**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**

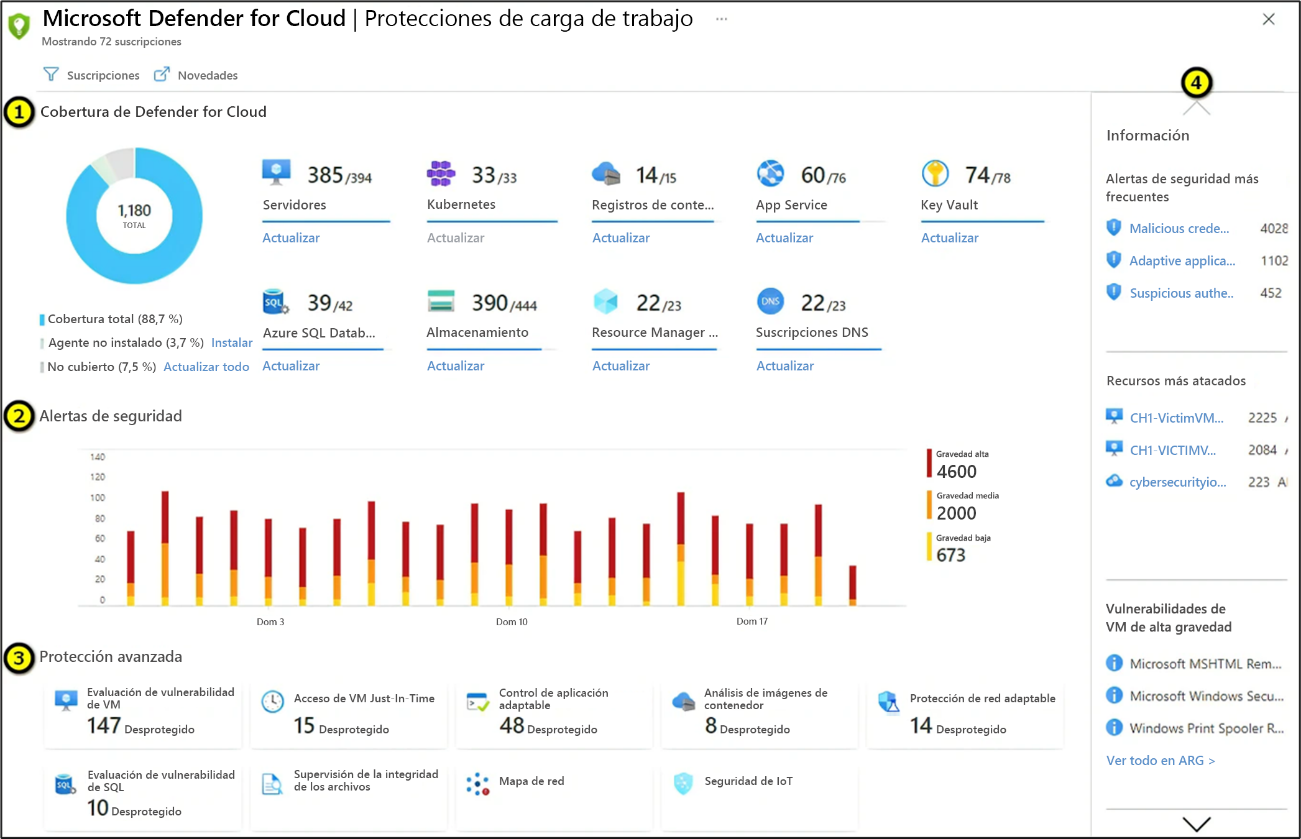
El módulo tiene como objetivo equipar a los participantes con los conocimientos y aptitudes necesarios para configurar y administrar soluciones de automatización y supervisión de seguridad de forma eficaz. Los participantes aprenderán a supervisar eventos de seguridad, configurar conectores de datos, 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.

**Habilitar servicios de protección de cargas de trabajo en Microsoft Defender for Cloud, incluidos Microsoft Defender para Storage, bases de datos, contenedores, App Service, Key Vault, Resource Manager y DNS**

Defender for Cloud ofrece alertas de seguridad con tecnología de Inteligencia sobre amenazas de Microsoft. También incluye una gama de protecciones avanzadas e inteligentes para las cargas de trabajo. Las protecciones de cargas de trabajo se proporcionan a través de planes de Microsoft Defender específicos de los tipos de recursos de las suscripciones. **Por ejemplo**, puede habilitar Microsoft Defender para Storage y recibir alertas sobre actividades sospechosas relacionadas con los recursos de almacenamiento.

**El panel de cargas de trabajo en la nube incluye las secciones siguientes:**

1. **Cobertura de Microsoft Defender for Cloud**: aquí puede ver los tipos de recursos que se encuentran en su suscripción y que pueden protegerse mediante Defender for Cloud. Siempre que sea pertinente, también puede actualizar aquí. Si desea actualizar todos los recursos válidos posibles, seleccione **Actualizar todo**.
2. **Alertas de seguridad**: cuando Defender for Cloud detecta una amenaza en cualquiera de las áreas del entorno, genera una alerta. Estas alertas describen los detalles de los recursos afectados, los pasos sugeridos para resolver la amenaza y, en algunos casos, una opción para **desencadenar una aplicación lógica** como respuesta. Al seleccionar cualquier parte de este gráfico, se abre la página de alertas de seguridad.
3. **Protección avanzada**: Defender for Cloud incluye muchas funcionalidades avanzadas de protección contra amenazas para máquinas virtuales, bases de datos de **Lenguaje de consulta estructurado (SQL)**, contenedores, aplicaciones web, la red y mucho más. En esta sección de protección avanzada, puede ver el estado de los recursos de las suscripciones seleccionadas para cada una de estas protecciones. Seleccione cualquiera de ellas para ir directamente al área de configuración de ese tipo de protección.
4. **Información detallada**: este panel continuo de noticias, lecturas sugeridas y alertas de alta prioridad aporta a Defender for Cloud información sobre aspectos de seguridad apremiantes que son pertinentes para usted y su suscripción. Tanto si se trata de una lista de **vulnerabilidades y exposiciones comunes (CVE)** de alta gravedad detectadas en sus máquinas virtuales por una herramienta de análisis de vulnerabilidades, o bien de una nueva publicación de blog de un miembro del equipo de Defender for Cloud, las encontrará en el panel de información detallada.



**Protección de cargas de trabajo en la nube**

Los principios de seguridad proactivos requieren que implementes prácticas de seguridad que protejan las cargas de trabajo frente a amenazas. Las protecciones de cargas de trabajo en la nube (CWP) exponen recomendaciones específicas de la carga de trabajo que le llevan a los controles de seguridad adecuados para proteger las cargas de trabajo.

Cuando el entorno está amenazado, las alertas de seguridad inmediatamente indican la naturaleza y la gravedad de la amenaza para que puedas planear la respuesta. Después de identificar una amenaza en tu entorno, debes responder rápidamente para limitar el riesgo a los recursos.

| **Funcionalidad** | **¿Qué problemas soluciona?** | **Introducción** | **Plan de Defender** |
| --- | --- | --- | --- |
| Proteger los servidores en la nube | Proporcionar protecciones de servidor a través de Microsoft Defender para punto de conexión o protección ampliada con acceso a la red Just-In-Time, supervisión de la integridad de los archivos, evaluación de vulnerabilidades y mucho más. | Proteger los servidores multinube y locales | Defender para servidores |
| Identificar amenazas para los recursos de almacenamiento | Detecta intentos inusuales y potencialmente dañinos de acceder o aprovechar las cuentas de almacenamiento mediante funcionalidades avanzadas de detección de amenazas y datos de Inteligencia sobre amenazas de Microsoft para proporcionar alertas de seguridad contextuales. | Proteger los recursos de almacenamiento en la nube | Defender para Storage |
| Proteger las bases de datos en la nube | Proteger todo el patrimonio de bases de datos con detección de ataques y respuesta a amenazas para los tipos de base de datos más populares de Azure para proteger los motores de base de datos y los tipos de datos, según sus riesgos de seguridad y superficie expuesta a ataques. | Implementar protecciones especializadas para bases de datos locales y en la nube | - Defender para bases de datos de Azure SQL - Defender para servidores SQL en máquinas - Defender para bases de datos relacionales de código abierto - Defender para Azure Cosmos DB |
| Proteger contenedores | Protege los contenedores para que puedas mejorar, supervisar y mantener la seguridad de los clústeres, contenedores y sus aplicaciones con protección del entorno, evaluaciones de vulnerabilidades y protección en tiempo de ejecución. | Buscar riesgos de seguridad en los contenedores | Defender para contenedores |
| Información del servicio de infraestructura | Diagnostica puntos débiles en la infraestructura de la aplicación que pueden dejar el entorno susceptible a ataques. | Identificación de ataques dirigidos a aplicaciones que se ejecutan mediante App Service Detección de intentos de vulnerar la seguridad de cuentas de Key Vault Obtención de alertas sobre operaciones sospechosas de Resource Manager Exposición de actividades anómalas de DNS | - Defender para App Service - Defender para Key Vault - Defender para Resource Manager - Defender para DNS |
| Alertas de seguridad | Obtén información sobre los eventos en tiempo real que amenazan la seguridad de tu entorno. Las alertas se clasifican y asignan niveles de gravedad para indicar las respuestas adecuadas. | Administración de alertas de seguridad | Cualquier plan de Defender de protección de cargas de trabajo |
| Incidentes de seguridad | Correlacionar alertas para identificar patrones de ataque e integrarse con las soluciones de administración de eventos e información de seguridad (SIEM), respuesta automatizada de orquestación de seguridad (SOAR) y administración de servicios de TI (ITSM) para responder a amenazas y limitar el riesgo a los recursos. | Exportar alertas a sistemas SIEM, SOAR o ITSM | Cualquier plan de Defender de protección de cargas de trabajo |

**Configuración de Microsoft Defender para servidores**

Defender para servidores en Microsoft Defender for Cloud brinda detección de amenazas y protección avanzada a las máquinas Windows y Linux que se ejecutan en Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP) y entornos locales. Este plan incluye la licencia integrada de Microsoft Defender para punto de conexión, líneas de base de seguridad y evaluaciones de nivel de sistema operativo, análisis de evaluación de vulnerabilidades, controles de aplicaciones adaptables (AAC), supervisión de la integridad de archivos (FIM) y mucho más.

Microsoft Defender para servidores incluye una integración nativa automática con Microsoft Defender para punto de conexión. Para obtener más información, consulte Protección de los puntos de conexión con la solución EDR integrada de Defender for Cloud: Microsoft Defender para puntos de conexión. Si ha habilitado esta integración, tendrá acceso a los hallazgos relacionados con vulnerabilidades de la administración de amenazas y vulnerabilidades de Microsoft.

**Habilitar el plan de Defender para servidores**

Puede habilitar el plan de Defender para servidores desde la página Configuración del entorno para proteger todas las máquinas de una suscripción de Azure, una cuenta de AWS o un proyecto de GCP.

**Para habilitar el plan de Defender para servidores:**

1. Inicie sesión en Azure Portal.
2. Busque y seleccione **Microsoft Defender for Cloud**.
3. En el menú de Defender for Cloud, seleccione **Environment Settings**.
4. Seleccione la suscripción correspondiente.
5. En la página Planes de Defender, cambie el botón de alternancia de Servidores a **Activado**.

**Selección de un plan de Defender para servidores**

Al habilitar el plan de Defender para servidores, se le da la opción de seleccionar qué plan (Plan 1 o Plan 2) habilitar. Hay dos planes entre los que puede elegir, que ofrecen distintos niveles de protección para los recursos.

Revise lo que incluye cada plan.

**Para seleccionar un plan de Defender para servidores:**

1. Inicie sesión en Azure Portal.
2. Busque y seleccione **Microsoft Defender for Cloud**.
3. En el menú de Defender for Cloud, seleccione **Environment Settings**.
4. Seleccione la suscripción de Azure, la cuenta de AWS o el proyecto de GCP pertinente.
5. Seleccione **Cambiar plan**.
6. En la ventana emergente, seleccione **Plan 2** o **Plan 1**.
7. Seleccione **Confirmar**.
8. Seleccione **Guardar**.

**Configuración de Microsoft Defender para Azure SQL Database**

Defender for Databases de Microsoft Defender for Cloud le permite proteger todo su patrimonio de bases de datos con detección de ataques y respuesta a amenazas para los tipos de base de datos más populares en Azure. Defender for Cloud proporciona protección para los motores de base de datos y para los tipos de datos, en función de su superficie expuesta a ataques y de sus riesgos de seguridad.

La protección de las bases de datos incluye:

* Microsoft Defender para servidores de la base de datos de Azure SQL
* Microsoft Defender para servidores SQL Server en máquinas
* Microsoft Defender para bases de datos relacionales de código abierto
* Microsoft Defender para Azure Cosmos DB

**Habilitar el plan Bases de datos**

Al habilitar la protección de las bases de datos, se habilitan los cuatro planes de Defender y se protegen todas las bases de datos admitidas en su suscripción.

**Para habilitar Defender para DNS en su suscripción:**

1. Inicie sesión en Azure Portal.
2. Busque y seleccione **Microsoft Defender for Cloud**.
3. En el menú de Defender for Cloud, seleccione **Environment Settings**.
4. Seleccione la suscripción de Azure, la cuenta de AWS o el proyecto de GCP pertinente.
5. En la página de planes de Defender, cambie el plan de Bases de datos a **Activado**.

**Habilitar las protecciones de bases de datos de planes específicos**

Al habilitar la protección de bases de datos, se habilitan los cuatro planes de Defender siguientes:

* Defender bases de datos de Azure SQL
* Defender para servidores SQL en máquinas
* Defender para bases de datos relacionales de código abierto
* Defender para Azure Cosmos DB

Estos planes protegen todas las bases de datos admitidas en su suscripción.

**Para habilitar protecciones de bases de datos específicas en su suscripción:**

1. Inicie sesión en Azure Portal.
2. Busque y seleccione **Microsoft Defender for Cloud**.
3. En el menú de Defender for Cloud, seleccione **Environment Settings**.
4. Seleccione la suscripción correspondiente.
5. En la página de planes de Defender, busque el plan Bases de datos y elija **Seleccionar tipos**.
6. En la ventana de selección Tipos de recursos, cambie los planes deseados a **Activado** o **Desactivado**.
7. (Opcional) Excluya los tipos de recursos de bases de datos específicos cambiándolos a **Desactivado**.
8. Seleccione **Continuar**.
9. Seleccione **Guardar**.

**Administración de alertas de seguridad y respuesta a ellas en Microsoft Defender for Cloud**

**¿Qué son las alertas de seguridad?**

Las alertas de seguridad son las notificaciones generadas por los planes de protección de cargas de trabajo de Defender for Cloud cuando se identifican amenazas en los entornos de Azure, híbridos o multinube.

* Las alertas de seguridad se desencadenan mediante detecciones avanzadas disponibles al habilitar los planes de Defender para tipos de recursos concretos.
* Cada alerta proporciona detalles de los recursos afectados, los problemas y los pasos de corrección.
* Defender for Cloud clasifica las alertas y las prioriza por gravedad.
* Las alertas se muestran en el portal durante 90 días, incluso si el recurso relacionado con la alerta se eliminó durante ese intervalo de tiempo. Esto se debe a que la alerta podría indicar una posible infracción de seguridad en la organización que debe investigarse más a fondo.
* Las alertas se pueden exportar en formato CSV.
* Las alertas también se pueden transmitir directamente a una solución de administración de eventos e información de seguridad (SIEM), como Microsoft Sentinel, de respuesta automatizada de orquestación de seguridad (SOAR) o de administración de servicios de TI (ITSM).
* Defender for Cloud utiliza la matriz de ataque MITRE para asociar alertas con su intención percibida, lo que ayuda a formalizar el conocimiento de dominios de seguridad.

**¿Cómo se clasifican las alertas?**

Las alertas tienen asignado un nivel de gravedad para ayudar a priorizar cómo atender cada alerta. La gravedad se basa en:

* El desencadenador específico.
* El nivel de confianza de que hubo intención malintencionada detrás de la actividad que condujo a la alerta.

| **Gravedad** | **Respuesta recomendada** |
| --- | --- |
| Alto | hay una probabilidad elevada de que el recurso esté en peligro. Debe investigarse de inmediato. El grado de certeza de Defender for Cloud sobre la mala intención de la acción y los hallazgos utilizados para emitir la alerta es elevado. Una alerta de este tipo sería podría detectar la ejecución de una herramienta malintencionada conocida; por ejemplo, Mimikatz, una herramienta que se usa habitualmente para robar credenciales. |
| Media | es probable que sea una actividad sospechosa que podría indicar que un recurso está en peligro. El grado de certeza de Defender for Cloud sobre el análisis o los hallazgos es medio, mientras que el grado de certeza sobre la mala intención es medio o alto. Normalmente, se trata de detecciones basadas en anomalías o aprendizaje automático, por ejemplo, un intento de inicio de sesión desde una ubicación inusual. |
| Baja | podría tratarse de un hallazgo benigno o de un ataque bloqueado. Defender for Cloud no tiene la certeza suficiente de que la intención fuera mala y la actividad pudiera ser inofensiva. Por ejemplo, borrar un registro es una acción que podría producirse si un atacante intenta ocultar sus huellas, pero en muchos casos es una operación rutinaria que realizan los administradores. Por lo general, Defender for Cloud no avisa cuando se bloquean ataques a menos que se considere un caso interesante que convenga examinar. |
| Informativo | Normalmente, las incidencias se componen de varias alertas, algunas de las cuales podrían parecer meramente informativas, aunque a tenor de otras alertas podría ser conveniente investigarlas. |

**¿Qué son los incidentes de seguridad?**

Un incidente de seguridad es una recopilación de alertas relacionadas.

Los incidentes proporcionan una vista única de un ataque y sus alertas relacionadas, de modo que pueda comprender rápidamente las acciones que realizó un atacante y los recursos afectados.

A medida que aumenta la cobertura de amenazas, así lo hace la necesidad de detectar incluso el menor riesgo. Es difícil que los analistas de seguridad evalúen diferentes alertas e identifiquen un ataque real. Al correlacionar alertas y señales de baja fidelidad en incidentes de seguridad, Defender for Cloud ayuda a los analistas a afrontar esta fatiga de alertas.

En la nube los ataques se producen a menudo a través de distintos inquilinos, por o que Defender for Cloud puede combinar algoritmos de inteligencia artificial para analizar las secuencias de ataque que se notifican en cada suscripción. Esta técnica identifica las secuencias de ataque como patrones de alerta más frecuentes, en lugar de asociarse simplemente entre sí.

Durante la investigación de un incidente, los analistas a menudo necesitan más contexto para llegar a un veredicto sobre la naturaleza de la amenaza y cómo mitigarla. Por ejemplo, incluso cuando se detecta una anomalía de red, sin saber qué más sucede en la red o con respecto al recurso objetivo, es difícil determinar las medidas que se deben tomar a continuación. En estos casos, pueden ser de utilidad los artefactos, los eventos relacionados y la información que un incidente de seguridad puede incluir. La información adicional disponible de los incidentes de seguridad variará según el tipo de amenaza detectada y la configuración de su entorno.

**Correlación de alertas en incidentes**

Defender for Cloud correlaciona las alertas y las señales contextuales en incidentes.

La correlación examina diferentes señales entre los recursos y combina el conocimiento de seguridad y la inteligencia artificial para analizar alertas, detectando nuevos patrones de ataque a medida que se producen.

Además, mediante el uso de la información recopilada para cada paso de un ataque, Defender for Cloud puede descartar actividades que parecen ser pasos de un ataque, pero en realidad no lo son.

**¿Cómo detecta Defender for Cloud las amenazas?**

Para detectar amenazas reales y reducir falsos positivos, Defender for Cloud supervisa los recursos, recopila y analiza los datos de amenazas, a menudo correlacionando datos de varios orígenes.

**Iniciativas de Microsoft**

Microsoft Defender for Cloud se beneficia de la existencia de equipos de científicos de datos e investigadores de seguridad de Microsoft que supervisan sin descanso los cambios que se registran en el terreno de las amenazas. Estos son algunas de las iniciativas que llevan a cabo:

* Especialistas en seguridad de Microsoft colaboración continua con equipos de Microsoft que trabajan en campos de seguridad especializados, como análisis forense y detección de ataques web.
* Estudios de seguridad de Microsoft: nuestros investigadores de seguridad de Microsoft trabajan sin descanso para localizar amenazas. Dada nuestra presencia global en la nube y en sistemas locales, tenemos acceso a un amplio conjunto de recursos de telemetría. La amplitud y diversidad de estos conjuntos de datos nos permite detectar nuevos patrones y tendencias de ataque tanto en nuestros productos locales, destinados a particulares y empresas, como en nuestros servicios en línea. Como resultado, Defender for Cloud es capaz de actualizar rápidamente los algoritmos de detección a medida que los atacantes idean nuevas y más sofisticadas vulnerabilidades de seguridad. Este enfoque le ayuda a mantenerse al día en entornos llenos de amenazas que cambian continuamente.
* Supervisión de la inteligencia sobre amenazas: la inteligencia sobre amenazas incluye mecanismos, indicadores, implicaciones y notificaciones para las amenazas nuevas o existentes. Esta información se comparte con la comunidad de seguridad, y Microsoft supervisa sin descanso las fuentes de orígenes internos y externos.
* Uso compartido de señales: la información que recopilan los equipos de seguridad en la amplia cartera de servicios tanto locales como en la nube, de servidores y de dispositivos cliente de punto de conexión de Microsoft se comparte y se analiza.
* Ajuste de la detección: los algoritmos se ejecutan en conjuntos de datos de clientes reales y los investigadores de seguridad trabajan en conjunción con los clientes para validar los resultados. Los falsos positivos y los positivos verdaderos se utilizan para perfeccionar los algoritmos de aprendizaje automático.

Toda esta combinación de esfuerzos culmina en nuevas y mejoradas técnicas de detección, de las que puede beneficiarse al instante sin ninguna acción por su parte.

**Análisis de seguridad**

Defender for Cloud utiliza análisis avanzados que superan con creces los enfoques basados en firmas. Los grandes avances registrados en las tecnologías de macrodatos y aprendizaje automático se utilizan para evaluar eventos en todo el tejido de la nube, lo que permite detectar amenazas que no se podrían identificar mediante enfoques manuales, así como predecir la evolución de los ataques. Estas técnicas de análisis son:

**Información integrada sobre amenazas**

Microsoft dispone de una ingente cantidad de información sobre amenazas globales. Los recursos telemétricos proceden de diferentes fuentes, como Azure, Microsoft 365, Microsoft CRM Online, Microsoft Dynamics AX, outlook.com, MSN.com, la Unidad de crímenes digitales de Microsoft (DCU) y Microsoft Security Response Center (MSRC). Los investigadores también reciben información sobre amenazas que comparten con los principales proveedores de servicios en la nube y que procede de fuentes de otros terceros. Microsoft Defender for Cloud puede usar todos estos datos para avisarle de las amenazas procedentes de actores malintencionados conocidos.

**Análisis del comportamiento**

El análisis del comportamiento es una técnica que analiza datos y los compara con una serie de patrones conocidos. No obstante, estos patrones no son simples firmas, sino que están determinados por unos complejos algoritmos de aprendizaje automático que se aplican a conjuntos de datos masivos. También se determinan por medio de un análisis cuidadoso, llevado a cabo por analistas expertos, de los comportamientos malintencionados. Microsoft Defender for Cloud puede utilizar el análisis del comportamiento para identificar recursos en peligro a partir del análisis de registros de las máquinas virtuales, registros de los dispositivos de redes virtuales, registros de los tejidos y otros orígenes.

**Detección de anomalías**

Defender for Cloud también usa la detección de anomalías para identificar amenazas. A diferencia del análisis del comportamiento, que depende de patrones conocidos obtenidos a partir de grandes conjuntos de datos, la detección de anomalías es una técnica más "personalizada" y se basa en referencias que son específicas de las implementaciones. El aprendizaje automático se aplica para determinar la actividad normal de las implementaciones. A partir de ahí, se generan reglas para definir condiciones de valores atípicos que podrían constituir un evento de seguridad.

**Exportación de alertas**

Tiene una variedad de opciones para ver las alertas fuera de Defender for Cloud, entre ellas:

* La descarga del informe de CSV en el panel de alertas proporciona una exportación única a CSV.
* La exportación continua de la configuración del entorno permite configurar flujos de alertas de seguridad y recomendaciones a áreas de trabajo de Log Analytics y a Event Hubs. Más información.
* El conector de Microsoft Sentinel transmite las alertas de seguridad de Microsoft Defender for Cloud a Microsoft Sentinel.

**Configuración de la automatización de flujos de trabajo con Microsoft Defender for Cloud**

La automatización de los procesos de supervisión y respuesta ante incidentes de la organización puede mejorar considerablemente el tiempo necesario para investigar y mitigar los incidentes de seguridad.

Para implementar las configuraciones de automatización en la organización, use las directivas "DeployIfNotExist" de Azure Policy proporcionadas que se describen a continuación para crear y configurar los procedimientos de automatización de flujos de trabajo.

Para implementar estas directivas:

1. Desde la tabla siguiente, seleccione la directiva que quiere aplicar:

| **Objetivo** | **Directiva** | **Id. de directiva** |
| --- | --- | --- |
| Automatización de flujos de trabajo para alertas de seguridad | Implementación de la automatización de flujos de trabajo para alertas de Microsoft Defender for Cloud | f1525828-9a90-4fcf-be48-268cdd02361e |
| Automatización de flujos de trabajo para recomendaciones de seguridad | Implementación de la automatización de flujos de trabajo para recomendaciones de Microsoft Defender for Cloud | 73d6ab6c-2475-4850-afd6-43795f3492ef |
| Automatización de flujos de trabajo para cambios de cumplimiento normativo | Implementación de la automatización de flujos de trabajo para el cumplimiento normativo de Microsoft Defender for Cloud | 509122b9-ddd9-47ba-a5f1-d0dac20be63c |

1. En la página pertinente de Azure Policy, seleccione Asignar.
2. Abra cada pestaña y establezca los parámetros como quiera:

* En la pestaña **Aspectos básicos**, establezca el ámbito de la directiva. Para usar la administración centralizada, asigne la directiva al grupo de administración que contiene las suscripciones que usarán la automatización de flujos de trabajo.
* En la pestaña "Parámetros", escriba la información necesaria.
* (Opcional) Aplique esta asignación a la suscripción existente en la pestaña Corrección y seleccione la opción para crear una tarea de corrección.

1. Revise la página de resumen y seleccione **Crear**.

**Evaluación de exámenes de vulnerabilidades de Microsoft Defender para servidores**

Cuando la herramienta de evaluación de vulnerabilidades notifica vulnerabilidades a Defender for Cloud, este presenta los resultados y la información relacionada como recomendaciones. Además, los resultados incluyen información relacionada, como pasos de corrección, CVE pertinentes, puntuaciones de CVSS, etc. Se pueden ver las vulnerabilidades identificadas para una o varias suscripciones, o para una máquina virtual específica.

**Visualización de los resultados de los análisis de las máquinas virtuales**

Para ver los resultados de la evaluación de vulnerabilidades (de todos los exámenes configurados) y corregir las vulnerabilidades identificadas:

1. En el menú de Defender for Cloud, abra la página Recomendaciones.
2. Seleccione la recomendación Las máquinas deben tener resueltos los resultados de vulnerabilidades.
   * Defender for Cloud le muestra todos los resultados de todas las máquinas virtuales de las suscripciones seleccionadas actualmente. Los resultados se ordenan por gravedad.
3. Para filtrar los resultados de una máquina virtual específica, abra la sección "**Recursos afectados**" y haga clic en la máquina virtual que le interese. También puede seleccionar una máquina virtual en la vista Estado de los recursos y ver todas las recomendaciones pertinentes para ese recurso.
   * En Defender for Cloud se muestran los resultados de esa máquina virtual, ordenados por gravedad.
4. Para obtener más información acerca de una vulnerabilidad específica, selecciónela.
   * El panel de detalles que aparece contiene información detallada acerca de la vulnerabilidad e incluye lo siguiente:
     + Vínculos a todos los CVE pertinentes (si están disponibles)
     + Pasos de corrección
     + Cualquier página de referencia adicional
5. Para corregir un resultado, siga los pasos de corrección de este panel Detalles.

**Deshabilitación de resultados específicos**

Si tiene una necesidad organizativa de omitir un resultado, en lugar de corregirlo, tiene la opción de deshabilitarlo. Los resultados deshabilitados no afectan a la puntuación de seguridad ni generan ruido no deseado.

Cuando un resultado coincide con los criterios que ha definido en las reglas de deshabilitación, no aparecerá en la lista de resultados. Entre los escenarios típicos se incluyen:

* Deshabilitar resultados con gravedad inferior a media
* Deshabilitar resultados que no se pueden revisar
* Deshabilitar resultados con una puntuación de CVSS por debajo de 6,5
* Deshabilitar resultados con texto específico en la categoría o la comprobación de seguridad (por ejemplo, "RedHat", "actualización de seguridad de CentOS para sudo")

**Importante**

*Para crear una regla, necesita permisos para editar directivas en Azure Policy.*

**Para crear una regla**

1. En la página de detalles de recomendaciones de "Las máquinas deberían tener resueltos los hallazgos de vulnerabilidad", seleccione **Deshabilitar regla**.
2. Seleccione el ámbito pertinente.
3. Defina los criterios. Puede utilizar cualquiera de los criterios siguientes:

* Identificador del resultado
* Category
* Comprobación de seguridad
* Puntuaciones de CVSS (v2, v3)
* Gravedad
* Estado revisable

1. Seleccione **Aplicar regla**.

**Importante**

*Los cambios pueden tardar hasta 24 horas en surtir efecto.*

1. Para ver, invalidar o eliminar una regla:

* Seleccione **Deshabilitar regla**.
* En la lista de ámbitos, las suscripciones con reglas activas se muestran como Regla aplicada.
* Para ver o eliminar la regla, seleccione el menú de puntos suspensivos **("...")**.

**Exportación de los resultados**

Para exportar los resultados de la valoración de vulnerabilidades, se debe usar **Azure Resource Graph** (ARG). Esta herramienta proporciona acceso instantáneo a la información de recursos en los entornos de nube con capacidades sólidas para filtrar, agrupar y ordenar. Es una forma rápida y eficaz de consultar información en las suscripciones de Azure mediante programación o desde Azure Portal.

**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 ventaja ofrece Microsoft Defender para Azure SQL Database?**

1. Habilitar el rendimiento de consultas más rápido para todas las bases de datos SQL.
2. Reducir automáticamente el tamaño de las bases de datos para ahorrar costes.
3. Proporcionar alertas de seguridad y detección de amenazas avanzadas para bases de datos.

**2. ¿Cómo se pueden gestionar las alertas de seguridad en Microsoft Defender for Cloud?**

1. A través de la revisión manual y la respuesta a cada alerta individualmente.
2. Usar la automatización del flujo de trabajo para responder ante las amenazas y corregirlas de forma eficaz.
3. Omitir todas las alertas para centrarse en la optimización del rendimiento.

**3. ¿Cómo está configurado Microsoft Defender para servidores a fin de proteger entornos en la nube?**

1. Mediante la aplicación de revisiones a las vulnerabilidades del servidor de forma manual.
2. Usar solo soluciones de firewall externas.
3. Mediante recomendaciones de seguridad automatizadas y características de protección contra amenazas.

**4.¿Cuál es una característica clave de la habilitación de los servicios de protección de cargas de trabajo en Microsoft Defender for Cloud?**

1. Mejorar la seguridad en varios servicios de Azure, como Storage, Databases y Containers.
2. Reducir el coste total de los servicios de Azure.
3. Proporcionar almacenamiento de datos ilimitado para todas las cargas de trabajo.

**5. ¿Cuál es el propósito de los exámenes de vulnerabilidades de Microsoft Defender para servidores?**

1. Para el análisis de publicidad y marketing de los patrones de uso del servidor.
2. Mejorar la interfaz gráfica de las aplicaciones.
3. Identificar y evaluar posibles vulnerabilidades de seguridad en los servidores.
4. C
5. B
6. C
7. A
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.