



CASO PRÁCTICO

Un Complejo Turístico Único En Estados Unidos Aumenta La Visibilidad En Todas Las Redes

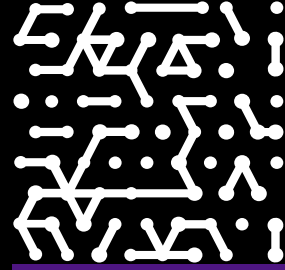
Armis permite al CISO y al departamento de TI obtener una visión centralizada de los activos de la red y centrarse en las prioridades principales

Sector

Complejo vacacional y centro de convenciones

Entorno de TI

Múltiples entornos (infraestructura PCI, red de invitados, instalaciones de audio/vídeo) con aproximadamente 5.000 activos en red



Introducción

Kalahari Resorts & Conventions ofrece experiencias únicas de vacaciones y convenciones a sus huéspedes en sus cuatro instalaciones en los EE. UU. Con tres redes muy activas que gestionar (corporativa, PCI y de huéspedes) el CISO implementó Armis para lograr una visibilidad más profunda y amplia de los dispositivos de red, los usuarios y el tráfico. El éxito de la implementación dio lugar a otros casos de uso que han mejorado significativamente las operaciones y han ahorrado tiempo al centrarse en áreas clave.

Kalahari Resorts & Conventions son destinos vacacionales y de conferencias con temática africana de servicio completo en los Estados Unidos, con alojamiento de primera clase, instalaciones de vanguardia para celebrar reuniones y convenciones, y los mayores parques acuáticos cubiertos de América. Actualmente, Kalahari Resorts cuenta con cuatro sedes: Wisconsin Dells (Wisconsin); Sandusky (Ohio); Pocono Mountains (Pensilvania); y Round Rock (Texas). Además, las propiedades de Kalahari Resorts incluyen un campo de golf y una sede corporativa.

Tim Everson ha sido el CISO de Kalahari Resorts durante tres años como parte del equipo de liderazgo responsable de unos 30 profesionales de TI. Está involucrado a nivel práctico en todo lo relacionado con la seguridad: diseño, arquitectura, implementación, estrategia, cumplimiento y problemas de los huéspedes.

En Kalahari Resorts, Everson y su equipo supervisan varios entornos: la infraestructura corporativa, la infraestructura del sector de las tarjetas de pago (PCI), una gran red de huéspedes y, instalaciones de audio y vídeo. Everson tuvo que evaluar Armis porque estaba cada vez más preocupado por la falta de visibilidad que había en todas estas áreas. Después de llevar a cabo una prueba de valor (PoV, por sus siglas en inglés) impecable en las instalaciones de Wisconsin Dells, Everson se convenció de que Armis era exactamente lo que estaba buscando.

«Armis destacaba sobre otros proveedores, principalmente por su facilidad de uso, su sencillez, sus interfaces directas, su implementación plug-and-play y su capacidad para segmentar, visualizar, clasificar y alertar. La rentabilidad fue inmediata, sin lugar a dudas. Pudimos trabajar con la plataforma desde el primer día», afirma. «Armis es genial para encontrar todo lo que está en mi entorno. Veo lo que necesito ver y valoro realmente las funciones que no tenía antes».

Además, Everson y su equipo están aprovechando al máximo las amplias capacidades de integración de Armis, que les permitirán obtener más valor de las herramientas existentes. Ya han completado las integraciones con Microsoft Active Directory; vCenter Server, la utilidad de gestión centralizada de VMware; Simple Network Management Protocol (SNMP), un protocolo para recopilar y organizar datos sobre los dispositivos gestionados en las redes; y una de las muchas integraciones con proveedores de servicios inalámbricos que ofrece Armis. En un futuro próximo, Everson y su equipo también tienen previsto utilizar otras integraciones de seguridad de terminales, así como de proveedores de equipos de terminales por cable e inalámbricos.

El entorno PCI se convierte en el centro de atención

Uno de los usos más importantes de Armis en Kalahari Resorts es obtener una mejor visibilidad de la infraestructura PCI, que es donde se obtiene y transmite la información de los titulares de tarjetas de crédito. Para garantizar la seguridad y la privacidad de los datos de los titulares de las tarjetas y prevenir el fraude con ellas, Kalahari Resorts debe cumplir las normas de seguridad de datos del sector de las tarjetas de pago (PCI-DSS).

Teniendo esto en cuenta, Armis ha sido fundamental para ayudar a Everson a asegurarse de que la segmentación de la red funciona correctamente. Armis también supervisa las comunicaciones entre los segmentos. Por último, proporciona una visibilidad completa y precisa de la actividad de los dispositivos y de las personas que los utilizan, junto con la garantía de que los datos de los titulares de las tarjetas están donde deben estar.

«Gracias a Armis, ahora podemos ver el entorno PCI y recibir alertas cuando nuevos dispositivos intentan entrar en él. La capacidad de ver claramente el tráfico anormal que atraviesa los cortafuegos y las subredes PCI ha sido enorme para nosotros», comenta Everson. «Cuando recibimos una notificación de Armis de que hay un dispositivo que intenta entrar en la red PCI, podemos volver al cortafuegos y asegurarnos de que los puertos están cerrados para que los datos no lleguen a ningún terminal. Este caso de uso por sí solo justifica y valida la inversión en Armis».

Obstáculos

- Dificultad para proporcionar una visibilidad más clara a nivel de gestión de las redes corporativas, PCI y de invitados
- Reto para obtener una visión más profunda y gestionar el tráfico problemático
- Dificultad para aumentar las capacidades de gestión de las vulnerabilidades para el personal de TI del complejo
- Sobrecarga de los recursos de seguridad que debe aliviarse

Inventario de dispositivos en todas las redes

Kalahari Resorts cuenta con un gran inventario de activos gestionados en red que consta de casi 2.200 equipos informáticos en toda la empresa, junto con cientos de conmutadores, cámaras de vídeo y otros dispositivos. Armis rastrea y clasifica estos activos, recopilando datos valiosos como el estado de la seguridad, las vulnerabilidades, las anomalías e información sobre dónde se utilizan los dispositivos y por quién.

Además, e igualmente importante, es la capacidad de Armis para descubrir dispositivos invitados. Everson señala que, en una semana cualquiera, Armis ha demostrado que casi 140.000 dispositivos pueden entrar en contacto con la red de Kalahari Resorts, desde teléfonos móviles y ordenadores portátiles hasta vehículos con conexión inalámbrica en los aparcamientos del complejo.

No es raro, señala, que se produzcan enormes picos de tráfico en la red de huéspedes. Cuando esto ocurre, Armis ayuda a Everson y a su equipo a identificar inmediatamente qué invitados de la red son los que los causan. Esto incluye la detección de la actividad causada por BitTorrent, un protocolo que permite a cualquiera descargar y compartir archivos multimedia, como vídeos, música, aplicaciones, imágenes y documentos. El problema del uso de BitTorrent es que no solo ralentiza la conexión a Internet, sino que también puede introducir potencialmente archivos maliciosos o malware en la red.

«Es increíble lo rápido que podemos ver cosas en nuestra red, como BitTorrent. Somos un centro turístico, pero tenemos que asegurarnos de que los huéspedes de nuestra red no están haciendo cosas como descargar torrents», explica Everson. «Con Armis, podemos ver ese tipo de actividad de los huéspedes inmediatamente. Seguidamente, podemos eliminarlos de la red y bloquear el punto de acceso y no tener que preocuparnos por ello».

Casos de uso inesperados de Armis

Además de aprovechar Armis para obtener una completa visibilidad y conocimiento de los dispositivos, Kalahari Resorts también ha encontrado otras aplicaciones para la solución.

Resultados de Armis

- Inventario de activos preciso y completo en las tres redes
- Control más estricto del comportamiento anómalo en la red de invitados
- Mejor supervisión del ancho de banda y del rendimiento de la red
- Mejora de la seguridad y el cumplimiento de la normativa PCI
- Paneles de control centralizados y de fácil acceso con datos granulares para una resolución de problemas más eficiente
- Importante ahorro de tiempo gracias a la reducción de la carga de trabajo de seguridad



La gestión de la vulnerabilidad, por ejemplo, se ha hecho más fácil con Armis, ya que localiza los dispositivos que utilizan aplicaciones sin parches o sistemas operativos antiguos que pueden aumentar el riesgo general. También supervisa los comportamientos sospechosos o anómalos. «Con Armis, vemos cosas que otros escáneres de gestión de vulnerabilidades no ven», observa Everson. «Hemos podido ver el tráfico de aplicaciones que intentaba subvertir nuestros cortafuegos y hemos podido frenarlo».

Otro caso de uso es la supervisión de los certificados de los protocolos de seguridad de la red. Armis ve los certificados que pasan por las redes y saca a la luz los que han caducado. Esto permite a Everson y a su equipo actualizar rápidamente los certificados para garantizar la seguridad de las transacciones y los flujos de trabajo de las aplicaciones de los usuarios.

Además, Armis ha descubierto fallos de autenticación de la red. Esto ocurre cuando las cuentas de usuario con contraseñas recientemente cambiadas intentan iniciar sesión en un sitio repetidamente sin éxito, lo que puede saturar el ancho de banda. Al identificar estos eventos, Everson puede asignar a una persona de su equipo para que solucione el problema y tome medidas correctivas.

El tiempo es oro

Todos estos casos de uso han permitido a Everson y a su equipo disfrutar de una mayor eficiencia operativa y mejorar su gestión del tiempo.

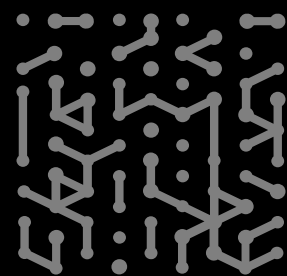
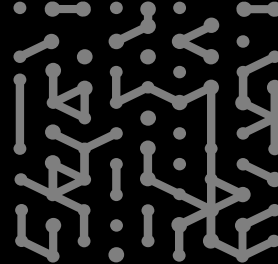
«Uno de los retos a los que nos enfrentábamos era que, aunque en la actualidad contamos con unas 30 personas en la plantilla de TI, Kalahari Resorts tiene un equipo de seguridad relativamente pequeño». Armis nos ha devuelto nuestro tiempo. Ahora podemos compartir el panel de control y dar al equipo de TI la información que necesita para actuar,” relata. «Esto ha sido crucial para nosotros, ya que nos ha quitado muchas cosas de encima y nos ha permitido realizar otras tareas importantes».

Armis recoge una gran cantidad de datos que Everson y su equipo pueden filtrar, ver en un panel y compartir. Les evita tener que recurrir a 15 herramientas diferentes para recopilar información y darle sentido. Armis ofrece al equipo de seguridad la capacidad de clasificar y segmentar la red para que puedan desglosar, en tiempo real, para ver y localizar todo tipo de dispositivos y recibir alertas cuando haya señales de alarma.

Everson recomienda Armis a otras organizaciones sin dudarlo: «Armis ha cambiado las reglas del juego para nosotros. Nos ha ahorrado mucho esfuerzo y es un placer darlo a conocer».

«Armis destacaba sobre otros proveedores, principalmente por su facilidad de uso, su sencillez, sus interfaces directas, su implementación plug-and-play y su capacidad para segmentar, visualizar, clasificar y alertar. La rentabilidad fue inmediata, sin lugar a dudas».

Tim Everson
Director de Seguridad
de la información
Kalahari Resorts
& Conventions



Armis, la empresa de ciberseguridad de inteligencia de activos, protege toda la superficie de ataque y gestiona la exposición a los riesgos de ciberseguridad de la organización en tiempo real.

En un mundo en constante evolución y sin perímetros definidos, Armis garantiza que las organizaciones puedan ver, proteger y gestionar de manera continua todos los activos críticos.

Armis protege a empresas Fortune 100, 200 y 500, así como a gobiernos nacionales y entidades estatales y locales, para ayudar a mantener seguras y protegidas las infraestructuras críticas, las economías y la sociedad las 24 horas del día, los 7 días de la semana.

Armis es una empresa privada con sede en California.

1.888.452.4011

Website

- Platform
- Industries
- Solutions
- Resources
- Blog

Try Armis

- Demo
- Free Trial

