bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INFORMANDO

Elastic SIEM

Ver en el centro de ayuda:
https://bitwarden.com/help/elastic-siem/

Elastic SIEM

Elastic es una solución que puede proporcionar opciones de búsqueda y observabilidad para monitorear su organización Bitwarden. Elastic Agent proporciona la capacidad de monitorear información de `colección`, `evento`, `grupo` y `políticas` con la integración de Elastic Bitwarden.

Configuración

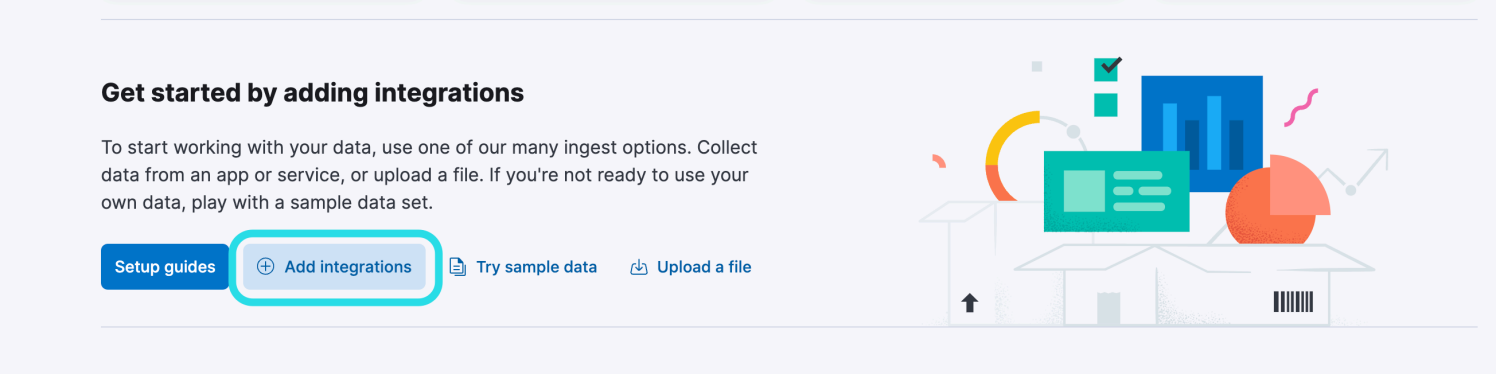
Crea una cuenta Elastic

Para comenzar, empieza por crear una cuenta Elastic. Este paso es necesario para configurar un tablero de control para monitorear los datos con el servicio alojado en la nube de Elastic (recomendado), o el servicio local.

Añadir integración de Bitwarden

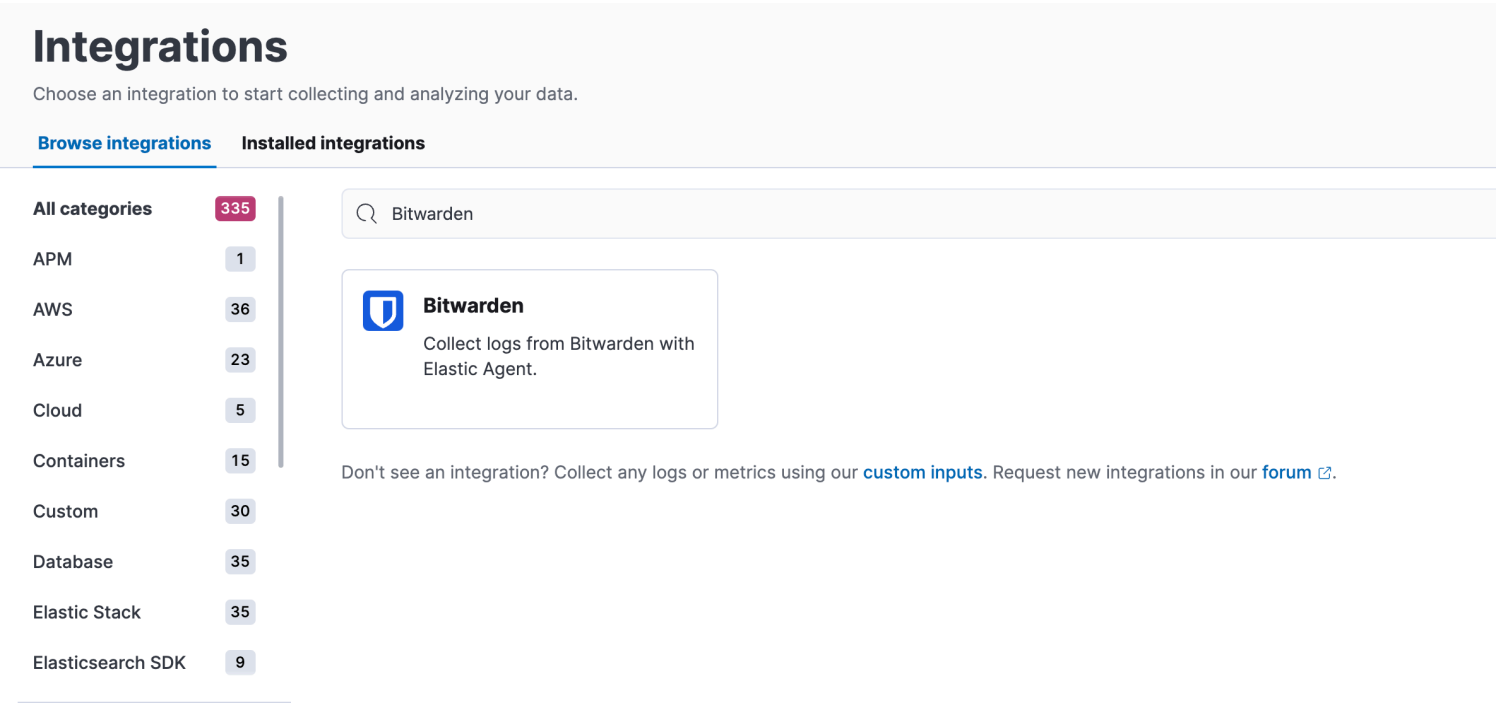
La monitorización de datos requerirá el uso de Elastic Search así como Kibana para visualizar los datos.

1. En la pantalla de inicio de Elastic, desplázate hacia abajo y localiza **Agregar Integraciones**.



Add Elastic Integration

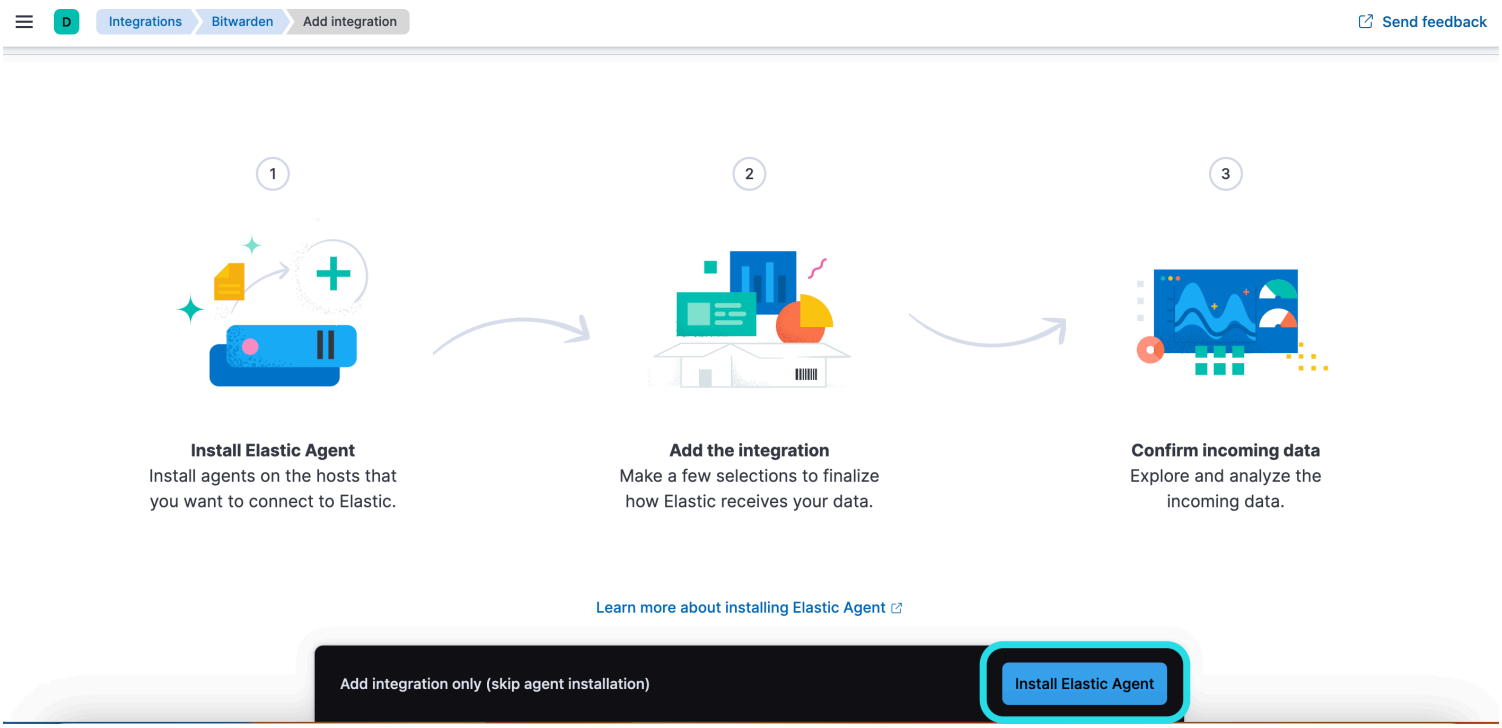
2. Una vez que estés en el catálogo de integraciones, ingresa **Bitwarden** en el campo de buscar y selecciona Bitwarden.



Bitwarden Elastic Integration

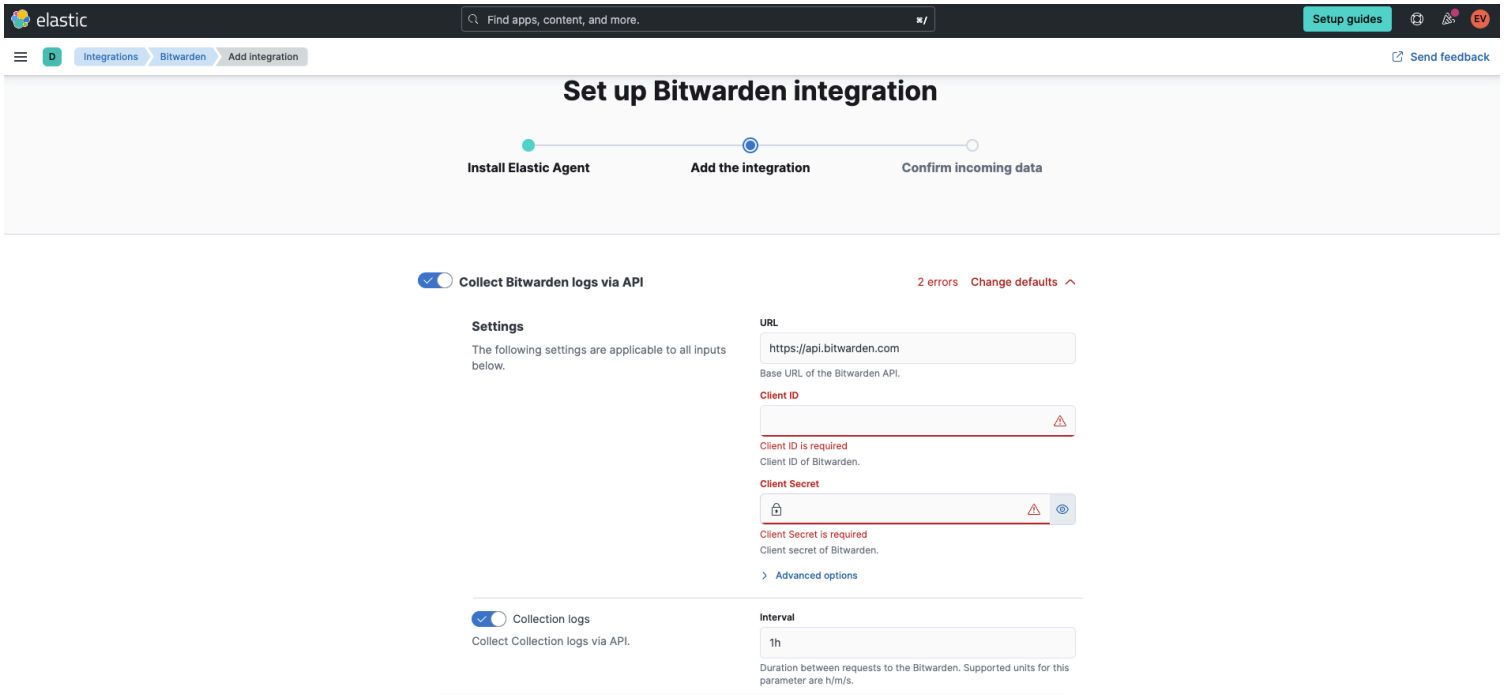
3. Seleccione el botón **Agregar Bitwarden** para instalar la integración.

4. Si esta es tu primera integración con Elastic, se te requerirá instalar el Agente Elastic. En la siguiente pantalla, seleccione **Instalar Elastic Agent** y siga las instrucciones de instalación.



Install Elastic Agent

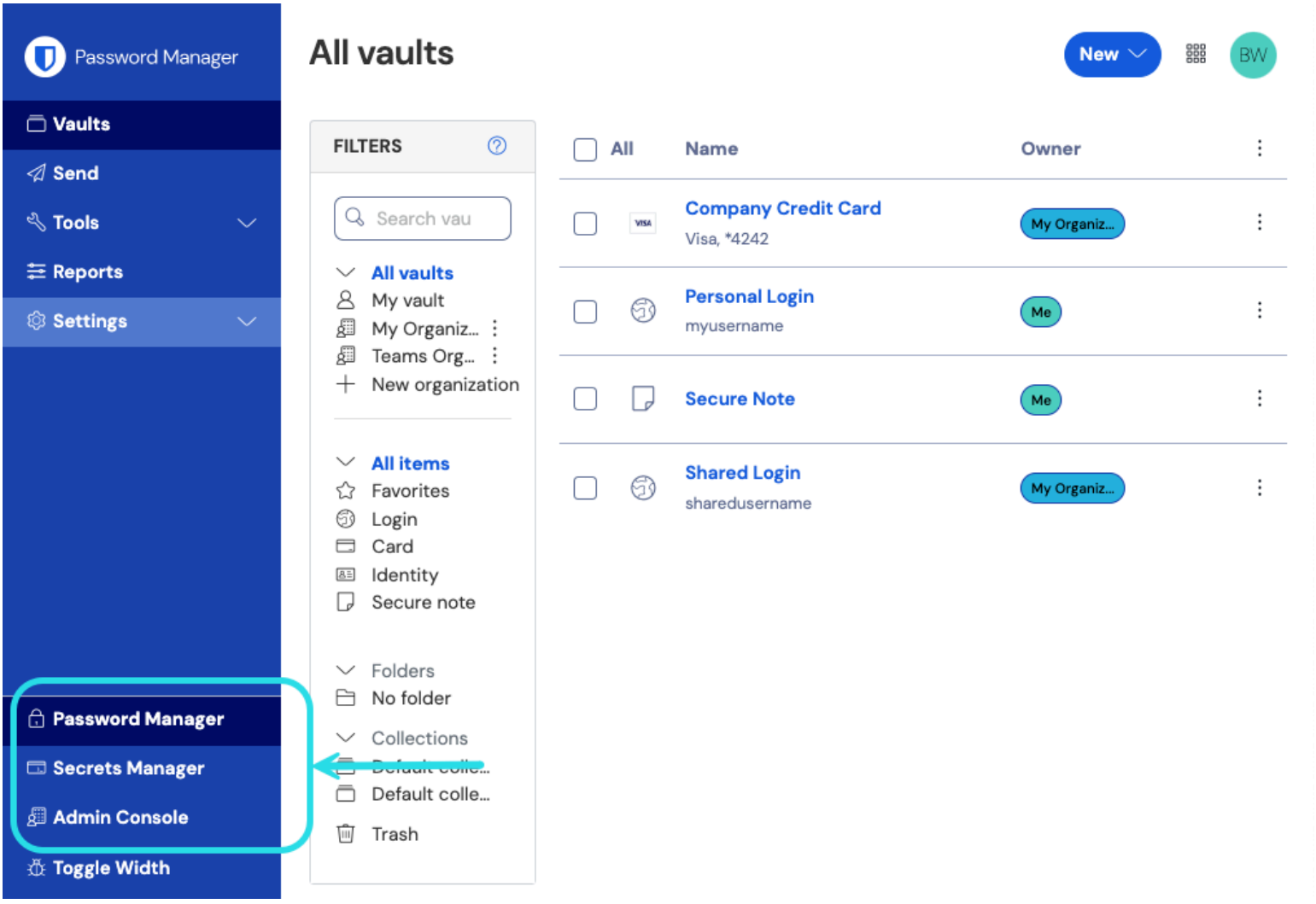
5. Para ejecutar la integración de Bitwarden, se requiere el Agente Elástico para mantener los datos de integración. Una vez que la instalación esté completa, Elastic detectará la instalación exitosa. Después de que el agente se haya configurado con éxito, seleccione **Agregar la integración**.



Elastic setup

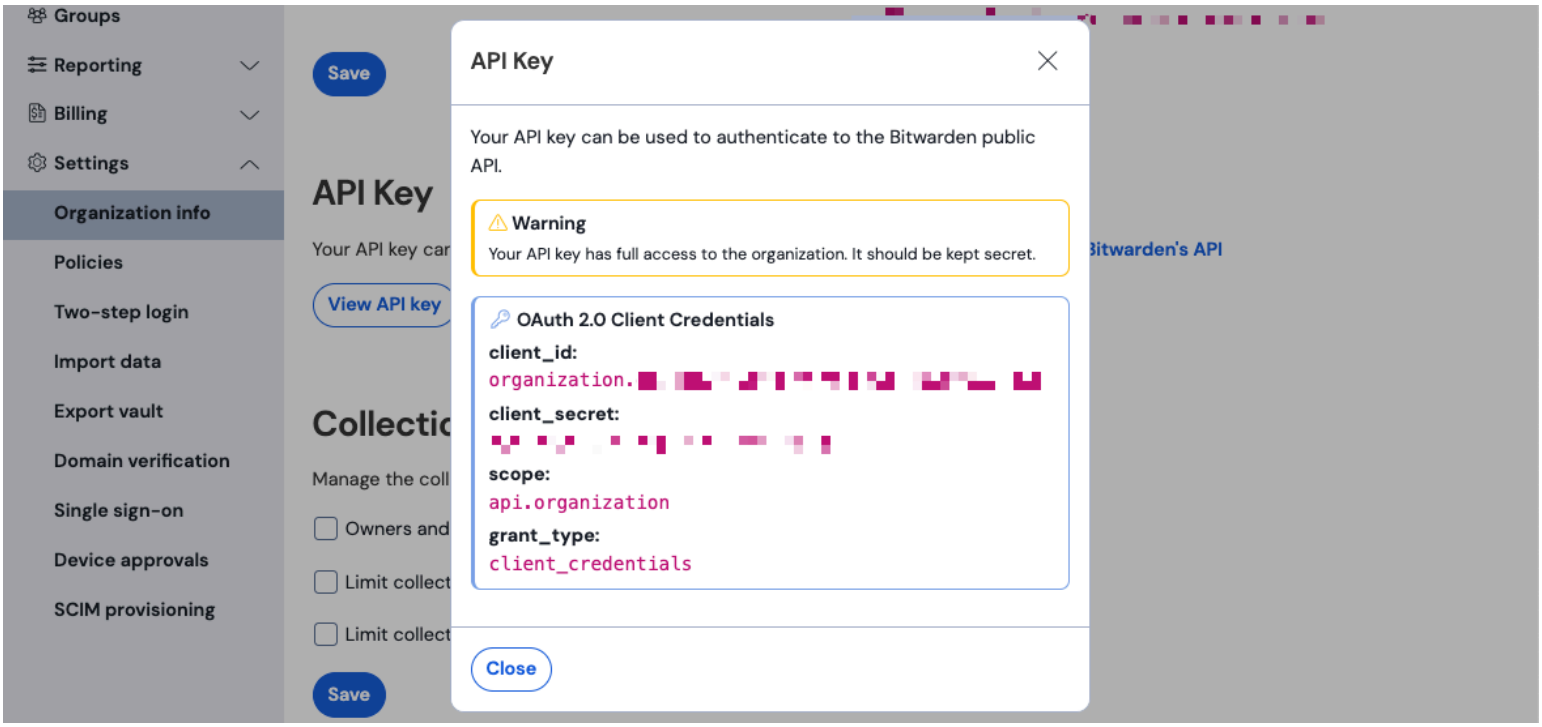
Conectar Integración a Bitwarden

Una vez que haya agregado la integración de Bitwarden, se le llevará a la pantalla de configuración para configurar la integración. Mantén esta pantalla abierta, en otra pestaña, inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador utilizando el conmutador de producto (⊞):



Selector de producto

Navegue a la pantalla de información de su **organización** → Ajustes y seleccione el botón **Ver clave API**. Se le pedirá que vuelva a ingresar su contraseña maestra para acceder a la información de su clave API.



Información de API de la organización

Ingrese la siguiente información en los campos correspondientes:

Campo Elástico	Valor
URL	Para los usuarios de la nube de Bitwarden, la URL predeterminada será `https://api.bitwarden.com`. Para los usuarios de Bitwarden autoalojado, ingrese su URL autoalojado. Asegúrate de que la URL no incluya ninguna barra inclinada hacia adelante al final de la URL "`/`"
ID de cliente	Ingrese el valor para `client_id` desde la ventana de la clave API de la organización Bitwarden.
Secreto del Cliente	Ingrese el valor para `client_secret` desde la ventana de la clave API de la organización Bitwarden.

Note

La información de la clave API de su organización es datos sensibles. No comparta estos valores en lugares no seguros.

Una vez que haya completado los campos requeridos, continúe desplazándose hacia abajo en la página para aplicar los ajustes de colección de datos deseados. Seleccione **Confirmar datos entrantes** una vez que haya terminado.

> **Note**
>
> Additional **Advanced options** are available for configuration at this point. The minimum required fields are highlighted above to add the Bitwarden integration. To access the integration at a later point to edit the setup, go to the menu and select **Integrations → Installed integrations → Bitwarden → Integration policies**.

Si todos los datos se ingresaron correctamente, Elastic confirmará los datos entrantes y proporcionará una vista previa de los datos entrantes. Seleccione **Ver activos** para monitorear sus datos.

Comienza a monitorear los datos

Una vez que la configuración esté completa, puedes comenzar a revisar los Datos de tu organización Bitwarden. Seleccione cualquiera de los paneles de Bitwarden para monitorear los datos relativos al panel. Aquí hay un breve resumen de los datos monitoreados de cada panel:

Tronco	Descripción
[Registros Bitwarden] Política	Revisar los cambios de políticas para una organización, como habilitar, deshabilitar o actualizar las políticas organizacionales.
[Registros Bitwarden] Grupo y Colección	Monitorear el evento grabado para grupos y colecciones relacionados con la organización.
[Registros Bitwarden] Evento	Monitorear los registros de eventos organizacionales. Aprende más sobre los registros de eventos aquí.

Entendiendo los tableros de control

Consultas

El monitoreo de datos elásticos utilizó el Lenguaje de Consulta de Kibana (KQL) para filtrar los datos. Para aprender más sobre consultas y búsquedas, vea la documentación de consulta Elastic.