



CASO PRÁCTICO

UDLAP

UDLAP®

Overview

Industria

- Educación

Desafío

- Necesitaba proteger información privada
- Preocupado por ataques internos maliciosos y no maliciosos
- Herramientas tradicionales creaban un alto número de alertas
- Un ambiente de red compleja con miles de dispositivos móviles

Resultados

- Visibilidad total de la red por medio del 3D Threat Visualizer (visualizador de amenazas)
- Algoritmos de AI (Inteligencia Artificial) que detectan amenazas emergentes
- Monitoreo continuo de dispositivos personales y no autorizados
- La tecnología disminuye el ruido y sólo marca alertas genuinas

Antecedentes de la organización

Fundada en 1940, La Universidad de Las Américas Puebla (UDLAP), se ha establecido como una de las universidades privadas más prestigiosas en América Latina. Ofreciendo más de 58 títulos/licenciaturas y más de 30 programas de pos grado, la UDLAP actualmente abarca a más de 10mil estudiantes y casi 2mil empleados. Los temas de tecnología e innovación juegan un papel importante en la cultura de la universidad, por esta razón, la universidad considera como prioridad tener un enfoque innovador en la seguridad cibernética.

“

A medida que pasaron los meses, Darktrace se convirtió en nuestro mejor aliado. La tecnología entiende todas las operaciones de nuestra red—las conexiones, el ancho de banda y las tareas de cada usuario. Cuando algo sospechoso ocurre, el Enterprise Immune System nos alerta inmediatamente.

Fernando Thompson, CIO, UDLAP

”

Desafío

Como una institución educativa líder, la UDLAP estaba preocupada por mantener su red en una época de amenazas agresivas, que incluyen ataques intencionales, ransomware y otras amenazas sofisticadas. La información personal y financiera de más de 12 mil estudiantes y empleados es almacenada en la red de la universidad, y una filtración de datos exitosa podría ser perjudicial para el prestigio y la reputación de la universidad.

Para agravar este desafío, el equipo de seguridad se vio abrumado por la investigación de miles de alertas falsas. Necesitaban una nueva solución que usara Inteligencia Artificial (AI) para comprender la red y solamente alertar al equipo de actividad realmente peligrosa. Además, el equipo de seguridad de la UDLAP necesitaba ser particularmente estratégico con sus inversiones.

“Tenemos que ser muy cuidadosos e inteligentes con nuestras inversiones”, comentó Fernando Thompson, CIO de la UDLAP. “Cada inversión tiene el potencial de afectar el centro del negocio de la universidad—nuestros estudiantes y su experiencia educativa”.

Solución

Para enfrentar estos desafíos, la UDLAP seleccionó a Darktrace para una Prueba de Valor de cuatro semanas. Después de una hora de instalación, Darktrace empezó a aprender el “patrón de vida” para cada dispositivo y usuario en la red de la universidad. Usando aprendizaje de máquina y AI, el Enterprise Immune System rápidamente formó un entendimiento preciso y exhaustivo de lo que constituye actividad ‘normal’ para la red de la UDLAP. Usando este entendimiento, Darktrace empezó a marcar serias amenazas en la red, dándole al equipo de seguridad la habilidad de responder y remediar amenazas en tiempo real.

“A medida que pasaron los meses, Darktrace se convirtió en nuestro mejor aliado. La tecnología entiende todas las operaciones de nuestra red—las conexiones, el ancho de banda, y las tareas de cada usuario. Cuando algo sospechoso ocurre, el Enterprise Immune System nos alerta inmediatamente”.

La UDLAP también quedó impresionada con el Threat Visualizer (Visualizador de Amenazas) de Darktrace. La herramienta presenta una vista dinámica e interactiva de la actividad de la red, la cual le brinda al equipo de seguridad visibilidad sin precedentes dentro de la red. “Nunca había visto una herramienta como la de Darktrace”, dijo Thompson. “El Enterprise Immune System nos da la habilidad de ver todos los dispositivos conectados, y analizar cualquier actividad y conexiones en tiempo real”.

Beneficios

Apoyado por el Enterprise Immune System, la UDLAP se siente segura de detectar ataques insólitos, sofisticados y a la velocidad de la luz en cuanto emergen. “Hay un gran número de amenazas nuevas y sofisticadas que a veces es imposible que una persona las detecte de manera oportuna”, comentó Thompson. “La tecnología de AI de Darktrace mejora, drásticamente, nuestra habilidad de defender nuestras redes”.

El equipo de seguridad de la universidad previamente había sido inundado por un gran número de alertas innecesarias y falsos positivos. Perdían tiempo respondiendo a estas alertas, y les dejaba poco tiempo para tomar un enfoque proactivo de ciberseguridad. Sin embargo, ya armado con Darktrace, su entendimiento único de la red y su avanzada AI, el equipo de seguridad es alertado sobre amenazas relevantes. “Darktrace reduce el número de alertas falsas”, dijo Thompson. “A medida que pasa el tiempo, la exactitud de la herramienta solo continúa mejorando”.

El Enterprise Immune System no sólo le da al equipo de seguridad tiempo para responder a serios ataques en tiempo real, sino también ahora tienen el tiempo y los recursos para enfocarse en mejorar y actualizar el programa de seguridad de la universidad. La AI de Darktrace ayuda a la UDLAP a detectar las amenazas de hoy y proteger de las amenazas del mañana.

“

La tecnología de AI de Darktrace mejora, drásticamente, nuestra habilidad de defender nuestras redes. Cuando actividad sospechosa empieza a tomar lugar, el Enterprise Immune System alerta a nuestro equipo inmediatamente, dándonos tiempo para responder y evitar que cualquier amenaza dañe nuestra red.

Fernando Thompson, CIO, UDLAP

”

Contacto

Sudamerica: +57 322 942 6401

Europa: +44 (0) 1223 394 100

Asia-Pacífico: +65 6804 5010

info@darktrace.com

darktrace.com