**Introducción**

Este módulo se centra en la configuración y administración de las soluciones de automatización y supervisión de seguridad mediante Azure Monitor y Microsoft Sentinel, lo que permite a las organizaciones identificar y responder proactivamente a incidentes de seguridad en sus entornos de nube.

**Escenario**

Imagine que es un especialista en ciberseguridad responsable de proteger los recursos en la nube de la organización. Debe implementar una supervisión de seguridad eficaz para detectar y responder a eventos de seguridad y automatizar las respuestas a incidentes de forma rápida y precisa.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Supervise los eventos de seguridad con eficacia mediante Azure Monitor para obtener visibilidad sobre su entorno de nube.
* Configure conectores de datos en Microsoft Sentinel para recopilar y agregar datos de seguridad de varios orígenes.
* Cree y personalice reglas de análisis en Microsoft Sentinel para detectar anomalías y amenazas de seguridad específicas.
* Evalúe alertas e incidentes en Microsoft Sentinel para valorar la gravedad y el impacto de los eventos de seguridad.
* Configure la automatización en Microsoft Sentinel para orquestar acciones de respuesta a incidentes y simplificar los flujos de trabajo de seguridad.

**Objetivos**

El módulo tiene como objetivo equipar a los participantes con los conocimientos y aptitudes necesarios para configurar y administrar soluciones de automatización y supervisión de seguridad de forma eficaz. Los participantes aprenderán a supervisar eventos de seguridad, configurar conectores de datos, crear reglas de análisis personalizadas, evaluar alertas e incidentes, y automatizar acciones de respuesta, lo que mejorará la capacidad de su organización para detectar y responder a amenazas de seguridad de forma oportuna y eficaz.

**Supervisar eventos de seguridad con Azure Monitor**

El registro de actividad de Azure Monitor es un registro de plataforma de Azure que proporciona información sobre los eventos del nivel de suscripción. El registro de actividad incluye información como, por ejemplo, cuándo se modificó un recurso o cuándo se inició una máquina virtual. Puede ver el registro de actividad en Azure Portal o recuperar entradas con PowerShell y la CLI de Azure. En este artículo, se proporciona información sobre cómo ver el registro de actividad y enviarlo a diferentes destinos.

Para obtener mas funcionalidades, debe crear una configuración de diagnóstico para enviar el registro de actividad a una o varias de estas ubicaciones por los siguientes motivos:

* Enviar a los registros de Azure Monitor para aumentar la complejidad de las consultas y las alertas, así como la duración de la retención, hasta dos años.
* Enviar a Azure Event Hubs para reenviarlo fuera de Azure.
* Enviar a Azure Storage para obtener un archivado a largo plazo y más barato.
* Las entradas del registro de actividad son generadas por el sistema y no se pueden cambiar ni eliminar.
* Las entradas del registro de actividad representan cambios en el plano de control, como los reinicios de máquinas virtuales. Cualquier entrada no relacionada debe escribirse en los registros de recursos de Azure.

**Período de retención**

Los eventos del registro de actividad se conservan en Azure durante 90 días y después se eliminan. No se aplican cargos por las entradas durante este tiempo, independientemente del volumen. Para obtener más funcionalidades, como un mayor tiempo de retención, cree una configuración de diagnóstico y enrute las entradas a otra ubicación en función de sus necesidades. Consulte los criterios de la sección anterior.

**Visualización del registro de actividad**

Puede acceder al registro de actividad desde la mayoría de los menús de Azure Portal. El menú en el que lo abra determinará el filtro inicial. Si lo abre desde el menú Supervisión, el único filtro estará en la suscripción. Si lo abre desde el menú de un recurso, el filtro se establecerá en ese recurso. Siempre puede cambiar el filtro para ver todas las demás entradas. Seleccione Agregar filtro para agregar más propiedades al filtro.

**Descarga del registro de actividad**

Seleccione **Descargar como archivo .csv** para descargar los eventos en la vista actual.

**Visualización del historial de cambios**

En el caso de algunos eventos, puede ver el historial de cambios, en el que se muestran los cambios que se han producido durante la hora del evento. Seleccione un evento en el registro de actividad que quiera examinar más profundamente. Seleccione la pestaña Historial de cambios para ver los cambios en el recurso hasta 30 minutos antes y después del tiempo de la operación.

Si hay cambios asociados con el evento, verá una lista de cambios que puede seleccionar. Al seleccionar un cambio, se abre la página **Historial de cambios**. En esta página, se muestran los cambios en el recurso. En el ejemplo siguiente, puede ver que la máquina virtual ha cambiado los tamaños.

**Otros métodos para recuperar eventos del registro de actividad**

También puede acceder a los eventos del registro de actividad mediante los métodos siguientes:

* Use el cmdlet Get-AzLog para recuperar el registro de actividad desde PowerShell. Vea Ejemplos de PowerShell de Azure Monitor.
* Use az monitor activity-log para recuperar el registro de actividad desde la CLI. Consulte los ejemplos de CLI de Azure Monitor.
* Use la API REST de Azure Monitor para recuperar el registro de actividad desde un cliente REST.

**Envío al área de trabajo de Log Analytics**

Envíe el registro de actividad a un área de trabajo de Log Analytics para habilitar la característica Registros de Azure Monitor, donde podrá hacer lo siguiente:

* Correlacionar los datos del registro de actividad con otros datos de supervisión recopilados por Azure Monitor.
* Consolidar las entradas de registro de varias suscripciones e inquilinos de Azure en una ubicación para su análisis conjunto.
* Usar las consultas de registro para realizar un análisis complejo y obtener información detallada sobre las entradas del registro de actividad.
* Usar las alertas de registro con entradas de actividad para una lógica de alertas más compleja.
* Almacenar las entradas del registro de actividad más allá del período de retención del registro de actividad.
* No hay cargos por ingesta o retención de datos para los datos del registro de actividad almacenados en un área de trabajo de Log Analytics.
* El período de retención predeterminado en el análisis de registros es de 90 días.

Seleccione Exportar registros de actividad para enviar el registro de actividad a un área de trabajo de Log Analytics. Puede enviar el registro de actividad desde cualquier suscripción única hasta un máximo de cinco áreas de trabajo.

Los datos del registro de actividad de un área de trabajo de Log Analytics se almacenan en una tabla denominada AzureActivity que se puede recuperar con una consulta de registro en Log Analytics. La estructura de esta tabla varía en función de la categoría de la entrada de registro.

*En algunos escenarios, es posible que los valores de los campos de AzureActivity tengan mayúsculas y minúsculas diferentes de los valores equivalentes. Tenga cuidado al consultar datos en AzureActivity con el uso de operadores que no distinguen mayúsculas de minúsculas para comparaciones de cadenas o use una función escalar para forzar un campo a un uso uniforme de mayúsculas y minúsculas antes de cualquier comparación. Por ejemplo, use la función tolower() en un campo para forzar que siempre esté en minúsculas o el operador =~ al realizar una comparación de cadenas.*

**Envío a Azure Storage**

Envíe el registro de actividad a una cuenta de Azure Storage si quiere conservar los datos de registro durante más de 90 días para la auditoría, el análisis estático o hacer una copia de seguridad. Si tiene que conservar los eventos durante 90 días o menos, no necesita configurar el archivado en una cuenta de almacenamiento. Los eventos del registro de actividad se conservan en la plataforma de Azure durante 90 días.

Cuando envíe el registro de actividad a Azure, se creará un contenedor de almacenamiento en la cuenta de almacenamiento en cuanto se produzca un evento.

Cada blob PT1H.json contiene un objeto JSON con eventos de los archivos de registro recibidos durante la hora especificada en la dirección URL del blob. Durante la hora actual, los eventos se anexan al archivo PT1H.json a medida que se reciben, independientemente de cuándo se generaron. El valor del minuto de la dirección URL m=00 siempre es 00, ya que los blobs se crean cada hora.

**Configuración de conectores de datos en Microsoft Sentinel**

Después de integrar Microsoft Sentinel en su área de trabajo, utilice conectores de datos para empezar a introducir sus datos en Microsoft Sentinel. Microsoft Sentinel viene con muchos conectores listos para usar para los servicios de Microsoft, que se integran en tiempo real. Por ejemplo, el conector Microsoft 365 Defender es un conector de servicio a servicio que integra datos de Office 365, Microsoft Entra ID, Microsoft Defender for Identity y Microsoft Defender for Cloud Apps.

Los conectores incorporados permiten la conexión con el ecosistema de seguridad más amplio para productos ajenos a Microsoft. Por ejemplo, utilice Syslog, Common Event Format (CEF) o REST APIs para conectar sus orígenes de datos con Microsoft Sentinel.

La página Conectores de datos de Microsoft Sentinel muestra la lista completa de conectores y su estado para su área de trabajo. Próximamente, esta página solo mostrará la lista de conectores de datos en uso.

**Nota**

Para agregar más conectores de datos, instale la solución asociada al conector de datos desde el **Centro de contenido**.

**Habilitación de un conector de datos**

En la página Conectores de datos, seleccione el conector activo o personalizado que desea conectar y, a continuación, seleccione Abrir página del conector. Si no ve el conector de datos que desea, instale la solución asociada a él desde el Centro de contenido.

Una vez que cumpla todos los requisitos previos enumerados en la pestaña Instrucciones, la página del conector describe cómo ingerir los datos en Microsoft Sentinel. Los datos pueden tardar algún tiempo en empezar a llegar.

Después de conectarse, verá un resumen de los datos en el gráfico Datos recibidos, y el estado de conectividad de los tipos de datos.

**Integración de la API REST para conectores de datos**

Muchas tecnologías de seguridad proporcionan un conjunto de API para recuperar archivos de registro, y algunos orígenes de datos pueden usar esas API para conectarse a Microsoft Sentinel.

Los conectores de datos que usan API se integran desde el lado del proveedor o se integran mediante Azure Functions, como se describe en las secciones siguientes.

**Integración de la API de REST en el lado del proveedor**

Una integración de la API creada por el proveedor se conecta con los orígenes de datos del proveedor e inserta los datos en las tablas de registro personalizadas de Microsoft Sentinel mediante la API de recopilador de datos de Azure Monitor.

Para más información sobre la integración de la API de REST, consulte la documentación del proveedor y Conexión del origen de datos a la API de REST de Microsoft Sentinel para ingerir los datos.

**Integración de la API de REST mediante Azure Functions**

Las integraciones que usan Azure Functions para conectarse con una API de proveedor dan formato primero a los datos y, a continuación, los envían a las tablas de registro personalizadas de Microsoft Sentinel mediante la API de recopilador de datos de Azure Monitor.

**Integración basada en agentes para conectores de datos**

Microsoft Sentinel puede usar el protocolo Syslog para conectar un agente a cualquier origen de datos que pueda realizar el streaming de registros en tiempo real. Por ejemplo, la mayoría de los orígenes de datos locales se conectan a través de la integración basada en agente.

En las secciones siguientes se describen los distintos tipos de conectores de datos basados en agente de Microsoft Sentinel. Siga los pasos descritos en cada página del conector de datos de Microsoft Sentinel para configurar las conexiones mediante mecanismos basados en agente.

**syslog**

Puede transmitir eventos desde dispositivos compatibles con Syslog basados en Linux a Microsoft Sentinel mediante el Agente de Azure Monitor (AMA). Dependiendo del tipo de dispositivo, el agente se instala directamente en el dispositivo o en un reenviador de registros basado en Linux. El agente de Azure Monitor recibe eventos del demonio de Syslog a través de UDP. El demonio de Syslog reenvía los eventos al agente internamente, comunicándose a través de UDS (sockets de dominio UNIX). A continuación, el agente de Azure Monitor transmite estos eventos al área de trabajo de Microsoft Sentinel.

Este es un flujo sencillo que muestra cómo Microsoft Sentinel transmite los datos de Syslog.

1. El demonio de Syslog integrado del dispositivo recopila los eventos locales de los tipos especificados y los reenvía localmente al agente.
2. El agente transmite los eventos al área de trabajo de Log Analytics.
3. Después de una configuración correcta, los datos aparecen en la tabla Syslog de Log Analytics.

**Formato de evento común (CEF)**

Los formatos de registro varían, pero muchos orígenes admiten el formato basado en CEF. El agente de Microsoft Sentinel, que es realmente el agente de Log Analytics, convierte los registros con formato CEF en un formato que Log Analytics puede ingerir.

En el caso de los orígenes de datos que emiten datos en CEF, configure el agente de Syslog y, a continuación, configure el flujo de datos CEF. Después de una configuración correcta, los datos aparecen en la tabla **CommonSecurityLog**.

**Registros personalizados**

Para algunos orígenes de datos, puede recopilar registros como archivos en equipos Windows o Linux mediante el agente de recopilación de registros personalizado de Log Analytics.

Siga los pasos descritos en cada página del conector de datos de Microsoft Sentinel para conectarse mediante el agente de recopilación de registros personalizados de Log Analytics. Después de una configuración correcta, los datos aparecen en tablas personalizadas.

**Integración entre servicios para conectores de datos**

Microsoft Sentinel usa la base de Azure para proporcionar compatibilidad integrada de servicio a servicio de serie con los servicios de Microsoft y Amazon Web Services.

**Implemente conectores de datos como parte de una solución**

Las soluciones de Microsoft Sentinel proporcionan paquetes de contenido de seguridad, incluidos conectores de datos, libros, reglas de análisis, cuadernos de estrategias, etc. Al implementar una solución con un conector de datos, se obtiene el conector de datos junto con el contenido relacionado en la misma implementación.

**Soporte técnico de los conectores de datos**

Tanto Microsoft como otras organizaciones crean conectores de datos de Microsoft Sentinel. Cada conector de datos tiene uno de los siguientes tipos de soporte técnico:

| **Tipo de soporte técnico** | **Descripción** |
| --- | --- |
| Admitido por Microsoft | Se aplica a los conectores de datos para orígenes de datos en los que Microsoft sea el proveedor de datos y el autor. Algunos conectores de datos creados por Microsoft para orígenes de datos que no son de Microsoft.  Microsoft admite y mantiene los conectores de datos en esta categoría de acuerdo con Planes de soporte técnico de Microsoft Azure.  Los asociados o los conectores de datos de soporte técnico de la comunidad creados por cualquier entidad distinta de Microsoft. |
| Asociado admitido | Se aplica a los conectores de datos creados por entidades distintas de Microsoft.  La empresa asociada proporciona soporte técnico o mantenimiento para estos conectores de datos. La empresa asociada puede ser un fabricante de software independiente, un proveedor de servicios administrados, un integrador de sistemas o cualquier organización cuya información de contacto se proporcione en la página de Microsoft Sentinel para ese conector de datos.  Para cualquier incidencia con un conector de datos compatible con un asociado, póngase en contacto con el contacto de soporte técnico del conector de datos especificado. |
| Comunidad admitida | Se aplica a los conectores de datos creados por Microsoft o desarrolladores asociados que no incluyen contactos para el soporte técnico y el mantenimiento de los conectores de datos en la página del conector de datos especificada de Microsoft Sentinel. |

**Búsqueda del contacto de soporte técnico para una conector de datos**

1. En la página Conectores de datos de Microsoft Sentinel, seleccione el conector correspondiente.
2. Para acceder al soporte técnico y el mantenimiento del conector, use el vínculo de contacto de soporte técnico en el campo Admitido por en el panel lateral del conector.

**Creación y personalización de reglas de análisis en Microsoft Sentinel**

Después de conectar los orígenes de datos a Microsoft Sentinel, cree reglas de análisis personalizadas que le ayuden a detectar las amenazas y los comportamientos anómalos de su entorno.

Las reglas de análisis buscan eventos o conjuntos de eventos específicos en el entorno, le avisan cuando se alcanzan determinados umbrales de eventos o condiciones, generan incidentes para que el SOC evalúe e investigue, y responden a las amenazas con procesos de seguimiento y corrección automatizados.

**Creación de una regla de análisis personalizada con una consulta programada**

En el menú de navegación de Microsoft Sentinel, seleccione Análisis.

En la barra de acciones de la parte superior, seleccione + Crear y elija Regla de consulta programada. Así se abre el Asistente para reglas de Analytics.

**Asistente para reglas de análisis: pestaña General**

* Proporcione un Nombre único y una Descripción.
* En el campo Tactics and techniques (Táctica y técnicas), puede elegir cualquiera de las categorías de ataques por las que se clasifica la regla. Se basan en las tácticas y técnicas del marco de MITRE ATT&CK.
* Los incidentes creados a partir de alertas detectadas por reglas asignadas a tácticas y técnicas de MITRE ATT&CK heredan automáticamente la asignación de la regla.
* Establezca la Gravedad de la alerta según sea necesario.
* Cuando cree la regla, el valor predeterminado del campo Status (Estado) es Enabled (Habilitado), lo que significa que se ejecutará inmediatamente después de que termine de crearla. Si no desea ejecutarla de inmediato, seleccione Disabled (Deshabilitado) para agregar la regla a la pestaña Active rules (Reglas activas), desde donde podrá habilitarla cuando sea necesario.

**Definición de la lógica de consulta de regla y configuración de los valores**

En la pestaña Establecer la lógica de la regla, puede escribir una consulta directamente en el campo Consulta de la regla, o bien crearla en Log Analytics y, después, copiarla y pegarla aquí.

* Las consultas se escriben en el lenguaje de consulta de Kusto (KQL).
* En el ejemplo que se muestra en esta captura de pantalla se consulta la tabla SecurityEvent para mostrar un tipo de eventos de inicio de sesión de Windows con errores.

**Enriquecimiento de alertas**

* Use la sección de configuración de **asignación de entidades** para asignar parámetros de los resultados de las consultas a entidades reconocidas por Microsoft Sentinel. Las entidades enriquecen la salida de las reglas (alertas e incidentes) con datos esenciales que actúan como bloques de creación de cualquier proceso de investigación y de las acciones de corrección posteriores. También son los criterios por los que puede agrupar las alertas en incidentes en la pestaña **Configuración de los incidentes**.
* Use la sección configuración de **Detalles personalizados** para extraer elementos de datos de eventos de la consulta y mostrarlos en las alertas generadas por esta regla, lo que le proporciona visibilidad inmediata del contenido del evento en sus alertas e incidentes.
* Use la sección de configuración de **Detalles de alertas** para invalidar los valores predeterminados de las propiedades de la alerta con detalles de los resultados de la consulta subyacente. Los detalles de la alerta le permiten mostrar, por ejemplo, la dirección IP o el nombre de cuenta de un atacante en el título de la propia alerta, por lo que aparecerá en la cola de incidentes. Esto ofrece una imagen mucho más completa y clara del panorama de las amenazas.

**Nota**

**El límite de tamaño de una alerta completa es de 64 KB**.

* Las alertas que crezcan más de 64 KB se truncarán. A medida que se identifican las entidades, se agregan a la alerta una por una hasta que el tamaño de la alerta alcanza los 64 KB y las entidades restantes se descartan de la alerta.
* Los demás enriquecimientos de alertas también contribuyen al tamaño de la alerta.
* Para reducir el tamaño de la alerta, use el operador project-away de la consulta para quitar los campos innecesarios. (Considere también el operador del proyecto si solo necesitase conservar algunos campos).

**Programación de consultas y umbral de alertas**

En la sección Query scheduling (Programación de consultas), establezca los siguientes parámetros:

* Establezca la opción **Ejecutar consulta cada** para controlar la frecuencia de ejecución de la consulta (puede establecer frecuencias de 5 minutos o de una vez cada 14 días).
* Establezca **Buscar datos del último** para determinar el periodo de los datos que cubre la consulta (por ejemplo, puede consultar los 10 últimos minutos de datos o las 6 últimas horas de datos). El máximo es de 14 días.
* Para la nueva configuración de **Comenzar a ejecutar** (en versión preliminar):
  + Déjelo establecido en Automáticamente para continuar con el comportamiento original: la regla se ejecutará por primera vez inmediatamente después de haberse creado y, después de eso, en el intervalo establecido en la configuración **Ejecutar consulta cada**.
  + Cambie el modificador a **En un momento específico** si quiere determinar cuándo se ejecuta la regla por primera vez, en lugar de que se ejecute inmediatamente. A continuación, elija la fecha con el selector de calendario y especifique la hora en el formato del ejemplo que se muestra.

Las ejecuciones futuras de la regla se producirán en el intervalo especificado después de la primera ejecución.

**Nota**

La línea de texto de la opción **Iniciar ejecución** (con el icono de información a la izquierda) resume la programación de consultas actual y la configuración de búsqueda.

**Intervalos de consulta y período de retrospectiva**

Estos dos valores son independientes entre sí, hasta cierto punto. Puede ejecutar una consulta a un intervalo corto que abarque un periodo mayor que el intervalo (teniendo en efecto consultas que se solapan), pero no puede ejecutar una consulta a un intervalo que supere el periodo de cobertura, ya que, de lo contrario tendrá lagunas en la cobertura general de la consulta.

**Retraso de la ingesta**

Para tener en cuenta la latencia que puede producirse entre la generación de un evento en el origen y su ingesta en Microsoft Sentinel, y para garantizar una cobertura completa sin duplicación de datos, Microsoft Sentinel ejecuta reglas de análisis programadas con un retraso de cinco minutos desde su hora programada.

Use la sección Umbral de alerta para definir el nivel de confidencialidad de la regla. Por ejemplo, en Generar alerta cuando el número de resultados de consulta, seleccione Es mayor que y escriba el número 1000 si desea que la regla genere una alerta solo si la consulta genera más de 1000 resultados cada vez que se ejecuta. Este es un campo obligatorio, por lo que si no desea establecer un umbral (es decir, si desea que su alerta registre todos los eventos), escriba 0 en el campo numérico.

**Configuración de la creación de incidentes**

En la pestaña Configuración de incidentes, puede elegir si Microsoft Sentinel convierte las alertas en incidentes sobre los que se pueden realizar acciones y cómo lo hace. Si esta pestaña no se modifica, Microsoft Sentinel creará un solo incidente independiente a partir de todas y cada una de las alertas. Puede elegir que no se creen incidentes o agrupar varias alertas en un solo incidente. Para ello, solo debe cambiar el valor de esta pestaña.

Configuración de los incidentes

En la sección Configuración de los incidentes, el valor predeterminado de Crear incidentes a partir de las alertas desencadenadas por esta regla de análisis es Habilitado, lo que significa que Microsoft Sentinel creará un solo incidente independiente para cada una de las alertas que desencadene la regla.

* Si no desea que esta regla provoque la aparición de incidentes (por ejemplo, si esta regla es solo para recopilar información para su posterior análisis), seleccione Disabled (Deshabilitado).
* Si desea que se cree un solo incidente a partir de un grupo de alertas, en lugar de uno para cada alerta, consulte la sección siguiente.

**Agrupación de alertas**

En la sección Alert grouping (Agrupación de alertas), si desea que se genere un solo incidente a partir de un grupo de hasta 150 alertas similares o recurrentes (consulte la nota), en Group related alerts, triggered by this analytics rule, into incidents (Agrupar en incidentes alertas relacionadas desencadenadas por esta regla de análisis) seleccione Enabled (Habilitado) y establezca los siguientes parámetros.

* Limite el grupo a las alertas creadas en el período de tiempo seleccionado: Determine el período de tiempo en el que se agruparán las alertas similares o periódicas. Todas las alertas correspondientes que se encuentren dentro de este periodo de tiempo generarán colectivamente un incidente o un conjunto de incidentes (en función de la configuración de agrupación que encontrará a continuación). Las alertas que aparezcan fuera de este periodo de tiempo generarán un incidente, o conjunto de incidentes, independientes.
* Agrupe las alertas desencadenadas por esta regla de análisis en un único incidente por: elija el motivo por el que se agruparán las alertas:

| **Opción** | **Descripción** |
| --- | --- |
| Agrupar las alertas en un solo incidente si todas las entidades coinciden | Las alertas se agrupan si comparten los mismos valores entre todas las entidades asignadas, definidas en la pestaña Set rule logic (Establecer lógica de regla) anterior. Esta es la configuración recomendada. |
| Agrupar todas las alertas desencadenadas por esta regla en un único incidente | Todas las alertas que genera esta regla se agrupan aunque no compartan valores idénticos. |
| Agrupar las alertas en un solo incidente si las entidades seleccionadas y los detalles coinciden | Las alertas se agrupan si comparten valores idénticos para todas las entidades asignadas, los detalles de las alertas y los detalles personalizados seleccionados en las listas desplegables correspondientes.  Es posible que quiera usar esta configuración si, por ejemplo, quiere crear incidentes independientes basados en las direcciones IP de origen o de destino, o si desea agrupar las alertas que coincidan con una entidad y gravedad específicas.  Nota: Al seleccionar esta opción, debe tener al menos un tipo de entidad o campo seleccionado para la regla. De lo contrario, se producirá un error en la validación de la regla y esta no se creará. |

* Vuelva a abrir los incidentes coincidentes cerrados: si se ha resuelto y cerrado un incidente y, posteriormente, se genera otra alerta que habría pertenecido a ese incidente, establezca esta opción en Enabled (Habilitado) si quiere que el incidente cerrado se vuelva a abrir, o bien déjela como Disabled (Deshabilitado) si quiere que la alerta cree un incidente nuevo.

**Nota**

Se pueden agrupar **hasta 150 alertas** en un solo incidente.

* El incidente solo se creará después de que se hayan generado todas las alertas. Todas las alertas se agregarán al incidente inmediatamente después de su creación.
* Si hay más de 150 alertas generadas por una regla que las agrupa en un solo incidente, se generará un nuevo incidente con los mismos detalles del incidente que el original, y las alertas sobrantes se agruparán en el nuevo incidente.

**Establecimiento de respuestas automatizadas y creación de la regla**

En la pestaña Respuestas automatizadas, puede usar las reglas de automatización para establecer respuestas automatizadas que se produzcan en cualquiera de estos tres tipos de ocasiones:

* Cuando esta regla de análisis genera una alerta.
* Cuando se crea un incidente con alertas generadas por esta regla de análisis.
* Cuando se actualiza un incidente con alertas generadas por esta regla de análisis.

La cuadrícula que se muestra en Reglas de automatización, muestra las reglas de automatización que ya se aplican a esta regla de análisis (asumiendo que cumple las condiciones definidas en esas reglas). Para editar cualquiera de estos puntos suspensivos, seleccione los puntos suspensivos al final de cada fila. O bien, puede crear una nueva regla de automatización.

Use reglas de automatización para realizar evaluaciones de prioridades básicas, asignaciones, flujos de trabajo y cierres de incidentes.

Automatice tareas más complejas e invoque respuestas de sistemas remotos para corregir amenazas mediante una llamada a los cuadernos de estrategias de estas reglas de automatización. Puede hacerlo tanto para incidentes como para alertas individuales.

* En Automatización de alertas (clásico) en la parte inferior de la pantalla, verá los cuadernos de estrategias que haya configurado para que se ejecuten automáticamente cuando se genere una alerta mediante el método anterior.
  + A partir de junio de 2023, ya no puede agregar cuadernos de estrategias a esta lista. Los cuadernos de estrategias que ya aparecen aquí seguirán ejecutándose hasta que este método esté en desuso, a partir de marzo de 2026.
  + Si sigue teniendo alguno de los cuaderno de estrategias enumerados aquí, debe crear una regla de automatización basada en el desencadenador creado por la alerta e invocar el cuaderno de estrategias desde allí. Una vez hecho esto, seleccione los puntos suspensivos al final de la línea del cuaderno de estrategias que se muestra aquí y seleccione Quitar.

Seleccione **Revisar y crear** para revisar todos los valores de configuración de la nueva regla de análisis. Cuando aparezca el mensaje “Validación superada”, seleccione **Crear**.

Visualización de la regla y su salida

* Es posible encontrar la regla personalizada recién creada (de tipo "Programado") en la tabla, en la pestaña Reglas activas de la pantalla principal de **Analytics**. Desde esta lista puede habilitar, deshabilitar o eliminar cada regla.
* Para ver los resultados de las reglas de análisis que cree, vaya a la página **Incidentes**, donde es posible realizar una evaluación de prioridades sobre los incidentes, investigarlos y solucionar las amenazas.
* Puede actualizar la consulta de regla para excluir falsos positivos.

**Configurar la automatización en Microsoft Sentinel**

**¿Qué son las reglas de automatización y los cuadernos de estrategias?**

Las reglas de automatización ayudan a evaluar incidentes en Microsoft Azure Sentinel. Puede usarlas para asignar automáticamente incidentes al personal adecuado, cerrar incidentes ruidosos o falsos positivos conocidos, cambiar su gravedad y agregar etiquetas. También son el mecanismo por el que puede ejecutar cuadernos de estrategias en respuesta a los incidentes o las alertas.

Los cuadernos de estrategias son colecciones de procedimientos que se pueden ejecutar desde Microsoft Sentinel en respuesta a un **incidente completo**, a una **alerta individual** o a una **entidad específica**. Un cuaderno de estrategias puede ayudarle a automatizar y organizar su respuesta y se puede configurar para que se ejecute automáticamente cuando se generen alertas o se creen o actualicen incidentes; para ello, se adjuntan a una regla de automatización. También se puede ejecutar manualmente a petición en incidentes, alertas o entidades específicos.

Los cuadernos de estrategias de Microsoft Azure Sentinel se basan en flujos de trabajo integrados en Azure Logic Apps, lo que significa que obtendrá toda la versatilidad, personalización y plantillas integradas de Logic Apps. Cada cuaderno de estrategias se crea para la suscripción específica a la que pertenece, pero en **Cuadernos de estrategia** se muestran todos los cuadernos de estrategias disponibles en todas las suscripciones seleccionadas.

Por ejemplo, si desea detener el movimiento en la red y el robo de información por parte de usuarios potencialmente en peligro, puede crear una respuesta automatizada y de varias facetas para los incidentes generados por reglas que detecten usuarios en peligro. Comience por crear un cuaderno de estrategias que lleve a cabo las siguientes acciones:

1. Cuando una regla de automatización llama al cuaderno de estrategias y le pasa un incidente, el cuaderno de estrategias abre una incidencia en ServiceNow o en cualquier otro sistema de vales de TI.
2. Envía un mensaje al canal de operaciones de seguridad en Microsoft Teams o Slack para asegurarse de que los analistas de seguridad sean conscientes del incidente.
3. También envía toda la información del incidente en un mensaje de correo electrónico al administrador de seguridad y al administrador de red sénior. El mensaje de correo electrónico incluirá los botones de opciones de usuario **Bloquear** e **Ignorar**.
4. El cuaderno de estrategias espera hasta que se reciba una respuesta de los administradores y, después, continúa con los pasos siguientes.
5. Si los administradores eligen **Bloquear**, envía un comando a Microsoft Entra ID para deshabilitar el usuario y uno al firewall para bloquear la dirección IP.
6. Si los administradores eligen **Ignorar**, el cuaderno de estrategias cierra el incidente en Microsoft Azure Sentinel y el vale en ServiceNow.
7. Para desencadenar el cuaderno de estrategias, cree una regla de automatización que se ejecute cuando se generen estos incidentes. Esa regla llevará a cabo estos pasos:
   * La regla cambia el estado del incidente a Activo.
   * Asigna el incidente al analista encargado de administrar este tipo de incidentes.
   * Agrega la etiqueta "usuario en peligro".
   * Por último, llama al cuaderno de estrategias que acaba de crear. (Se requieren permisos especiales para este paso).

Los cuadernos de estrategias se pueden ejecutar automáticamente en respuesta a incidentes mediante la creación de reglas de automatización que llaman a los cuadernos de estrategias como acciones, como en el ejemplo anterior. También se pueden ejecutar automáticamente en respuesta a alertas, indicando a la regla de análisis que ejecute automáticamente uno o varios cuadernos de estrategias cuando se genere la alerta.

También puede elegir ejecutar un cuaderno de estrategias manualmente a petición, como respuesta a una alerta seleccionada.

Obtenga una introducción más completa y detallada para la automatización de las respuestas a amenazas mediante reglas de automatización y cuadernos de estrategias en Microsoft Azure Sentinel.

**Crear un cuaderno de estrategias**

Para crear un nuevo cuaderno de estrategias en Microsoft Sentinel, siga estos pasos

1. En el menú de navegación de **Microsoft Azure Sentinel**, seleccione **Automation** (Automatización).
2. En el menú superior, seleccione **Crear**.
3. El menú desplegable que aparece en **Crear** ofrece cuatro opciones para crear cuadernos de estrategias:
   * Si va a crear un cuaderno de estrategias **Estándar** (el nuevo tipo: consulte Tipos de aplicaciones lógicas), seleccione **Cuaderno de estrategias en blanco** y, a continuación, siga los pasos de la pestaña Estándar de Logic Apps a continuación.
   * Si va a crear un cuaderno de estrategias **Consumo** (el tipo original y clásico), en función del desencadenador que quiera usar, seleccione **Cuaderno de estrategias con desencadenador de incidentes**, **Cuaderno de estrategias con desencadenador de alertas** o **Cuaderno de estrategias con desencadenador de entidad**. A continuación, siga los pasos descritos en la pestaña **Logic Apps Consumption** siguiente.
4. En la pestaña **Básicos**:
   * Seleccione la **suscripción**, el **grupo de recursos** y la región que prefiera en sus listas desplegables respectivas. La región elegida es donde se almacenará la información de la aplicación lógica.
   * Escriba un nombre para el cuaderno de estrategias en **Nombre del cuaderno de estrategias**.
   * Si desea supervisar la actividad de este cuaderno de estrategias con fines de diagnóstico, marque la casilla **EnablediagnosticslogsinLog Analytics** y elija el **área de trabajo de Log Analytics** en la lista desplegable.
   * Si los cuadernos de estrategias necesitan acceso a recursos protegidos que están dentro de una red virtual de Azure o conectados a una, es posible que tenga que usar un entorno de servicio de integración (ISE). Si es así, marque la casilla **Asociar con el entorno del servicio de integración** y seleccione el ISE deseado en la lista desplegable.
   * Seleccione **Siguiente: conexiones**.
5. En la pestaña **Conexiones**:
   * Lo ideal sería dejar esta sección tal cual y configurar Logic Apps para la conexión con Microsoft Sentinel con identidad administrada. Aprenda sobre esta y otras alternativas de autenticación.
6. Seleccione **Siguiente: Revisar y crear**.
7. En la pestaña **Revisar y crear**:
   * Los incidentes pueden tener dos orígenes posibles: se pueden crear dentro de Microsoft Sentinel y también se pueden importar y sincronizar con Microsoft 365 Defender.
     + Si seleccionó uno de los desencadenadores de incidentes y desea que la regla de automatización tenga efecto solo en los incidentes con origen en Microsoft Sentinel o, alternativamente, en Microsoft 365 Defender, especifique el origen en la condición **Si el proveedor del incidente es igual a**. (Esta condición solo se mostrará si se selecciona un desencadenador de incidentes).
   * Para todos los tipos de desencadenador, si desea que la regla de automatización solo tenga efecto en determinadas reglas de análisis, especifique cuáles modificando la condición **Si el nombre de la regla de análisis contiene**.
   * Agregue cualquier otra condición que desee determinar si se ejecuta esta regla de automatización. Seleccione + Agregar y elija condiciones o grupos de condiciones en la lista desplegable. La lista de condiciones se rellena mediante los campos de detalles de la alerta e identificador de la entidad.
   * Puesto que usa esta regla de automatización para ejecutar un cuaderno de estrategias, elija la acción Ejecutar cuaderno de estrategias en la lista desplegable. A continuación, se le pedirá que elija en una segunda lista desplegable que muestra los cuadernos de estrategias disponibles. Una regla de automatización solo puede ejecutar esos cuadernos de estrategias que comiencen con el mismo desencadenador (incidente o alerta) que el desencadenador definido en la regla, por lo que solo aparecerán esos cuadernos de estrategias en la lista.
   * Debe tener permisos de **propietario** en cualquier grupo de recursos al que quiera conceder permisos de Microsoft Sentinel y debe tener el rol Colaborador de aplicaciones lógicas en cualquier grupo de recursos que contenga cuadernos de estrategias que quiera ejecutar.
   * En una implementación multiinquilino, si el cuaderno de estrategias que desea ejecutar estuviera en un inquilino diferente, deberá conceder a Microsoft Sentinel permiso para ejecutar el cuaderno de estrategias en el inquilino del cuaderno de estrategias.
     + En el menú de navegación de Microsoft Azure Sentinel del inquilino de los cuadernos de estrategias, seleccione **Settings** (Configuración).
     + En la hoja **Settings** (Configuración), seleccione la pestaña **Settings** (Configuración) y, a continuación, el expansor de **Playbook permissions** (Permisos del cuaderno de estrategias).
     + Haga clic en el botón Configurar permisos para abrir el panel **Administrar permisos** mencionado anteriormente y continúe con lo descrito allí.
   * Si, en un escenario de **MSSP**, desea **ejecutar un cuaderno de estrategias en un inquilino del cliente** a partir de una regla de automatización creada con la sesión iniciada en el inquilino del proveedor de servicios, debe conceder a Microsoft Azure Sentinel permiso para ejecutarlo en ***ambos inquilinos***. En el inquilino **cliente**, siga las instrucciones para la implementación multiinquilino en la viñeta anterior. En el inquilino del **proveedor de servicios**, es necesario agregar la aplicación **Azure Security Insights** en la plantilla de incorporación de Azure Lighthouse:
     + En Azure Portal, vaya a **Microsoft Entra ID**.
     + Haga clic en **Aplicaciones empresariales**.
     + Seleccione **Tipo de aplicación** y filtre por **Aplicaciones de Microsoft**.
     + En el cuadro de búsqueda, escriba **Azure Security Insights**.
     + Copie el campo **Id. de objeto**. Deberá agregar esta autorización adicional a la delegación de Azure Lighthouse existente.
   * El rol **Colaborador de automatización de Microsoft Sentinel** tiene un GUID fijo, que es f4c81013-99ee-4d62-a7ee-b3f1f648599a.
   * Agregue cualquier otra acción que desee para esta regla. Puede cambiar el orden de ejecución de las acciones seleccionando las flechas arriba o abajo situadas a la derecha de cualquier acción.
8. Revise las opciones de configuración que ha realizado y seleccione **Crear y continuar con el diseñador**.

El cuaderno de estrategias tardará unos minutos en crearse e implementarse, después de lo cual verá el mensaje "Se completó la implementación" y se le llevará al nuevo diseñador de aplicaciones lógicas del cuaderno de estrategias. El desencadenador que eligió al principio se agregará automáticamente como primer paso y, a partir de aquí, podrá seguir diseñando el flujo de trabajo.

**Incorporación de una acción**

Ahora puede definir lo que ocurre cuando se llame al cuaderno de estrategias. Puede agregar acciones, condiciones lógicas, bucles o condiciones switch-case; para ello, seleccione **Nuevo paso**. Esta selección abre un nuevo marco en el diseñador, donde puede elegir un sistema o una aplicación con la que interactuar o una condición para establecer. Escriba el nombre del sistema o la aplicación en la barra de búsqueda de la parte superior del marco y, a continuación, elija entre los resultados disponibles.

En cada uno de estos pasos, al hacer clic en cualquier campo se muestra un panel con dos menús: **Contenido dinámico** y **Expresión**. Desde el menú **Contenido dinámico**, es posible agregar referencias a los atributos de la alerta o incidente que se pasó al cuaderno de estrategias, incluyendo los valores y atributos de todas las entidades asignadas y los detalles personalizados contenidos en la alerta o incidente. En el menú **Expresión**, puede elegir entre una gran biblioteca de funciones para agregar lógica adicional a los pasos.

En esta captura de pantalla se muestran las acciones y condiciones que agregaría en la creación del cuaderno de estrategias descrito en el ejemplo que aparece al principio de este documento. Obtenga más información sobre cómo agregar acciones a los cuadernos de estrategias.

**Automatizar las respuestas frente a amenazas**

Ha creado el cuaderno de estrategias y ha definido el desencadenador, ha establecido las condiciones y ha indicado las acciones que realizará y las salidas que generará. Ahora debe determinar los criterios según los cuales se ejecutará y configurar el mecanismo de automatización que lo ejecutará cuando se cumplan los criterios.

**Respuesta a incidentes y alertas**

Para usar un cuaderno de estrategias para responder automáticamente a un **incidente completo** o a una **alerta individual**, cree una regla de automatización que se ejecutará cuando se cree o actualice, o bien cuando se genere la alerta. Esta regla de automatización incluirá un paso que llama al cuaderno de estrategias que desea usar.

**Para crear una regla de automatización**:

1. En la hoja **Automatización** del menú de navegación de Microsoft Sentinel, seleccione **Crear** en el menú superior y elija **Regla de automatización**.
2. Se abre el panel **Create new automation rule** (Creación de una regla de automatización). Escriba un nombre para la regla.
3. **Desencadenador:** seleccione el desencadenador adecuado según la circunstancia para la que esté creando la regla de automatización: **Cuando se crea un incidente**, **Cuando se actualiza un incidente** o **Cuando se crea una alerta**.
4. **Condiciones:**

* Los incidentes pueden tener dos orígenes posibles: se pueden crear dentro de Microsoft Sentinel y también se pueden importar desde y sincronizar con Microsoft Defender XDR.
* Si seleccionó uno de los desencadenadores de incidentes y desea que la regla de automatización surta efecto solo en incidentes de Microsoft Sentinel o, como alternativa, en Microsoft Defender XDR, especifique el origen en la condición Si el proveedor de incidentes es igual a. (Esta condición solo se mostrará si se selecciona un desencadenador de incidentes).
* Para todos los tipos de desencadenador, si desea que la regla de automatización solo tenga efecto en determinadas reglas de análisis, especifique cuáles modificando la condición Si el nombre de la regla de análisis contiene.
* Agregue cualquier otra condición que desee determinar si se ejecuta esta regla de automatización. Seleccione + Agregar y elija condiciones o grupos de condiciones en la lista desplegable. La lista de condiciones se rellena mediante los campos de detalles de la alerta e identificador de la entidad.

1. **Acciones:**

* Puesto que usa esta regla de automatización para ejecutar un cuaderno de estrategias, elija la acción Ejecutar cuaderno de estrategias en la lista desplegable. A continuación, se le pedirá que elija en una segunda lista desplegable que muestra los cuadernos de estrategias disponibles. Una regla de automatización solo puede ejecutar esos cuadernos de estrategias que comiencen con el mismo desencadenador (incidente o alerta) que el desencadenador definido en la regla, por lo que solo aparecerán esos cuadernos de estrategias en la lista.

**Importante**

**Se deben conceder permisos explícitos a Microsoft Sentinel para ejecutar cuadernos de estrategias**, ya sea manualmente o a partir de reglas de automatización. Si un cuaderno de estrategias aparece "atenuado" en la lista desplegable, significa que Sentinel no tiene permisos para el grupo de recursos de este cuaderno de estrategias. Haga clic en el vínculo **Manage playbook permissions** (Administrar permisos del cuaderno de estrategias) para asignar permisos.

En el panel **Manage permissions** (Administrar permisos) que se abre, active las casillas de los grupos de recursos que contienen los cuadernos de estrategias que desea ejecutar y haga clic en **Apply** (Aplicar).

1. Establezca una fecha de expiración para la regla de automatización si desea que tenga una.
2. Escriba un número en **Order** (Orden) para determinar en qué punto de la secuencia de reglas de automatización se ejecutará esta regla.
3. Haga clic en **Aplicar**. ¡Y ya está!

**Prueba de conocimientos**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

**Comprobación de conocimientos**

Principio del formulario

**1. ¿Qué acción habilita la sección Configuración de incidentes en Microsoft Sentinel?**

1. Agrupar automáticamente todas las alertas en un único incidente
2. Deshabilitación de la creación de incidentes para todas las reglas de análisis
3. Habilitación o deshabilitación de la creación de incidentes para alertas desencadenadas por una regla de análisis específica

**2. Un analista de seguridad necesita recopilar registros de un origen de datos personalizado en un equipo Linux. ¿Qué método deberían usar para recopilar los registros?**

1. Use el agente de Log Analytics para recopilar los registros como archivos en equipos Linux.
2. Configure el demonio de Syslog para reenviar eventos al área de trabajo de Microsoft Sentinel.
3. Use el agente de recopilación de registros personalizados de Log Analytics para recopilar los registros como archivos en equipos Linux.

**3. Una empresa desea consolidar las entradas de registro de varias suscripciones e inquilinos de Azure en una ubicación para su análisis. También desean realizar un análisis complejo y obtener información detallada sobre las entradas del registro de actividad. ¿Qué característica deberían habilitar mediante el envío del registro de actividad a un área de trabajo de Log Analytics?**

1. Habilitación de la cuenta de Azure Storage
2. Exportación de registros de actividad a un archivo
3. Envío del registro de actividad a un área de trabajo de Log Analytics

**4. Un equipo de seguridad debe garantizar la configuración segura de sus recursos de Azure. Quieren usar una herramienta que pueda evaluar la posición de seguridad de sus recursos y proporcionar recomendaciones de mejora. ¿Qué servicio de Azure deberían usar?**

1. Microsoft Defender for Cloud
2. Azure Policy
3. Azure Advisor

**5. Un analista de seguridad está creando un cuaderno de estrategias en Microsoft Sentinel. Quieren automatizar la respuesta a un incidente o alerta. ¿Cuál es el siguiente paso que deben realizar después de definir el desencadenador, las condiciones y las acciones del cuaderno de estrategias?**

1. Adición de lógica adicional a los pasos mediante una biblioteca de funciones
2. Creación de una nueva regla de automatización
3. Determinación de los criterios en los que se ejecutará el cuaderno de estrategias y configuración del mecanismo de automatización que lo ejecutará cuando se cumplan dichos criterios
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, ha aprendido a configurar y administrar soluciones de automatización y supervisión de seguridad, incluida la supervisión de eventos de seguridad mediante Azure Monitor, la configuración de conectores de datos en Microsoft Sentinel, la creación de reglas de análisis personalizadas, la evaluación de alertas e incidentes y la implementación de la automatización para mejorar la respuesta y administración de incidentes de seguridad.