Manual de usuario

En este documento se explican los diferentes parámetros que se pueden utilizar para crear nuevas reglas de correlación.

Campos generales

En primer lugar tenemos los campos generales de la regla, donde ### es el identificador de la regla:

- R###_NAME
  - Descripción: Se trata del nombre que le vamos a dar a la regla de correlación
  - Valores permitidos: Cualquiera
  - Obligatorio: Sí
  - Valor por defecto: No hay
  - Ejemplo:
    - R001_NAME:Posible equipo infectado
- R###_DESCRIPTION
  - Descripción: Se trata de la descripción de la regla
  - Valores permitidos: Cualquiera
  - Obligatorio: Sí
  - Valor por defecto: No hay
  - Ejemplo:
    - Descarga de fichero malicioso y deteccion IDS
- R###_ LEVEL
  - Descripción: Se trata del nivel de severidad de la regla de correlación
  - Valores permitidos: Cualquiera
  - Obligatorio: Sí
  - Valor por defecto: No hay
  - Ejemplo:
    - R001_LEVEL:HIGH
- R###_ CONTEXTO
  - Descripción: Se trata del campo que se utilizará para identificar el contexto de correlación, de manera que si llegan varios eventos que podrían provocar el análisis de la misma regla y además tienen algún campo en común se puede limitar para que sólo se analice el primer evento
  - Valores permitidos: Cualquier campo del evento escrito entre corchetes
  - Obligatorio: Sí
  - Valor por defecto: No hay
  - Ejemplo:
    - R001_CONTEXTO:[srcip]

Campos del evento disparador, N0

A continuación se deben definir las condiciones que el evento debe cumplir para que se inicialice la regla de correlación, donde ### es el identificador de la regla y $ el identificador de la condición:

- R###_N0_C$
  - Descripción: Se trata de las condiciones que se deben cumplir para que se analice la regla de correlación.
  - Valores permitidos: En primer lugar se debe definir YES o NOT para que el resultado de la consulta se devuelva sin alterar o se devuelva invertido.
    A continuación se define una condición booleana, utilizando el esquema:
    - Nombre del campo entre corchetes

        - Símbolo “==” que define una operación de igualdad o “=~” que define una operación de contener
        - Valor del campo entre comillas dobles
    - Obligatorio: Sí
    - Valor por defecto: No hay
    - Ejemplo:
        - R001_N0_C0:YES [rule_description]=="Detected_malicious_file_HASH"
        - R001_N0_C1:NOT [regla]=="R001"

Campos de los diferentes niveles de correlación

A continuación se deben definir los diferentes eventos con los que se desea correlar el evento inicial teniendo en cuenta que cada tipo de evento se definirá en un nivel distinto con propiedades propias, donde ### es el identificador de la regla y $ el identificador de la condición y % el nivel. Si se cumplen todos los niveles de la regla de correlación se generará una alerta.

- R###_N%_C$
    - Descripción: Se trata de las condiciones que se deben cumplir para que se cumpla este nivel de la regla de correlación.
    - Valores permitidos: En primer lugar se debe definir YES o NOT para que el resultado de la consulta se devuelva sin alterar o se devuelva invertido.
      A continuación se define una condición booleana, utilizando el esquema:
        - Nombre del campo entre corchetes
        - Símbolo “==” que define una operación de igualdad o “=~” que define una operación de contener
        - Valor del campo entre comillas dobles

      Se pueden añadir varias condiciones separadas por la operación OR
      Se pueden referenciar los valores de campos de otros niveles
        - El valor se debe colocar entre corchetes. En primer lugar se define el nivel del que queremos obtener el valor, a continuación “___”, y por último el nombre del campo.
    - Obligatorio: Sí
    - Valor por defecto: No hay
    - Ejemplo:
        - R001_N1_C0:YES [syslog_programname]=="snort"
        - R001_N1_C1:YES [srcip]==[0___srcip]
- R###_N%_SL
    - Descripción: Se trata de un sleep en segundos antes de iniciar la correlación de eventos de ese nivel. Es interesante si los eventos de un tipo sabemos que llegan con cierto retraso.
    - Valores permitidos: cualquier número positivo
    - Obligatorio: No
    - Valor por defecto: 10
    - Ejemplo: R001_N1_SL:1
- R###_N%_SQ
    - Descripción: Se trata de un sleep en segundos entre consultas del mismo nivel.
    - Valores permitidos: cualquier número positivo
    - Obligatorio: No
    - Valor por defecto: 60
    - Ejemplo: R001_N1_SQ:6

- R###_N%_Tmin
  - Descripción: Se trata del espacio temporal en segundos a analizar antes del evento del nivel anterior
  - Valores permitidos: cualquier número
  - Obligatorio: No
  - Valor por defecto: -60
  - Ejemplo:
    - R001_N1_Tmin:-1
- R###_N%_Tmax
  - Descripción: Se trata del espacio temporal en segundos a analizar después del evento del nivel anterior
  - Valores permitidos: cualquier número
  - Obligatorio: No
  - Valor por defecto: +1200
  - Ejemplo:
    - R001_N1_Tmax:10
- R###_N%_ Rnot
  - Descripción: Se trata de una propiedad que define el comportamiento de la regla
  - Valores permitidos: 0 o 1
    - 0 significa comportamiento normal: Al pasar el valor RyOK la firma salta, al agotarse el tiempo la firma desaparece
    - 1 significa comportamiento inverso: Al pasar el valor RyOK la firma desaparece, al agotarse el tiempo la firma salta
  - Obligatorio: No
  - Valor por defecto: 0
  - Ejemplo:
    - R001_N1_Rnot:0
- R###_N%_ RyOK
  - Descripción: Se trata del umbral, el número de eventos para que se cumpla este nivel de la regla(en comportamiento normal) o de que se desestime(en comportamiento inverso)
  - Valores permitidos: Cualquier número positivo
  - Obligatorio: No
  - Valor por defecto: 1
  - Ejemplo:
    - R001_N1_RyOK:1
- R###_N%_Event
  - Descripción: Propiedad que permite elegir con que evento encontrado nos quedamos para el siguiente nivel.
  - Valores permitidos: 0 o 1
  - Obligatorio: No
  - Valor por defecto: 0
  - Ejemplo:
    - R001_N1_Event:0