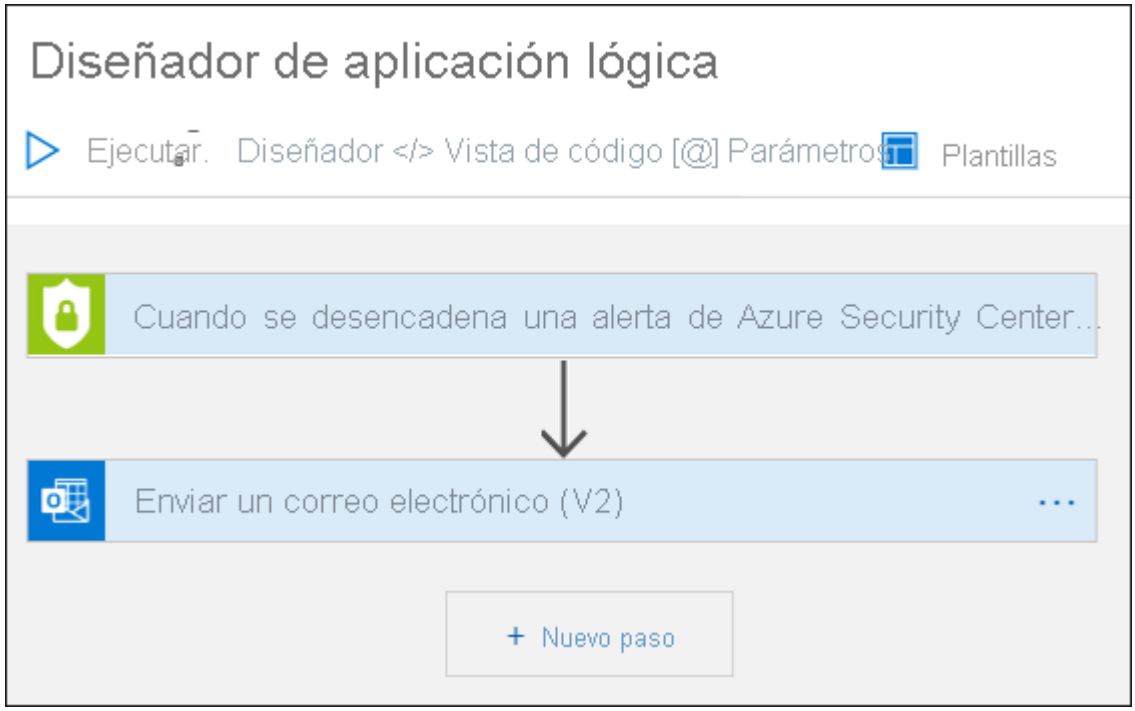
Configuración de cuadernos de estrategias

Automatización y orquestación de seguridad permite automatizar las tareas comunes y simplificar la orquestación de seguridad con cuadernos de estrategias que se integran con los servicios de Azure, así como con las herramientas existentes. Construida sobre la base de Azure Logic Apps, la solución de automatización y orquestación de Azure Sentinel proporciona una arquitectura muy extensible que permite la automatización escalable a medida que emergen nuevas tecnologías y amenazas. Para crear cuadernos de estrategias con Azure Logic Apps, puede elegir de una galería creciente de cuadernos de estrategias integrados. Estos incluyen más de 200 conectores para servicios, como Azure Functions. Los conectores permiten aplicar cualquier lógica personalizada en el código, ServiceNow, Jira, Zendesk, solicitudes HTTP, Microsoft Teams, Slack, Windows Defender ATP y Cloud App Security.

Por ejemplo, si usa el sistema de vales de ServiceNow, puede usar las herramientas proporcionadas para usar Azure Logic Apps para automatizar los flujos de trabajo y abrir un vale en ServiceNow cada vez que se detecta un evento determinado.



Las herramientas de investigación profunda de Microsoft Sentinel están actualmente en **versión preliminar** y le ayudan a conocer el ámbito de una posible amenaza de seguridad y a encontrar la causa principal. Puede elegir una entidad en el gráfico interactivo para hacer preguntas interesantes sobre ella y explorar en profundidad esa entidad y sus conexiones para llegar a la causa principal de la amenaza.

Un incidente puede incluir varias alertas, a modo de agregado de todas las pruebas relevantes en una investigación en concreto. Los incidentes se crearán en función de las reglas de análisis que haya creado en la página Analytics (Análisis). Las propiedades relacionadas con alertas, como la gravedad y el estado, se establecen en el nivel de incidente. Después de indicar a Microsoft

Configuración de cuadernos de estrategias

Sentinel qué tipos de amenazas está buscando y cómo detectarlas, puede supervisar las amenazas que se detecten investigando cada incidente.

Uso del gráfico de investigación para un análisis en profundidad

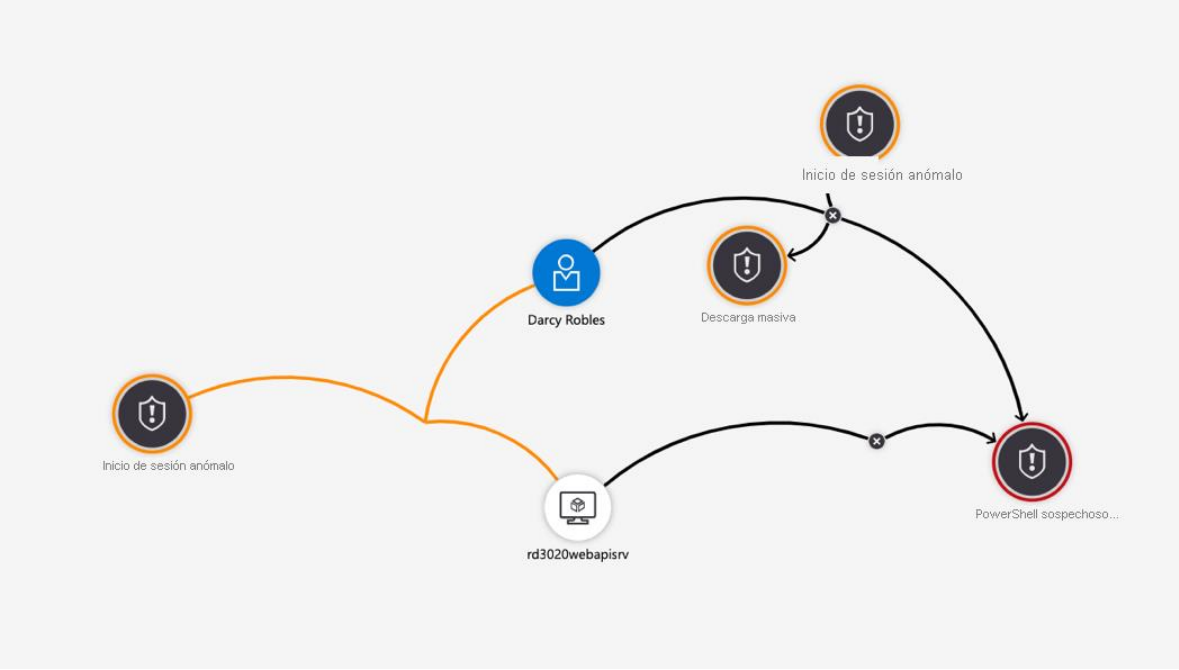
El gráfico de investigación permite a los analistas formular las preguntas adecuadas para cada investigación. El gráfico de investigación le ayuda a comprender el ámbito y a identificar la causa principal de una posible amenaza de seguridad al correlacionar los datos pertinentes con las entidades implicadas. Puede profundizar e investigar cualquier entidad presentada en el gráfico seleccionándola y eligiendo entre las diferentes opciones de expansión.

El gráfico de investigación le proporciona:

- **Contexto visual de datos sin procesar**: El gráfico visual y dinámico, muestra las relaciones de entidad extraídas automáticamente de los datos sin procesar. Esto le permite ver fácilmente las conexiones entre distintos orígenes de datos.
- **Detección del ámbito completo de la investigación**: Amplíe el ámbito de la investigación mediante consultas de exploración integradas para exponer el ámbito completo de una infracción de seguridad.
- **Pasos de investigación integrados**: Use opciones de exploración predefinidas para asegurarse de que está formulando las preguntas adecuadas en caso de una amenaza.

Para usar el gráfico de investigación:

Seleccione un incidente y, a continuación, seleccione **Investigar**. Esto le llevará al gráfico de investigación. El gráfico proporciona un mapa ilustrativo de las entidades conectadas directamente a la alerta y de cada recurso conectado más allá.



Configuración de cuadernos de estrategias

Solo podrá investigar el incidente si ha usado los campos de asignación de entidades al configurar la regla de análisis. El gráfico de investigación requiere que el incidente original incluya entidades.

Búsqueda

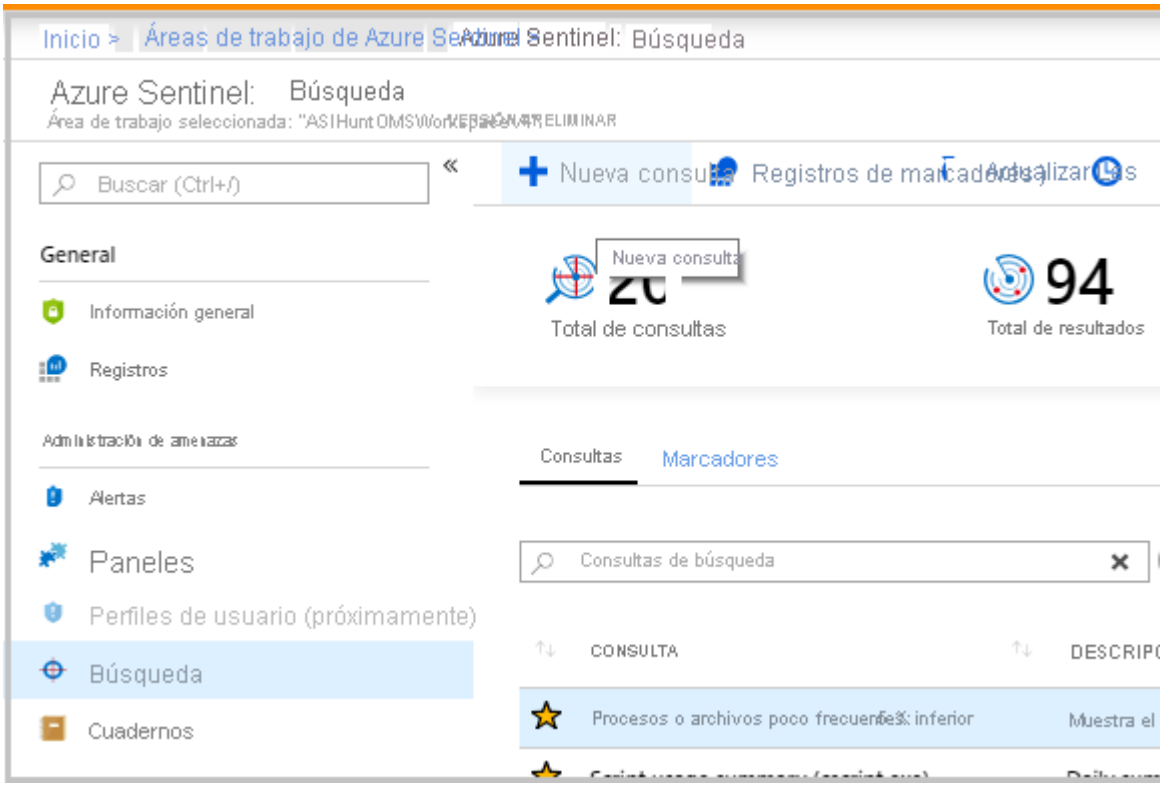
Use las eficaces herramientas de búsqueda y consulta de Microsoft Sentinel, basadas en el **marco MITRE**, que le permiten buscar de forma proactiva amenazas de seguridad en todos los orígenes de datos de la organización, antes de que se desencadene una alerta. Una vez que ha descubierto qué consulta de búsqueda proporciona las conclusiones más valiosas sobre posibles ataques, también puede crear reglas de detección personalizadas basadas en la consulta y exponer esas conclusiones como alertas para los respondedores a los incidentes de seguridad. Durante la búsqueda puede crear marcadores de los eventos interesantes, para así poder volver a ellos más tarde, compartirlos con otros usuarios y agruparlos con otros eventos correlacionados para crear un incidente de investigación convincente.

Por ejemplo, una consulta integrada proporciona datos sobre los procesos menos habituales que se ejecutan en la infraestructura. Es posible que no quiera una alerta cada vez que se ejecuten.

Con la búsqueda de Microsoft Sentinel, puede aprovechar las siguientes funcionalidades:

- **Consultas integradas**: para empezar, una página de inicio proporciona ejemplos de consultas cargados previamente diseñados para que empiece a trabajar y se familiarice con las tablas y el lenguaje de consulta. Estas consultas de búsqueda integradas están desarrolladas por investigadores de seguridad de Microsoft, y lo hacen de forma continua, agregando nuevas consultas y ajustando las consultas existentes para que sean un punto de entrada para buscar nuevas detecciones y averiguar dónde empezar a buscar comienzos de nuevos ataques.
- **Lenguaje de consulta eficaz con IntelliSense**: se basa en un lenguaje de consulta que proporciona la flexibilidad necesaria para llevar la búsqueda al siguiente nivel.
- **Creación de sus propios marcadores**: durante el proceso de búsqueda, puede encontrar coincidencias o resultados, paneles o actividades que parezcan inusuales o sospechosos. A fin de marcar esos elementos de forma que se pueda volver a ellos en el futuro, utilice la funcionalidad de marcador. Los marcadores permiten guardar los elementos para usarlos más adelante para crear un incidente de investigación.
- **Uso de cuadernos para automatizar la investigación**: los cuadernos son como cuadernos de estrategias paso a paso que puede crear para seguir los pasos de una investigación y búsqueda. Los cuadernos aglutinan todos los pasos de búsqueda en un cuaderno de estrategias reutilizable que se puede compartir con otras personas de la organización.
- **Consultar los datos almacenados**: los datos se encuentran en tablas y se pueden consultar. Así, por ejemplo, se puede consultar la creación de procesos, los eventos DNS y otros muchos tipos de eventos.
- **Vínculos a la comunidad**: aproveche la capacidad de una gran comunidad para buscar consultas y orígenes de datos adicionales.

Configuración de cuadernos de estrategias



Comunidad

La comunidad Microsoft Azure Sentinel es un recurso muy eficaz para la detección y la automatización de amenazas. Nuestros analistas de seguridad de Microsoft crean y agregan constantemente nuevos libros, cuadernos de estrategias, consultas de búsqueda, etc. y los publican en la comunidad para que los pueda usar en su entorno. Puede descargar contenido de ejemplo del repositorio de GitHub privado de la comunidad para crear libros personalizados, consultas de búsqueda, cuadernos y cuadernos de estrategias Microsoft Azure Sentinel.