



DARKTRACE

CASO PRÁCTICO

Catholic Charities of Santa Clara County



Overview

Industria

- Beneficencia/no comercial

Desafío

- Defender un gran volumen de información personal almacenada cada vez más en línea
- Atacantes cibernéticos sofisticados y nuevos métodos de ataques de rápida evolución
- Proteger la reputación para mantenerse una organización responsable
- Visibilidad inadecuada de las herramientas de seguridad existentes

Resultados

- Mejor entendimiento del comportamiento del usuario y del dispositivo
- Visibilidad completa de actividades internas y externas
- Alertas de las amenazas a medida que ocurren, permitiendo mitigación de riesgo
- Capacidad de llevar a cabo investigaciones a fondo sobre anomalías

Antecedentes de la empresa

Catholic Charities of Santa Clara County (CCSCC), fundada hace más de 60 años, ayuda a más de 54.000 personas con necesidades cada año y, debido a su afiliación a Catholic Charities USA, es parte de la red de servicios sociales más grande del país. Esta entidad trabaja con organizaciones de la comunidad, alianzas interreligiosas, representantes del gobierno y líderes de negocios para lograr su objetivo global de reducir la pobreza en el condado de Santa Clara.

“

El Enterprise Immune System de Darktrace puede detectar amenazas que ninguna otra herramienta de seguridad podría encontrar. La tecnología de Machine Learning es única en su tipo.

Will Bailey, director de IT, CCSCC

”

Desafío

Las entidades de beneficencia, tales como CCSCC, están cada vez más conectadas debido a sus sistemas de información en línea y redes de computadoras. Por lo tanto CCSCC reconoció la necesidad de mejorar su solución de ciberseguridad para poder manejar el panorama de amenazas actual.

La entidad gestiona grandes volúmenes de información médica, financiera y de vivienda altamente confidencial de las personas a las que ayuda. Para mantener su reputación como organización responsable, CCSCC deseaba adoptar una tecnología capaz de defender sus datos cruciales de las novedosas ciberamenazas de rápida evolución y de las amenazas internas, fuesen maliciosas o no.

CCSCC había descubierto que las herramientas de seguridad existentes eran inadecuadas para proporcionar el nivel de visibilidad de la red que la entidad requería. Dada la gran cantidad de empleados y voluntarios conectados constantemente a su red, la entidad necesitaba un mejor conocimiento general de su comportamiento y actividades.

Solución

La efectividad del Enterprise Immune System de Darktrace quedó claramente demostrada durante un breve período de prueba de valor, durante el cual la tecnología de autoaprendizaje detectó e informó que ransomware estaba atacando activamente la red desde dentro, lo cual no había podido ser detectado por las demás herramientas de seguridad de la entidad. La amenaza se manejó inmediatamente y se evitó que causara daños.

La tecnología de Darktrace puede detectar amenazas en tiempo real, gracias al Machine Learning y las matemáticas desarrolladas por especialistas de la Universidad de Cambridge. Aprende rápidamente el 'patrón de vida' de la red modelando los comportamientos de cada usuario, dispositivo y red en su totalidad.

Utilizando este conocimiento dinámico y adaptativo del "sí mismo", la tecnología alerta a la entidad acerca de todo comportamiento o actividad que se desvía de la norma. Por lo tanto, se informa al equipo de seguridad de IT acerca de la actividad genuinamente anómala, permitiéndoles realizar una investigación con mayor profundidad y mitigar los riesgos que representa.

Beneficios

Gracias a la premiada tecnología del Enterprise Immune System de Darktrace, CCSCC ahora está alertada de los ciberataques en cuanto se presentan, permitiéndole a la entidad mitigar los riesgos de manera rápida y eficiente. El equipo de seguridad de IT de la organización ahora tiene más confianza al saber que las potenciales amenazas desde dentro y aún las 'incógnitas desconocidas' no pasarán inadvertidas.

Además, CCSCC está utilizando la interfaz del Threat Visualizer, que brinda un panorama gráfico en 3D de toda su red, permitiéndole a la entidad ser testigo, en tiempo real, de toda la actividad interna y externa. Significativamente el equipo de seguridad de IT tiene la capacidad de llevar a cabo investigaciones en profundidad de las anomalías utilizando las características pragmáticas de la interfaz.

“

La tecnología ofrece una ciberdefensa central que es específica para nuestra red. A medida que utilizamos el Enterprise Immune System y examinamos a fondo las anomalías que nos presenta, podemos ajustar parámetros, modificar los criterios de actividad anómala, verificar comportamientos que son realmente legítimos y, en general, implementar las mejores prácticas.

Will Bailey, director de IT, CCSCC

”

Contacto

Sudamerica: +57 322 942 6401

Europa: +44 (0) 1223 394 100

Asia-Pacífico: +65 6804 5010

info@darktrace.com

darktrace.com