Estudio de Caso

Gigamon ayuda al Hospital Sirio-Libanés a mejorar la visibilidad, la seguridad y el compliance

Cuando buscamos una observabilidad profunda, Gigamon nos muestra todo lo que tenemos en todas las capas de nuestra infraestructura, incluida la nube. Vemos el tráfico de la red de acceso, el paquete, el flujo, etc., toda la información que procede de los metadatos de nuestras aplicaciones.

LEANDRO RIBEIRO
Director de Seguridad de la Información,
Hospital Sirio-Libanés

Desafíos

- Visibilidad completa de las amenazas a la red
- Seguridad en la nube para aplicaciones e infraestructura
- Seguridad del Internet de las cosas (IoT) para dispositivos
- Cumplimiento de la normativa regional sobre protección de datos personales y de salud

Beneficios para el cliente

- Mayor conocimiento del tráfico de red
- Mayor capacidad para identificar amenazas internas
- Reducción de la necesidad de herramientas adicionales
- Mayor protección de los datos confidenciales de los pacientes

Solution

- GigaVUE Cloud Suite™
- Serie GigaVUE® HC
- Serie GigaVUE TA
- GigaVUE-FM fabric manager
- GigaSMART®

Sobre el cliente

El Hospital Sirio-Libanés es un gran proveedor brasileño de servicios de salud con 103 años de experiencia que ha dado lugar a la actual institución médica de vanguardia con equipos especializados, inversiones en enseñanza e investigación e iniciativas pioneras. La institución, que cuenta con uno de los mayores centros de diagnóstico por imagen de Brasil, se encuentra entre los 100 mejores hospitales del mundo y opera en 9 ubicaciones en São Paulo y Brasilia, donde emplea a una plantilla de 14.000 personas.

El hospital cuenta con un entorno de TI híbrido en la nube, con entre el 70% y el 80% de sus aplicaciones e infraestructuras alojadas en la nube, principalmente en Amazon AWS. El Director de Seguridad de la Información, Leandro Ribeiro, un profesional experimentado con más de 15 años de experiencia en ciberseguridad y 20 años en atención médica, se unió al Hospital Sirio-Libanés para mejorar su programa de ciberseguridad. Antes de incorporarse al hospital, Leandro trabajó para importantes empresas de asistencia médica, entre ellas UnitedHealth Group. Su experiencia en ciberseguridad en el sector de la salud le convierte en un valioso activo para la organización.

Desafío comercial

Cuando Ribeiro se incorporó al Hospital Sirio-Libanés, descubrió que la pila de seguridad heredada carecía de la visibilidad y las capacidades que necesitaba el equipo de seguridad para detectar y responder eficazmente a las ciberamenazas, especialmente en la nube.

Como resultado, Ribeiro y su equipo de 22 profesionales de redes y ciberseguridad tenían tres preocupaciones principales. En primer lugar, el personal de ciberseguridad tenía dificultades para supervisar el tráfico de red desde todas las direcciones, especialmente el tráfico este-oeste dentro del centro de datos. Esta visibilidad limitada dificultaba la identificación y el tratamiento de la TI en la sombra y las posibles amenazas internas a la seguridad que pudieran originarse dentro de la red. En segundo lugar, el creciente número de dispositivos IoT, como equipos médicos y dispositivos wearables, expuso nuevas vulnerabilidades, amplió la superficie de ataque y puso en riesgo la salud y los datos personales de los pacientes.

Estos dispositivos, a menudo con controles de seguridad limitados, podrían ser explotados por atacantes para obtener acceso no autorizado a la red del hospital. Por último, el hospital necesitaba cumplir la Ley General de Protección de Datos Personales (LGPD) brasileña, que exige fuertes medidas de ciberseguridad para la protección y privacidad de los datos de los pacientes. El incumplimiento de esta normativa podría acarrear importantes multas y daños a la reputación.

En sus anteriores funciones en otras instituciones de salud, Ribeiro tuvo una experiencia positiva con Deep Observability Pipeline y el equipo que le prestó apoyo. “Había trabajado estrechamente con el equipo de Gigamon en Brasil, que era proactivo a la hora de resolver problemas de visibilidad específicos de nuestro entorno. Mis equipos no siempre estaban familiarizados con las herramientas, por lo que el apoyo que recibimos de Gigamon fue inestimable para conseguir que todo el mundo se pusiera al día tan rápidamente”, dijo. “Supe inmediatamente que Gigamon era la mejor solución para el Hospital Sirio-Libanés”.

Solución

Los retos empresariales del Hospital Sirio-Libanés se resolvieron obteniendo un conocimiento más profundo de la actividad de la red para identificar y abordar los posibles riesgos de seguridad con mayor eficacia.

El hospital implementó una solución integral de ciberseguridad con Gigamon, ExtraHop y Claroty Medigate, dos socios de ciberseguridad de Gigamon. Gigamon proporciona una visión unificada de los datos en movimiento en toda la red, lo que permite al hospital supervisar el tráfico desde todas las direcciones (Norte-Sur y lateral Este-Oeste). ExtraHop, una solución de detección y respuesta (NDR), complementa a Gigamon ofreciendo capacidades avanzadas de detección y análisis de amenazas. “La solución integrada nos facilita la detección de amenazas internas y comportamientos anómalos en puntos terminales y servidores”, señala Ribeiro.

En concreto, Deep Observability Pipeline proporciona una pila completa de herramientas de seguridad y rendimiento que elimina los puntos ciegos con una visibilidad completa de toda la infraestructura. ExtraHop recibe paquetes sin procesar proporcionados por Gigamon desde toda la infraestructura, extrae metadatos del paquete mediante aprendizaje automático y analiza la inteligencia utilizando más de un millón de modelos predictivos diferentes para obtener un conocimiento exhaustivo de la actividad de la red del hospital. Los algoritmos de aprendizaje automático de ExtraHop analizan el tráfico de red para identificar actividades sospechosas y técnicas de movimiento lateral que exponen la presencia de amenazas en las primeras fases, como malware, ransomware y amenazas internas para ayudar a mitigar los riesgos y prevenir las brechas de seguridad.

La solución también permite al hospital descubrir, supervisar y gestionar eficazmente los dispositivos IoT, identificando vulnerabilidades y evitando el acceso no autorizado a estos activos críticos, sin necesidad de invertir en hardware caro y de alto mantenimiento. "Aquí es donde Gigamon pudo ayudarnos a ahorrar dinero. Nunca supimos realmente cuántos dispositivos teníamos en nuestra red. Ahora que tenemos una visibilidad completa de todos nuestros dispositivos, podemos implementar la segmentación de red para protegerlos mejor", afirma Ribeiro.

Gracias a la combinación de Gigamon y ExtraHop, el hospital puede demostrar el cumplimiento de las normativas aportando pruebas de sus sólidas medidas de ciberseguridad y, en última instancia, mejorando la seguridad de los pacientes y de los datos.

Beneficios

La implementación de Gigamon ofrece muchas ventajas significativas para el Hospital Sirio-Libanés. Al obtener un conocimiento exhaustivo del tráfico de red, Ribeiro puede identificar y abordar los posibles riesgos de seguridad con mayor rapidez y eficacia, tanto en las instalaciones como en AWS.

"Cuando buscamos una observabilidad profunda, Gigamon nos muestra todo lo que tenemos en todas las capas de nuestra infraestructura. Vemos el tráfico de la red de acceso, el paquete, el flujo, etc., toda la información que procede de los metadatos de nuestras aplicaciones", dice Ribeiro.

La solución combinada permite al hospital detectar y responder a las amenazas con mayor rapidez, reduciendo la frecuencia y el impacto de los incidentes de seguridad. Además, el hospital puede proteger sus dispositivos IoT, evitando el acceso no autorizado y mitigando el riesgo de filtración de datos. Al consolidar varias herramientas de seguridad en en una única plataforma, el hospital también consigue un importante ahorro de costos. Por ejemplo, Gigamon aumenta la eficacia de la detección de amenazas de Claroty Medigate, una plataforma de asistencia médica SaaS que protege la tecnología y los dispositivos médicos conectados, desde bombas intravenosas hasta ultrasonidos.

La integración de Gigamon y Claroty amplía la visibilidad del tráfico de red que atraviesa los dispositivos médicos XIoT/OT en el hospital, lo que permite una detección de amenazas y una respuesta más rápidas y precisas.

Por último, la solución ayuda a cumplir los requisitos de conformidad proporcionando una sólida postura de ciberseguridad. Al reforzar la ciberseguridad, el hospital puede proteger los datos confidenciales de los pacientes y garantizar la continuidad de los servicios críticos, mejorando la seguridad de los pacientes y la eficiencia operativa general.

"En el entorno de la salud, ofrecer la mejor atención posible a nuestros pacientes es una misión crítica, por lo que todo lo que hacemos depende del tiempo. Gracias a la visibilidad ampliada y profunda que nos ofrece Gigamon, ahora vamos varios pasos por delante cuando se produce un incidente. En cuanto identificamos una amenaza, podemos detenerla en seco y asegurarnos de que no afecte al funcionamiento del hospital ni a la salud y seguridad de nuestros pacientes", señala Ribeiro.

En un futuro próximo, él y su equipo planean explorar más a fondo otras capacidades de Gigamon, incluida la integración con SIEM, TLS/SSL Decryption para todo el tráfico y la tecnología Gigamon Precryption™ para eliminar los puntos ciegos en el tráfico de la nube Este-Oeste.

Sobre Gigamon

Gigamon® ofrece una plataforma de observabilidad profunda que proporciona de forma eficiente inteligencia derivada de la red a herramientas de nube, seguridad y observabilidad. Esto ayuda a eliminar los puntos ciegos de seguridad y a reducir los costos de herramientas, lo que le permite proteger y gestionar mejor su infraestructura de nube híbrida. Gigamon ha prestado servicio a más de 4.000 clientes en todo el mundo, incluyendo más del 80 por ciento de las empresas Fortune 100, 9 de los 10 mayores proveedores de redes móviles, y cientos de gobiernos y organizaciones educativas Para obtener más información visite gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

01.25_01