DARKTRACE

CASO PRÁCTICO

Sunsweet

Resumen

Industria

- Fábrica agrícola

Desafío

- Imposibilidad de ver el tráfico de intrusos
- Preocupación debida al creciente número de amenazas automatizadas y sofisticadas
- Modesto equipo de seguridad
- Necesidad de un enfoque proactivo hacia la ciberdefensa

Resultados

- El Threat Visualizer proporciona visibilidad de la red
- El Enterprise Immune System detecta ataques a gran velocidad en tiempo real
- Goza de mayor confianza en la pila de seguridad
- Ahora posee capacidad para mitigar las amenazas en cuestión de minutos

Antecedentes de la empresa

Fundada en 1917 y con sede en Yuba City, California, la empresa Sunsweet es el fabricante más grande del mundo de fruta deshidratada y controla más de un tercio del mercado mundial de ciruela pasa. La empresa, que dirige la planta de producción de fruta deshidratada más grande del mundo, produce anualmente cerca de 70 mil toneladas de ciruelas pasas. Su red contiene datos confidenciales de casi 300 productores miembros, además de información propietaria, de empleados y de clientes.

> El Enterprise Immune System ha revolucionado nuestra seguridad. La visibilidad que logramos gracias a su enfoque hacia el aprendizaje de máquina es incomparable. Ahora encontramos anomalías en tiempo real que nos hubiera costado semanas, o incluso meses, detectar por nuestra cuenta.
>
> **Terrell Johnson, director de sistemas y redes, Sunsweet**

Desafío

Debido a la naturaleza cada vez más compleja de las amenazas cibernéticas y a la frecuencia de ataques automatizados, la principal preocupación de Sunsweet era la adopción de un enfoque proactivo hacia la ciberdefensa. Las amenazas a gran velocidad, como el ransomware, pueden causar estragos en una red en cuestión de minutos y Sunsweet necesitaba una herramienta que pudiera alertar al equipo de seguridad – en tiempo real – sobre estos tipos de ataques, y capacitarlos para mitigar la amenaza antes de que se convirtiera en una crisis. Por otra parte, consideraban que su estrategia anterior se centraba más en emprender acciones retroactivamente contra las amenazas, por lo que necesitaban una herramienta que pudiera instalarse dentro de la red para identificar los ataques cibernéticos conforme se producían y no semanas más tarde.

"Estábamos cada vez más preocupados por la frecuencia de ataques automatizados, como el ransomware", explicó Terrell Johnson, director de sistemas y redes, Sunsweet. "Se está haciendo casi imposible intentar mantenernos actualizados respecto a estas nuevas amenazas automáticas. Necesitábamos una herramienta que pudiera garantizar la seguridad de nuestra red desde adentro hacia afuera e identificar estas amenazas en tiempo real".

En Sunsweet también pensaban que carecían de una visibilidad completa de su vasta red. Querían tener la capacidad para ver todo el tráfico de intrusos, incluyendo dispositivos no autorizados y el IoT. Además, el equipo carecía de confianza en su capacidad para detectar vulnerabilidades de día cero o 'amenazas desconocidas'. Debido a que, Sunsweet cuenta con un modesto equipo de, por lo que deseaba ndisponer de una herramienta que le permitiera cumplir todos estos objetivos aliviando al mismo tiempo la carga de trabajo del personal.

Solución

En su empeño por poner en marcha un enfoque más proactivo hacia la seguridad, la empresa implementó el Enterprise Immune System de Darktrace en el núcleo de su red. Tras una rápida instalación, sin necesidad de ajustes ni configuraciones especiales, Sunsweet pudo tener una visibilidad total del tráfico de su red mapeado en el 3D Threat Visualizer.

"El aprendizaje de máquina de Darktrace es verdaderamente incomparable", afirmó Johnson. "Tan pronto como implementamos la tecnología, pudimos ver al instante cada dispositivo de nuestra red. Desde el primer día, fue evidente que la tecnología estaba aprendiendo realmente, con un nivel de detalle sorprendente, lo que era 'normal' para nuestra red".

Unas semanas después de la implementación, la tecnología demostró su poder cuando alertó a Sunsweet de una anomalía dentro de la red, un malware había infectado una máquina de la empresa. El equipo de seguridad fue capaz de limpiar la máquina y resolver el problema en menos de una hora después de la infiltración.

"Normalmente habríamos tardado semanas en detectar algo así", agregó Johnson. "Con Darktrace, fuimos capaces de detectar la infección conforme se producía".

Sobre la base del aprendizaje automático sin supervisión, Darktrace funciona aprendiendo el 'patrón de vida' de cada usuario y dispositivo de toda la red, incluida la red física, el IoT y los dispositivos no autorizados. Partiendo de esta comprensión precisa de la 'forma de ser', puede identificar amenazas en sus primeras fases, en tiempo real, sin depender de reglas, firmas ni presuposiciones.

Sobre la base del aprendizaje de máquina sin supervisión, Darktrace funciona aprendiendo el 'patrón de vida' de cada usuario y dispositivo de toda la red, incluyendo la red física, el IoT y los dispositivos no autorizados. Partiendo de esta comprensión precisa de la 'forma de ser', puede identificar amenazas en sus primeras fases, en tiempo real, sin depender de reglas, firmas ni presuposiciones.

Ventajas

Después de equipar a Sunsweet con el Enterprise Immune System, la empresa tiene ahora una mayor confianza en su capacidad para mantenerse actualizada frente al cada vez más sofisticado panorama en el que las máquinas pueden ejecutar ataques fulgurantes. Además, debido a que la tecnología comprende de manera innata y completa lo que es 'normal', clasifica las amenazas en función de su grado de anormalidad, alivianando así la carga de trabajo del equipo de seguridad.

"El aprendizaje de máquina de Darktrace ha permitido a mi equipo de operaciones de TI mejorar su eficacia", comentó Johnson. "Gracias al enfoque del 'sistema inmunológico', ya no tenemos que pasar horas revisando registros e intentando predecir el nivel del 'daño' con antelación".

Además, Sunsweet posee ahora un conocimiento sin precedentes de su red, incluido todo el tráfico de intrusos. El Threat Visualizer les ofrece visibilidad completa de la red en tiempo real, permitiendo al equipo no solo detectar amenazas emergentes, sino también identificar áreas más débiles, lo que en última instancia les ayuda a aumentar su eficacia.

"El Enterprise Immune System ha revolucionado nuestra seguridad", afirmó Terrell Johnson, director de sistemas y redes, Sunsweet. "La visibilidad que logramos gracias a su enfoque hacia el aprendizaje automático es incomparable. Ahora encontramos anomalías en tiempo real que nos hubiera costado semanas, o incluso meses, detectar por nuestra cuenta".

Con el Enterprise Immune System, Sunsweet se ha posicionado como líder de la industria. Basándose en los últimos avances en aprendizaje automático sin supervisión e inteligencia artificial, han aumentado su productividad, disfrutando al mismo tiempo de una mayor confianza en su capacidad para mantenerse actualizados frente al panorama de las amenazas que se caracteriza cada vez más por la velocidad, la sofisticación y la automatización.

> El aprendizaje de máquina de Darktrace es incomparable.
>
> **Terrell Johnson, director de sistemas y redes, Sunsweet**

Contacto

Norteamérica: +1 (415) 229 9100
Europa: +44 (0) 1223 394 100
Asia-Pacífico: +65 6804 5010

info@darktrace.com
darktrace.com