САВРУС

СРЕДА АНАЛИЗА И ВИЗУАЛИЗАЦИИ РИСКОВ
В УПРАВЛЕНЧЕСКИХ СИСТЕМАХ

Функциональные характеристики системы САВРУС

ООО «САВРУС»
125445, г. Москва, ул. Смольная, д. 24А, этаж 10, офис № 1029
ИНН/КПП 7743266740/774301001, ОГРН 1187746699546

Цели системы

- мониторинг информационных процессов в организации;
- быстрый анализ и реагирование на критичные события (риски);
- помощь в расследовании инцидентов.

Задачи системы

- сбор данных с информационных и управленческих систем организации;
- централизованное хранение собранных данных в БД;
- визуализация собранных данных для их дальнейшего анализа;
- детектирование инцидентов и рисков ИБ;
- оповещение об инцидентах и рисках ИБ;
- корреляция событий в online и offline режимах;
- подготовка информационных панелей для различных отделов организации, таких как ИТ, ИБ и другие;
- подготовка подробной инфографики и отчётов о состоянии организации для руководства.

Архитектура системы

САВРУС представляет собой программный комплекс, состоящий из:

- коннекторов и модуля сбора и обработки событий;
- модуля управления и анализа;
- модуля хранения событий;
- модуля корреляции;
- консоли визуализации САВРУС.

Коннекторы и модуль сбора и обработки событий обеспечивают:

- сбор и первичную обработку от источников событий;
- нормализацию, фильтрацию и категоризацию событий;
- маршрутизацию и кэширование данных.

Модуль управления и анализа обеспечивает:

- хранение системных ресурсов и служебных процедур в БД;
- управление активными каналами, активными листами, элементами визуализации и отчётами;

- взаимодействие между компонентами САВРУС и мониторинг их работы;
- аналитическую обработку данных.

Модуль хранения событий обеспечивает:

- хранение данных в БД в течение заданного временного интервала;
- управление партициями, резервное копирование, режим высокой доступности.

Модуль корреляции обеспечивает:

- корреляцию событий в online и offline режимах.

Консоль визуализации САВРУС обеспечивает:

- управление компонентами и настройками САВРУС;
- работу с событиями и инцидентами в активных каналах;
- предоставление функций по визуализации событий и инцидентов;
- визуализацию, фильтрацию и группировку событий и инцидентов;
- подготовку настраиваемых отчётов и рассылку их по расписанию.

База данных представляет собой колоночную СУБД для OLAP (online обработки аналитических запросов) ClickHouse.

Модули могут быть развёрнуты на отдельной виртуальной машине или на выделенном сервере.