Synack

Member of Microsoft Intelligent Security Association

Microsoft

La integración de Synack con Microsoft Sentinel acelera la gestión de las vulnerabilidades de seguridad

Resumen

Microsoft Sentinel es una solución única, expansible y nativa de la nube para el análisis de seguridad inteligente, la gestión de eventos, la detección de amenazas, la visibilidad de las mismas, la caza proactiva y la respuesta a las amenazas.
Ayuda a proporcionar una detección temprana de las amenazas y una respuesta rápida a los ataques sofisticados para reducir los tiempos de resolución y el volumen de incidentes de seguridad en sus activos en la nube de Microsoft Azure. Para reducir aún más los tiempos de reparación y resolución, Synack ofrece ahora una integración directa con Microsoft Sentinel que permite generar automáticamente incidentes de Microsoft Sentinel a partir de los datos de las pruebas de vulnerabilidad de Synack.

- Proteja su nube de Microsoft Azure sincronizando los resultados de las pruebas de vulnerabilidad de Synack con Microsoft Sentinel
- Las nuevas vulnerabilidades encontradas generan automáticamente incidentes en Microsoft Sentinel para poder realizar un rápido análisis y llevar a cabo su corrección
- Su fácil integración y configuración le permiten empezar a trabajar rápidamente
- Consulte y gestione los incidentes en las pantallas habituales de Microsoft Sentinel

Synack y Microsoft Sentinel colaboran para acelerar el tiempo de resolución

Microsoft Sentinel combina dos tecnologías de seguridad en una sola solución: la gestión de eventos e información de seguridad (SIEM) y la orquestación, automatización y respuesta de seguridad (SOAR). Incorpora diferentes fuentes de datos de toda la empresa y realiza una correlación de los mismos entre estas fuentes, aprovechando los análisis de seguridad inteligentes y la inteligencia de amenazas. Con Microsoft Sentinel, las operaciones de seguridad pueden:

- Recibir alertas en tiempo real
- Solucionar incidentes utilizando el aprendizaje automático y la inteligencia artificial (IA) para detectar, analizar e identificar las amenazas
- Llevar a cabo una caza proactiva

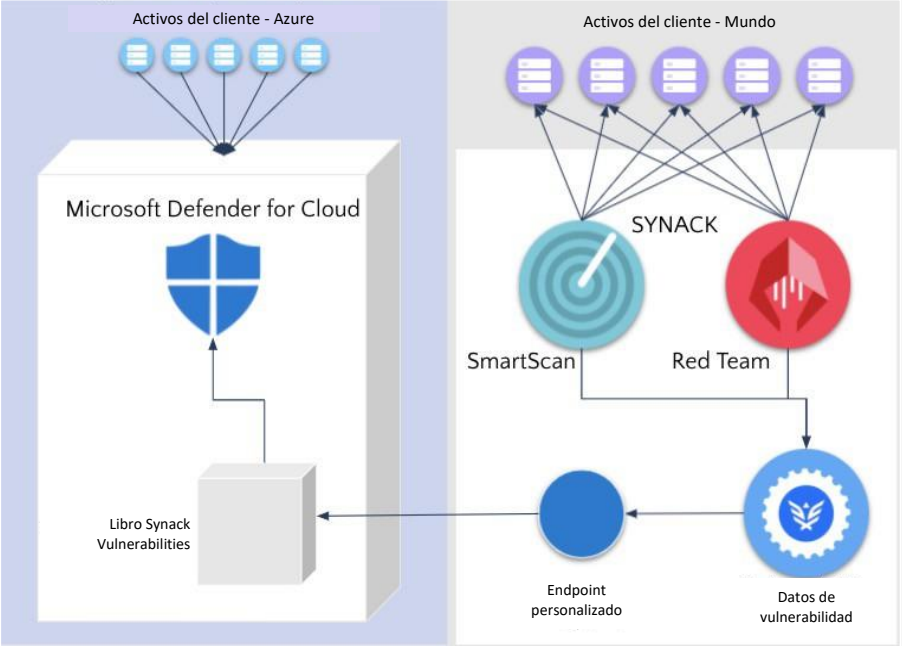
Esto proporciona a los equipos de seguridad una visibilidad integral de los eventos relacionados con la seguridad y les ayuda a obtener información directa y a analizar las capacidades, todo en un solo lugar. Microsoft Sentinel puede explorar e intentar hacer frente a posibles amenazas en la nube por sí mismo o puede alertarle de las mismas.

La rápida gestión y corrección de las posibles vulnerabilidades es la clave para minimizar las amenazas en su nube. Synack cuenta con el equipo de pruebas de penetración más cualificado y fiable del mundo, junto con una tecnología de IA propia, para descubrir vulnerabilidades constantemente o en un momento puntual. La solución Microsoft Sentinel de Synack ayuda a reducir los tiempos de resolución al sincronizar estos resultados con Microsoft Sentinel.

La solución Microsoft Sentinel de Synack proporciona un conector de datos para sincronizar los datos de vulnerabilidad de su cuenta de Synack con Microsoft Sentinel. Genera un incidente en Microsoft Sentinel para cada vulnerabilidad y mantiene los datos del incidente actualizados con los últimos cambios en la vulnerabilidad. No es necesaria la intervención humana para introducir la información sobre la vulnerabilidad en Microsoft Sentinel. Así, Microsoft Sentinel puede utilizar la información de Synack de esos incidentes en el análisis de amenazas y su procesamiento. Además, puede gestionarlo todo en el entorno de Microsoft Sentinel con el que ya está familiarizado.

Integración sencilla

La sincronización de los datos se lleva a cabo mediante una función de Microsoft Azure que utiliza las API de Synack y de Microsoft Sentinel para transferir los datos de Synack a Microsoft Sentinel. La solución Microsoft Sentinel de Synack está disponible en el portal de Microsoft Azure en el *marketplace* de Visual Studio. Una vez instalado correctamente el recopilador de datos de Microsoft Sentinel, la sincronización se iniciará automáticamente. No es necesario realizar ninguna otra configuración en el portal de Microsoft Azure o Synack. Siempre que todos los parámetros introducidos durante el despliegue del conector de datos sean correctos, debería empezar a ver nuevos incidentes generados en Microsoft Sentinel de las vulnerabilidades de Synack. También puede comprobar los registros de la función de Microsoft Azure implementada.



La pantalla de incidentes de Microsoft Sentinel que muestran las vulnerabilidades de Synack

Cada vulnerabilidad de Synack generará un nuevo incidente en Microsoft Sentinel. Los valores de los campos de Synack se introducen en la descripción del campo en el incidente de Microsoft Azure. Si la situación de una vulnerabilidad de Synack cambia, el estado del correspondiente incidente de Microsoft Sentinel se actualiza en consecuencia en la siguiente sincronización. En Microsoft Sentinel, los incidentes presentan uno de estos tres estados: Nuevo, Activo, Cerrado. Este conjunto de estados en Microsoft Sentinel es fijo y no se puede configurar. En Synack, puede disponer de diversos estados. Sin embargo, cada uno de ellos pertenece a alguna de las 3 grandes categorías: Nuevo, Abierto, Cerrado.