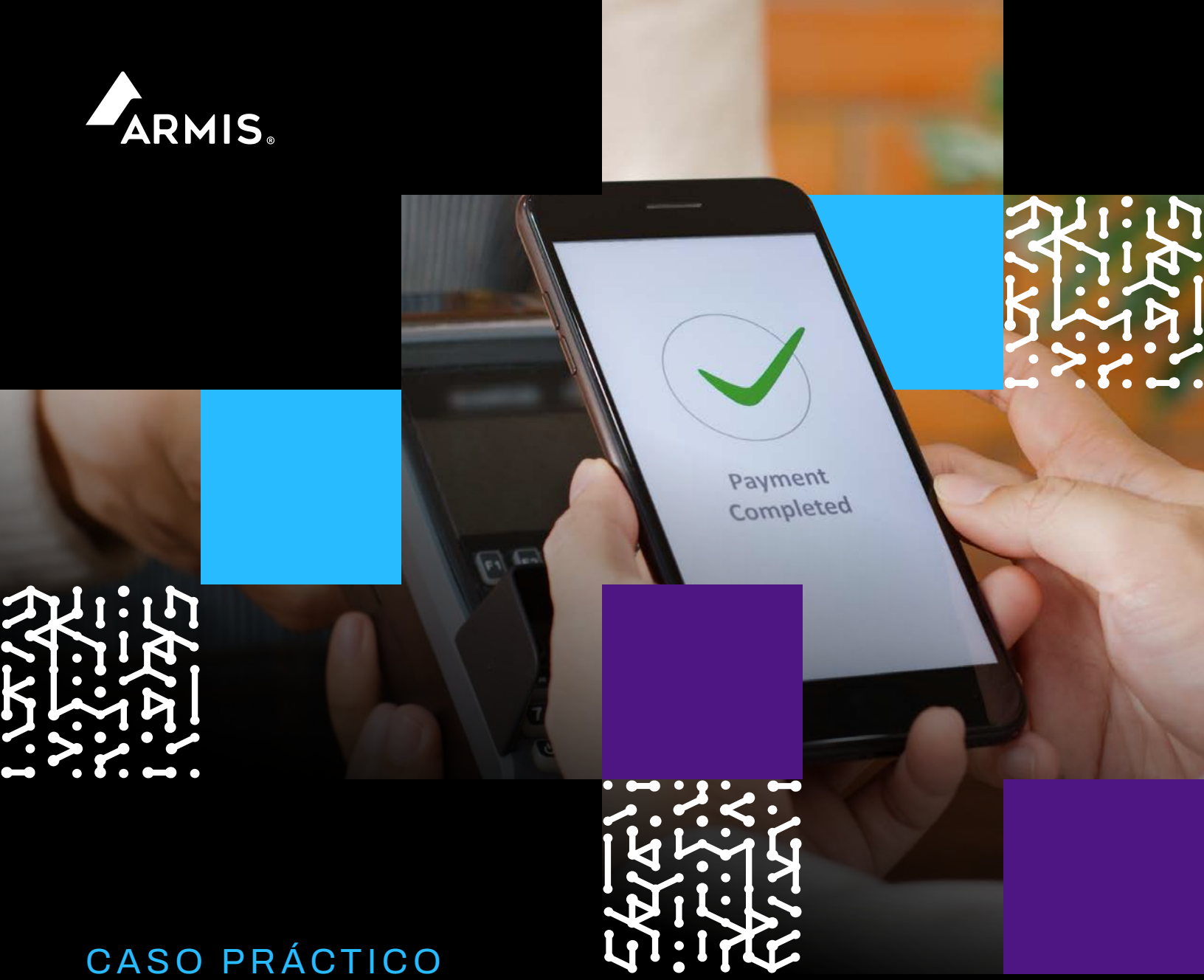
ARMIS®



CASO PRÁCTICO

Organización internacional de servicios financieros alcanza su objetivo de una visibilidad del 100 % como parte de su estrategia de madurez de la seguridad

Varias integraciones de Armis correlacionan los datos de los dispositivos para ayudar a detectar y priorizar las vulnerabilidades.

Sector

Financiero

Entorno de TI

Más de 5000 empleados en todo el mundo y miles de dispositivos.

Introducción

Esta organización mundial de servicios financieros se enorgullece de buscar la excelencia en todas las áreas, incluida la ciberseguridad. Armis se implementó como parte de su iniciativa de madurez de la seguridad y proporcionó a la organización una visibilidad del 100 % de todos los activos.

Armis se integra con el amplio conjunto de soluciones de los datos de dispositivos amplificados y correlacionados de la arquitectura de seguridad de la organización para ayudar a orientar la gestión de vulnerabilidades mediante la identificación y la priorización de las vulnerabilidades más críticas que deben solucionarse para reducir su superficie de ataque.

Asimismo, gracias a Armis, el equipo de seguridad pudo realizar análisis de deficiencias para determinar qué dispositivos carecían de protecciones de seguridad actualizadas y esenciales. Al cubrir estas lagunas, la organización consiguió un perfil de riesgo más sólido y puede afirmar con confianza que la cobertura fue del 100 % en el momento de la auditoría.

Cuando se trata de proteger su entorno tecnológico, esta organización internacional de servicios financieros cree que la proactividad y la meticulosidad deben formar parte de sus mejores prácticas. Con más de 5000 empleados en varias ubicaciones en todo el mundo, el parque técnico es de amplio alcance, con miles de dispositivos en uso.

La organización cuenta con un gran arsenal de herramientas de seguridad, desde el análisis de vulnerabilidades hasta la detección y respuesta de terminales (EDR, endpoint detection and response), además de soluciones de confianza cero. «Tenemos casi todas las herramientas del mundo», afirma el gerente de ingeniería de seguridad. «Pero faltaba una cosa: 100 % de visibilidad de todos los activos».

Señaló que la organización está en una misión de madurez de seguridad, con el objetivo de ser «la mejor de su sector». Él y su equipo realizaron una autoauditoría y determinaron que una de las mayores deficiencias era la visibilidad de todo el entorno. Luego explicó que pronto resultó evidente que él y otros equipos carecían de datos suficientes sobre una parte significativa de los activos de la organización en su base de datos de gestión de la configuración (CMDB, configuration management database).

Miles de activos descubiertos durante una prueba de valor de Armis

El gerente conoció Armis en una conferencia de Black Hat, en la que le hicieron una demostración. Él y su supervisor estuvieron de acuerdo de inmediato con llevar a cabo una prueba de valor (PoV). Como parte de la PoV, trabajó con su equipo para integrar alrededor de 20 productos en la pila tecnológica existente para obtener una imagen más clara de cómo Armis podría ayudarlo a él y a su equipo a obtener una visibilidad más amplia al correlacionar los datos relevantes de varias fuentes. El fundamento era mejorar la gestión de vulnerabilidades al obtener una visibilidad total de todos los riesgos en el entorno de la organización y realizar análisis de deficiencias para todas las herramientas de seguridad.

Mientras que el equipo de CMBD de la organización afirmaba que esta tenía poco más de 5000 activos, Armis descubrió una cantidad de activos entre tres y cuatro veces superior en solo dos semanas. Antes de eso, el supervisor del gerente pasó muchos meses desarrollando de forma manual herramientas internas que extraían interfaces de programación de aplicaciones (API, application programming interfaces) de varias herramientas en una base de datos y correlacionaban los datos, todo lo que Armis podía hacer en cuestión de semanas.

«Puedo afirmar, con total seguridad, que Armis nos proporcionó una visión del 100 % de los activos de nuestro entorno», aseveró. «Estamos estableciendo referencias cruzadas de todas las herramientas, y eso nos está llevando a la visibilidad que buscamos».

Obstáculos

- Obtención de visibilidad de todos los activos del entorno
- Extracción de información más detallada sobre vulnerabilidades
- Mejora de la precisión de la CMDB
- Mantenimiento del cumplimiento de las normativas industrial y gubernamental

Las integraciones con herramientas relacionadas con la seguridad mejoran y aceleran la gestión de vulnerabilidades

Después de la prueba de valor de Armis, el gerente le mostró los resultados a su supervisor, y fue «amor a primera vista». Armis reveló importantes deficiencias en la base de datos de gestión de la configuración (CMDB). El gerente de ingeniería de seguridad y su equipo utilizan el análisis de deficiencias proporcionado por Armis para determinar qué activos carecen de protecciones de seguridad esenciales, como detección y respuesta de terminales (EDR).

En lo más alto de la lista de tareas pendientes del gerente está completar las integraciones de Armis con el resto de las herramientas y los servicios de software de la extensa arquitectura de seguridad de la organización. Entre ellas se incluyen los servicios de directorio, la gestión de dispositivos virtuales, los firewalls avanzados, la gestión de vulnerabilidades, el software de mapeo de redes, las plataformas de computación en la nube y la gestión de identidades y accesos, y otras. Gracias a estos esfuerzos de integración, la organización de servicios financieros “dispondrá de un único panel de control que unifique los suministros de datos y proporcione una visión más amplia y profunda de los activos que ayudará a que los equipos identifiquen y corrijan las vulnerabilidades.

En la actualidad, el gerente trabaja con Armis en otras tres nuevas integraciones adicionales. Esto no solo ayudará a la organización de servicios financieros, sino que también ampliará la cartera de integración de Armis y ayudará a otros clientes de Armis. «Armis es como una base de datos de API. Si hay una API, Armis puede rastrearla y correlacionar los datos», señaló el gerente de ingeniería de seguridad. «Estoy seguro de que de aquí pueden salir algunas buenas asociaciones».

Resultados de Armis

- 100 % de visibilidad de todos los activos en toda la propiedad
- Integraciones con herramientas relacionadas con la ciberseguridad que proporcionan datos enriquecidos de los dispositivos
- Un panel de control único y centralizado para la supervisión y los informes de cumplimiento
- Priorización de vulnerabilidades para una corrección más rápida
- Menos tiempo dedicado a la creación de herramientas de integración de API propias
- Integración simplificada de fusiones y adquisiciones

En los últimos años, la organización de servicios financieros ha pasado por una fase de crecimiento rápido, con alrededor de 20 fusiones y adquisiciones (M&A, mergers and acquisitions). Para los equipos técnicos, eso significa incorporar nuevas infraestructuras de red, servidores y centros de datos. Armis desempeña un papel clave en la optimización de esos esfuerzos y proporciona una línea de base precisa de los activos. «Sin la capa de visibilidad que proporciona Armis, las cosas pasarían inadvertidas. Antes de Armis, teníamos que basarnos en suposiciones para saber si ciertas cosas existían o no», remarcó.

«Puedo afirmar, con total seguridad, que Armis nos proporcionó una visión del 100 % de los activos de nuestro entorno. Estamos estableciendo referencias cruzadas de todas las herramientas, y eso nos está llevando a la visibilidad que buscamos».

Gerente de ingeniería de seguridad
Servicios financieros

Armis llena los vacíos para reducir el riesgo y mantener el cumplimiento

El sector de los servicios financieros es una de las industrias más reguladas de EE. UU. Las instituciones financieras están obligadas a cumplir con una lista cada vez mayor de normativas, que incluye el cumplimiento de estrictos estándares de ciberseguridad. La identificación y corrección de vulnerabilidades para evitar su explotación por parte de atacantes es un objetivo clave en esta organización y una parte integral de su esfuerzo de gestión de riesgos.

Como observa el director, «las herramientas de gestión de la vulnerabilidad tienen un límite, y requieren mucho 'cuidado y suministro'. Armis proporciona evaluaciones basadas en el riesgo y análisis de deficiencias para garantizar que tengamos una cobertura completa. Me gusta tener la confianza de poder decirle a un auditor que tenemos una cobertura del 100 %».

En la actualidad está creando informes de indicadores clave de rendimiento (KPI, key performance indicators) para medir la cobertura de la seguridad. Con su modelo de políticas basadas en riesgos, Armis puede proporcionar métricas para una evaluación precisa y una mejora continua.

«El enfoque con respecto a la vulnerabilidad basado en el riesgo es enorme para nosotros. Es como encontrar una aguja en un pajar. Si entrara en nuestro actual gestor de vulnerabilidades, es probable que encontrara más de un millón de vulnerabilidades sin parchear. Pero en mi cabeza, esa no es una cifra real», explica el gerente.

«Armis puede eliminar el ruido e identificar los activos más vulnerables, que pueden reducirse a unos pocos centenares según los criterios innovadores de Armis. Es reconfortante poder cribar todos esos datos en cuestión de segundos».

Paso siguiente: Integración de la base de datos de gestión de la configuración (CMDB)

Una de las iniciativas en el horizonte es la integración de Armis con la CMDB para enriquecer los datos de los activos. El equipo del proyecto —formado por seis ingenieros— lleva varios meses trabajando en la integración manual del almacén de activos con otras herramientas.

Ahora que Armis hizo el trabajo pesado de identificar miles de activos desconocidos hasta el momento, su labor será mucho más fácil.

«Nuestro equipo de gestión de vulnerabilidades está entusiasmado con la posibilidad de ahorrarse un año de trabajo de ingeniería. Gracias a Armis, pueden pasar de cero a cien con mucha rapidez e identificar mejor las deficiencias de datos en nuestra CMDB», afirmó el gerente de ingeniería de seguridad.

Después de completar la integración de Armis con la CMDB, los servicios financieros dispondrán de una única fuente verídica exhaustiva, que ayudará a que los equipos identifiquen riesgos, prioricen vulnerabilidades y mantengan el cumplimiento.