Общие сведения

В данной статье приведены общие сведения о Системе.

Назначение Системы

Система предназначена для сбора, обработки, передачи, а также долговременного хранения и анализа Событий.

Ключевые возможности Системы

Система обеспечивает реализацию следующего ключевого функционала:

- Сбор Событий из различных источников, таких как операционные системы, сетевые устройства, базы данных и т.д.;
- Нормализация, агрегация, обогащение и фильтрация Событий;
- Эффективное долговременное хранение большого количества Событий с высоким коэффициентом сжатия;
- Интеграция с внешними системами, такими как системы класса SIEM, IRP и т.д.;
- Автоматическая конвертация правил нормализации и корреляции из MP SIEM;
- Формирование запросов и представление выборки Событий в виде таблицы;
- Построение графиков для анализа и визуализации Событий с гибкой настройкой отображения:
- Формирование и отправка оповещений по срабатыванию настраиваемых триггеров.

Пользователь может выполнять с помощью Системы следующие действия:

- Формирование запросов и представление выборки Событий в виде таблицы;
- Настройка графического представления выборки в формате Виджетов;
- Создание и настройка Дашбордов;
- Импорт и экспорт запросов, Виджетов и Дашбордов.

Требования к рабочему месту Пользователя

На рабочей станции Пользователя должны быть настроены:

1. Веб-браузер для работы с Системой;
2. Доступ к сети.

Требования к квалификации Пользователя

Администратор должен обладать следующими навыками:

- знание языка SQL;
- знание особенностей написания SQL-запросов в СУБД **ClickHouse**.

ID статьи: 207
Последнее обновление: 23 дек., 2024
Обновлено от: Егоров В.
Ревизия: 1
База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.3.0 -> LogIQ. Руководство пользователя -> Введение -> Общие сведения
https://docs.axel.pro/entry/207/