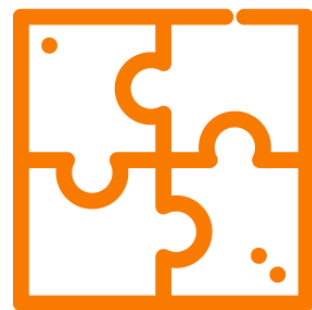




SIEM

SEARCHINFORM

Какие задачи бизнеса решает SIEM?

ПРОБЛЕМА

IT-инфраструктура компании – сложный механизм, состоящий из множества корпоративных систем:

- Сетевые экраны
- Антивирусы
- Приложения
- Базы данных
- ОС сервера и ПК
- Почтовые сервера
- Active Directory
- Сетевые и другие устройства

Каждая система – источник корпоративных и финансовых данных, которые стремятся получить злоумышленники.

Угрозой для компании могут стать как действия администраторов систем (несанкционированное предоставление прав, создание и удаление учетных записей, отключение фаервола), так и уязвимости в ПО, через которые преступники могут получить доступ к данным.

РЕШЕНИЕ

SIEM (Security information and event management) – система для обработки потока событий, выявления ИБ-инцидентов и реагирования на них.

SIEM аккумулирует информацию из различных источников, анализирует ее, фиксирует инциденты и оповещает о них.

Механизм работы «СёрчИнформ SIEM» сводится к алгоритму:



Какие инциденты выявляет «СёрчИнформ SIEM»?



- **Вирусные эпидемии** или отдельные вирусные заражения.
- **Попытки несанкционированного доступа** к конфиденциальным данным.
- **Ошибки и сбои** в работе информационных систем.
- **Критические события** в средствах защиты.

Какие источники анализирует «СёрчИнформ SIEM»?

SIEM-система может собирать информацию практически из любого источника. Главное – правильная подача данных, так как различные источники могут именовать одно и то же событие по-разному. Для приведения событий к общему знаменателю используются коннекторы сбора событий журналов Eventlog или Syslog.

«СёрчИнформ SIEM» анализирует:

ЖУРНАЛЫ СОБЫТИЙ СЕРВЕРОВ И РАБОЧИХ СТАНЦИЙ

Применяются для контроля доступа, обеспечения соблюдения политик ИБ.

СЕТЕВОЕ АКТИВНОЕ ОБОРУДОВАНИЕ

Используется для контроля доступа, учета сетевого трафика, обнаружения атак, информирования об ошибках и сетевых статусах.

КОНТРОЛЬ ДОСТУПА, АУТЕНТИФИКАЦИЯ

Контроль доступа к информационным системам и использования привилегий.

АНТИВИРУСЫ

Информация о наличии, работоспособности и актуальности антивирусного ПО, наличие заражений, вирусных эпидемий, вредоносном ПО.

Что контролирует «СёрчИнформ SIEM»?

- Контроллеры домена Active Directory;
- Журналы EventLog;
- Обращения к файловым ресурсам;
- Активность пользователей;
- Почтовые сервера (MS Exchange, Postfix);
- Антивирусы (Kaspersky, Symantec);
- СУБД (MS SQL, Oracle);
- Syslog аппаратных устройств (серверов, роутеров, принтеров и т.п.) и приложений;
- Файловые операции на подключаемых внешних устройствах;
- DLP «КИБ СёрчИнформ»;
- Сетевые устройства Cisco;
- Устройства комплексной сетевой безопасности FortiGate;

- Среды виртуализации VMware ESXi;
- HTTP-сервера Apache;
- FTP-сервера vsftpd;
- Linux-сервера и рабочие станции;
- Контрольно-весовые аппараты

- Поддержка NetFlow и OPSEC
- Динамические дашборды
- Расширение списка антивирусов, СУБД и почтовых серверов
- Поддержка IDS и IPS

в разработке и тестировании

Что отличает «СёрчИнформ SIEM»?



Одно из ключевых преимуществ «СёрчИнформ SIEM» – простота внедрения и возможность работы фактически «из коробки». Система поставляется с набором готовых политик и учитывает опыт и задачи компаний из всех областей бизнеса и отраслей экономики.

Система работает по принципу «берем практические задачи и решаем их с помощью SIEM». Мы собрали мнение, практику и потребности клиентов «СёрчИнформ» и оформили их в виде готовых политик. Развиваться система будет аналогично: с добавлением поддержки новых источников данных, клиент получает предустановленный набор правил.



Для Syslog

- Собственные правила Syslog
- События ядра операционной системы
- События пользовательского уровня
- События почтовых систем
- События системных демонов
- События безопасности, авторизации и другие события

Для событий «КИБ СёрчИнформ»

- Инциденты и изменения в AlertCenter
- События DataCenter



По активности пользователя

- Активность пользователя вне рабочего времени
- Активность давно отсутствующего пользователя



Для контроллеров домена Active Directory

- Временное переименование учетной записи
- Подбор паролей и устаревшие пароли
- Временное включение/добавление учетной записи
- Контроль старых учетных записей AD
- Временная выдача прав доступа AD
- Одна учетная запись на нескольких ПК и другие события



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

ПРИМЕРЫ ГОТОВЫХ ПОЛИТИК



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

Для Oracle



- Неудачные попытки входа в систему.
- Удачные попытки входа в систему.
- Создание/удаление пользователя или роли.
- Блокировка/разблокировка пользователя.
- Изменения пароля пользователя.
- События Listener и другие события



Для почтовых серверов

- Доступ к почтовому ящику не владельцем
- Смена владельца почтового ящика
- Предоставление доступа к ящику
- Изменение политики аудита
- Изменение критических ролей и другие события



Для подключаемых устройств

- Копирование на съемное устройство
- Копирование большого числа файлов на съемное устройство
- Операции с исполняемыми файлами на устройствах
- Выполнение файла со съемного устройства
- Копирование большого объема данных на съемное устройство



Для среды виртуализации

- События входа/выхода VMview и VMware
- Неправильные пароли
- Неудачные попытки входа
- Создание группы пользователей
- Смена пароля пользователя
- Создание/удаление пользователей
- Удаление снапшотов и другие события



Для серверов и рабочих станций Linux

- Вход неизвестного пользователя
- Вход с повышенными привилегиями
- Изменение пользовательской оболочки входа
- Неуспешная попытка входа
- Неудачные попытки авторизации
- События входа/выхода SSH
- Открытие/закрытие сессии
- Неуспешные попытки доступа SSH и другие события

ПРИМЕРЫ ГОТОВЫХ ПОЛИТИК

Для CISCO

- События входа/выхода
- Вход под встроенной учетной записью
- Вход с повышенными привилегиями
- Ошибки при работе системы
- Ошибки питания
- Отказ системы охлаждения
- Ошибки DHCP
- Ошибки маршрутизации
- Найден дублирующий ID роутера
- Сбой аутентификации Wi-Fi

Для антивирусов

- Самозащита антивируса отключена
- Обнаружен вирус
- Выявлена вирусная эпидемия
- Выявлена сетевая атака
- Компоненты антивирусной защиты отключены
- Критический статус компьютера
- Не удалось выполнить задачу администрирования
- Отсутствует лицензия на антивирус
- Обнаружено потенциально опасное ПО



ПРИМЕРЫ ГОТОВЫХ ПОЛИТИК

Для веб-серверов Apache

- 
- Ошибки авторизации
 - Пользователь не найден
 - Неправильный пароль
 - Использована неправильная схема авторизации
 - Клиент отклонен в связи с конфигурацией сервера
 - Неизвестный алгоритм шифрования
 - Ошибки Nonce и другие ошибки.

Для FTP-серверов vsftpd

- Соединение клиента с FTP
- Скачивание файла с FTP
- Создание/удаление файла на FTP
- Создание/удаление директории на FTP

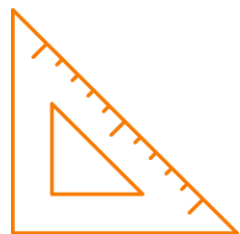
И еще **100+ политик**, которые используются в различных сочетаниях. Список коннекторов и правил непрерывно пополняется.

ПРЕИМУЩЕСТВА «СёрчИнформ SIEM»



ЛЕГКОЕ ВНЕДРЕНИЕ

«СёрчИнформ SIEM» не требует долгой предварительной настройки. Предустановленные политики основаны на перечне типовых задач из практики клиентов «СёрчИнформ» в России и странах СНГ. SIEM дает первые аналитические результаты «из коробки».



ПРОСТОТА ИСПОЛЬЗОВАНИЯ

Работа с «СёрчИнформ SIEM» не требует навыков программирования. С настройкой пользовательской конфигурации SIEM справится любой специалист. Решению поставляется с набором готовых правил, что избавляет от необходимости создавать скрипты, писать правила корреляции событий.

Отдел внедрения «СёрчИнформ» помогает клиенту настраивать индивидуальные политики.

ПРЕИМУЩЕСТВА «СёрчИнформ SIEM»



ПОДХОДИТ СРЕДНЕМУ И МАЛОМУ БИЗНЕСУ

У «СёрчИнформ SIEM» низкие требования к аппаратно-программным средствам. Решение быстро интегрируется и требует минимальной настройки.

Количество влияет на стоимость: больше лицензий – меньше цена.



УЧИТЫВАЕТ ОПЫТ ТЫСЯЧ КЛИЕНТОВ

Мы изучили опыт крупнейших клиентов компании, выявили общие потребности и лучшие практики, чтобы использовать их в «СёрчИнформ SIEM».



РОССИЙСКИЙ ПРОДУКТ

Программное обеспечение «СёрчИнформ SIEM» является продуктом российского разработчика и удовлетворяет требованиям закона об импортозамещении.

ПРЕИМУЩЕСТВА «СёрчИнформ SIEM»



СИМБИОЗ SIEM И DLP

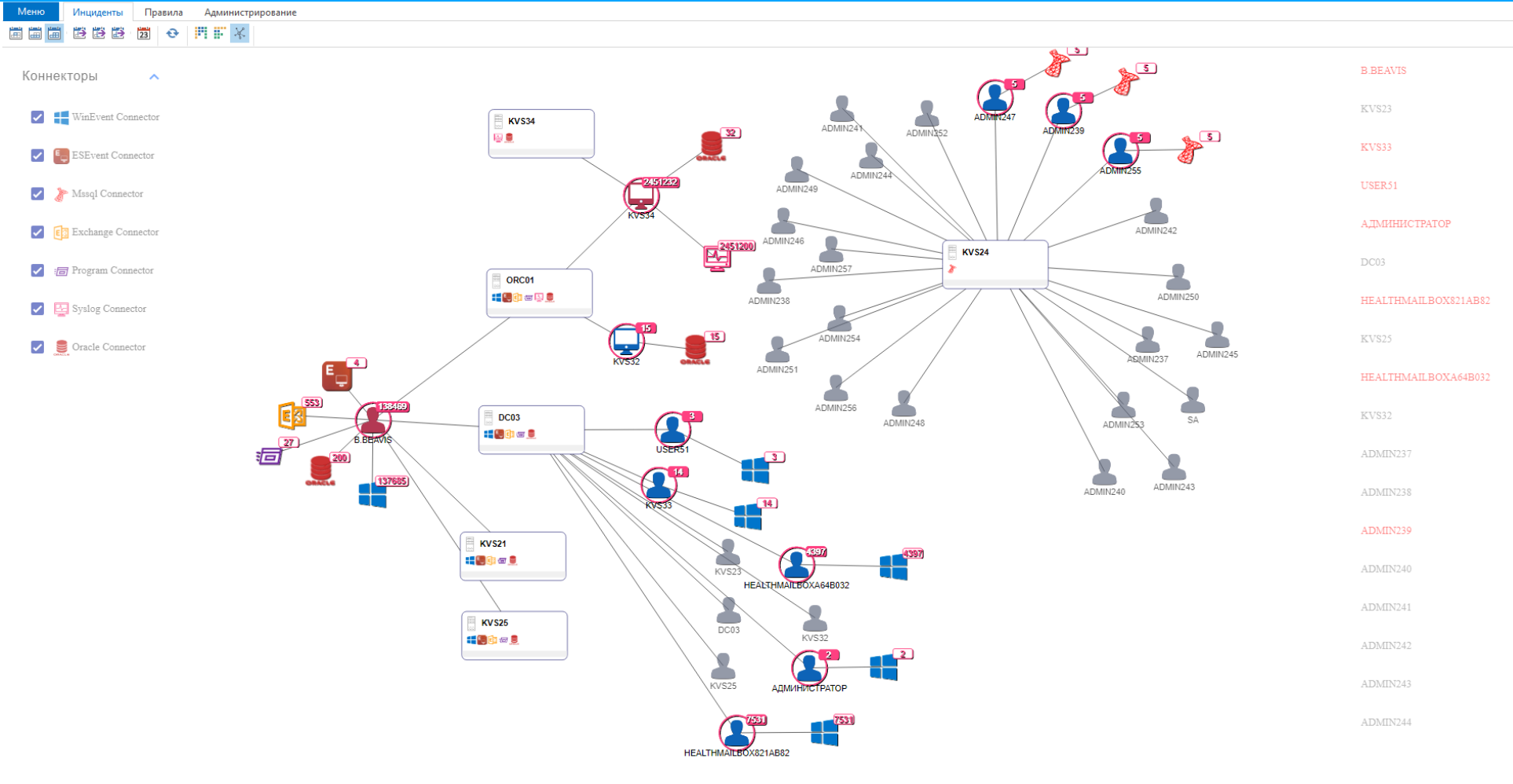
Одновременная работа «СёрчИнформ SIEM» и DLP «КИБ СёрчИнформ» многократно повышает уровень информационной безопасности компании. SIEM выявляет аномальное поведение и определяет способ получения доступа к информации. КИБ оценивает содержимое всех коммуникаций. Связка систем дает возможность максимально полно расследовать преступление и собрать доказательную базу.



СОЗДАЕТ УСЛОВИЯ ДЛЯ ПОЛНОЦЕННОГО ИНЦИДЕНТ-МЕНЕДЖМЕНТА

SIEM постоянно обращается к источникам событий и обрабатывает новые события еще на входе в систему. Специалист по безопасности получает запас времени, чтобы оперативно отреагировать на угрозу и сохранить стабильность защиты.

КАРТА ИНЦИДЕНТОВ



Карта отражает состояние корпоративной системы за выбранный интервал времени. На интерактивной карте отображаются объекты ИТ-инфраструктуры компании и зафиксированные по ним инциденты безопасности с подробным описанием.

«СёрчИнформ SIEM»: КЕЙСЫ



ПОДБОР ПАРОЛЕЙ

SIEM оповестит службу безопасности о многократных попытках подобрать пароли к учетным записям сотрудников на одном или нескольких ПК.



ВХОД ПОЛЬЗОВАТЕЛЯ ПОД СЛУЖЕБНОЙ УЧЕТНОЙ ЗАПИСЬЮ

При использовании SQL Server создается доменная учетная запись с полным доступом ко всем базам данных. SIEM уведомляет, если при помощи служебных логина и пароля для SQL Server авторизовался пользователь, поскольку велика вероятность похищения конфиденциальной информации из этих баз.



НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К КОРПОРАТИВНОМУ ПОЧТОВОМУ ЯЩИКУ

Администратор почтового сервера может перенастроить систему так, чтобы получить доступ к почте топ-менеджера или другого работника. SIEM-система своевременно отреагирует на инцидент и оповестит службу ИБ.

«СёрчИнформ SIEM»: КЕЙСЫ

УЧЕТНЫЕ ЗАПИСИ AD: РАЗБЛОКИРОВКА, ПЕРЕИМЕНОВАНИЕ, ПРОСТОЙ ПАРОЛЬ



В зоне риска также работники, которые давно не меняли пароль или передали его посторонним. Кроме того, администратор может временно переименовать чью-то учетную запись и предоставить доступ в сеть злоумышленникам. «СёрчИнформ SIEM» сообщит, если обнаружит подобные инциденты.

КОРРЕЛЯЦИЯ НАПРЯМУЮ НЕ СВЯЗАННЫХ ДАННЫХ



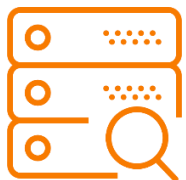
Бывают ситуации, когда внешне безобидные события, полученные из различных источников, в совокупности несут угрозу. Например, когда происходит сброс пароля учетной записи топ-менеджера. В единичном случае это событие не привлечет внимание, но если с этой учетной записи впоследствии произойдет обращение к критичным ресурсам, SIEM-система зафиксирует инцидент.

«СёрчИнформ SIEM»: КЕЙСЫ



«МЕРТВЫЕ ДУШИ» В КОМПАНИИ

IT-специалисты компании могут ослабить защиту корпоративной сети бездействием. SIEM определит, если администратор не удаляет учетные записи уволившихся сотрудников. Например, бывший руководитель использовал логин и пароль, чтобы просматривать коммерческие документы на сетевом диске. При очередной авторизации SIEM зафиксирует событие на ПК сотрудника и уведомит ИБ-служб.



ОБНАРУЖЕНИЕ «НЕСТАНДАРТНЫХ» НАРУШЕНИЙ

Один из «продвинутых» сотрудников пытался скопировать базу клиентов необычным способом. Собственная учетная запись не позволяла ему получить информацию из CRM. Пользователь создал новую учетную запись СУБД и попытался получить информацию напрямую из базы данных. Политика «СёрчИнформ SIEM» контролировала обращение новых учетных записей к базе и система оперативно уведомила службу ИБ о нарушении.

Компания «СёрчИнформ» сегодня

11 лет на рынке DLP
22 года в IT

1 000 000+ ПК
под защитой
ПО «СёрчИнформ»

23 уголовных дела
выиграли клиенты
против инсайдеров

6 филиалов в России

11 представительств за рубежом

2000+ клиентов
в **16** странах мира

«КИБ СёрчИнформ»
включен в **Реестр
отечественного ПО**

В 2017 году
«КИБ СёрчИнформ» вошел в
«магический квадрант» Gartner



Инцидент обнаружен.

Время расследовать.

+7 (495) 721-84-06
info@searchinform.ru
searchinform.ru

