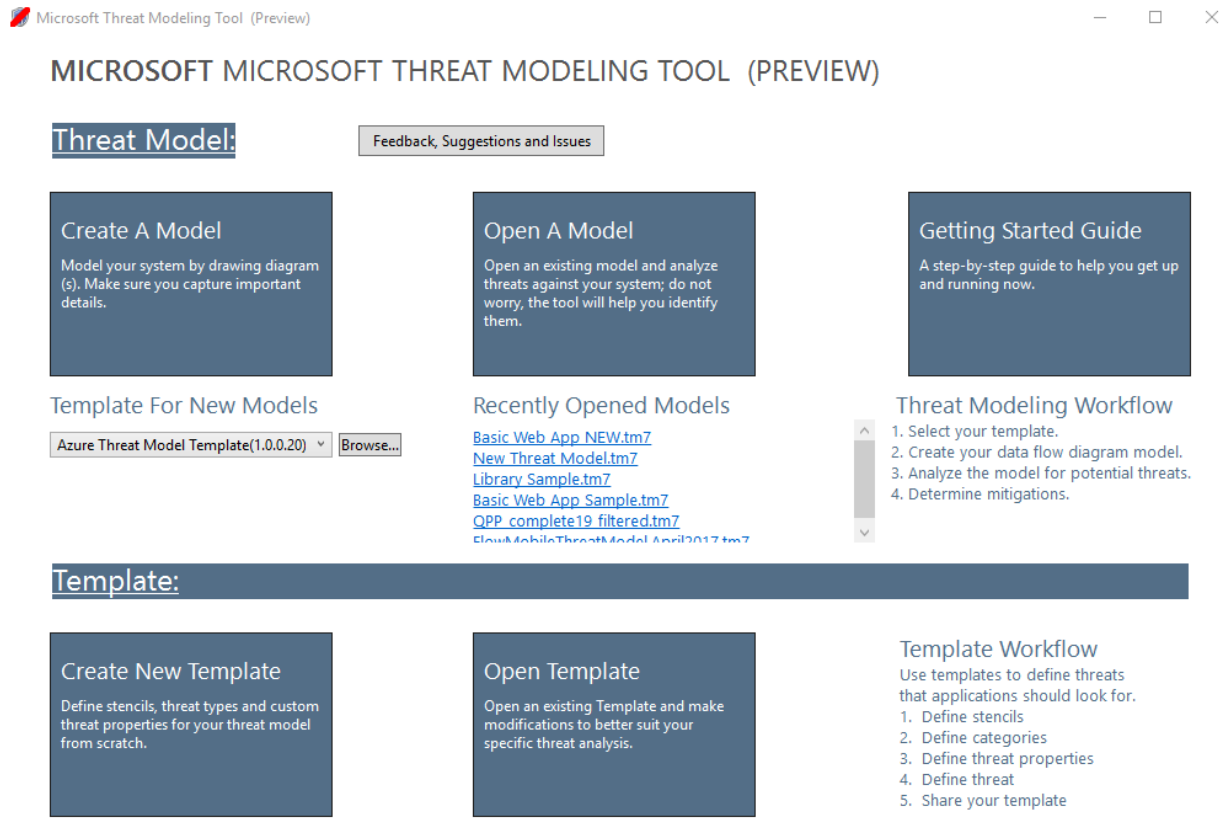
Información general de las características de Threat Modeling Tool

Artículo • 01/06/2023

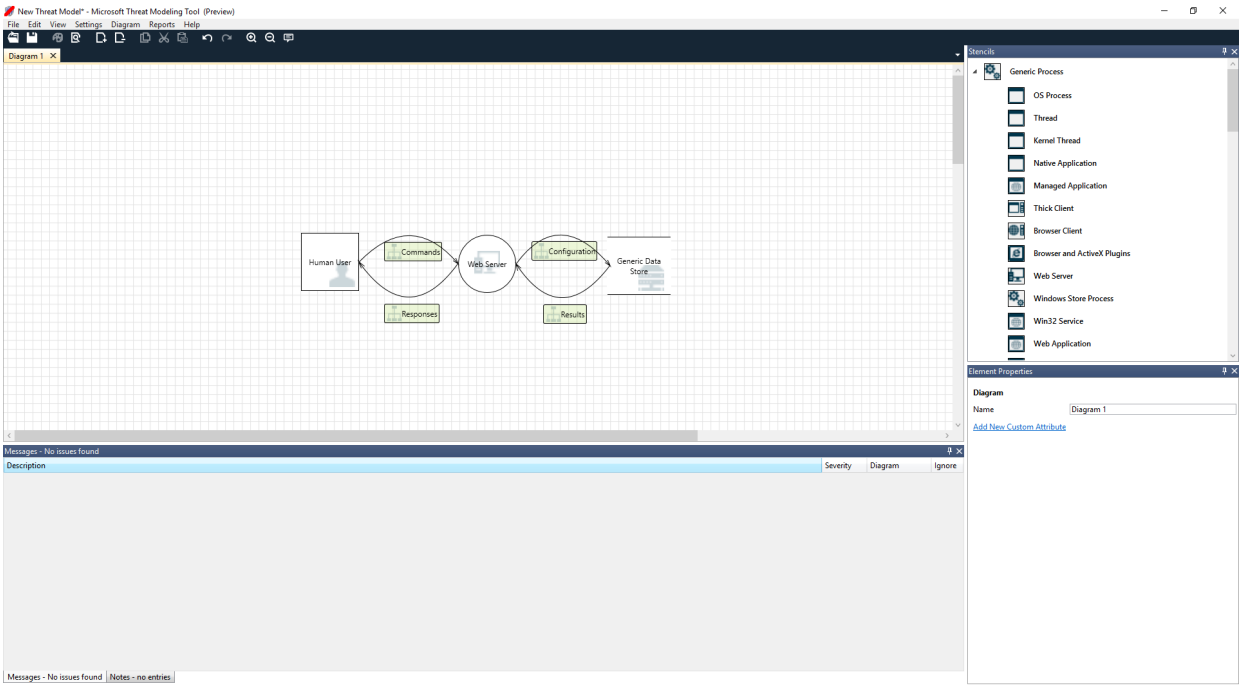
Threat Modeling Tool puede ayudarle con sus necesidades de modelado de amenazas. Para una introducción básica a la herramienta, consulte Introducción a Threat Modeling Tool.

> **Nota**
>
> Threat Modeling Tool se actualiza con frecuencia, de modo que revise esta guía a menudo para ver nuestras últimas características y mejoras.

Para abrir una página en blanco, seleccione **Crear un modelo**.



Para ver las características actualmente disponibles en la herramienta, utilice el modelo de amenazas creado por nuestro equipo en el ejemplo de Introducción.

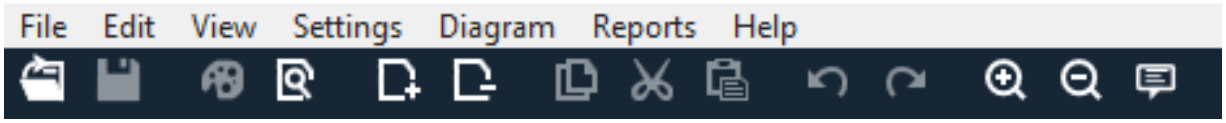


Navegación

Antes de profundizar en las características integradas, veamos los componentes principales de la herramienta.

Elementos de menú

La experiencia es similar a la de otros productos de Microsoft. Vamos a revisar los elementos del menú de nivel superior.



Etiqueta	Detalles
Archivo	• Abrir, guardar y cerrar archivos • Iniciar y cerrar sesión en cuentas de OneDrive. • Compartir vínculos (vista y edición). • Ver información de archivo. • Aplicar una plantilla nueva a modelos existentes.
Edición	Acciones de deshacer y rehacer, además de copiar, pegar y eliminar.
Vista	• Cambiar entre las vistas **Análisis** y **Diseño**. • Abrir las ventanas cerradas (por ejemplo, galerías de símbolos, propiedades de elementos y mensajes). • Restablecer el diseño a la configuración predeterminada.
Diagrama	Agregar y eliminar diagramas y navegar a través de pestañas de diagramas.

Etiqueta	Detalles
Informes	Crear informes HTML para compartir con otros usuarios.
Ayuda	Encontrar guías para ayudarle a usar la herramienta.

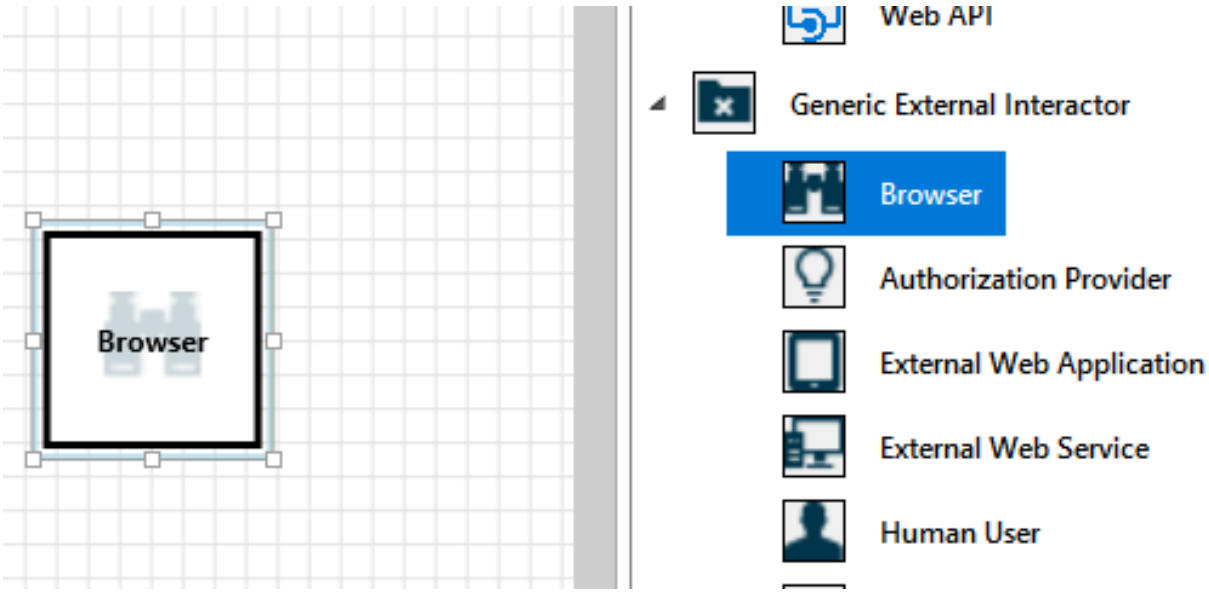
Los símbolos son accesos directos para los menús de nivel superior:

Símbolo	Detalles
Abrir	Abre un nuevo archivo.
Guardar	Guarda el archivo actual.
Diseño	Abre la vista **Diseño**, donde puede crear modelos.
Análisis	Muestra las amenazas generadas y sus propiedades.
Agregar diagrama	Agrega un nuevo diagrama (similar a las nuevas pestañas de Excel).
Eliminar diagrama	Elimina el diagrama actual.
Copiar/Cortar/Pegar	Copia, corta y pega elementos.
Deshacer/Rehacer	Deshace y rehace acciones.
Acercar/Alejar	Acerca y aleja el diagrama para obtener una mejor vista.
Comentarios	Abre el Foro de MSDN.

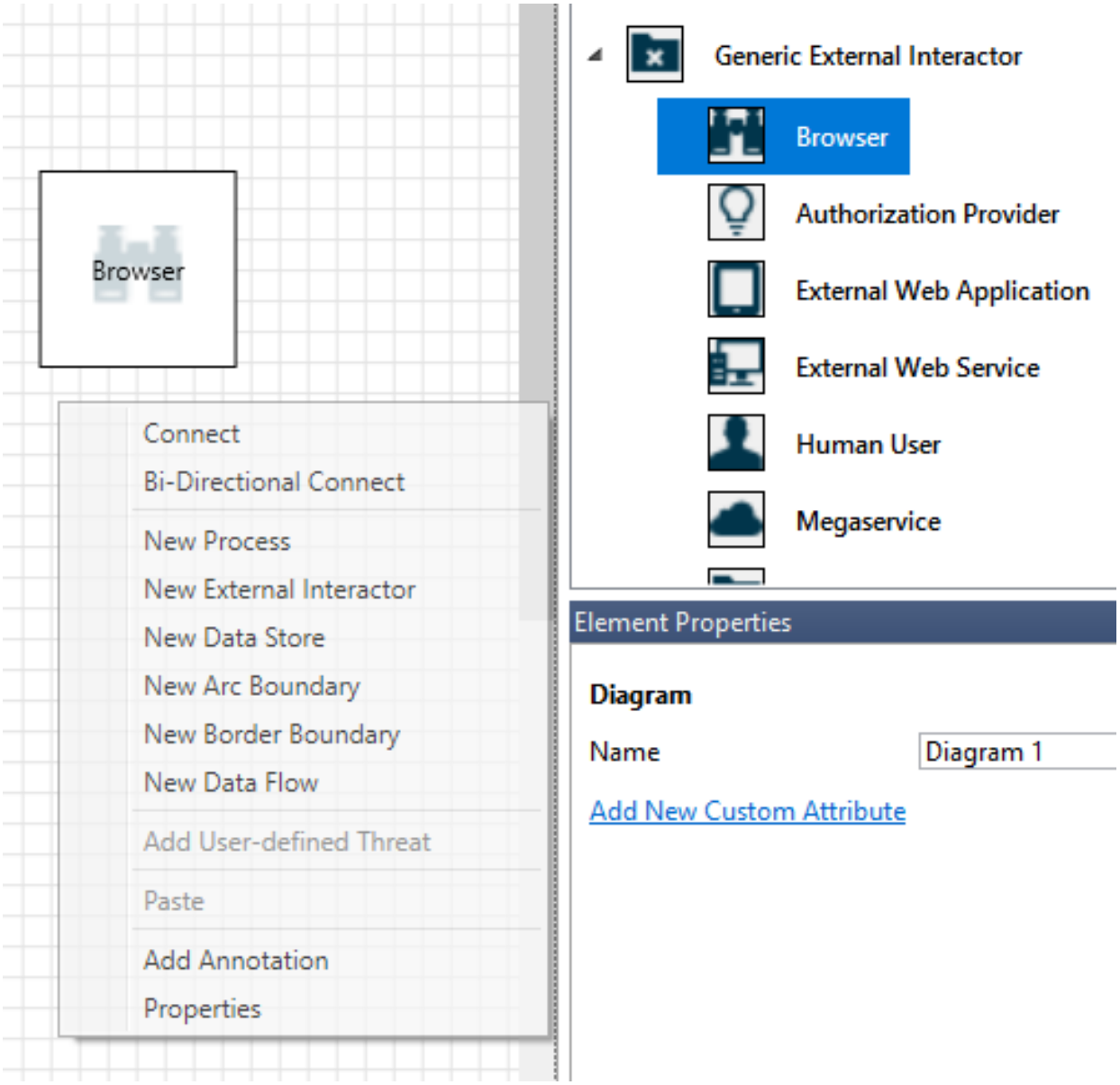
Lienzo

El lienzo es el espacio donde arrastrar y colocar elementos. Arrastrar y colocar es la manera más rápida y eficaz para crear modelos. También puede hacer clic con el botón derecho y seleccionar elementos en el menú para agregar versiones genéricas de elementos, como se muestra:

Colocar la galería de símbolos en el lienzo



Seleccionar la galería de símbolos



Galerías de símbolos

En función de la plantilla que seleccione, puede encontrar todas las galerías de símbolos disponibles para su uso. Si no encuentra los elementos adecuados, utilice otra plantilla. O bien, puede modificar una plantilla para ajustarla a sus necesidades. Por lo general, puede encontrar una combinación de categorías como las siguientes:

Nombre de la galería de símbolos	Detalles
Proceso	Aplicaciones, complementos de explorador, subprocesos, máquinas virtuales
Interactivo externo	Proveedores de autenticación, exploradores, usuarios, aplicaciones web
Almacén de datos	Caché, almacenamiento, archivos de configuración, bases de datos, registro
Flujo de datos	Binario, ALPC, HTTP, HTTPS/TLS/SSL, IOCTL, IPSec, Canalización con nombre, RPC/DCOM, SMB, UDP
Línea de confianza/Límite de borde	Redes corporativas, Internet, máquina, espacio aislado, modo Kernel/Usuario

Notas/Mensajes

Componente	Detalles
Mensajes	Lógica de herramienta interna que alerta a los usuarios cada vez que hay un error, por ejemplo, cuando no hay flujos de datos entre los elementos.
Notas	Notas manuales que los equipos de ingeniería agregan al archivo durante el proceso de diseño y revisión.

Propiedades del elemento

Las propiedades del elemento varían en función de los elementos seleccionados. A excepción de los límites de confianza, todos los demás elementos contienen tres selecciones generales:

Propiedad del elemento	Detalles
Nombre	Resulta útil para asignar nombres a los procesos, almacenes, elementos interactivos y flujos para que se reconozcan con facilidad.
Fuera de ámbito	Si se selecciona, el elemento se saca de la matriz de generación de amenazas (no se recomienda).
Motivo de elegir Fuera de ámbito	Campo de justificación para que los usuarios sepan por qué se seleccionó la opción de fuera de ámbito.

Se cambian las propiedades de cada categoría de elemento. Seleccione cada elemento para inspeccionar las opciones disponibles. O bien, puede abrir la plantilla para más información. Vamos a revisar las características.

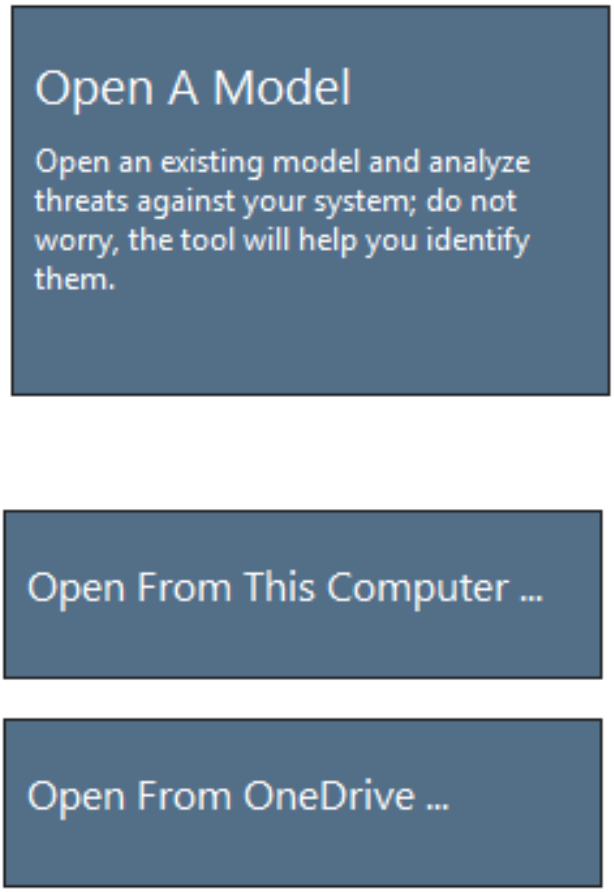
Pantalla principal

Cuando se abre la aplicación, verá la pantalla de **Bienvenida**.

Abrir un modelo

Mantenga el ratón sobre **Abrir un modelo** para mostrar dos opciones: **Abrir desde este equipo** y **Abrir desde OneDrive**. La primera opción abre la pantalla **Abrir archivo**. La segunda opción

le guiará por el proceso de inicio de sesión en OneDrive. Tras la autenticación correcta, puede seleccionar los archivos y carpetas.



Comentarios, sugerencias y problemas

Cuando se selecciona **Comentarios, sugerencias y problemas**, se abre el foro de MSDN para herramientas de SDL. Puede leer lo que dicen otros usuarios acerca de la herramienta, incluidas nuevas ideas y soluciones.

Vista de diseño

Al abrir o crear un nuevo modelo, se abre la vista **Diseño**.

Agregar elementos

Puede agregar elementos en la cuadrícula de dos maneras:

- **Arrastrar y colocar**: arrastre el elemento deseado a la cuadrícula. A continuación, utilice las propiedades del elemento para proporcionar información adicional.
- **Hacer clic con el botón derecho**: haga clic con el botón derecho en cualquier parte de la cuadrícula y seleccione elementos en el menú desplegable. Aparecerá una representación genérica del elemento seleccionado en la pantalla.

Conectar elementos

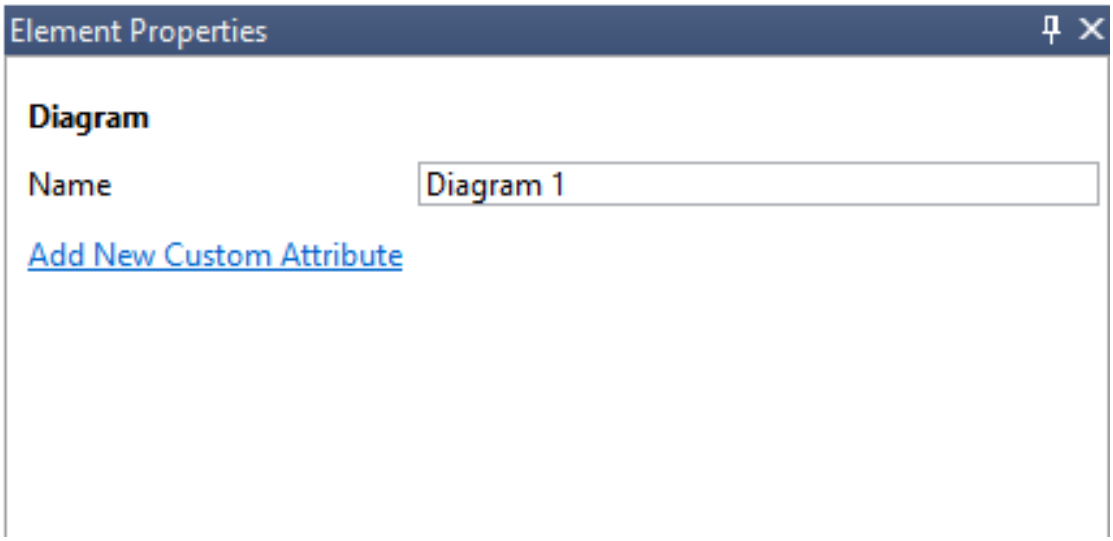
Puede conectar elementos de dos maneras:

- **Arrastrar y colocar**: arrastre el flujo de datos deseado a la cuadrícula y conecte ambos extremos a los elementos correspondientes.
- **Hacer clic + Mayús**: haga clic en el primer elemento (enviar datos) y mantenga presionada la tecla Mayús y luego seleccione el segundo elemento (recibir datos). Haga clic con el botón derecho y seleccione **Conectar**. Si usa un flujo de datos bidireccional, el orden no es tan importante.

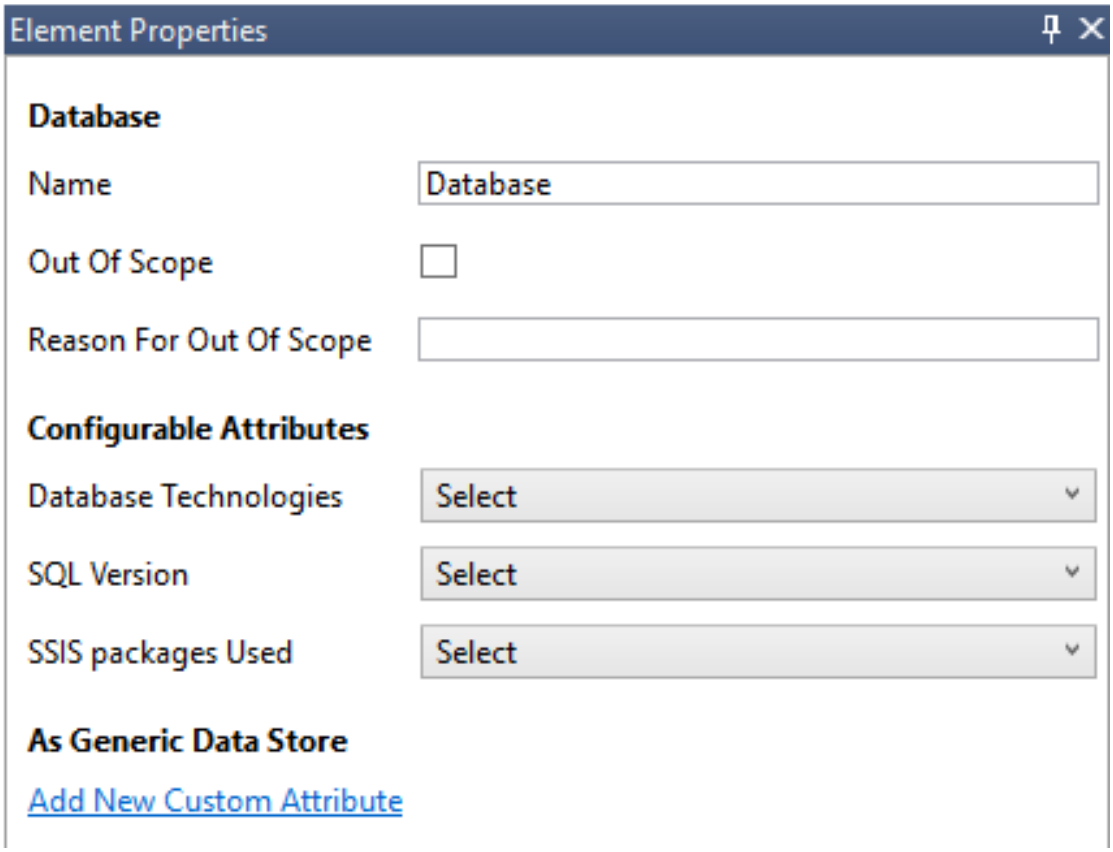
Propiedades

Para ver las propiedades que pueden modificarse en las galerías de símbolos, seleccione la galería de símbolos y la información se rellena en consecuencia. En el ejemplo siguiente se muestra la situación antes y después de arrastrar una galería de símbolos **Base de datos** al diagrama:

Antes del

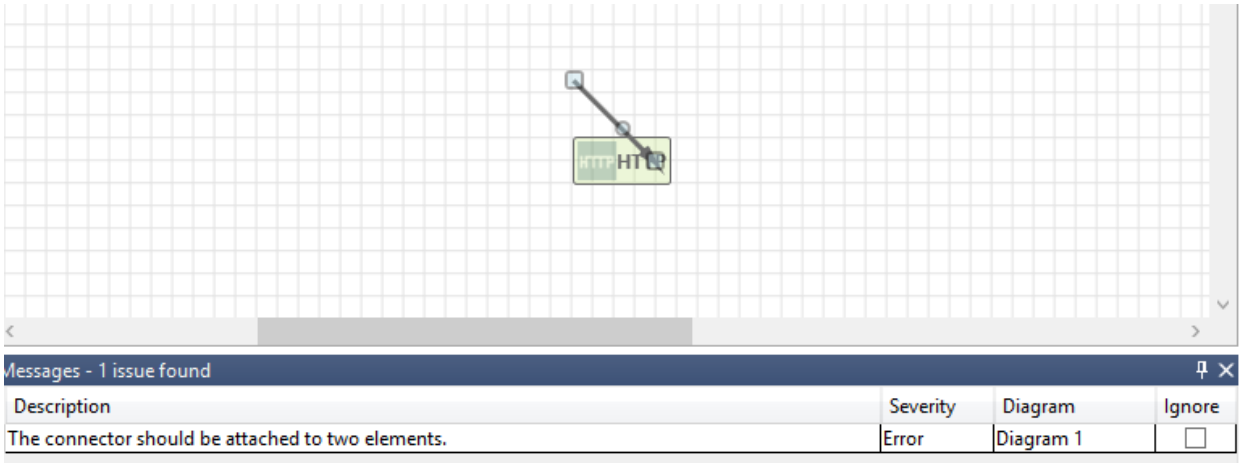


Después



error de Hadoop

Si crea un modelo de amenazas y olvida conectar los flujos de datos a los elementos, recibirá una notificación. Puede elegir omitirla o seguir las instrucciones para solucionar el problema.

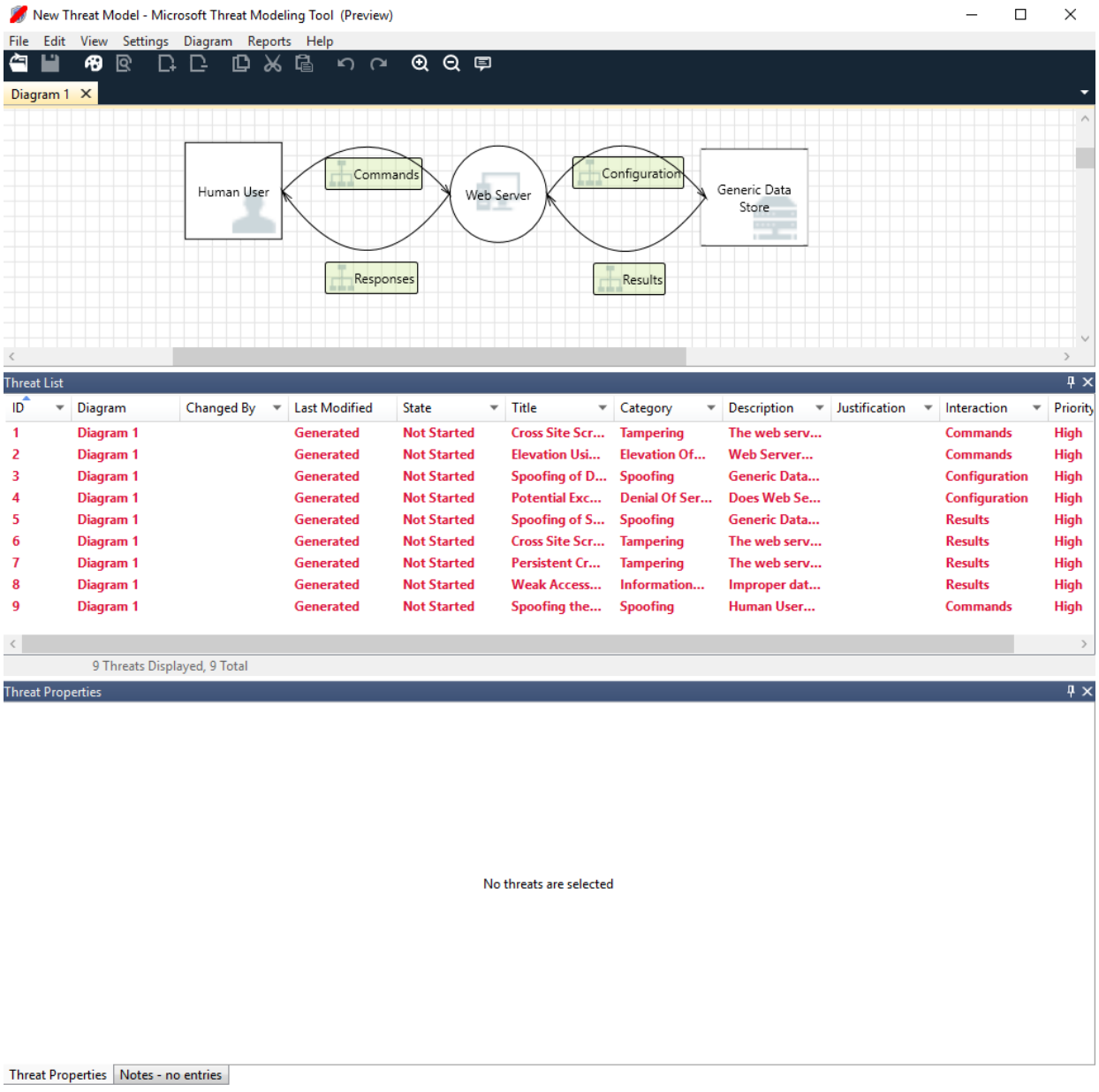


Notas

Para agregar notas al diagrama, cambie de la pestaña **Mensajes** a la pestaña **Notas**.

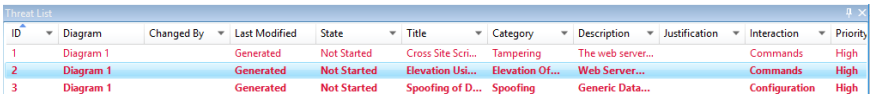
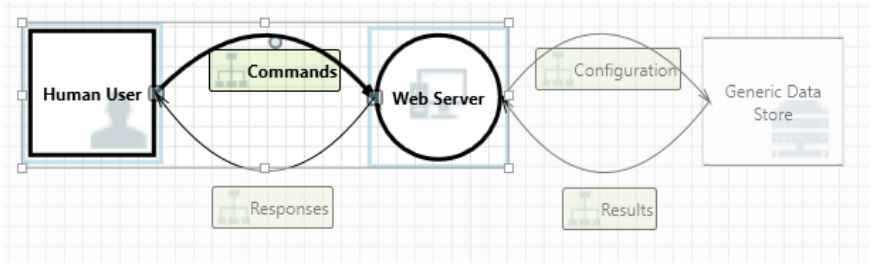
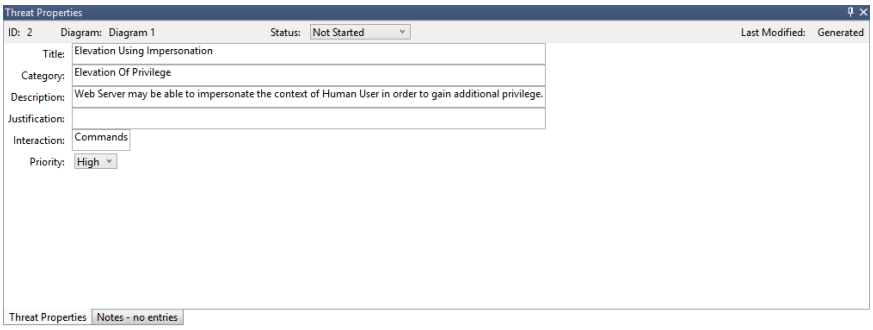
Vista de análisis

Después de crear el diagrama, seleccione el símbolo **Análisis** (Lupa) en la barra de herramientas de accesos directos para cambiar a la vista **Análisis**.



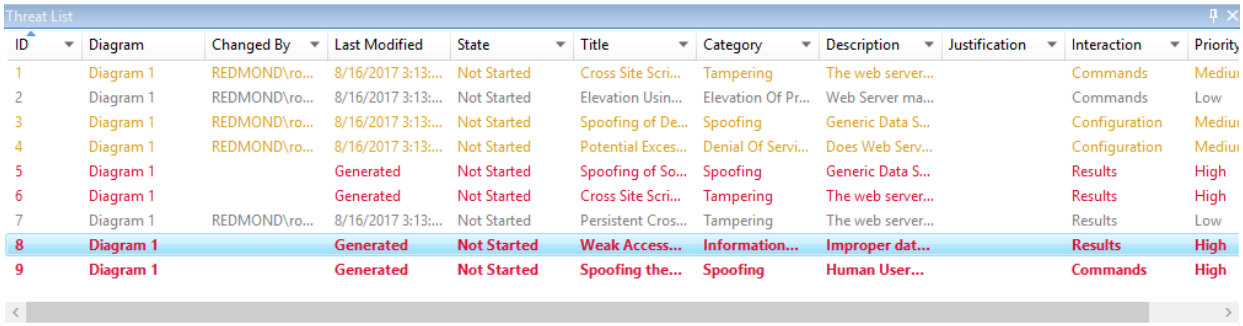
Selección de amenaza generada

Cuando se selecciona una amenaza, puede usar tres funciones distintas:

Característica	Information
Indicador de leído	La amenaza se marca como leída, lo que ayuda a realizar un seguimiento de los elementos que ha revisado. 
Foco de interacción	Se resalta la interacción en el diagrama que pertenece a una amenaza. 
Propiedades de la amenaza	Aparece información adicional sobre la amenaza en la ventana **Propiedades de la amenaza**.  (Propiedades de amenaza)

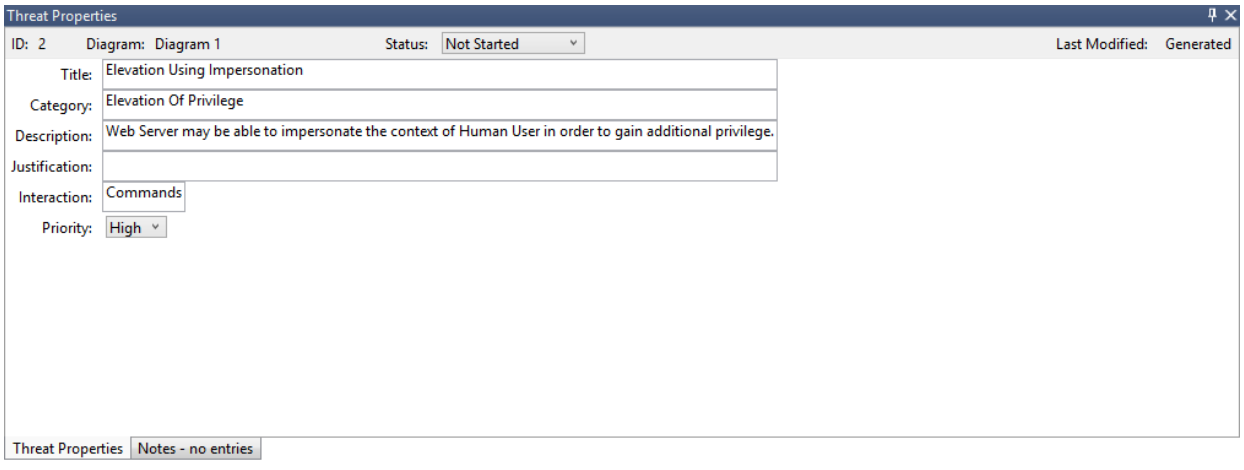
Priority change (Cambio de prioridad)

Puede cambiar el nivel de prioridad de cada amenaza generada. Colores diferentes hacen fácil identificar las amenazas de prioridad alta, media y baja.



Campos modificables de las propiedades de amenaza

Tal como se muestra en la imagen anterior, puede cambiar la información generada por la herramienta. También puede agregar información a algunos de los campos, como la justificación. Estos campos son generados por la plantilla. Si necesita más información para cada amenaza, puede realizar modificaciones.



Informes

Una vez que haya terminado de cambiar las prioridades y de actualizar el estado de cada amenaza generada, puede guardar el archivo o imprimir un informe. Vaya a **Informe**>**Crear informe completo**. Asigne nombre al informe y debería ver algo similar a la siguiente imagen:

Threat Modeling Report

Created on 7/31/2017 12:35:42 PM
Threat Model Name:
Owner:
Reviewer:
Contributors:
Description:
Assumptions:
External Dependencies:

Threat Model Summary:

Not Started	9
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	9
Total Migrated	0

Diagram: Diagram 1

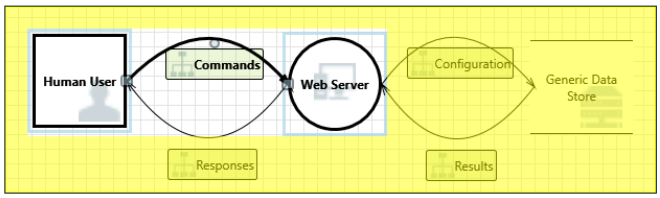
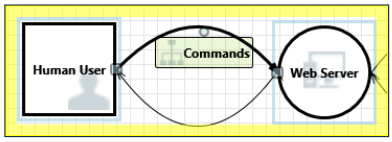


Diagram 1 Diagram Summary:

Not Started	9
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	9
Total Migrated	0

Interaction: Commands



1. Spoofing the Human User External Entity [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Human User may be spoofed by an attacker and this may lead to unauthorized access to Web Server. Consider using a standard authentication mechanism to identify the external entity.
Justification:	<no mitigation provided>
Possible Mitigation(s):	
SDL Phase:	Design

2. Cross Site Scripting [State: Not Started] [Priority: High]

Category:	Tampering
Description:	The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification:	<no mitigation provided>
Possible Mitigation(s):	
SDL Phase:	Design

Pasos siguientes

- Envíe sus preguntas, comentarios y preocupaciones a tmtextsupport@microsoft.com. **Descargue** Threat Modeling Tool para empezar.
- Para contribuir con una plantilla para la comunidad, vaya a nuestra página de GitHub .