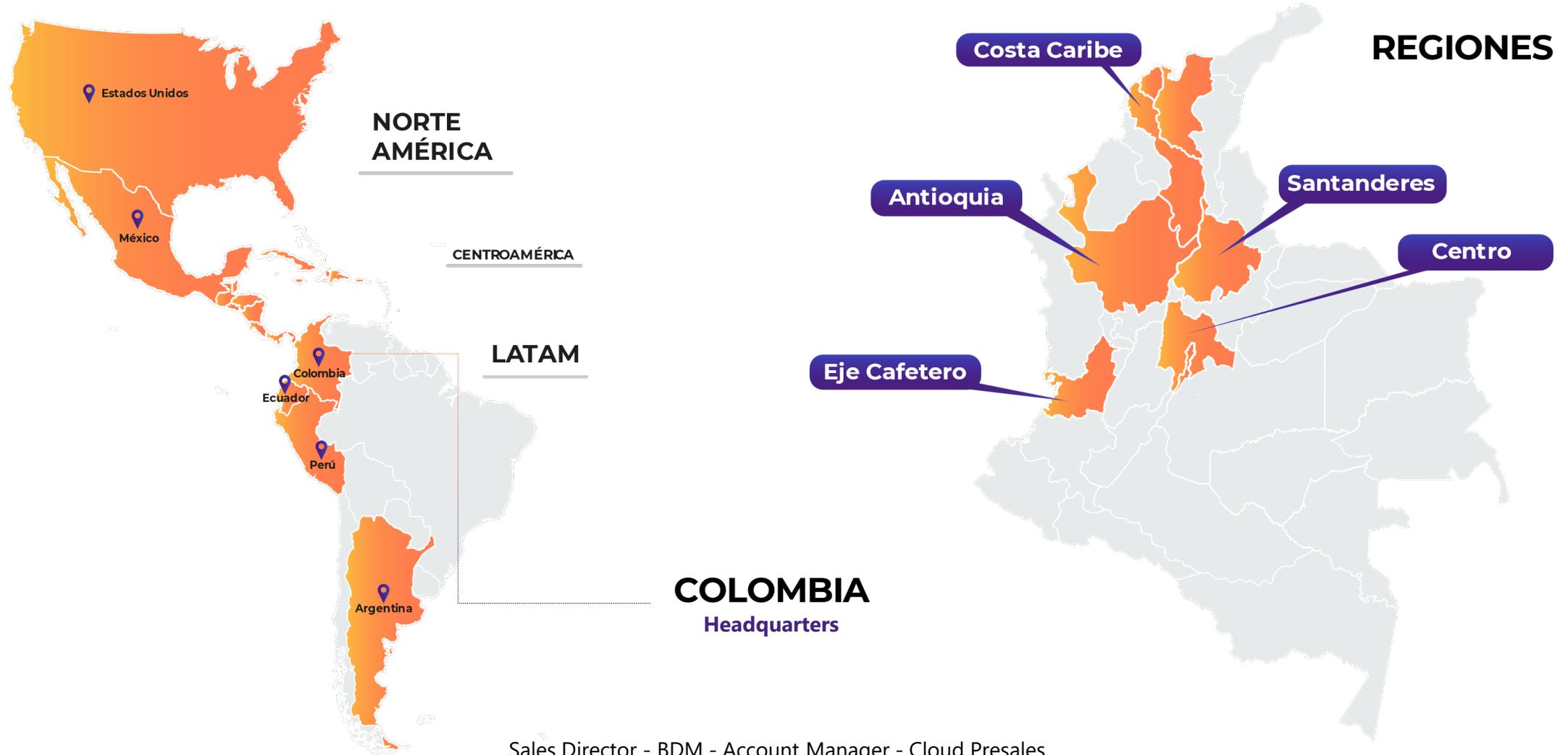


Sentinel



Talento y Cobertura:

60+ especialistas en Cloud, Datos y Analítica, presentes en diversos países: COL, USA, MEX y PERU.



Sales Director - BDM - Account Manager - Cloud Presales

AGENDA

¿Qué es Sentinel ?

- Como funciona
- Características
- Funcionalidades

Microsoft Azure Sentinel



Cloud + Artificial Intelligence

Microsoft Azure Sentinel

Microsoft Sentinel es un sistema SIEM nativo de nube que permite al equipo de operaciones de seguridad hacer lo siguiente:

- Obtener conclusiones de seguridad en toda la empresa mediante la recopilación de datos desde prácticamente cualquier origen.
- Detectar e investigar amenazas rápidamente con el aprendizaje automático integrado y la inteligencia sobre amenazas de Microsoft.
- Automatizar las respuestas a amenazas usando los cuadernos de estrategias e integrando Azure Logic Apps.

Microsoft Sentinel le ayudará a habilitar operaciones de seguridad de un extremo a otro, como las de recopilación, detección, investigación y respuesta.



Microsoft Azure Sentinel

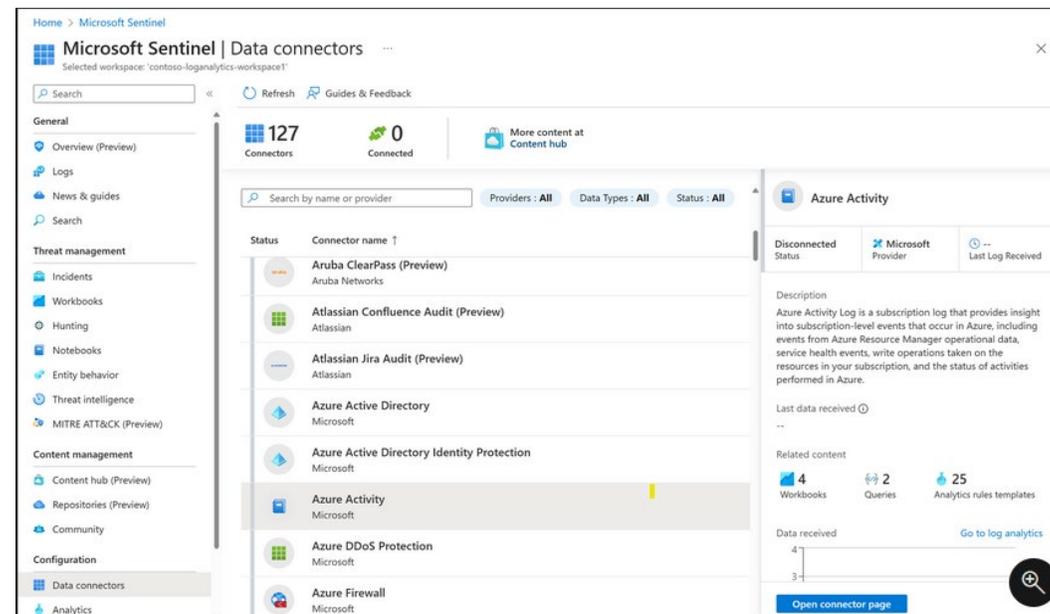
Conectores de datos

Lo primero que se debe hacer es ingerir los datos en Microsoft Sentinel. Los conectores de datos te permiten hacer precisamente eso.

Puede agregar servicios, como registros de actividad de Azure, de forma muy rápida. Otros requieren una ligera labor configuración, como syslog.

Hay conectores de datos que abarcan todos los escenarios y orígenes, incluidos, entre otros, los siguientes:

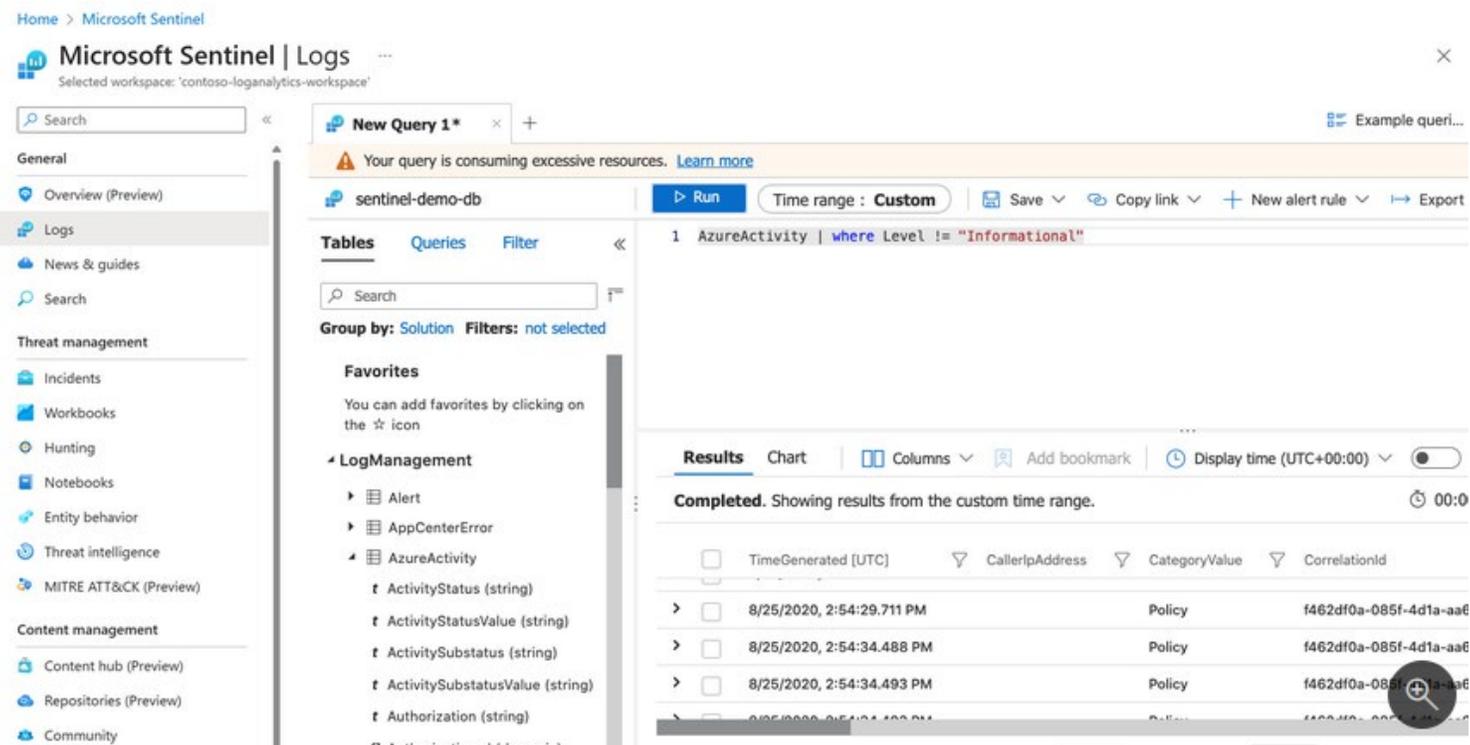
- syslog
- Formato de evento común (CEF)
- Trusted Automated eXchange of Indicator Information (TAXII) (para la inteligencia sobre amenazas)
- Azure
- Servicios de AWS



Microsoft Azure Sentinel

Retención de registros

Una vez que se han ingerido en Microsoft Sentinel, los datos se almacenan mediante Log Analytics. Entre las ventajas de usar Log Analytics se incluye la capacidad de usar el lenguaje de consulta de Kusto (KQL) para consultar los datos. KQL es un lenguaje de consulta enriquecido que ofrece una gran capacidad para profundizar y obtener conclusiones de los datos.



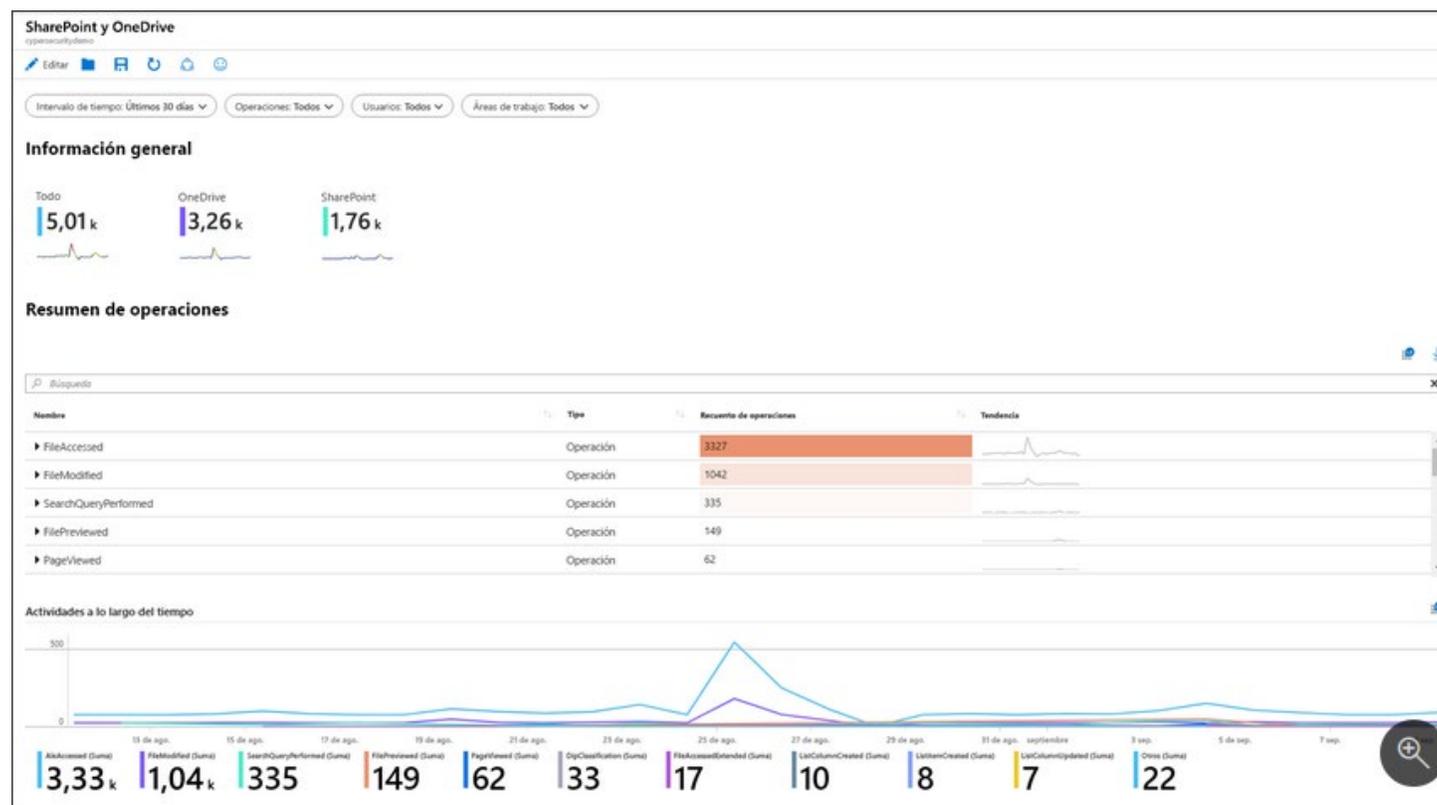
The screenshot displays the Microsoft Sentinel Logs interface. The left sidebar contains navigation options such as Overview, Logs, Threat management, and Content management. The main area shows a query editor with a KQL query: `1 AzureActivity | where Level != "Informational"`. The results table shows the following data:

TimeGenerated [UTC]	CallerIpAddress	CategoryValue	CorrelationId
8/25/2020, 2:54:29.711 PM		Policy	f462df0a-085f-4d1a-aa6
8/25/2020, 2:54:34.488 PM		Policy	f462df0a-085f-4d1a-aa6
8/25/2020, 2:54:34.493 PM		Policy	f462df0a-085f-4d1a-aa6

Microsoft Azure Sentinel

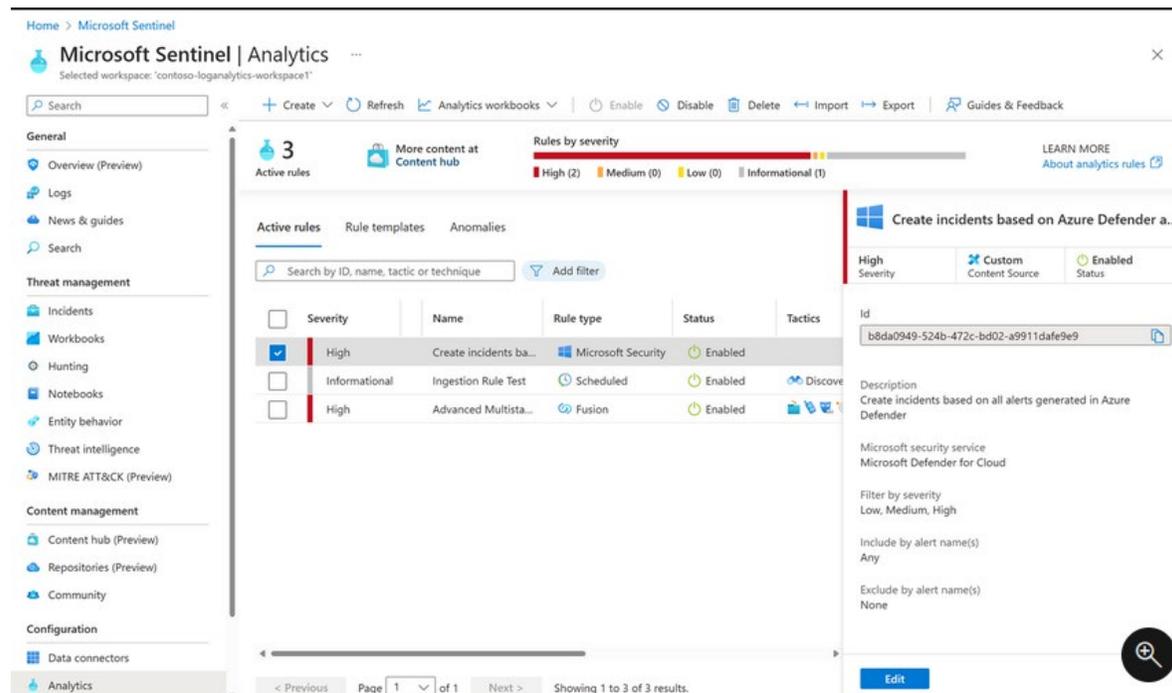
Workbooks

Puede usar libros para visualizar los datos en Microsoft Sentinel. Los libros son similares a los paneles o Dashboard. Cada componente de ellos se genera mediante una consulta KQL subyacente de los datos. Puede usar los libros integrados en Microsoft Sentinel y editarlos para ajustarlos a necesidades propias, o bien crear libros propios desde cero.



Alertas y análisis

Ahora Sentinel dispone de análisis proactivos de los datos, para que reciba una notificación cuando se produzca algo sospechoso. Puede habilitar las alertas de análisis integradas en el área de trabajo de Sentinel. Existen varios tipos de alertas, algunas de las cuales puede editar según sus necesidades. Otras alertas se basan en modelos de aprendizaje automático que son propiedad de Microsoft. También puede crear alertas programadas personalizadas desde cero.



The screenshot displays the Microsoft Sentinel Analytics interface. The top navigation bar shows 'Home > Microsoft Sentinel' and 'Microsoft Sentinel | Analytics'. Below this, there's a search bar and a toolbar with options like '+ Create', 'Refresh', 'Analytics workbooks', 'Enable', 'Disable', 'Delete', 'Import', 'Export', and 'Guides & Feedback'. The main content area is divided into a left sidebar with navigation options (General, Threat management, Content management, Configuration) and a central pane. The central pane shows 'Active rules' with a 'Rules by severity' bar indicating 2 High, 0 Medium, 0 Low, and 1 Informational rules. A table lists the active rules:

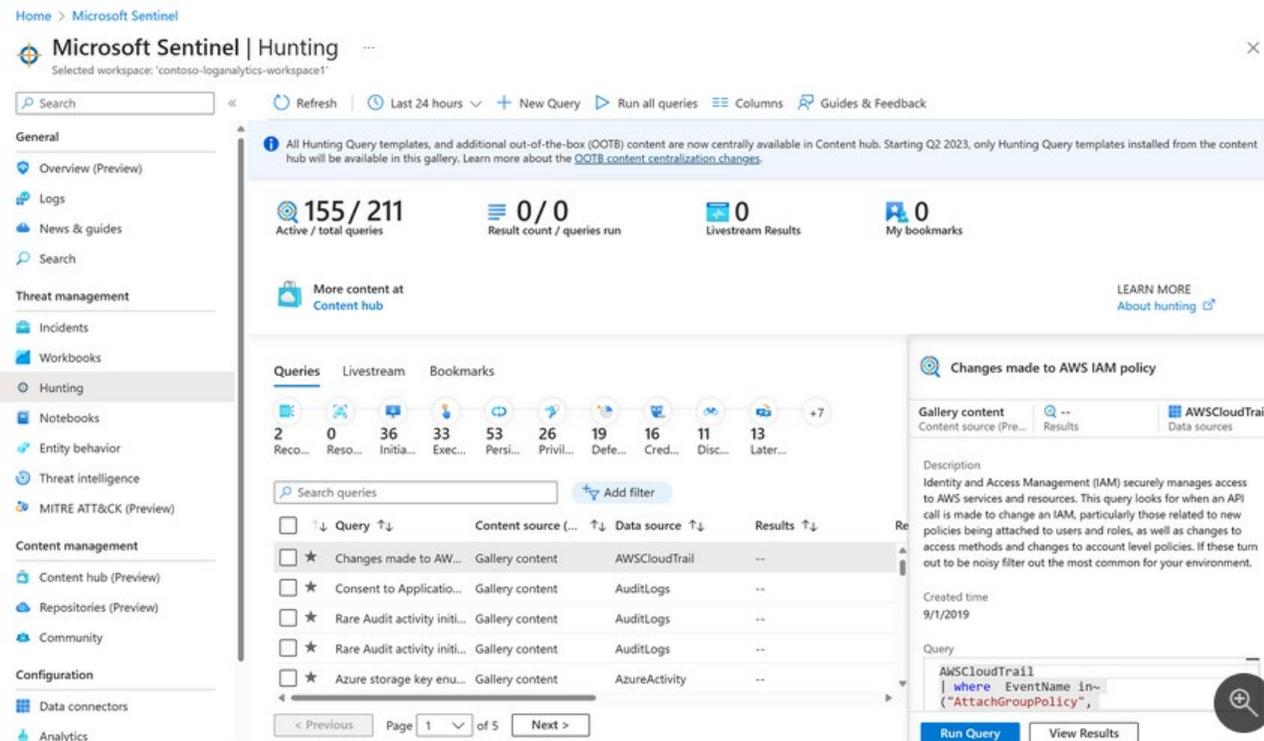
Severity	Name	Rule type	Status	Tactics	
<input checked="" type="checkbox"/>	High	Create incidents ba...	Microsoft Security	Enabled	
<input type="checkbox"/>	Informational	Ingestion Rule Test	Scheduled	Enabled	Discover
<input type="checkbox"/>	High	Advanced Multista...	Fusion	Enabled	Discover, Investigate, Mitigate

On the right, a configuration panel for the selected rule 'Create incidents based on Azure Defender a...' is visible. It shows settings for Severity (High), Content Source (Custom), and Status (Enabled). The ID is 'b8da0949-524b-472c-bd02-a9911d4fe9e9'. The description is 'Create incidents based on all alerts generated in Azure Defender'. The filter by severity is set to 'Low, Medium, High'. The include and exclude by alert name(s) are set to 'Any' and 'None' respectively. An 'Edit' button is at the bottom of the panel.

Microsoft Azure Sentinel

Búsqueda de amenazas

Si los analistas de SOC necesitan buscar actividades sospechosas, hay algunas consultas de búsqueda integradas que pueden usar. Los analistas también pueden crear sus propias consultas. Sentinel también se integra con Azure Notebooks. Esta solución proporciona cuadernos de ejemplo para investigadores expertos que deseen usar toda la potencia de un lenguaje de programación para buscar en sus datos.

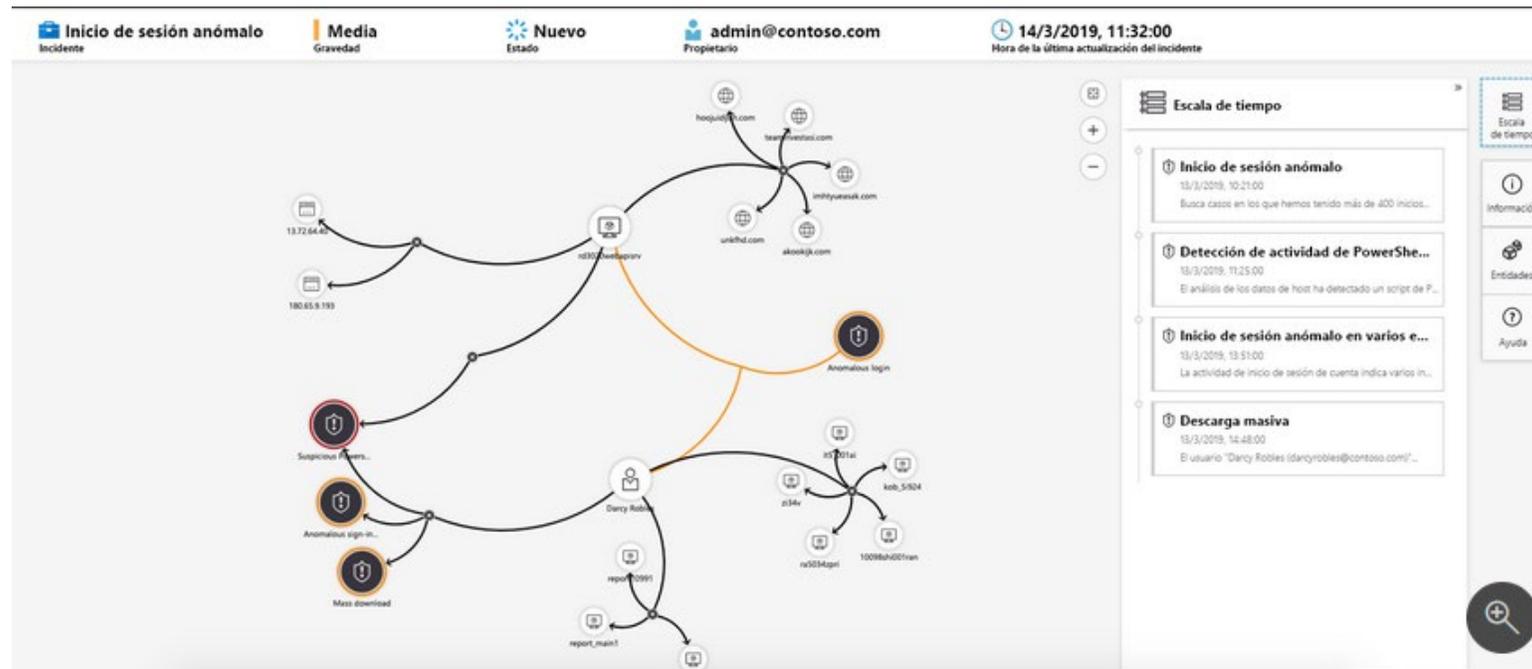


The screenshot displays the Microsoft Sentinel Hunting interface. The top navigation bar includes 'Home > Microsoft Sentinel' and 'Microsoft Sentinel | Hunting'. Below this, there's a search bar and navigation options like 'Refresh', 'Last 24 hours', 'New Query', 'Run all queries', 'Columns', and 'Guides & Feedback'. A notification banner states: 'All Hunting Query templates, and additional out-of-the-box (OOTB) content are now centrally available in Content hub. Starting Q2 2023, only Hunting Query templates installed from the content hub will be available in this gallery. Learn more about the OOTB content centralization changes.' The main dashboard shows statistics: '155 / 211 Active / total queries', '0 / 0 Result count / queries run', '0 Livestream Results', and '0 My bookmarks'. A 'More content at Content hub' link is present. Below, there's a 'Queries' section with a table of query templates. The table has columns for 'Query', 'Content source', 'Data source', and 'Results'. The first query is 'Changes made to AWS IAM policy' from 'Gallery content' using 'AWSCloudTrail' as the data source. A detailed view of this query is shown on the right, including its description, created time (9/1/2019), and the query text: 'AWSCloudTrail | where EventName in~ ("AttachGroupPolicy",'. The interface also includes a sidebar with navigation options like 'Overview', 'Logs', 'Threat management', and 'Configuration'.

Query	Content source	Data source	Results
Changes made to AWS IAM policy	Gallery content	AWSCloudTrail	--
Consent to Application...	Gallery content	AuditLogs	--
Rare Audit activity initi...	Gallery content	AuditLogs	--
Rare Audit activity initi...	Gallery content	AuditLogs	--
Azure storage key enu...	Gallery content	AzureActivity	--

Incidentes e investigaciones

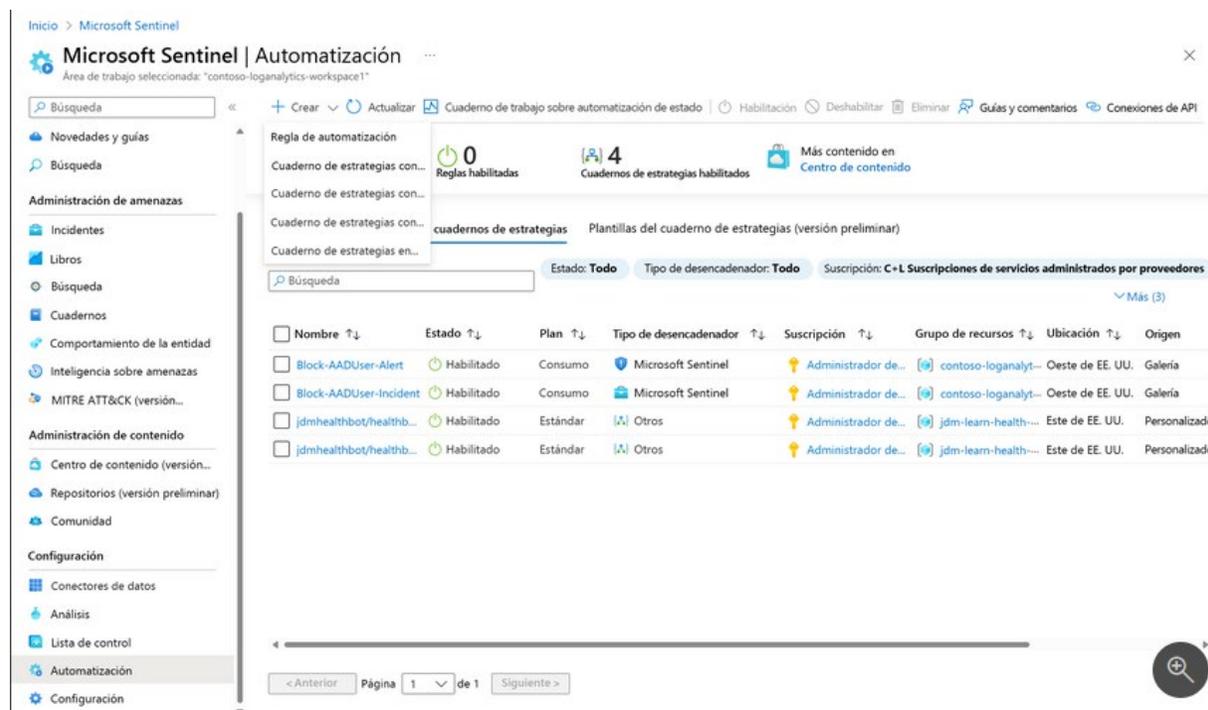
Cuando se desencadena una alerta que ha habilitado, se crea un incidente. En Microsoft Sentinel, puede realizar tareas de administración de incidentes estándar como cambiar el estado o asignar incidentes a individuos para su investigación. Microsoft Sentinel también tiene una funcionalidad de investigación que le permite investigar los incidentes visualmente mediante la asignación de entidades en los datos de registro a lo largo de una escala de tiempo.



Microsoft Azure Sentinel

Cuadernos de estrategias de automatización

Poder responder a los incidentes de forma automática permite automatizar algunas de las operaciones de seguridad y aumentar la productividad de los SOC. Microsoft Sentinel le permite crear flujos de trabajo automatizados, o *cuadernos de estrategias*, en respuesta a eventos. Esta funcionalidad se podría usar para realizar tareas de administración de incidentes, enriquecimiento, investigación o corrección. Estas labores suelen denominarse *orquestración de seguridad, automatización y respuesta (SOAR)*.



Microsoft Sentinel | Automatización

Área de trabajo seleccionada: "contoso-loganalytics-workspace1"

Regla de automatización

Cuaderno de estrategias con... 0 Reglas habilitadas 4 Cuadernos de estrategias habilitados Más contenido en Centro de contenido

Cuaderno de estrategias con...

Cuaderno de estrategias con...

Cuaderno de estrategias con...

Cuaderno de estrategias en...

cuadernos de estrategias Plantillas del cuaderno de estrategias (versión preliminar)

Cuaderno de estrategias en...

Estado: Todo Tipo de desencadenador: Todo Suscripción: C=L Suscripciones de servicios administrados por proveedores

Nombre	Estado	Plan	Tipo de desencadenador	Suscripción	Grupo de recursos	Ubicación	Origen
Block-AADUser-Alert	Habilitado	Consumo	Microsoft Sentinel	Administrador de...	contoso-loganalyt--	Oeste de EE. UU.	Galería
Block-AADUser-Incident	Habilitado	Consumo	Microsoft Sentinel	Administrador de...	contoso-loganalyt--	Oeste de EE. UU.	Galería
jdmhealthbot/healthb...	Habilitado	Estándar	Otros	Administrador de...	jdm-learn-health...	Este de EE. UU.	Personalizado
jdmhealthbot/healthb...	Habilitado	Estándar	Otros	Administrador de...	jdm-learn-health...	Este de EE. UU.	Personalizado

< Anterior Página 1 de 1 Siguiente >

¡Gracias!

