# СёрчИнформ SIEM

SEARCHINFORM

INFORMATION SECURITY

## Проблема

Утечки не случаются внезапно: им всегда предшествует ряд событий. Но, увы, значение некоторых становится ясным только постфактум. Упустили несанкционированное обращение сотрудника к определенному ресурсу, не заметили назначения администратором расширенных прав доступа – сколько еще событий не вызвали подозрений, но предваряли инцидент? Проблема таких упущений – в постоянно растущем объёме данных, с которым приходится работать специалистам служб безопасности.

## Решение

**«СёрчИнформ SIEM»** – это приложение, предназначенное для сбора и автоматического анализа событий различных корпоративных систем с целью выявления угроз и нарушений политик информационной безопасности.

Сложный механизм работы «СёрчИнформ SIEM» сводится к довольно простому алгоритму:

- Сбор событий с разных систем (сетевое оборудование, программное обеспечение, средства защиты, ОС).
- Приведение разнородных данных к общему виду.
- Анализ данных и выявление угроз.
- Фиксация инцидентов и оповещение в реальном времени.

## Что контролирует система?

Источниками данных для «СёрчИнформ SIEM» являются:

- Контроллеры домена Active Directory.
- Контроль локальных журналов Windows.
- Обращения к файловым ресурсам.
- Активность пользователей.
- Почтовые серверы Exchange.
- Антивирус Kaspersky.
- СУБД (MS SQL, Oracle).
- Syslog аппаратных устройств и приложений.
- DLP «КИБ СёрчИнформ».
- Файловые операции на подключаемых внешних устройствах.

В разработке и тестировании:

- Среды виртуализации и терминальные серверы.
- Поддержка NetFlow и OPSEC.
- Динамические дашборды.
- Расширение списка антивирусов, СУБД и почтовых серверов.
- Поддержка IDS И IPS.

## Цели и задачи системы

### 1. Сбор и обработка событий с различных источников

Количество источников данных сегодня так велико, что контролировать все события в инфраструктуре «вручную» невозможно. Отсюда появляются риски:

- «пропустить» инцидент;
- не обнаружить деталей и не установить причин (удалены журналы событий и т.д.);
- не восстановить данные.

И SIEM – как агрегатор информации из разных устройств – решает эту проблему. Система приводит данные к единому виду и становится защищённым хранилищем.

## 2. Анализ событий и разбор инцидентов real-time

«СёрчИнформ SIEM» не просто унифицирует события, но и оценивает их значимость: система визуализирует информацию с акцентом на важные и критические события.

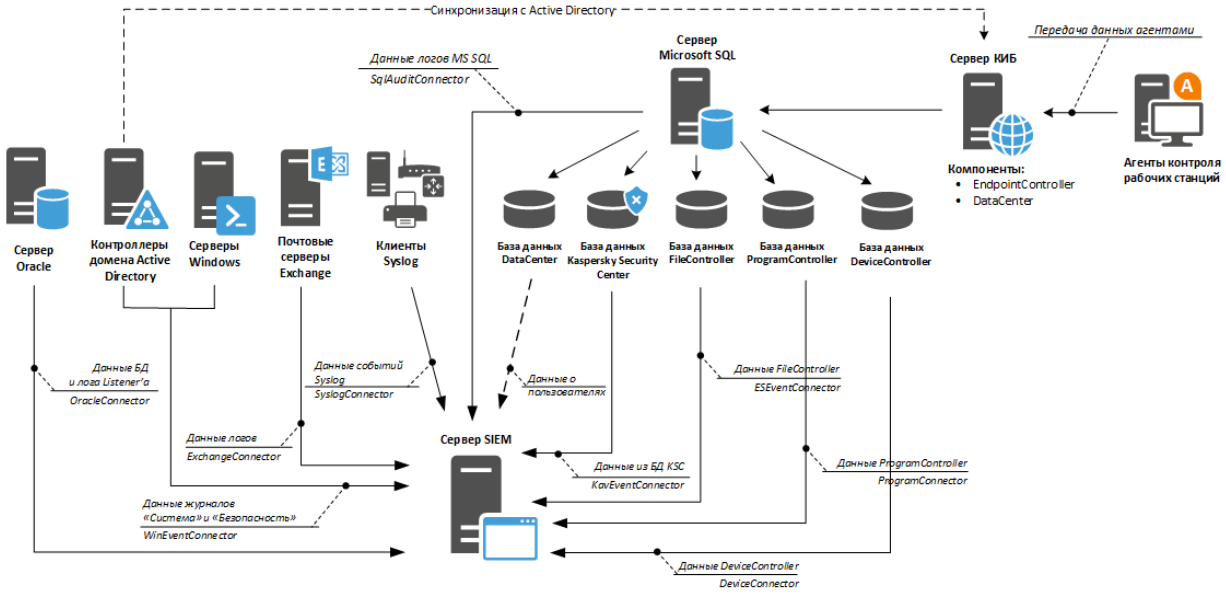
## 3. Корреляция и обработка по правилам

По одному событию не всегда можно судить об инциденте. Например, неудачная авторизация может быть просто случайностью, но три и более попыток могут говорить о подборе. Чтобы распознавать действительно критичные инциденты, «СёрчИнформ SIEM» работает по правилам, которые содержат целый перечень условий и учитывают самые разные сценарии действий.

## 4. Автоматическое оповещение и инцидент-менеджмент

Позволяют «СёрчИнформ SIEM» выполнять свое главное предназначение: создание условий для быстрого реагирования службой безопасности на инциденты. Процесс обнаружения этих инцидентов система автоматизирует и полностью берет на себя.

## Архитектура и алгоритм работы




- С помощью консоли управления «СёрчИнформ SIEM» осуществляется настройка подключения к источникам данных, конфигурирование правил и настройка оповещений.
- Сервер SIEM осуществляет вычитку журналов «Система» и «Безопасность» контроллеров доменов и серверов Windows, почтовых серверов Exchange, баз данных Kaspersky Security Center, MS SQL, Oracle, FileController, ProgramController и DeviceController, а также получает события от клиентов Syslog, после чего в реальном времени анализирует полученные данные согласно настроенным правилам и записывает инциденты в собственную базу данных под управлением Mongo DB.
- В случае обнаружения инцидентов система незамедлительно отправляет уведомление сотруднику службы информационной безопасности.
- Консоль управления «СёрчИнформ SIEM» позволяет строить отчеты по зафиксированным инцидентам, а также экспортировать выбранные события в файл.

## Преимущества

- **Решение учитывает реальный опыт тысяч клиентов**

  «СёрчИнформ» поставляет заказчику готовые сценарии, которые способны эффективно работать и давать результаты сразу после установки системы. «СёрчИнформ SIEM» проектировалась, исходя из анализа запросов крупнейших клиентов компании из разных отраслей.

- **Решение готово к работе “из коробки”**

  «СёрчИнформ SIEM» быстро интегрируется и требует минимальной настройки. В систему встроены универсальные политики безопасности (актуальный перечень политик приведен в конце документа).

- **Решение доступно даже для небольших компаний**

  Ценовая политика и стоимость обслуживания «СёрчИнформ SIEM» в лучшую сторону отличаются от других подобных решений. Кроме того, ПО «СёрчИнформ» имеет низкие требования к аппаратно-программным средствам.

- **Интеграция с DLP «СёрчИнформ»**

  «СёрчИнформ SIEM» собирает, анализирует и коррелирует данные с агентами DLP или с перехваченным сетевым трафиком. Связка SIEM+DLP позволяет детализировать нарушения в мельчайших подробностях.

## Системные требования

| | Минимальные системные требования (все правила в 1-м экземпляре, 1 контроллер домена) |
|---|---|
| Процессор | 4-ядерный частотой 2,1 ГГц |
| Оперативная память | 4 ГБ[1] |
| Винчестер | 200 ГБ[2] |
| Сетевая карта | 100 Мбит/с |

[1] При создании политик требования к оперативной памяти возрастают (~15 Мб для каждой новой политики).

[2] По мере сохранения событий в базу данных SIEM может потребоваться дополнительное дисковое пространство.

# Предустановленные политики «СёрчИнформ SIEM» *

Предустановленные политики для контроллеров домена Active Directory:

- Временное переименование учетной записи.
- Подбор паролей.
- Несколько учетных записей на одном ПК.
- Задание пароля администратором домена.
- Устаревшие пароли.
- Статистика входов в систему.
- Одна учетная запись на нескольких ПК.
- Смена пароля пользователем.
- Подбор пароля.
- Попытка входа под несуществующим пользователем.
- Попытка входа под заблокированным пользователем.
- Временное включение учетной записи.
- Временное добавление учетной записи в группу.
- Устаревшие учетные записи AD.
- Временная выдача прав доступа AD.
- Создание временной учетной записи.
- Операции над учетной записью.
- Изменение состава критичных групп пользователей.
- Использование служебных учетных записей сотрудника.
- Очистка журнала событий пользователем.
- Изменение политики аудита.

Предустановленные политики для обращения к файловым ресурсам:

- Временная выдача прав на файл/папку.
- Обращение к критичным ресурсам.
- Большое количество пользователей, работающих с файлом.
- Работа с определенными типами файлов.
- Статистика изменений прав доступа к файлам/папкам.

Предустановленные политики для MS SQL:

- Временное создание учетных данных MS SQL.
- Временное включение учетных данных MS SQL.
- Статистика изменения прав доступа MS SQL.
- Временное включение пользователя в роль безопасности БД.
- Задание пароля учетной записи SQL администратором БД.
- Временное переименование учетных данных MS SQL.

Предустановленные политики для антивируса Kaspersky:

- Самозащита антивируса заблокировала выполнение программ.
- Самозащита антивируса отключена.
- Отключены антивирусные компоненты защиты.
- Критический статус компьютера.
- Обнаружена потенциально опасная программа.
- Не удалось выполнить административную задачу управления.
- Отсутствует лицензия на антивирус.
- Изменение в составе административной группы управления.
- Заблокированные и зараженные программы.
- Выявлена вирусная эпидемия.

Предустановленные политики для Exchange:

- Изменение параметров аудита администратора.
- Группы ролей управления изменены.
- Доступ к почтовому ящику не владельцем.
- Предоставление доступа к почтовому ящику.
- Изменение статуса почтового ящика.
- Изменение состава ролей управления.
- Доступ по OutLook Web App.

Предустановленные политики по активности пользователей:

- Активность вне рабочего времени.
- Активность давно отсутствующего пользователя.

Предустановленные политики для Syslog:

- Собственные правила Syslog.
- События ядра операционной системы.
- События пользовательского уровня.
- События почтовых систем.
- События системных демонов.
- События безопасности и авторизации.
- Внутренние события Syslog.
- События протокола построчной печати.
- События новостного протокола.
- События подсистем UUCP.
- События сервисов времени.
- События FTP демонов.
- События подсистем NTP.
- События журналирования.
- Предупреждения журналирования.
- События сервисов планирования.
- Другие события.

Предустановленные политики для событий КИБ SearchInform:

- Изменения в AlertCenter.
- Инциденты в AlertCenter.
- События DataCenter.

Предустановленные политики для Device:

- Копирование на съемное устройство.
- Операции с исполнимыми фалами на устройствах.
- Выполнение файла со съемного устройства.
- Копирование большого числа файлов на съемное устройство.
- Копирование большого объема данных на устройство.

Предустановленные политики для Oracle:

- Неудачные попытки входа в систему.
- Удачные попытки входа в систему.
- Создание пользователя или роли.
- Удаление пользователя или роли.
- Блокировка/разблокировка пользователя.
- Изменения пароля пользователя.
- События Listener.

* Данные актуальны для версии SIEM 1.8.0.7 от 18.08.2017.