



Información Técnica

AMEZQUITA



Información para crear regla de seguimiento en falsificación de actividad. Se crearon 2 reglas para poder disparar alarmas de que alguien incurra en estas prácticas. Como dato general ambas están en la categoría de actividad y pulsación de teclado.



Categoría de regla:

SELECCIONA EL TIPO DE REGLA

Actividad

MARCA ESTA POLÍTICA CON ETIQUETAS PARA IDENTIFICAR SU PROPÓSITO

Tipos de actividades

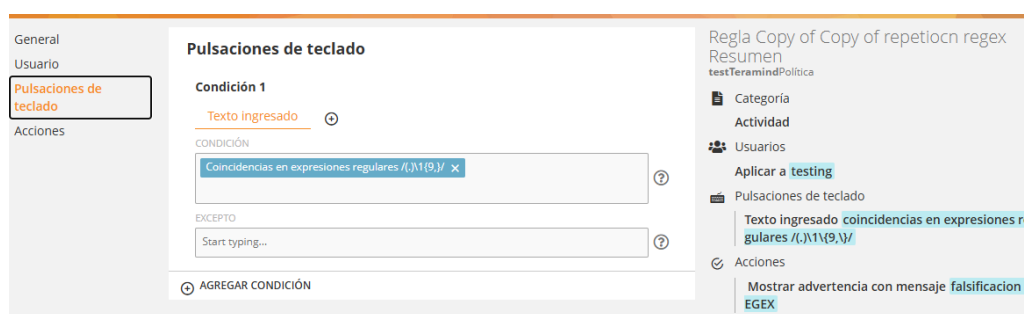
Tipos de actividades	Estado
PÁGINAS WEB	NO
APLICACIONES	NO
PULSACIONES DE TECLADO	SÍ
ARCHIVOS	NO
CORREOS ELECTRÓNICOS	NO
MENSAJERÍA INSTANTÁNEA	NO
PLUGINS DEL NAVEGADOR	NO
IMPRESIÓN	NO
REDES	NO
REGISTRO	NO
USO DE CÁMARA	NO

Figura 1: General

1. Regla 1

Se crea una regla para que se reporte cualquier carácter repetido, esto se hace a través del uso de expresiones regulares, tomando la siguiente sentencia.

`/(\.)\{1{9,}\}/`



Pulsaciones de teclado

Condición 1

Texto Ingresado

CONDICIÓN

Coincidencias en expresiones regulares `/(\.)\{1{9,}\}/`

EXCEPTO

Start typing...

AGREGAR CONDICIÓN

Regla Copy of Copy of repetiocrn regex

Resumen

testTeramindPolitica

Categoría

Actividad

Usuarios

Aplicar a testing

Pulsaciones de teclado

Texto ingresado coincidencias en expresiones regulares `/(\.)\{1{9,}\}/`

Acciones

Mostrar advertencia con mensaje falsificación R EGEX

Figura 2: Uso de expresión regular

Configuramos cualquier acción del modo simple en la parte reactiva de Teramind. Una vez que hacemos esto, puedes guardar la regla y con esto podemos generar las alertas que se buscan. Esta regla disparara la alerta de cualquier carácter con patrón repetitivo, como lo son:

uuuuuuuuuu
aaaaaaaaaa

Para que se dispare la regla se requiere que se repitan 10 veces el patron, si modificamos el número nueve podemos ajustar la cantidad de veces que debe coincidir, la coincidencia sería la siguiente:

$$n + 1$$

2. Regla 2

Esta regla se crea para los caracteres de flecha arriba o abajo, la configuración es la siguiente. Se toma el apartado de tecla especial y se selecciona la flecha arriba y flecha abajo

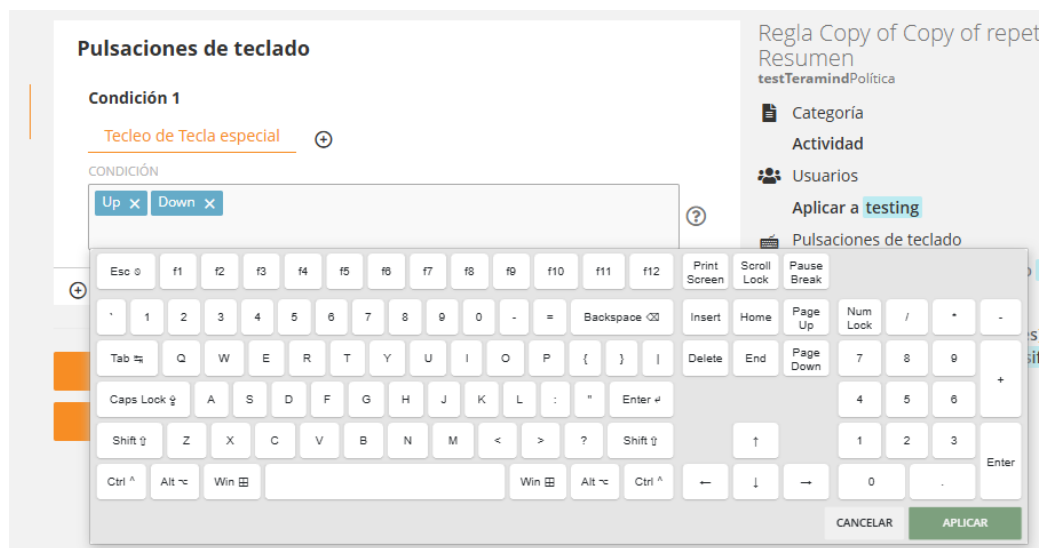


Figura 3: Caracteres especiales

En la parte de acciones se tiene que hacer la configuración del sistema en modo avanzado.

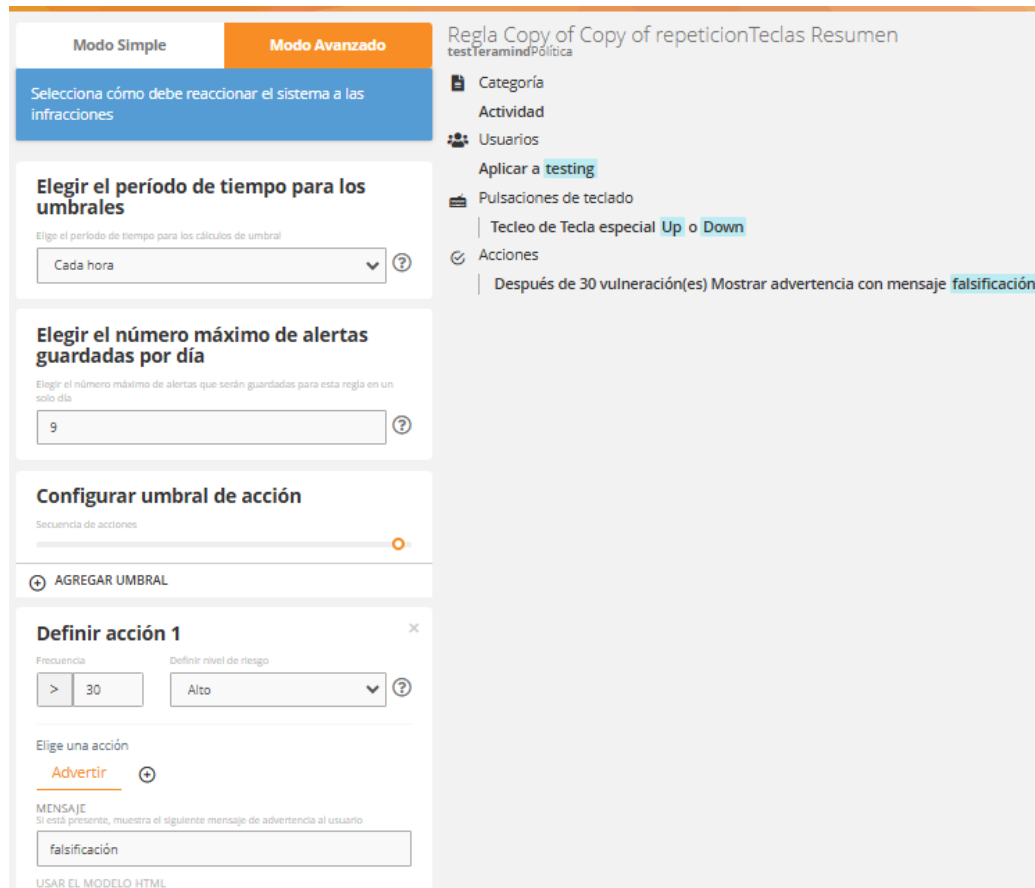


Figura 4: Configuración avanzada

Aquí podemos jugar con los requerimientos en cada caso, para este particular tomamos el umbral del tiempo en cada hora, el umbral de alertas en 9 alertas por cada hora, después de 30 veces que sea pulsada de manera repetitiva la tecla, se disparara la alarma y la acción a tomar es alertar al usuario, estos parámetros se pueden cambiar y ajustar.

3. Consideraciones adicionales

Se puede revisar la configuración del monitoreo de cada usuario para garantizar que el check de pulsación de teclado esté activo, si se han creado más perfiles, debemos verificar en qué perfil está el usuario que queremos monitorear.




	<input checked="" type="checkbox"/> DOCUMENTOS IMPRESOS	<input checked="" type="radio"/> SIEMPRE	Tamaño máximo de captura de un documento (páginas): 50,Capturar el documento actual,Eliminar documentos impresos después de (días): 0
	<input checked="" type="checkbox"/> PULSACIONES DE TECLADO	<input checked="" type="radio"/> SIEMPRE	Monitorear portapapeles
	<input checked="" type="checkbox"/> MENSAJERÍA INSTANTÁNEA	<input checked="" type="radio"/> SIEMPRE	Monitorear estas aplicaciones: Skype, Google Chat, Skype Web, Microsoft Teams,Monitorear mensajes entrantes,Monitorear mensajes salientes,Ignorar eventos mayores que (días): 0

Figura 5: Configuración de monitoreo para el usuario

Dentro de las configuraciones globales se tienen como Default el conteo máximo de alertas por días, limitado a 5 y el umbral de alertas de usuario en 120 segundos, esto quiere decir que se limita a 5 alertas por día, para un intervalo entre alerta y alerta de 2 minutos, esto se puede modificar para los parámetros que consideremos necesarios.

Este menú se encuentra en la ruta:

- Engranaje superior del lado derecho
- Configuración

■ Alertas

Configuración

ed palomino

Ubicación

Ajustes de monitoreo

Integraciones

Configuración

Valores predeterminados del agente

Actualización automática

Alertas

Seguridad

Localización

Alertas de Licencia

Resumen de Alertas Diario

UBICACIÓN DE LA PANTALLA

Centro de la pantalla

ANCHO

200

ALTURA

100

LÍMITE DE CORREOS DE ALERTA

16

UMBRAL DE ALERTAS DE USUARIO (SEGUNDOS)

120

LÍMITE DE ALERTAS DE REGISTRO (SEGUNDOS)

1

CONTEO DIARIO MÁXIMO DE ALERTAS

5

REGLA TAREAS SELECCIÓN ACCIÓN TIEMPO DE ESPERA (SEGUNDOS)

300

VISTA PREVIA

GUARDAR

Figura 6: Configuración global