Creación de libros para explorar datos de Sentinel

Después de que haya conectado los orígenes de datos a Microsoft Sentinel, puede supervisar los datos mediante la integración de Microsoft Sentinel con los libros de Azure Monitor, lo que proporciona versatilidad al crear libros personalizados. Aunque los libros se muestran de forma diferente en Microsoft Sentinel, puede resultar útil determinar cómo crear informes interactivos con los libros de Azure Monitor. Microsoft Sentinel permite crear libros personalizados en los datos y también incluye plantillas de libro integradas que permiten obtener información rápidamente en los datos en cuanto se conecta con un origen de datos.

Los libros combinan texto, consultas de análisis, métricas de Azure y parámetros en informes interactivos enriquecidos. Otros miembros del equipo que tienen acceso a los mismos recursos de Azure pueden editar los libros.

Los libros son útiles en escenarios como:

- Exploración del uso de la aplicación cuando no conoce de antemano las métricas de interés: número de usuarios, tasas de retención, tasas de conversión, etc. A diferencia de otras herramientas de análisis de uso, los libros le permiten combinar varios tipos de visualizaciones y análisis, lo que los hace idóneos para este tipo de exploración de forma libre.
- A la hora de explicar al equipo el rendimiento de una característica recientemente publicada, mostrando recuentos de usuarios para las interacciones principales y otras métricas.
- Uso compartido de los resultados de un experimento A o B de la aplicación con otros miembros del equipo. Puede explicar los objetivos del experimento con texto y luego mostrar cada métrica de uso y la consulta de Analytics que se usa para evaluar el experimento, junto con indicadores claros sobre si cada métrica está por encima o por debajo del objetivo.
- Notificación del impacto de una interrupción del servicio en el uso de la aplicación, combinación de datos, explicación del texto y análisis de los pasos siguientes para evitar más interrupciones en el futuro.

Almacenamiento y uso compartido de libros con el equipo

Los libros se guardan en un recurso de Application Insights, ya sea en la sección Mis informes que es privada para usted o en la sección Informes compartidos accesible para todos los usuarios con acceso al recurso Application Insights. Un libro se puede compartir con un vínculo o por correo electrónico. Tenga en cuenta que los destinatarios del vínculo necesitarán acceder a este recurso en Azure Portal para ver el libro. Para realizar ediciones, los destinatarios necesitan al menos permisos de colaborador para el recurso.

Análisis

Para reducir el ruido y minimizar el número de alertas que tiene que revisar e investigar, Microsoft Azure Sentinel usa análisis para correlacionar las alertas con los incidentes. Los incidentes son

grupos de alertas relacionadas que crean conjuntamente una amenaza procesable que se puede investigar y resolver. Use las reglas de correlación integrada tal cual, o úselas como punto de partida para crear las suyas propias. Microsoft Azure Sentinel también proporciona reglas de aprendizaje automático para asignar el comportamiento de red y buscar luego anomalías en los recursos. Estos análisis conectan los puntos mediante la combinación de alertas de baja fidelidad sobre diferentes entidades en posibles incidentes de seguridad de alta fidelidad.