SIEM (ElasticSearch)

Компоненты

ElasticSearch	Серверная часть - бэкенд обработки данных
Агенты	На клиентах, агрегируют и отправляют данные
Kibana	Визуализация данных ElasticSearch, возможно на отдельном сервере. Серьезные проблемы с получением интеграций, нужно отдельно скачивать + EPR (пакетный менеджер)
Fleet	Бэкенд для управления агентами, фронт через kibana. Управление через политики.

ELK-запросы. KQL

Для составления запросов в Kibana используется KQL(Kibana Query Language). Подробнее по ссылке.

Рассмотрим основной интерфейс вкладки Discover в Kibana:

1. Окно выбора временного периода для ограничения поиска.
2. Выбор индекса с данными. Данные с различных источников могут иметь разный формат и записываться в разные индексы(базы).
3. Строка запросов KQL.
4. Доступные в текущем поиске поля данных.
5. Результаты поиска.

Выбор времени и индекса

Выбирается абсолютный /относительный диапазоны времени. Список доступных индексов находится в левой части экрана.

Поля с данными

После выполнения запроса в левой части экрана Kibana покажет доступные в результатах поиска поля данных, например такие как имя агента, IP и прочие. Имена полей можно искать с помощью строки поиска, если кликнуть на поле, Kibana покажет статистику.

Для удобной работы с чтением логов имеет смысл выбрать интересующие специалиста поля для отображения в результатах поиска(5). Для выбора необходимо нажать на символ (+) рядом с именем поля. Поле timestamp выбрано по умолчанию.

Результаты поиска с выбранными полями host.ip, host.name, host.os.family и message. Полученный вид можно сохранить для дальнейшего использования нажав кнопку "Save" в правом верхнем углу экрана.

Это очень удобно для работы с разными наборами данных, например, для изучения сетевого трафика имеет смысл выбрать поля связанные с src/dst портами, IP/MAC адресами и протоколами, для изучения логов веб-сервера добавить url, http response code, XFF, user-agent, для изучения поведения процессов - command line, process.pid, process.parent.pid, user, итд.

Примечание: по умолчанию Kibana показывает 500 последних документов в результатах поиска.

KQL.

KQL использует логические операторы и ключевые слова для составления запроса. Также в запросе можно фильтровать результаты по полям. Например, запрос message: error будет искать ключевое слово error в поле message.

Оператор (:) обозначает, что мы ищем полное совпадение ключевого слова "error" среди текста в поле message.

Если мы попробуем найти неполное совпадение, например message:err , то результат поиска будет пустым. Для поиска частичного совпадения можно использовать символ (*), message:err* . Помимо поиска совпадений в KQL также доступны операторы <,>, >=, <= и логические AND, NOT, OR. Рассмотрим следующий пример:

(host.name: web*)   AND (NOT http.response.status_code: 200) AND (http.response.status_code: *)

В данном примере мы ищем результаты которые содержат http.response.status_code и где http.response.status_code не равняется 200 на машинах с именем начинающимся на web.

http.response.status_code оказался в запросе дважды, поскольку в результаты запроса

(NOT http.response.status_code:200)попадут все данные, в которых поле http.response.status_code не существует в принципе. Чтобы это исправить, мы ищем данные, где это поле имеется (http.response.status_code: *) и сужаем фильтр до результатов, где значение поля не равняется 200.

Revision #9
Created 15 October 2025 18:23:24 by Admin
Updated 25 October 2025 18:45:05 by Admin