Synack

Member of Microsoft Intelligent Security Association

Microsoft

Gestione los resultados de las pruebas de penetración desde Microsoft Defender for Cloud

Synack y Microsoft Defender for Cloud: una potente colaboración para la seguridad

Mantener su nube híbrida a salvo de los ciberdelincuentes es una tarea abrumadora. Los *hackers* buscan constantemente vulnerabilidades en los activos alojados en la nube que puedan aprovechar para acceder a los sistemas principales. Microsoft Defender for Cloud ayuda a proteger contra las amenazas, proporcionando herramientas para gestionar la política de seguridad y el cumplimiento de su empresa. Permite supervisar las configuraciones erróneas y las vulnerabilidades conocidas, ofreciendo a los ingenieros y gestores de seguridad una visión en tiempo real del estado de seguridad de la nube de Microsoft Azure en paneles fáciles de ver.

Pero hay una pieza importante que falta en esta visión de la seguridad. Tiene que ser capaz de validar esas malas configuraciones y crear vectores de ataque para buscar e informar de las vulnerabilidades en la capa de red, así como internamente en su entorno en la nube. Synack, con el equipo de pruebas de penetración de origen colectivo más capacitado y fiable del mundo, y la tecnología de IA patentada, puede realizar una prueba de penetración e informar de los resultados a Microsoft Defender for Cloud, desde donde se pueden investigar y resolver las vulnerabilidades.

Como parte de la asociación global de Microsoft y Synack, los resultados de su evaluación de Synack se introducen automáticamente en Microsoft Defender for Cloud a través de una de nuestras sencillas actualizaciones de la plataforma de Microsoft.

- Integre los datos de las vulnerabilidades descubiertas por Synack en su cuenta de Microsoft Defender for Cloud para agilizar los procesos de gestión de vulnerabilidades.
- Ayude a proteger su entorno dinámico en la nube con las pruebas de penetración de Synack y las pruebas continuas a través de la integración de Microsoft Azure.
- Envíe automáticamente los resultados de la evaluación de Synack a Microsoft Defender for Cloud a través de nuestra sencilla integración.
- Consulte y gestione el estado de las vulnerabilidades de su red en las pantallas habituales de Microsoft Defender for Cloud.

Optimización de la gestión de vulnerabilidades en Microsoft Azure

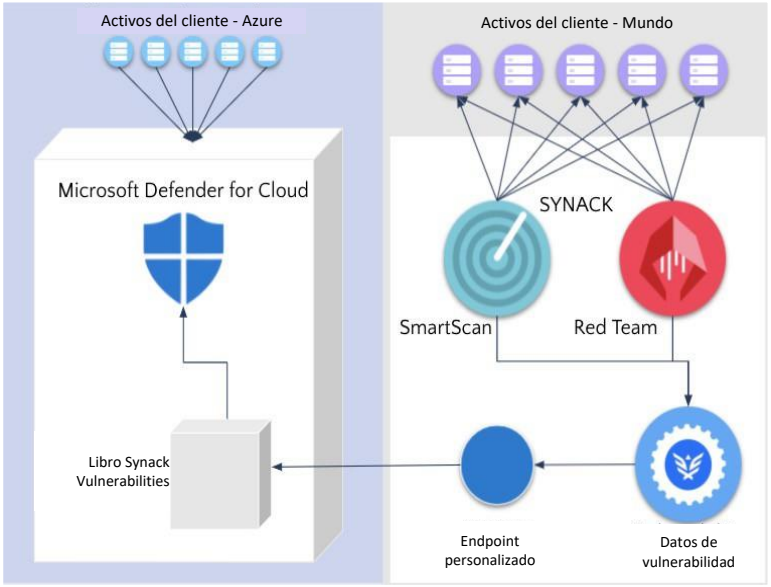
A través de la integración de Synack con Microsoft Defender for Cloud, puede hacer que los resultados de su prueba de penetración de Synack se envíen automáticamente y se muestren en un libro personalizado de Microsoft Defender for Cloud. Esto significa que los ingenieros y gestores de seguridad que ya están familiarizados con los paneles y pantallas de Microsoft Defender for Cloud no tienen que aprender el formato de visualización de otra herramienta para ver y actuar sobre la información de vulnerabilidad.

Integración

Synack proporciona un libro personalizado de Microsoft Azure con datos de vulnerabilidad de Synack dentro de su Microsoft Defender for Cloud. Una aplicación *backend* alojada por Synack proporciona un *endpoint* para el libro. Synack proporciona la plantilla por defecto para el libro Synack Vulnerabilities, permitiendo al usuario final modificar aún más el aspecto del mismo o utilizar el *endpoint* para crear nuevos libros.

Synack hace que la integración sea simple.

Para desplegar la plantilla Synack Workbook ARM (Microsoft Azure Resource Manager) con Microsoft Defender for Cloud es necesario crear primero un *token* de la API de Synack.



El libro estará disponible en Microsoft Defender for Cloud. Cada vez que Synack realice una prueba de penetración, los resultados se mostrarán en el libro de Microsoft Defender for Cloud.

Más del 90 % de los problemas de seguridad en la nube provienen directamente de una mala configuración.

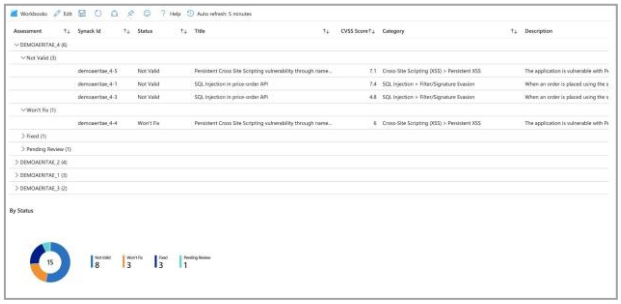
Ver los resultados de la evaluación de Synack en Microsoft Defender for Cloud

Más del 90 % de los problemas de seguridad en la nube provienen directamente de una mala configuración.[1] Synack le ayuda a descubrir las posibles vulnerabilidades que pueden derivarse de estas malas configuraciones.
Las vulnerabilidades de autenticación de la sesión, incluidas las credenciales predeterminadas, el contenido del directorio y la inyección de código, constituyen el 40 % de los *exploits* en la nube notificados por Synack. Ahora puede consultar y gestionar estas vulnerabilidades directamente en Microsoft Defender for Cloud.

Con esta integración, los clientes pueden sincronizar automáticamente sus datos del Portal de clientes de Synack con Microsoft Defender for Cloud. Toda la información sobre vulnerabilidades se centraliza y se aprovechan los formatos más utilizados por los usuarios de Microsoft Azure, lo que permite a los ingenieros y gestores de seguridad supervisar eficazmente la situación general de la seguridad de la red.

Synack calcula manualmente y asigna a cada vulnerabilidad descubierta una puntuación CVSS como parte de la rigurosa revisión de garantía de calidad incluida en cada evaluación. Cualquier vulnerabilidad identificada se muestra en el libro de Microsoft Defender for Cloud. Los equipos de seguridad pueden ver el estado de la vulnerabilidad en el libro y tomar las medidas adecuadas.
Los usuarios autorizados pueden solicitar información adicional sobre cualquier vulnerabilidad identificada y ponerla a su disposición en el Portal de clientes de Synack.

Lista de vulnerabilidades en el libro de Microsoft Defender for Cloud



1. XM Cyber, "What is Cloud Security Posture Management," 2021, https://www.xmcyber.com/what-is-cloud-security-posture-management/