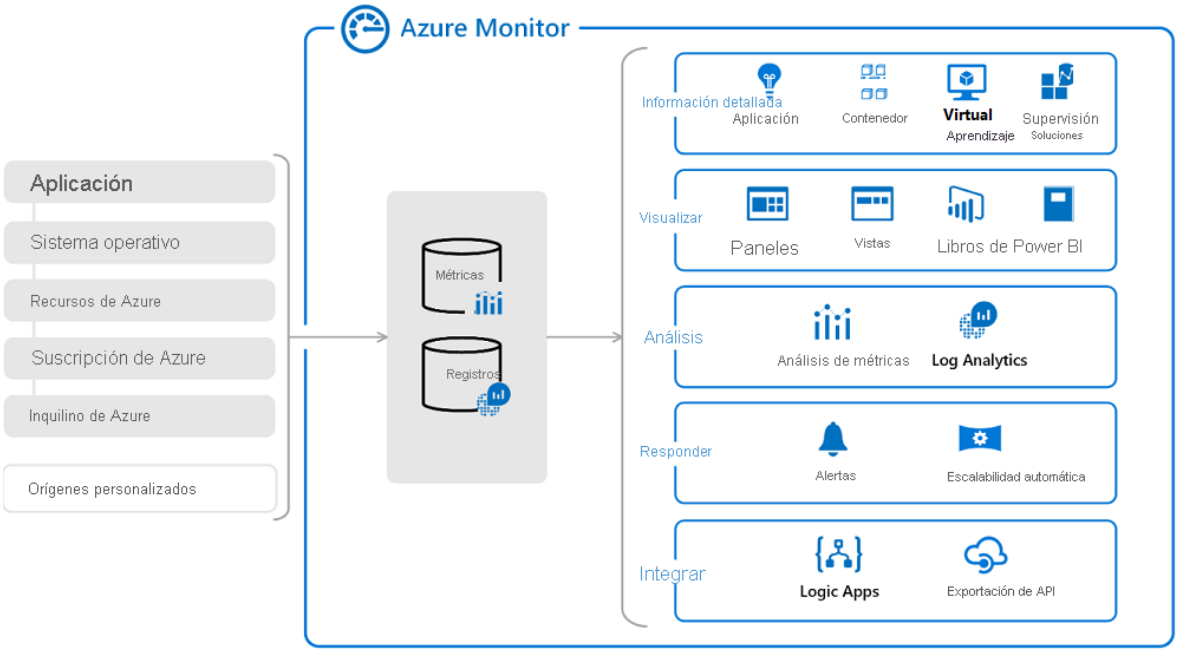
Explorar Azure Monitor

Anteriormente, en este curso se ha proporcionado información sobre Microsoft Azure Monitor. En el siguiente diagrama de alto nivel, se muestran los dos tipos de datos fundamentales que usa Azure Monitor: las métricas y los registros.



En la parte izquierda de la ilustración, se encuentran los orígenes de datos de supervisión que rellenan estos almacenes de datos. En la parte derecha se encuentran las diferentes funciones que realiza Azure Monitor con los datos recopilados, como el análisis, el envío de alertas y el streaming a sistemas externos.

Para muchos recursos de Azure, encontrará los datos que recopila Azure Monitor directamente en la **página de información general** del recurso en Azure Portal. Consulte cualquier máquina virtual (VM), por ejemplo, y verá varios gráficos con métricas de rendimiento. Seleccione cualquiera de los gráficos para abrir los datos en el **Explorador de métricas**, lo que le permite representar los valores de varias métricas a lo largo del tiempo. Puede ver los gráficos de forma interactiva o anclarlos a un panel para verlos con otras visualizaciones.

Puede analizar los datos de registro que Azure Monitor recopila mediante consultas para recuperar, consolidar y analizar rápidamente los datos recopilados. Puede crear y probar consultas mediante el análisis de registros en Azure Portal y, después, analizar directamente los datos mediante estas herramientas o guardar consultas para usarlas con visualizaciones o reglas de alertas.

En este módulo se analizará la transmisión de los datos de supervisión recopilados a soluciones externas de Administración de eventos e información de seguridad (SIEM) mediante Microsoft Defender for Cloud. Por lo general, el reenvío o la transmisión se realizan directamente desde los recursos supervisados a través Azure Event Hubs.

Exportación de datos a un SIEM

Los eventos procesados que genera Microsoft Defender for Cloud se publican en el registro de actividad de Azure, uno de los tipos de registro disponibles a mediante Azure Monitor. Azure Monitor ofrece una canalización consolidada para el enrutamiento de cualquiera de los datos supervisados en una herramienta SIEM. Esto se hace transmitiendo los datos a un centro de eventos, donde luego se pueden extraer a una herramienta de asociado.

Esta canalización usa la canalización única de Azure Monitor para acceder a los datos de supervisión desde el entorno de Azure. Esto le permite configurar fácilmente los SIEM y las herramientas de supervisión para consumir los datos. Actualmente, los datos de seguridad expuestos de Microsoft Defender for Cloud a una SIEM constan de alertas de seguridad.

Ver las alertas de seguridad en Microsoft Defender para la nube

Security Center recopila, analiza e integra automáticamente los datos de registro de los recursos de Azure, la red y las soluciones de asociados conectadas, como firewalls y soluciones de protección de puntos de conexión, para detectar amenazas reales y reducir los falsos positivos. Security Center muestra una lista de alertas de seguridad prioritarias junto con la información necesaria para investigar rápidamente el problema y las recomendaciones sobre cómo corregir un ataque.

En las secciones siguientes se describe cómo configurar los datos que se transmitirán a un centro de eventos. En los pasos se da por hecho que ya tiene Microsoft Defender for Cloud configurado en su suscripción de Azure.

Azure Event Hubs

Azure Event Hubs es una plataforma de streaming y un servicio de ingesta de eventos que puede transformar y almacenar datos mediante cualquier proveedor de análisis en tiempo real o adaptadores de almacenamiento o procesamiento por lotes. Use Event Hubs para transmitir datos de registro de Azure Monitor a una instancia de Microsoft Sentinel o a un SIEM de asociado y herramientas de supervisión.

¿Qué datos se pueden enviar a un centro de eventos?

En el entorno de Azure hay varios "niveles" de datos de supervisión, cuyo método de acceso varía ligeramente. Normalmente, estos niveles se pueden describir como:

- **Datos de supervisión de aplicaciones**: datos sobre el rendimiento y la funcionalidad del código que ha escrito y que se ejecuta en Azure. El seguimiento del rendimiento, los registros de aplicaciones y la telemetría de usuario son ejemplos de datos de supervisión de aplicaciones. Normalmente se recopilan datos de supervisión de aplicaciones de una de las maneras siguientes:
    - Mediante la instrumentación del código con un SDK como el **SDK de Application Insights**.
    - Mediante la ejecución de un agente de supervisión que escucha los registros de aplicaciones nuevos en la máquina donde se ejecuta la aplicación, como el **agente de Azure Diagnostics para Windows** o el **agente de Azure Diagnostics para Linux**.
- **Datos de supervisión del sistema operativo invitado:** datos sobre el sistema operativo en el que se ejecuta la aplicación. Ejemplos de datos de supervisión de sistema operativo invitado serían los syslog de Linux o los eventos de sistema de Windows. Para recopilar este tipo de datos, debe instalar un agente como el **agente de Azure Diagnostics para Windows** o el **agente de Azure Diagnostics para Linux**.
- **Datos de supervisión de recursos de Azure:** datos acerca del funcionamiento de un recurso de Azure. Para algunos tipos de recursos de Azure, como las máquinas virtuales, hay un sistema operativo invitado y aplicaciones que supervisan el interior de ese servicio de Azure. Para otros recursos de Azure, como los grupos de seguridad de red, los datos de supervisión de recursos son el nivel más alto de datos disponible (porque no hay ningún sistema operativo invitado ni aplicación que se ejecute en esos recursos). Estos datos se pueden recopilar con la configuración de diagnóstico de recursos.
- **Datos de supervisión de la suscripción de Azure**: datos sobre el funcionamiento y la administración de una suscripción de Azure, así como sobre el mantenimiento y el funcionamiento del propio Azure. El registro de actividad contiene la mayoría de los datos de supervisión de suscripciones, como los incidentes de estado del servicio y las auditorías de Azure Resource Manager. Puede recopilar estos datos mediante un perfil de registro.
- **Datos de supervisión del inquilino de Azure**: datos sobre el funcionamiento de los servicios de Azure en el nivel del inquilino, como Azure Active Directory. Las auditorías y los inicios de sesión de Azure Active Directory son ejemplos de datos de supervisión de inquilino. Estos datos se pueden recopilar con la configuración de diagnóstico de inquilino.

Los datos de cualquier nivel se pueden enviar a un centro de eventos, donde se pueden extraer a una herramienta. Algunos orígenes pueden configurarse para enviar datos directamente a un centro de eventos, mientras que es posible que se requiera otro proceso, como una aplicación lógica, para recuperar los datos necesarios.

Conexión a Microsoft Sentinel

Microsoft Sentinel está ahora disponible de forma general. Ahora, con Microsoft Sentinel, empresas de todo el mundo pueden mantener el ritmo del crecimiento exponencial de los datos de seguridad, mejorar los resultados de seguridad sin agregar recursos de analista y reducir los

costos operativos y de hardware. Microsoft Sentinel reúne las características avanzadas de Azure y la inteligencia artificial para permitir que los centros de operaciones de seguridad mejoren su rendimiento.

Algunas de las características de Microsoft Sentinel son las siguientes:

- **Más de 100 reglas de alertas integradas**
    - Asistente para reglas de alertas de Sentinel para crear las suyas propias.
    - Las alertas se pueden desencadenar mediante un único evento o en función de un umbral, o bien mediante la correlación de diferentes conjuntos de datos o a través de algoritmos de aprendizaje automático integrados.
- **Cuadernos de Jupyter Notebook** que usan una colección creciente de consultas de búsqueda, consultas exploratorias y bibliotecas de Python.
- **Gráfico de investigación** para visualizar y recorrer las conexiones entre entidades, como usuarios, recursos, aplicaciones o direcciones URL, y actividades relacionadas, como inicios de sesión, transferencias de datos o uso de aplicaciones, para comprender rápidamente el ámbito y el impacto de un incidente.

El repositorio de GitHub de Microsoft Sentinel ha aumentado a más de 400 consultas de detección, exploración y búsqueda, además de muestras de Azure Notebooks y bibliotecas de Python relacionadas, muestras de cuadernos de estrategias y analizadores. La mayor parte de ellas las han desarrollado los investigadores de seguridad de Microsoft basándose en su amplia experiencia de seguridad global e inteligencia sobre amenazas.

Para incorporar Microsoft Sentinel, primero debe habilitarlo y, después, conectar sus orígenes de datos. Microsoft Sentinel incluye varios conectores para soluciones de Microsoft, que están disponibles inmediatamente y proporcionan integración en tiempo real, entre los que se incluyen las soluciones de **Protección contra amenazas de Microsoft** y **orígenes de Microsoft 365**, incluido **Microsoft 365, Azure AD, Azure ATP** y **Microsoft Cloud App Security**, entre otros. Además, hay conectores integrados al amplio ecosistema de seguridad para soluciones que no son de Microsoft. También puede usar el formato de evento común, Syslog o las API de REST para conectar los orígenes de datos con Azure Sentinel.

Después de conectar los orígenes de datos, puede elegir de una galería de paneles creados de forma experta que exponen información basada en los datos. Estos paneles se pueden personalizar fácilmente en función de sus necesidades.