы аналитиков.

UX/UI
Система простая в управлении и использовании. Сотрудники легко смогут разобраться с тем, как ей пользоваться. Особенно если они до этого уже работали с продуктами от компании UserGate, например, нашим NGFW.

10–15 МИНУТ
Установка системы так же простая, вы сможете установить UserGate SIEM всего за 10-15 минут.

UGOS
Собственная ОС. И как следствие отсутствие сложностей, связанных с поиском, выбором и поддержкой необходимой для работы SIEM операционной системы.

ГосСОПКА
Отправка инцидентов в ГосСОПКу. Как в ручном режиме, так и в автоматическом.

РОЛЕВАЯ МОДЕЛЬ
Гибкая система настройки ролевой модели и прав доступа для конкретных пользователей.

УДОБСТВО
Помогаем соответствовать требованиям регулятора, в рамках реализации следующих нормативных документов:

- ФЗ РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- ФЗ РФ от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»;
- приказ ФСТЭК № 31;
- указ президента №250;
- стандарт ГОСТ Р 57580.1-2017;
- стандарт ГОСТ Р 57580.2-2018.

UserGate SIEM

ОСТАВЬТЕ ЗАЯВКУ НА ТЕСТИРОВАНИЕ

usergate.ru
8 (800) 500 4032