searchinform.ru

SIEM
SEARCHINFORM

СёрчИнформ SIEM

Система мониторинга и корреляции событий информационной безопасности

- **ПЕРВАЯ «КОРОБОЧНАЯ» SIEM**
- **СОЗДАНИЕ ПОЛИТИК В 2 КЛИКА**

ИТ-инфраструктура компании – сложный механизм, который состоит из множества корпоративных систем: сетевых экранов, ОС, почтовых серверов, БД, сетевых устройств. Все эти источники данных интересуют злоумышленников, а значит, нуждаются в особой защите.

Сегодня даже в небольшой компании ИТ-инфраструктура генерирует миллионы событий. Только по статистике входов Active Directory коллектив из 100 человек способен сгенерировать более 3000 событий, а одна работающая в штатном режиме VMware – до 4 миллионов событий в день. Поэтому потребность в мониторинге и постоянном поиске потенциальных угроз возникает даже у малой компании.

Решение

Для предупреждения инцидентов и укрепления внутренних процессов **необходим автоматический контроль событий безопасности**.

«СёрчИнформ SIEM» – система управления событиями и инцидентами информационной безопасности в режиме реального времени. Система аккумулирует информацию из различных источников, анализирует ее, фиксирует ИБ-инциденты и оповещает о них службу безопасности.

Как работает система

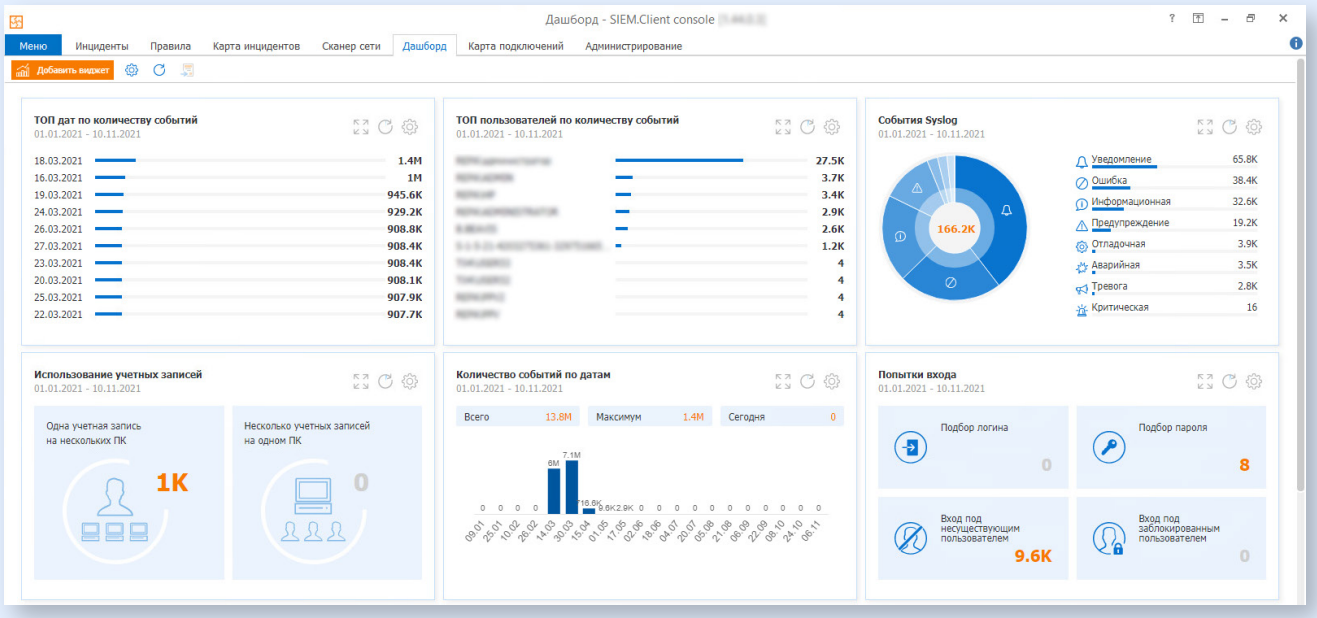
SIEM проводит комплексный аудит и выявляет угрозы по совокупности событий, которые по отдельности выглядят безопасными.

Это происходит в несколько этапов:

1. Сбор событий из различных источников: сетевое оборудование, ПО, средства защиты, ОС.
2. Приведение разнородных данных к общему виду.
3. Анализ данных и выявление угроз.
4. Фиксация инцидентов и оповещение в реальном времени.

«СёрчИнформ SIEM» выявляет:

- Вирусные эпидемии и отдельные заражения.
- Попытки несанкционированного доступа к данным.
- Подбор паролей к учетным записям.
- Активные аккаунты уволенных сотрудников, которые забыли удалить.
- Ошибки конфигурации оборудования.
- Нарушения допустимого температурного режима работы оборудования.
- Удаление информации с критически важных ресурсов.
- Использование корпоративных ресурсов в нерабочее время.
- Удаление виртуальных машин и снапшотов.
- Подключение к IT-инфраструктуре нового оборудования.
- Изменение групповых политик.
- Использование TeamViewer, удаленный доступ к корпоративным ресурсам.
- Критические события в средствах защиты.
- Многие другие события информационной безопасности.



Дашборд со статистикой событий

Решение «СёрчИнформ» – это не «очередная SIEM», которая идет по пути, проложенному другими вендорами. Мы видим проблемы и действуем в «мире клиента», а не «представляем простое сложным» в собственных интересах.

Преимущества «СёрчИнформ SIEM»:

- **Быстрое внедрение без долгой предварительной настройки** (ПО может быть введено в эксплуатацию за один день). Результаты с первого запуска.
- **Простое использование**: с программой справится специалист без IT-навыков, т.к. для создания правил корреляции и кросс-корреляции не нужно знать языки программирования.
- **Аналитика «из коробки»**: система поставляется с набором готовых правил и учитывает опыт и задачи компаний из всех областей бизнеса и отраслей экономики.
- **Инцидент-менеджмент**. Создание расследования на базе одного и более инцидентов.
- Готовые механизмы взаимодействия с **ГосСОПКА**.
- Невысокие аппаратные требования, понятное лицензирование, **комфортная стоимость владения**.

- **Бесшовная интеграция с DLP-системой «СёрчИнформ КИБ»** повышает уровень информационной безопасности компании и дает возможность максимально полно расследовать инцидент, собрать доказательную базу.

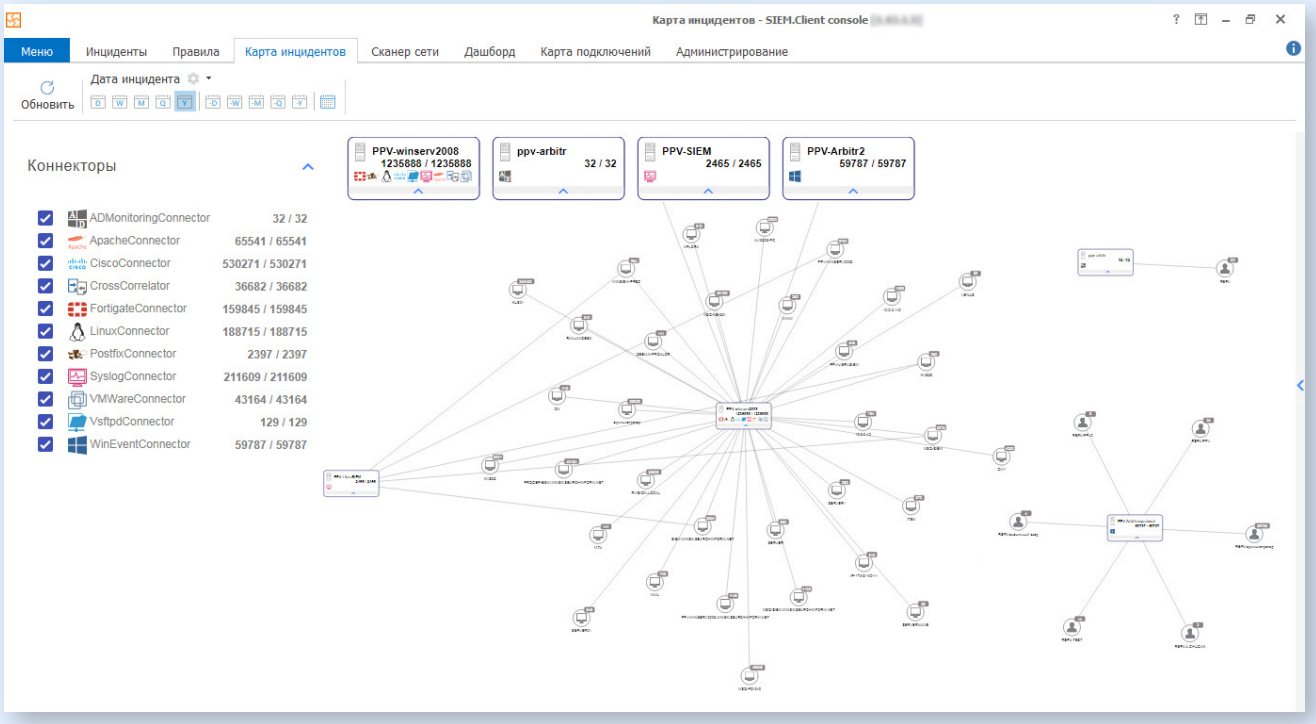
Готовые правила в «СёрчИнформ SIEM»

После установки системы служба ИБ получает доступ к 300+ готовым правилам корреляции событий. Пользователи могут редактировать и настраивать уже существующие и создавать уникальные правила, выбирать источники из предустановленного списка и подключать собственные (функция «пользовательский коннектор»).

Правила корреляции «из коробки» используют следующие источники данных:

- операционные системы;
- почтовые серверы;
- контроллеры домена и рабочих станций;
- серверы и рабочие станции Linux;
- СУБД;
- DLP-системы;
- файловые серверы;
- среды виртуализации;
- антивирусы;
- межсетевые экраны и устройства комплексной сетевой безопасности;
- СКУД;
- решения на платформе 1С;
- иные Syslog-источники;
- сканер уязвимостей;
- другие.

Для поиска инцидентов в связке событий из разных источников используется механизм кросс-корреляции.



Карта инцидентов

Примеры готовых правил корреляции в «СёрчИнформ SIEM»

Для почтовых серверов

- Доступ к почтовому ящику не владельцем
- Смена владельца почтового ящика
- Предоставление доступа к ящику

Для контроллеров домена и рабочих станций

- Временное включение/добавление учетной записи
- Одна учетная запись на нескольких ПК
- Подбор паролей и устаревшие пароли

Для серверов и рабочих станций Linux

- Вход неизвестного пользователя
- Вход с повышенными привилегиями
- Многочисленные попытки неверной аутентификации SSH

Для СУБД

- Изменение пароля имени входа админом БД
- Временное включение имени входа в состав роли
- Временная выдача доступа к объекту БД

Для подключаемых устройств

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

Для антивирусов

- Самозащита антивируса отключена
- Выявлена вирусная эпидемия
- Выявлена сетевая атака

Для среды виртуализации

- События входа/выхода VMview/VMware
- Неправильные пароли
- Удаление снапшотов

Для обращения к файловым ресурсам

- Обращение к критичным ресурсам
- Временная выдача прав на файл/папку
- Большое количество пользователей, работающих с файлом

Для сетевых экранов и устройств комплексной сетевой безопасности

- События маршрутизации локального/запрещенного/разрешенного трафика
- Изменение конфигурации брандмауэра
- События VPN-соединений и работы с оборудованием контроля и сбора данных

По активности пользователя

- Активность пользователя вне рабочего времени
- Активность давно отсутствующего пользователя

Для CISCO

- Вход под встроенной учетной записью
- Вход с повышенными привилегиями
- Ошибки маршрутизации

Для Syslog

- События ядра операционной системы
- События пользовательского уровня
- События системных демонов

Кейсы

Подбор паролей

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.

«Мертвые души» в компании

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

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.

Перегрев оборудования

Скачкообразное изменение температуры серверного оборудования может быть признаком серьезной поломки, а в некоторых случаях и начинающегося пожара. SIEM-система позволит вовремя обратить внимание и устранить проблему.

Контакты

РОССИЯ

Москва (головной офис)

121069, Скатертный пер., 8/1, строение 1, этаж 2
Телефоны:
+7 (495) 721-84-06
+7 (495) 721-84-06, доб. 125 (техническая поддержка)
+7 (499) 703-04-57
Email:
info@searchinform.ru – общие вопросы
support@searchinform.ru – технические вопросы
order@searchinform.ru – вопросы приобретения
pr@searchinform.ru – для прессы

Санкт-Петербург

Коломяжский пр-т, 27
Телефоны:
+7 (812) 309-73-35
+7 (495) 721-84-06, доб. 119
Email: a.yanchuk@searchinform.ru

Екатеринбург

ул. Серафимы Дерябиной, 24, оф. 801
Телефоны:
+7 (495) 721-84-06, доб. 105
+7 (343) 344-50-88
+7 (343) 344-51-38
Email: a.popov@searchinform.ru

Казань

ул. Островского, 57В, оф. 301–302
Телефоны:
+7 (495) 721-84-06, доб. 126
+7 (843) 206-07-43
+7 (965) 600-53-07
Email: t.latushkina@searchinform.ru

Новосибирск

ул. Владимировская, 2/1, оф. 109
Телефоны:
+7 (495) 721-84-06, доб. 106
+7 (913) 772-60-06
+7 (383) 280-46-57
Email: alena.bugaenko@searchinform.ru

Хабаровск

ул. Пушкина, 54, оф. 403
Телефоны:
+7 (495) 721-84-06, доб. 131
+7 (4212) 47-59-92
+7 (924) 104-04-04
Email: d.kazakov@searchinform.ru

АРГЕНТИНА, Буэнос-Айрес

Гало 353, C1172ABG
Телефоны: +54 11 5984 2618
+54 911 5158 8557
Email: r.martinez@searchinform.com

БРАЗИЛИЯ, Сан-Паулу

Вила-Олимпиа, Руа Гомес де Карвальо 1356, оф.16
Телефон: +55 11 4380 1913
Email: v.prestes@searchinform.com

ВЕЛИКОБРИТАНИЯ, Лондон

Телефон: +44 (0) 203 808 4340
Email: uk@searchinform.com

КАЗАХСТАН, Алматы

ул. Ауэзова, 84, оф. 200
Телефон: +7 (777) 239-30-36
Email: r.sabitova@searchinform.ru

ЮАР, Центурион

Блок 32, Кембриджский офисный парк,
ул. Баухиния, 5, Хайвелд технопарк, Центурион, 0157
Телефон: +27 12 683 8816
Email: jorina@searchinform.com

Ещё больше полезных материалов по информационной безопасности – в разделе «Практика и аналитика» на сайте searchinform.ru