GoToCloud
www.gotocloud.com.co

Sentinel

Talento y Cobertura:

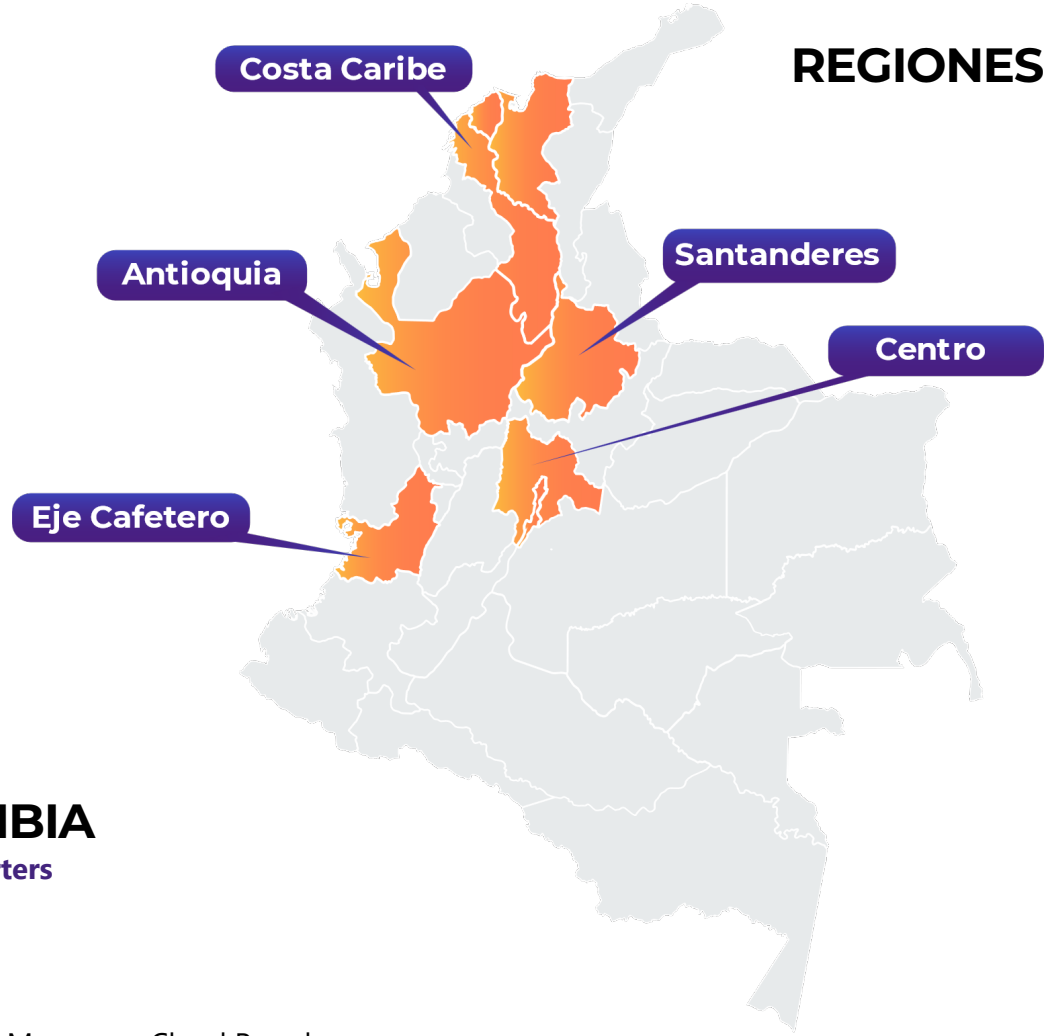
60+ especialistas en Cloud, Datos y Analítica, presentes en diversos países: COL, USA, MEX y PERU.

NORTE AMÉRICA

CENTROAMÉRICA

LATAM

COLOMBIA
Headquarters



REGIONES

Sales Director - BDM - Account Manager - Cloud Presales

Microsoft Sentinel

¿Qué es Sentinel ?

- Como funciona
- Características
- Funcionalidades

Microsoft Azure Sentinel

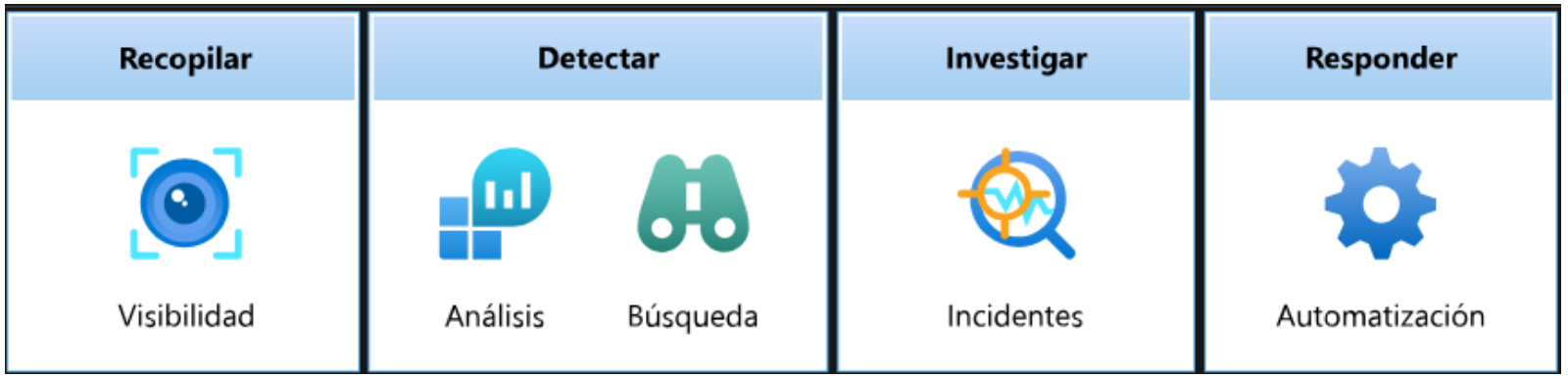
GoToCloud
www.gotocloud.com.co

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.



GoToCloud
www.gotocloud.com.co

Microsoft Azure Sentinel

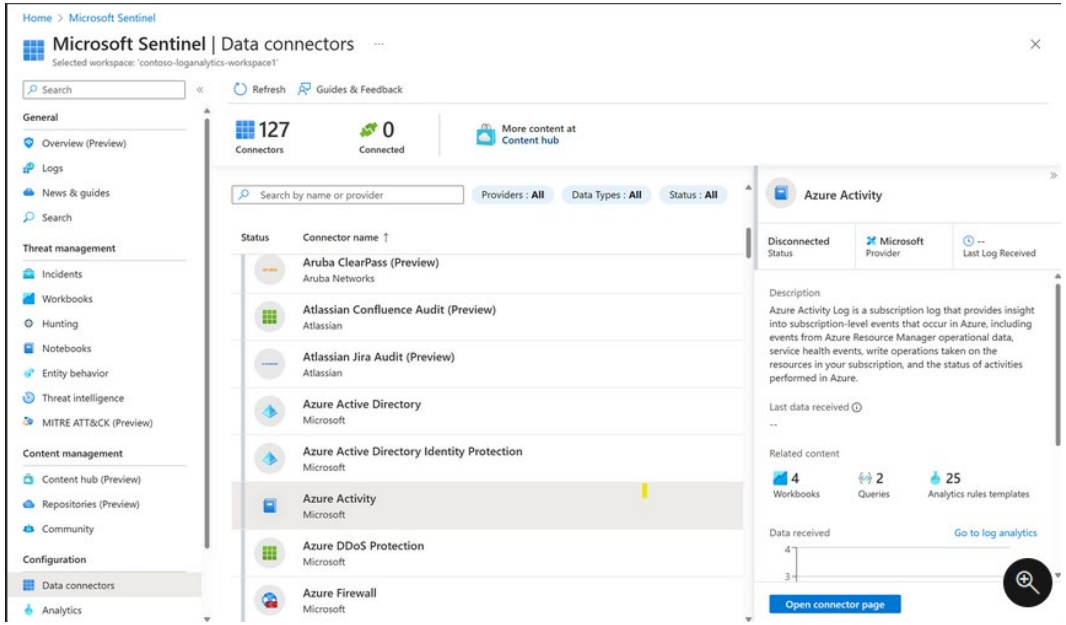
Conectores de datos

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 rapida.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



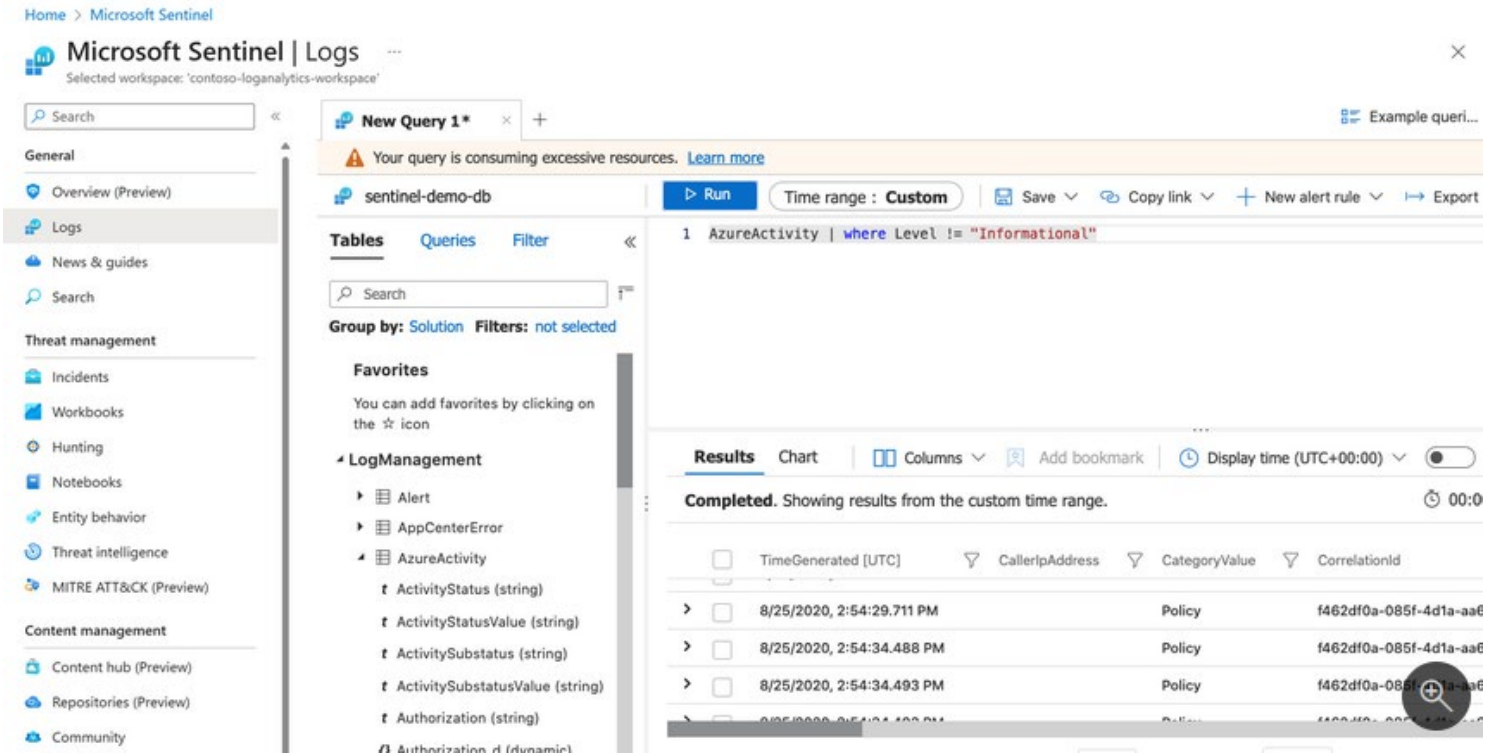
GoToCloud
www.gotocloud.com.co

Microsoft Azure Sentinel

Microsoft 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.



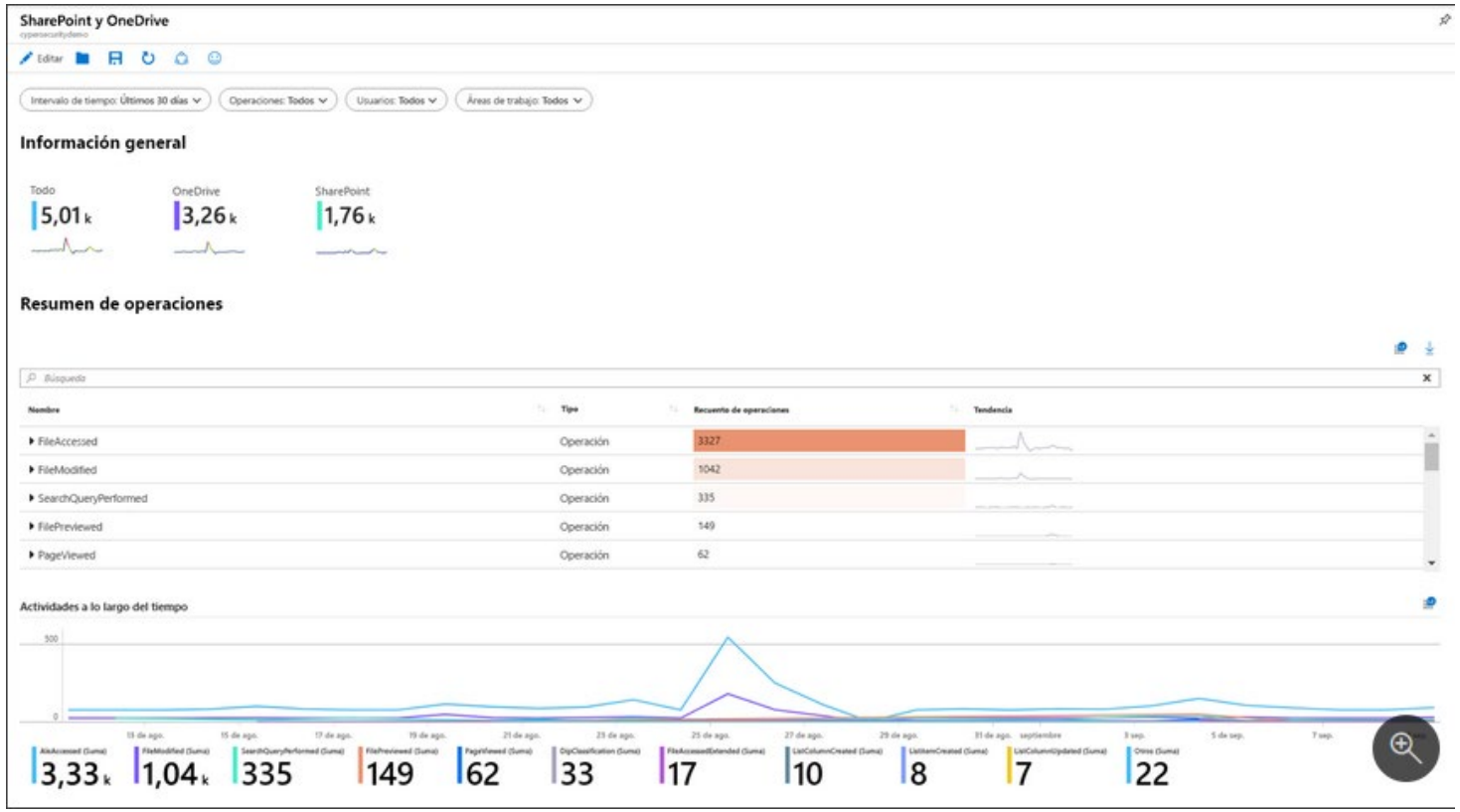
GoToCloud
www.gotocloud.com.co

Microsoft Azure Sentinel

Microsoft 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.



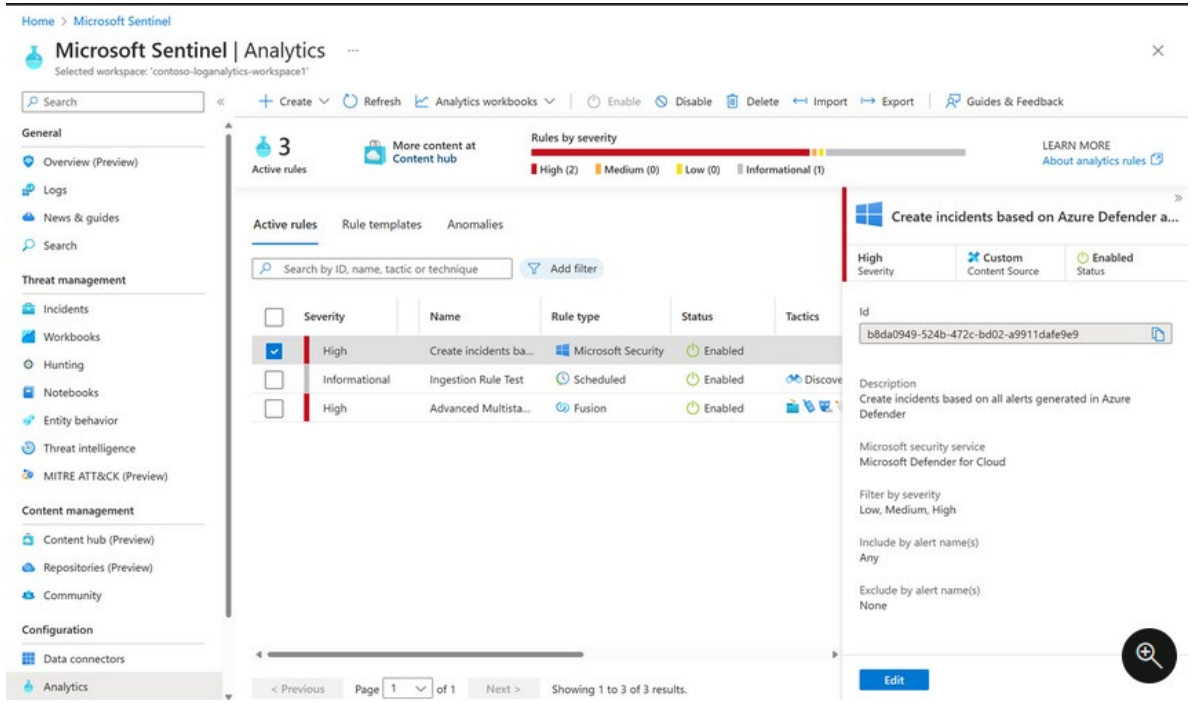
GoToCloud
www.gotocloud.com.co

Microsoft Azure Sentinel

Microsoft Sentinel

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.



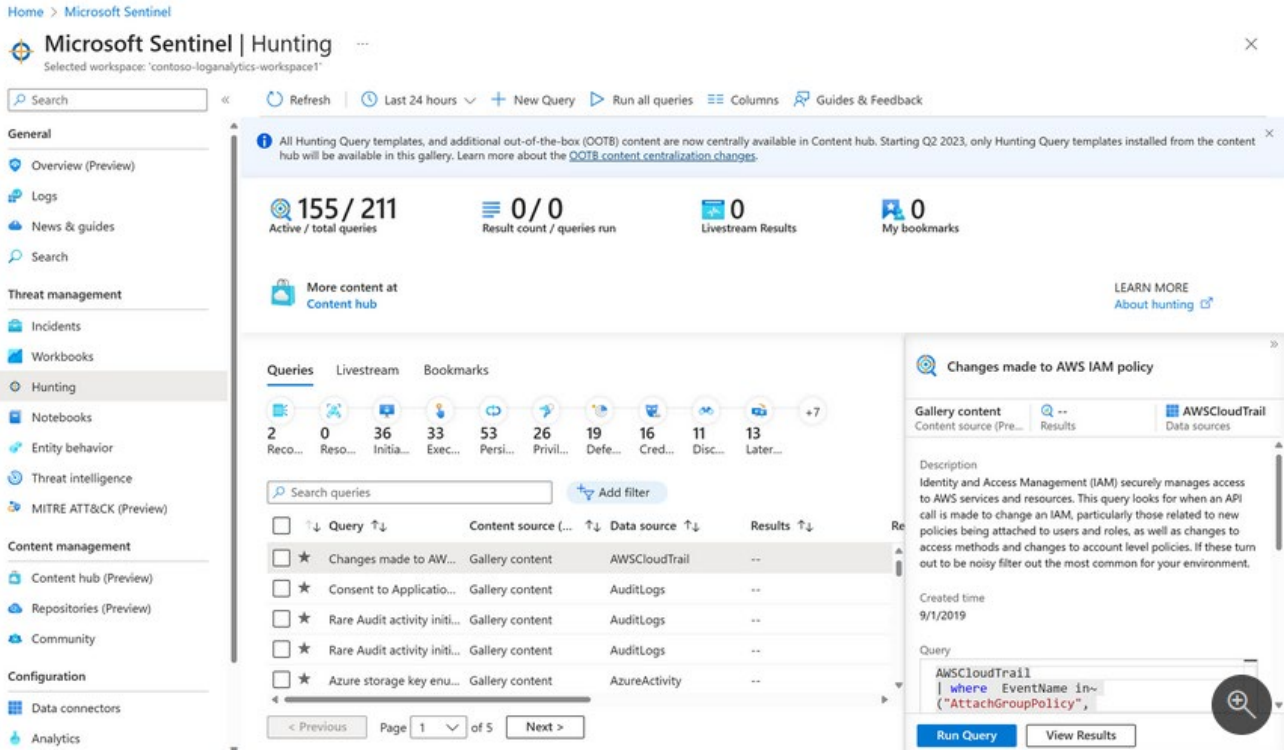
GoToCloud
www.gotocloud.com.co

Microsoft Azure Sentinel

Microsoft 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.



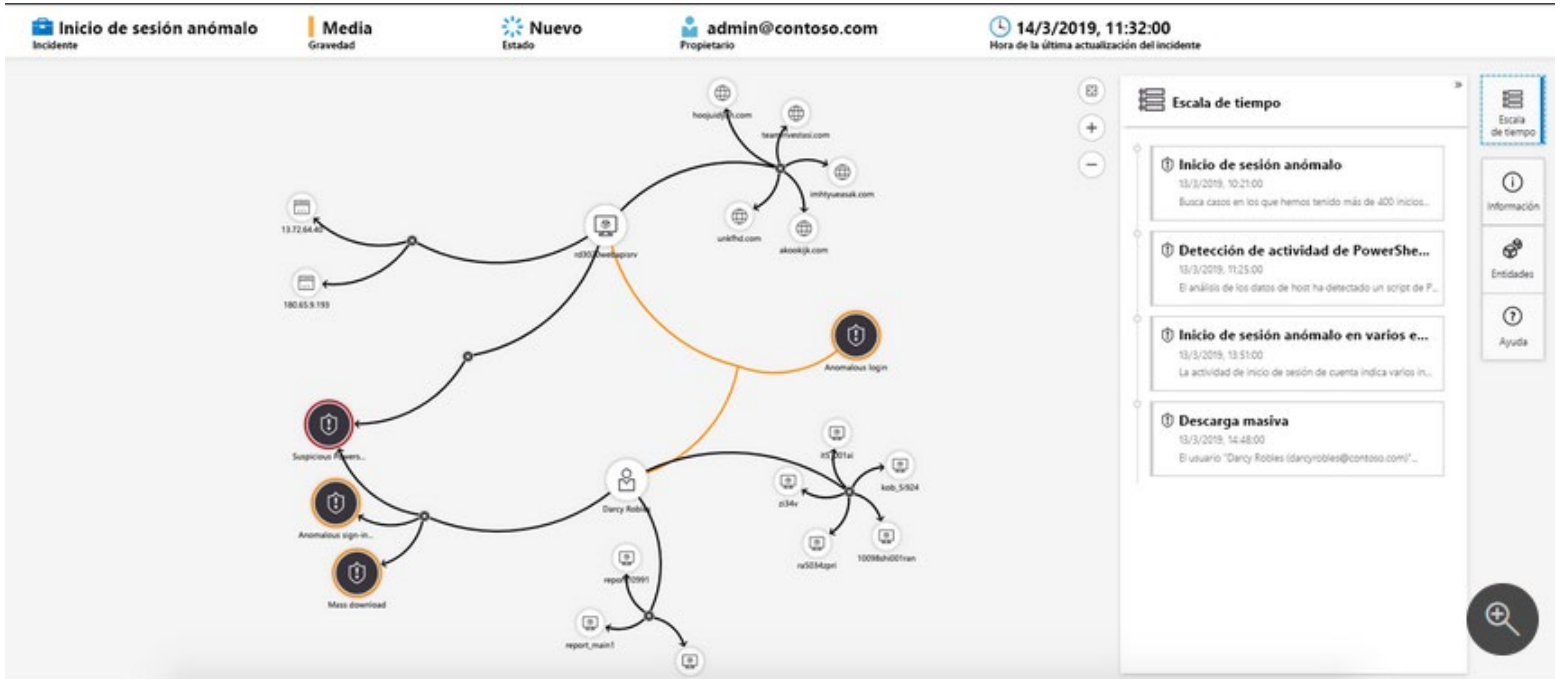
GoToCloud
www.gotocloud.com.co

Microsoft Azure Sentinel

Microsoft Sentinel

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.



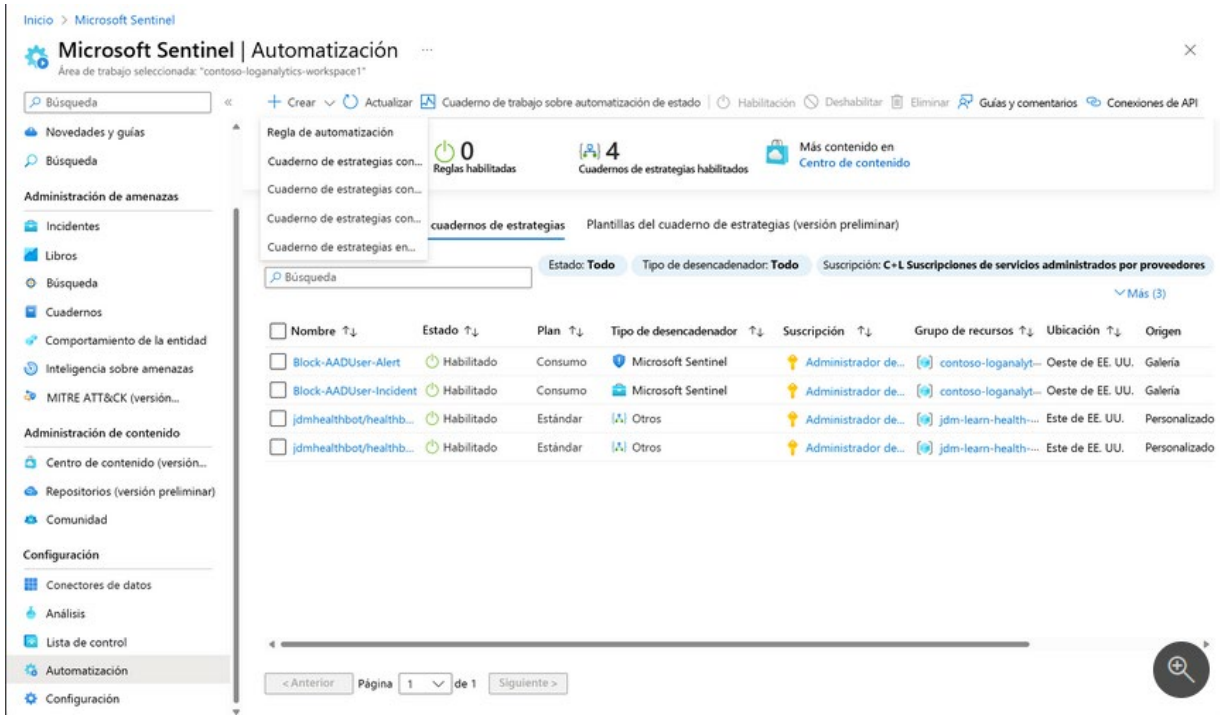
GoToCloud
www.gotocloud.com.co

Microsoft Azure Sentinel

Microsoft 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 *orquestación de seguridad, automatización y respuesta (SOAR)*.



GoToCloud
www.gotocloud.com.co

GoToCloud
www.gotocloud.com.co

@GoToCloudSAS

¡Gracias!

Comercial: comercial@gotocloud.com.co
Información General: info@gotocloud.com.co