

**Table of Contents**

|                           |   |
|---------------------------|---|
| Table of Contents         | 1 |
| Введение                  | 2 |
| Архитектура UserGate SIEM | 3 |



Documentation: ☒

Product: SIEM

Version: 7.x

Technology: SIEM

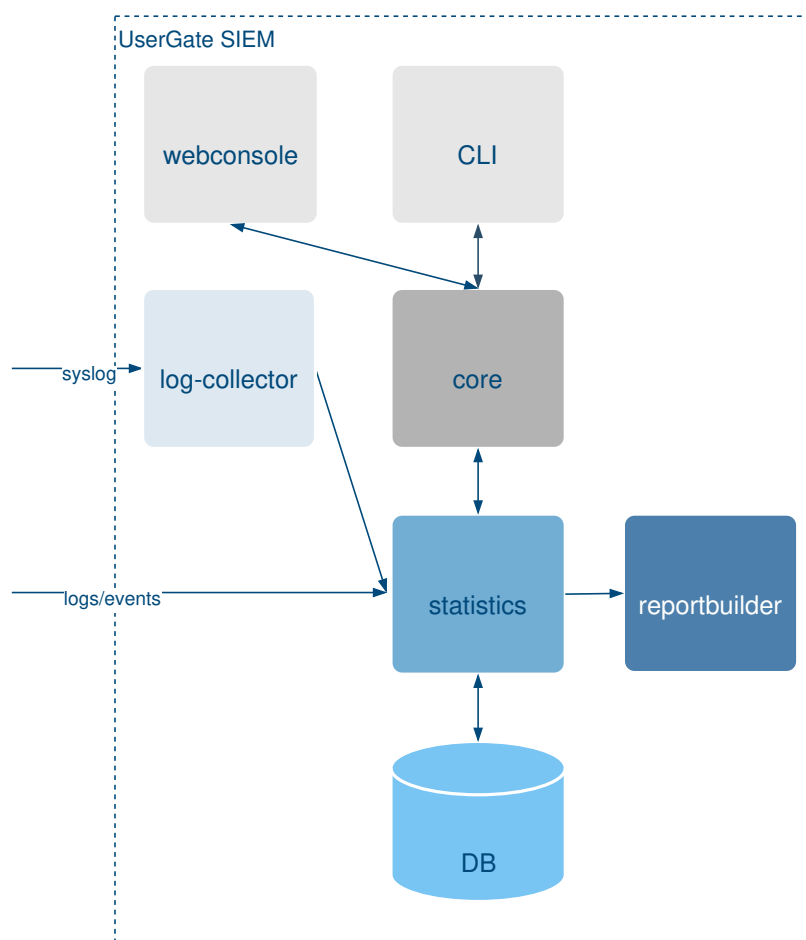
UserGate SIEM — система управления событиями информационной безопасности, которая собирает системные журналы и данные о событиях с различных устройств в подконтрольной сетевой инфраструктуре. Данные подвергаются обработке и анализу, в результате которого могут быть выявлены подозрительные действия или признаки известных сетевых угроз. В зависимости от степени опасности выявленных угроз могут быть произведены определенные действия реагирования, включающие в себя оповещения, создание инцидентов безопасности для дальнейшего расследования или отправка команд на определенные устройства сети с целью предотвращения угрозы.

Результаты обработки данных отображаются в едином веб-интерфейсе, а также предоставляются в виде файлов с отчетами для изучения характерных особенностей инцидентов безопасности. Для проведения расследований инцидентов кибербезопасности используется встроенная в UserGate SIEM система IRP. IRP — это платформа управления процессами реагирования на инциденты информационной безопасности. Она позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании.

UserGate SIEM поставляется в виде образа виртуальной машины, предназначенного для развертывания в виртуальной среде.

## Архитектура решения

В основе решения UserGate SIEM лежат следующие программные модули:

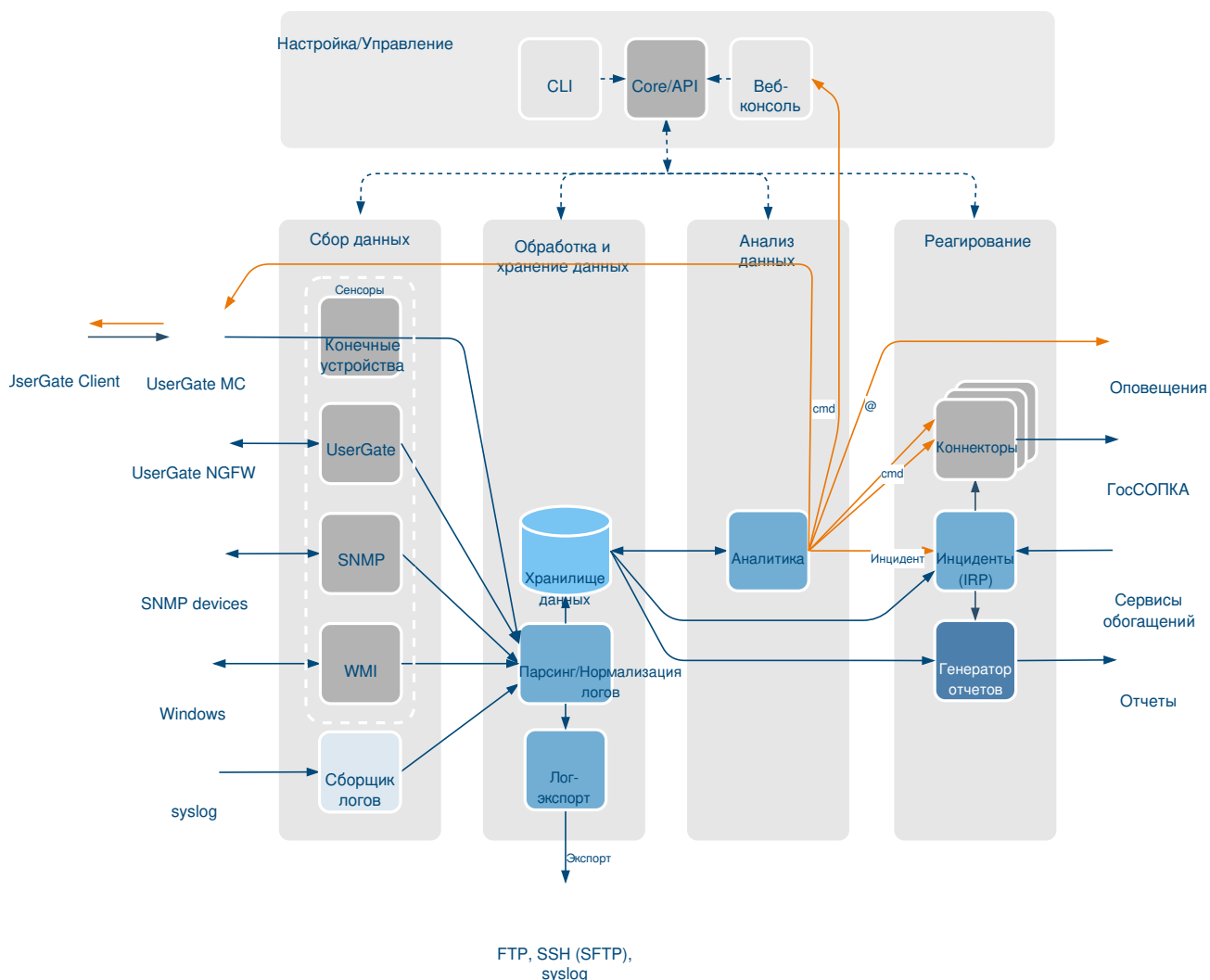


- core — модуль ядра системы, реализующий функции настройки, управления, API, хранения конфигурации.
- statistics — основной функциональный модуль системы, реализующий функции приема, обработки, анализа, хранения данных, создания инцидентов безопасности, управления процессами реагирования, экспорта данных и создания отчетов.
- log-collector — модуль сбора событий от сетевых устройств по протоколу syslog.
- DB — хранилище данных.
- webconsole — модуль веб-консоли управления системой.
- CLI — модуль интерфейса командной строки для управления системой.
- reportbuilder — модуль генерации отчетов в форматах HTML и PDF.

## Функциональная модель

Функциональную модель UserGate SIEM можно описать с помощью следующих основных блоков:

- Блок сбора данных.
- Блок обработки данных.
- Блок анализа данных.
- Блок реагирования.
- Блок настройки и управления системой.



## Сбор данных

UserGate SIEM собирает данные с внешних источников с помощью сборщика логов (модуль log-collector) и с помощью сенсоров (настраиваются и хранятся в модуле core).

Сборщик логов предназначен для сбора событий от сетевых устройств по протоколу syslog. Настраиваемые правила syslog позволяют осуществлять фильтрацию записей событий по времени, критичности событий, объектам, названию устройств, приложениям, упрощая поиск необходимой информации.

Сенсоры позволяют собирать данные с межсетевых экранов UserGate (сенсор UserGate), конечных устройств с установленным ПО UserGate Client (сенсор конечных устройств), компьютеров под управлением ОС Windows (сенсор WMI), а также с любых других сетевых устройств, способных передавать данные по протоколу SNMP (сенсор SNMP).

При интеграции с межсетевым экраном UserGate NGFW устройство UserGate SIEM сначала подключается к UserGate NGFW с помощью параметров, настроенных в сенсоре UserGate, и передает в UserGate NGFW настройки для подключения. Далее UserGate NGFW собирает свои данные в локальном кэше и периодически передает их в модуль statistics в UserGate SIEM по таймеру.

С помощью сенсора SNMP можно подключить SNMP-совместимое сетевое устройство к UserGate SIEM для сбора и анализа его метрик. SIEM может отображать любые метрики, полученные с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB на управляемое устройство. Базы MIB устройств сторонних производителей могут импортироваться в систему SIEM.

С помощью сенсора WMI можно подключить WMI-совместимое сетевое устройство (компьютер под управлением ОС Windows) к UserGate SIEM для сбора и анализа его данных. В настройках сенсора WMI указываются адрес устройства, атрибуты входа в устройство, пространство имен и параметры event-лога Windows, которые будут контролироваться системой SIEM.

Конечные устройства с установленным ПО UserGate Client подключаются к UserGate SIEM не напрямую, а через UserGate Management Center. При интеграции UserGate SIEM с UserGate MC между ними устанавливается SSH-туннель, по которому параметры настройки и данные статистики с интегрированных в MC конечных устройств передаются на UserGate SIEM.

## Обработка и хранение данных

Собираемые данные поступают в модуль statistics, где они подвергаются предварительному анализу и нормализации. В процессе нормализации записи журналов, полученные из различных источников, приводятся к единому виду, пригодному для записи в стандартные поля базы данных UserGate SIEM. Далее нормализованные записи передаются в сервис лог-экспорта и в хранилище данных.

Сервис лог-экспорта с помощью настраиваемых правил позволяет экспортировать журналы (в формате CEF или JSON) на внешние серверы FTP, SSH (SFTP) и syslog. Отправка на серверы SSH и FTP проводится по указанному в настройках правил расписанию или разово. Отправка на серверы syslog происходит сразу же при добавлении записи в журнал.

В таблицах хранилища данных содержатся все собранные записи журналов как самого устройства UserGate SIEM, так и подключенных к нему устройств. Также в таблицах хранилища данных содержатся созданные инциденты и оповещения.

Данные устройств в таблицах хранятся по ключу, который содержит в себе ClusterID. Например, при регистрации UserGate NGFW в UserGate SIEM в модуле statistics для него создается аккаунт, в котором ему прописывается ClusterID и токен. Токен возвращается в UserGate NGFW и используется для авторизации.

Журналы в хранилище данных циклически перезаписываются, обеспечивая необходимое для работы свободное дисковое пространство. Ротация записей журналов (всех, кроме журнала событий) происходит автоматически по критерию свободного пространства на данном разделе. Записи о ротации базы данных отображаются в журнале событий UserGate SIEM. Ротация записей журнала событий не производится.

## Анализ данных

Сервис аналитики работает также в модуле statistics. С его помощью производится анализ журналов событий безопасности, полученных с настроенных сенсоров. В процессе анализа данных сервис аналитики производит агрегацию повторяющихся событий и их корреляцию, используя условия правил аналитики, написанные с помощью SQL-подобного синтаксиса. В случае срабатывания правила будет выполнено действие реагирования, настроенное для данного правила.

## Реагирование

В качестве мер реагирования на выявленные в результате анализа данных аномалии и угрозы безопасности могут использоваться следующие действия:

- Визуализация срабатываний системы анализа данных в консоли управления системой.
- Оповещение персонала служб информационной безопасности.
- Создание инцидента информационной безопасности для дальнейшего расследования.
- Создание отчетов об инцидентах информационной безопасности.
- Отправка команд на определенные сетевые устройства с целью снижения угрозы.

В правилах аналитики UserGate SIEM задаются действия реагирования, которые должны выполняться в случае их срабатывания. В качестве таких действий могут быть использованы оповещения по email или SMS, отображение информации на специальной веб-странице (webhook), отправка команд для выполнения на сетевом устройстве, создание инцидента. Создание инцидента как действие реагирования позволяет автоматизировать процесс создания инцидентов информационной безопасности. Информация о срабатывании правил аналитики и о созданных инцидентах безопасности выводится в режиме онлайн на информационных экранах и дашбордах в веб-консоли администратора UserGate SIEM.

Расследование инцидентов информационной безопасности производится с помощью платформы управления процессами реагирования — IRP (Incident Response Platform). Сервис IRP интегрирован с сервисом аналитики и необходим для управления процессами реагирования на инциденты информационной безопасности. При расследовании инцидентов сервис IRP использует внешние ресурсы для сбора дополнительной информации — внешние сервисы обогащений. В случае, если в качестве улики к инциденту прикреплены записи журнала, то IRP автоматически извлекает сведения об индикаторах компрометации (IP-адресе, URL, домене, названии файла, хэше) для работы с внешними сервисами обогащений.

С помощью модуля генерации отчетов могут создаваться отчеты по инцидентам безопасности в формате PDF или HTML, которые доступны для скачивания или отправки на электронную почту.

С помощью настраиваемых программных коннекторов возможна организация подключения системы UserGate SIEM к различным средствам защиты или службам обмена данными об инцидентах информационной безопасности. Через коннектор с типом сервера SSH возможна передача команд на подключенное устройство в качестве реакции на срабатывание правила аналитики. По умолчанию в системе создан коннектор Gossorka, предназначенный для автоматизации обмена информацией об инцидентах информационной безопасности с ГосСОПКА (Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак).

## Настройка и управление

Модуль веб-консоли взаимодействует с большинством модулей UserGate SIEM и выполняет функции управления и представления данных. Модуль позволяет формировать и просматривать отчеты и журналы, использовать графическое представление данных с помощью виджетов дашборда, производить настройки в веб-интерфейсе управления (общие настройки SIEM, настройки правил аналитики, управление инцидентами безопасности и т. д.).

Запросы из веб-консоли приходят сначала в модуль core в специальный сервис Web Console Proxy, затем запросы на чтение данных напрямую (не попадая в API) перебрасываются в модуль statistics. Statistics обрабатывает эти запросы, формирует корректные SQL-запросы к базе данных и возвращает данные обратно по прямому туннелю в веб-консоль.

Настройка UserGate SIEM также может выполняться с использованием интерфейса командной строки посредством модуля CLI. Команды интерфейса CLI реализованы с помощью API.

