USO DE ELASTICK STACK

PRÁCTICA 3.4 | PARTE 1

ERIC SERRANO MARÍN

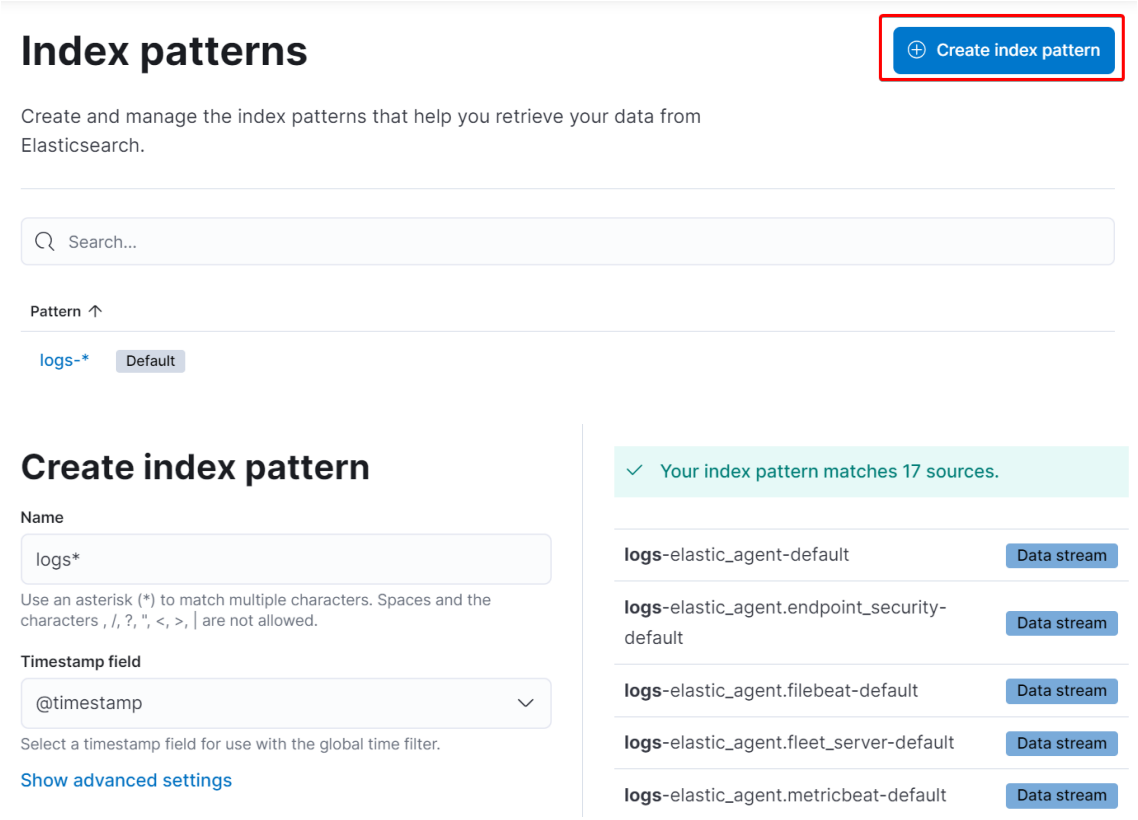
INCIDENTES DE CIBERSEGURIDAD

Contenido

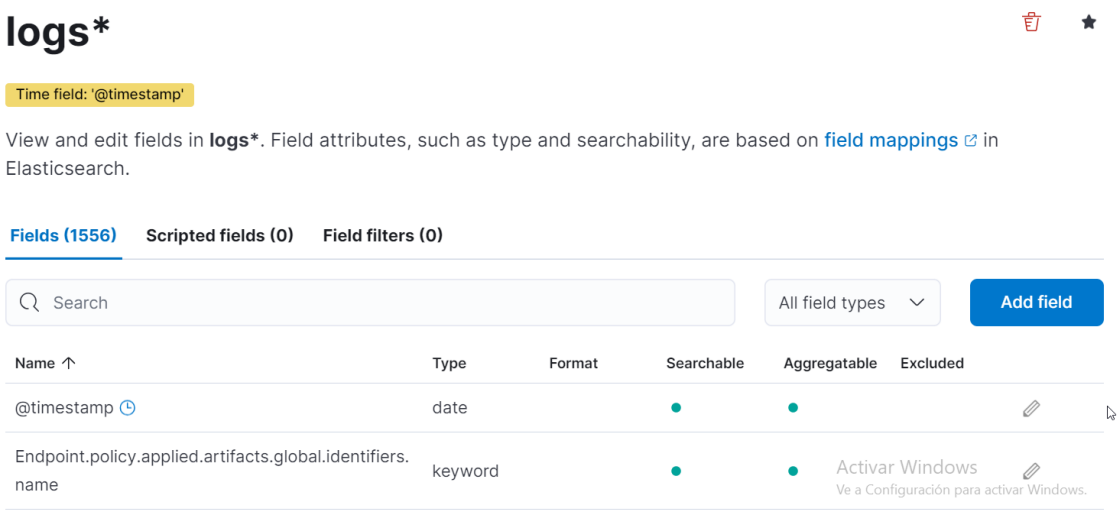
ENUNCIADO

En esta práctica vamos a hacer uso de Elastic Stack para revisar los datos recogidos por el módulo en los puntos finales, tratados por Logstack y almacenados en Elastic Search.

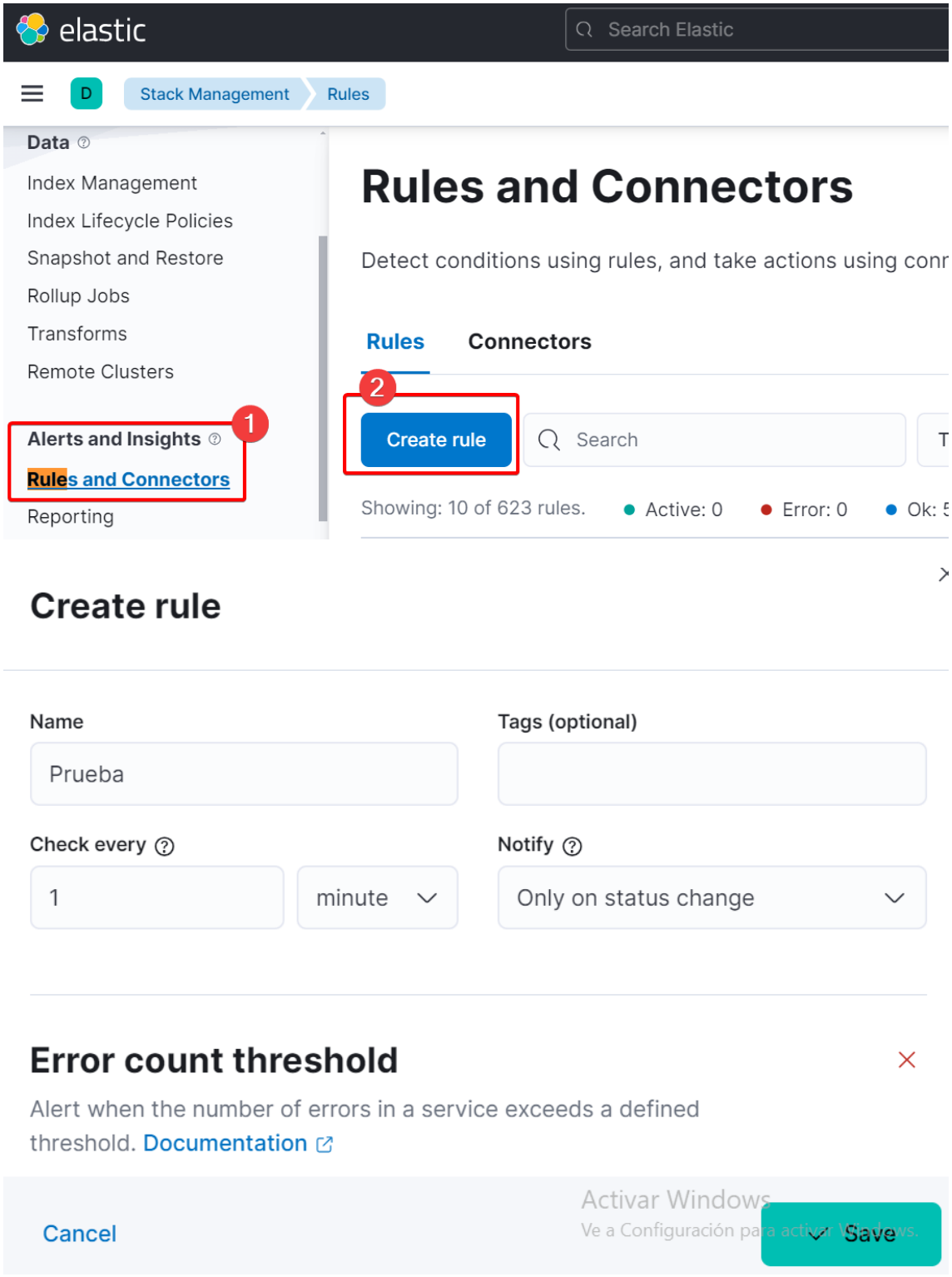
1. Crea un patrón de índice.

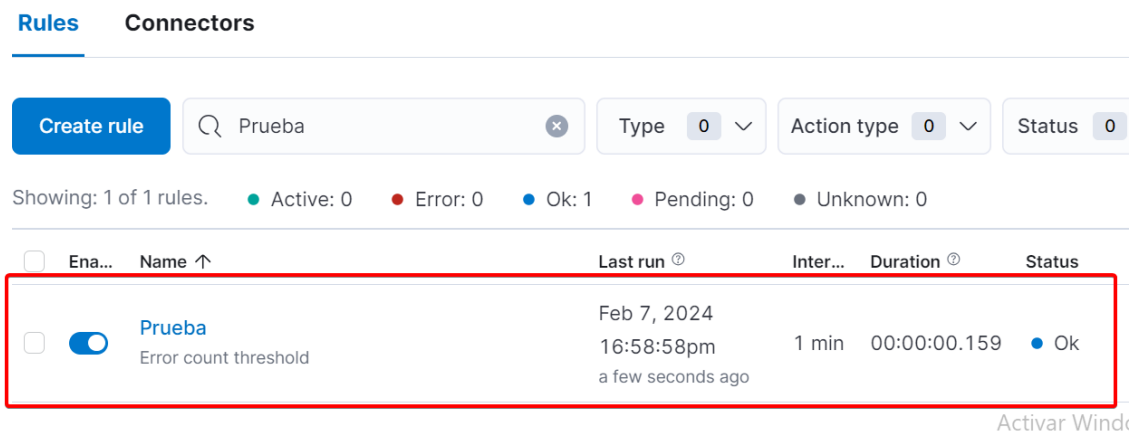


Ya se nos ha creado



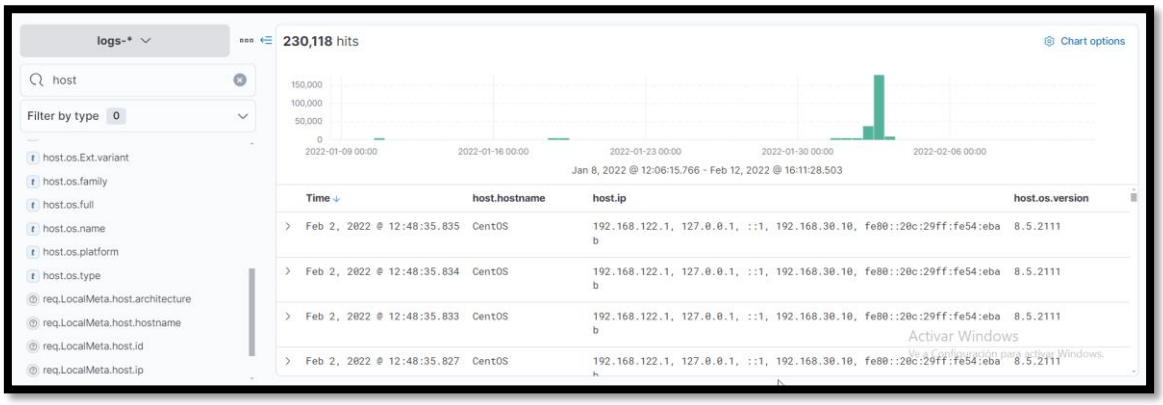
2. Crea una regla de detección.



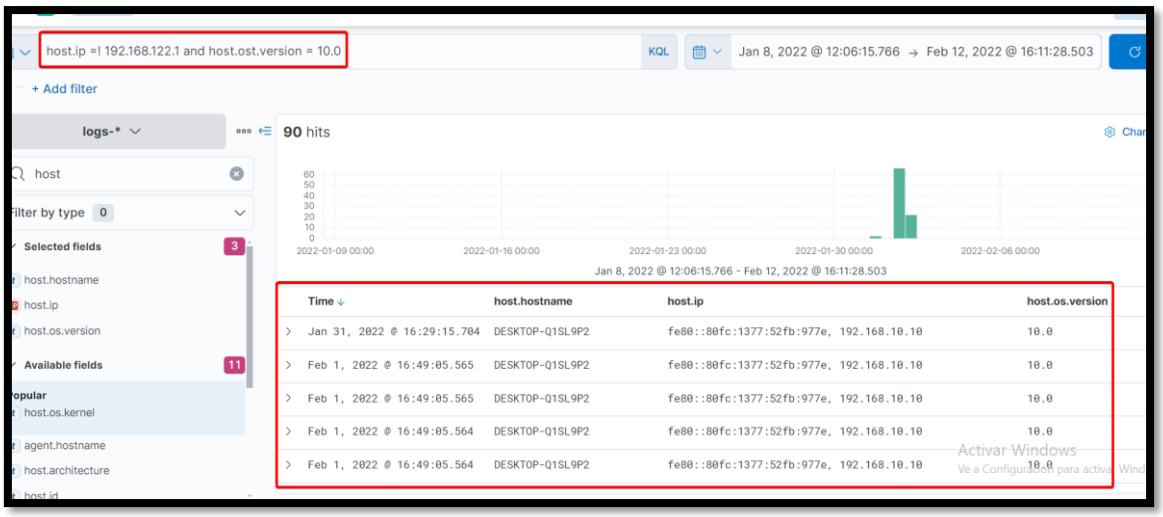


3. **Haz una búsqueda de información en la pantalla de logs (Discover): Configura una vista con 4 columnas que contengan información y haz una consulta con al menos 2 parámetros.**

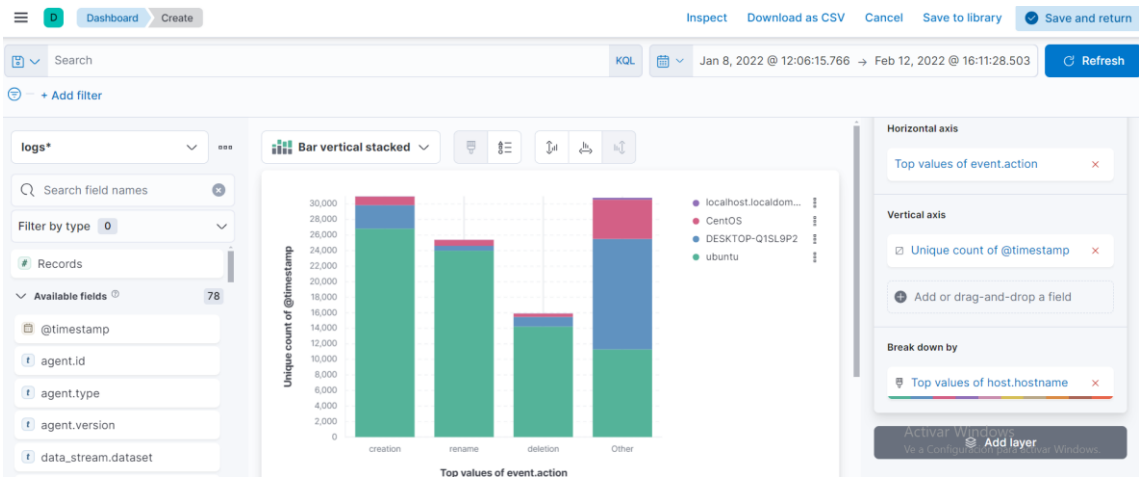
Vista con cuatro columnas.



Consulta con dos parámetros.



4. **Crea un tablero con 3 gráficas de diferente tipo, donde al menos una de las gráficas muestra información de 2 parámetros conjuntamente.**



Esta gráfica proporcionaría una visión detallada de cómo se distribuyen diferentes tipos de eventos para cada acción principal en tu conjunto de datos.