McAfee Enterprise Log Search

Поиск по миллиардам событий на высоких скоростях

Отделам ИБ необходимы инструменты, позволяющие быстрее ориентироваться в средах, в которых генерируется очень много предупреждений. Аналитикам этих отделов необходим доступ к более подробному контексту и возможность быстро выявлять важные сведения о событиях, связанных с тем или иным инцидентом. McAfee® Enterprise Log Search ускоряет процесс поиска угроз безопасности за счет сверхбыстрого поиска по необработанным, несжатым данным о событиях. Для оптимизации скорости запросов используется поисковый модуль на базе Elasticsearch, мгновенно предоставляющий доступ к необработанным журналам. Расширенный набор функций поиска позволяет создавать запросы путем ввода как простых ключевых слов на естественном языке, так и более сложных шаблонов из регулярных выражений для целенаправленного поиска данных.

Оптимизация управления журналами событий

В основе McAfee Enterprise Log Search лежит Elasticsearch — технология, в которой для хранения данных используется инвертированный индекс. Инвертированный индекс осуществляет каталогизацию данных в структуру, способствующую эффективному извлечению искомой информации. Поскольку технология Elasticsearch предназначена для приема и индексирования данных на высоком уровне быстродействия, после сбора и каталогизации необработанных данных в McAfee Enterprise Log Search они становятся доступными для поиска на высоких скоростях.

McAfee Enterprise Log Search является одним из компонентов McAfee® Enterprise Security Manager, решения для управления информацией о безопасности и событиями безопасности (SIEM). Одним из смежных компонентов является McAfee® Enterprise Log Manager, предназначенный для хранения журналов. Он обеспечивает целостность входящих необработанных журналов путем их хэширования (MD5), а для экономии места в хранилище проводит их сжатие. Сочетание этих компонентов используется в специализированных решениях для хранения информации, позволяющих максимально повысить скорость поиска (посредством McAfee Enterprise Log Search) и при этом обеспечить хранение журналов в соответствии с нормативно-

Ключевые преимущества

- Оптимизированное управление журналами, обеспечивающее как сохранность журналов, так и быстрый поиск по ним
- Поисковый модуль на базе Elasticsearch поддерживает операции приема, индексирования и поиска данных на высоком уровне быстродействия
- Поиск на естественном языке
- Быстрый и простой переход от представлений с проанализированными данными к необработанным журналам
- Полная интеграция с McAfee Enterprise Security Manager
- Возможны различные варианты развертывания с использованием физических и виртуальных устройств (в разных сочетаниях)

Подписаться

правовыми требованиями (посредством McAfee Enterprise Log Manager). Это избавляет клиентов от необходимости идти на компромисс и решать, какой из этих двух компонентов им нужнее.

McAfee Enterprise Log Search позволяет указывать в политиках хранения журналов разные сроки хранения несжатых данных, выраженные в годах (365 дней), кварталах (90 дней) или месяцах (30 дней). Пользователям предоставляется возможность указать источники данных, которые должны быть ассоциированы с McAfee Enterprise Log Search, и создать от одной до шести отдельных политик хранения журналов.

Расширенные функции поиска

Используемая в McAfee Enterprise Log Search функция поиска похожа на функции поиска в популярных поисковых системах: она позволяет вводить данные на естественном языке, в виде простого текста или ключевых слов. Помимо этого, поиск можно выполнять с использованием более сложных шаблонов, включающих в себя булеву логику, подстановочные знаки и регулярные выражения (RegEx). Для еще большего сужения результатов поиска пользователи могут применять фильтры по источникам данных и по дате. Фильтр по дате дает пользователям возможность фильтровать события в журналах по времени их генерирования: например, за прошлый час, за текущие сутки, за прошлый год или в заданный пользователем период.

Интеграция с McAfee Enterprise Security Manager

Тесная интеграция с McAfee Enterprise Security Manager дает аналитикам возможность одним щелчком мыши переходить от проанализированных данных к необработанным. При генерировании события в McAfee Enterprise Security Manager осуществляется привязка проанализированных файлов события непосредственно к исходному файлу журнала и к конкретной записи в необработанном журнале. При необходимости аналитик может ознакомиться с этой записью или ее фрагментами. Для этого ему нужно просто выбрать соответствующий журнал, после чего автоматически активируется функция поиска по необработанному журналу, и аналитик может сразу приступать к углубленному анализу: не нужно ни запускать отдельное приложение, ни открывать специальный интерфейс.

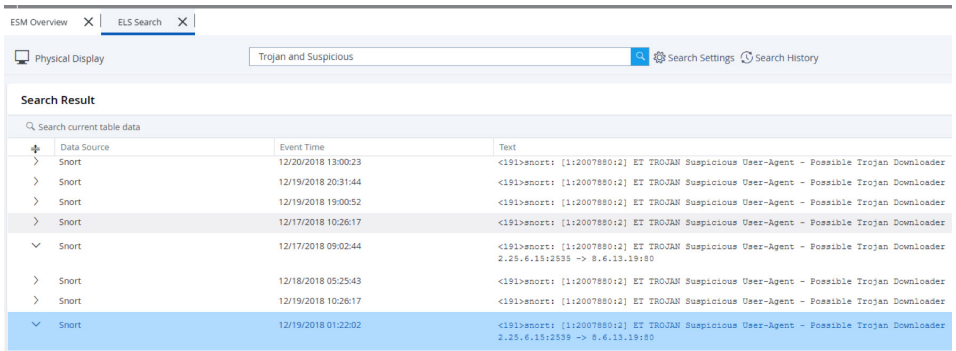

Рис. 1. Поиск по ключевым словам с использованием булевой логики для обнаружения событий, содержащих троян и являющихся подозрительными.

Различные варианты развертывания и гибкая система ценообразования

Решение поставляется в виде аппаратных и виртуальных устройств. Аппаратные устройства оцениваются и продаются исходя из их способности принимать определенное количество событий

в секунду (EPS), а не по цене за источник данных, за EPS или за индексированный объем данных. Виртуальные машины (ВМ) лицензируются по тому же принципу: их цена определяется исходя из количества ядер процессора, необходимых для обеспечения того или иного количества обрабатываемых событий (EPS). Это позволяет клиентам по мере необходимости приобретать дополнительные ядра, не меняя аппаратное обеспечение.

Сбор необходимых вам данных и быстрый поиск по ним

При развертывании McAfee Enterprise Log Search различается шесть типов журналов, обычно используемых для поиска угроз безопасности. Именно в этих журналах может находиться конкретная информация по инцидентам безопасности и соответствующий контекст.

Тип журнала	Обычно имеющиеся в журнале данные
Журналы DNS	▪ Запрошенное доменное имя ▪ IP-адрес источника DNS-запроса ▪ Успех или неудача DNS-запросов ▪ Определенный IP-адрес, если запрос был успешным ▪ Значение TTL, указанное в ответе ▪ Использованный DNS-сервер
Журналы прокси-серверов	▪ Домен/IP-адрес, к которому осуществляется подключение ▪ Количество переданных байтов ▪ Метка времени подключения ▪ Используемый идентификатор ресурса (URI) ▪ Ссылающийся домен ▪ Строка с указанием агента пользователя
Журналы SMTP	▪ Домен отправителя сообщения электронной почты ▪ Тема сообщения электронной почты ▪ IP-адрес отправителя
Журналы Windows	▪ События журнала безопасности Windows ▪ События журнала приложений Windows ▪ События системного журнала Windows ▪ События журнала целостности кода Windows
Журналы DHCP	▪ MAC-адрес источника ▪ Предоставленный IP-адрес ▪ Срок аренды ▪ Метка времени запроса и предоставления аренды
Журналы VPN	▪ IP-адрес источника ▪ Идентификатор, используемый при проверке подлинности ▪ Метка времени установления VPN-соединения ▪ Тип соединения: возобновление или новое ▪ Неудачные попытки прохождения проверки подлинности (если таковые имеются) и соответствующие идентификаторы

Дополнительная информация

За дополнительной информацией обращайтесь по адресу **www.mcafee.com/enterprise/ru-ru/products/siem-products.html**.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru