Tecnologías SIEM

Adán Avilés

Julio 2020

Índice

1. Presentación y resolución de los problemas **3**

1. Presentación y resolución de los problemas

Durante el curso, hemos visto qué son los eventos correlados y los agregados. ¿Podría definir brevemente cada uno de ellos? Emplee gráficos, dibujos, ejemplos, etc., si lo cree oportuno.

En primer lugar, definiremos lo que entendemos por **evento**. Un evento es todo registro que ha sido generado en una fuente de datos, la cual contiene información sobre las tareas y acciones realizadas por el sistema. Dependiendo de la aplicación o sistema que genere el evento, este será creado en un formato u otro, dependiendo de la aplicación.

Hablaremos de correlación cuando tengamos correspondencia o relación entre dos o más cosas, o series de cosas. Así, un motor de correlación es una aplicación software que entiende las relaciones de forma programática. Esta, encuentra relaciones simples entre eventos similares. Generalmente, uno de ellos marca el inicio de un determinado proceso, y el segundo su finalización.

Entendemos los **eventos correlados** como aquellos eventos que nacen de la correlación o relación de otros, definidos mediante reglas. Esta relación nos permite identificar situaciones extraordinarias, para identificar la causa raíz de un problema, o para realizar predicciones sobre posibles tendencias.

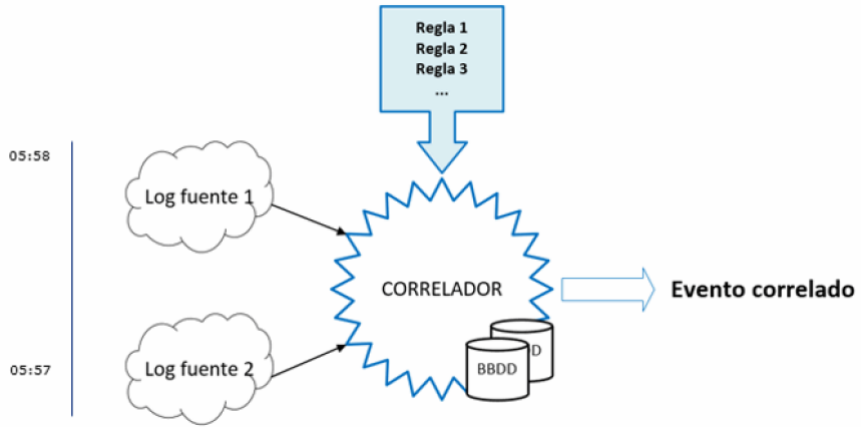

Figura 1: *Esquema de un evento correlado*

La correlación de eventos es útil en distintos escenarios, como el análisis de datos

financieros o detección de fraude. Por ejemplo, detectar los patrones de uso infrecuente de una tarjeta de crédito nos permitiría ver ese posible fraude. Por otro lado, podemos utilizarlo para el análisis de logs de un sistema, agrupando eventos y mensajes similares o análisis de gestión y sistemas.

Por otro lado, hablaremos de **agregación o eventos agregados** cuando se agrupen aquellos eventos de la misma tipología, que compartan ciertos campos con idéntico valor, recibidos en un periodo de tiempo t definido, con el fin de reducir el número de eventos recibidos. Estos campos son generalmente configurables por el administrador de la plataforma SIEM, así como la propia agregación puede ser deshabilitada si así se desea. La agregación de eventos proporciona soluciones para la administración de logs desde múltiples fuentes, incluyendo aplicaciones, redes, servidores o bases de datos, proporcionando la capacidad de consolidar y agrupar los datos estudiados, para evitar la pérdida de los eventos cruciales.

Figura 2: *Ejemplo de opciones de agregación de McAffe*

Un ejemplo de uso simplista, podría ser que si encontramos múltiples intentos de inicio de sesión de un usuario específico fallidos debido a una contraseña incorrecta, puede reflejarse en un sólo evento de .ªutenticación fallida"que incluye varios duplicados.

¿Se emplean siempre los mismos criterios de agregación en todos los eventos o tipologías de eventos que se reciben en un SIEM? ¿Por qué? Justifique y razone su respuesta de acuerdo a eventos concretos o tipologías de eventos concretas.

En general, no considero que se empleen los mismos criterios de agregación en los eventos o tipologías, ya que cada sistema generará unos eventos distintos y estos habrán de ser tratados de manera distinta. Según la configuración que tengan esos eventos, habrán de ser tratados y filtrados de forma diferente.

Pongamos como ejemplo los eventos que sirven apra monitorizar el rendimiento del sistema, o si la seguridad del mismo está comprometida, no serán tratados de la misma forma. Además, no todos los SIEM ofertarán las mismas características de agregación pues sabemos que *Splunk* a día de hoy no tiene agregación.
También hemos de tener en cuenta criterios como la capacidad de almacenamiento (generamos MUCHOS eventos sin ni siquiera saberlo) de nuestros sistemas, factores económicos (pues a mayor cantidad de datos, mayor la inversión que hemos de hacer) o que Windows y Linux no van a generar los mismos eventos.

Durante el curso, hemos estudiado los tipos de visualizaciones que se pueden utilizar para diferentes casuísticas (Compliance, Estado). Si quisiéramos hacer un panel en el que se desea representar gráficamente la evolución de eventos de dos fuentes de datos en un mismo periodo de tiempo, ¿cuál sería la gráfica que utilizaría para dicho fin? Justifique su elección.

Para este caso utilizaría un dashboard con gráficos de distribución pues nos permite visualizar de mejor manera la evolución de los eventos en distintas fuentes de datos en un mismo periodo de tiempo. Además de permitir ver la información resumida de forma visual, permite que la visualización sea en un espacio temporal determinado por el usuario. Adjunto también un diagrama para saber qué representación suele ser la más adecuada para qué tipo de datos y casos.

Durante el curso, hemos estudiado los tipos de visualizaciones que se pueden utilizar para diferentes casuísticas (Compliance, Estado). Si quisiéramos hacer una visualización de los eventos tal cual, ¿cuál sería la gráfica o el tipo de visualización para mostrar estos datos? Justifique su respuesta.

Aparentemente un dashboard sería la mejor opción visual, pero nos obligaría a tratar los datos y no nos sirve (ya que el enunciado dice que queremos los eventos "tal cual"), entonces una tabla de datos es la solución adecuada.

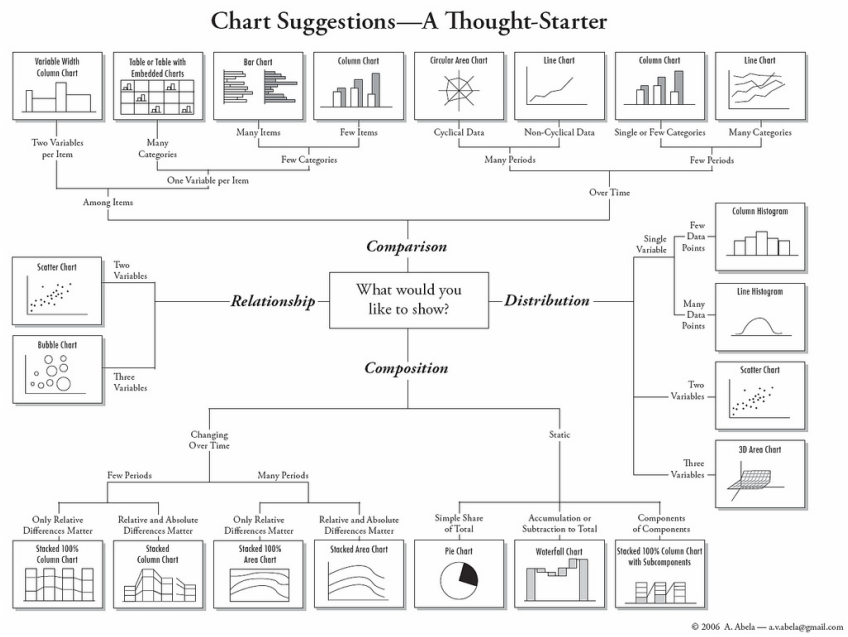

Figura 3: *Criterios para charts*