DARKTRACE

CASO PRÁCTICO

Ciudad de Las Vegas

Información

Industria

- Gobierno y defensa

Desafío

- Contención de ataques a la velocidad de la máquina con un equipo de seguridad sometido a presión
- Falta de visibilidad del tráfico de intrusos y amenazas transmitidas por correo electrónico
- Defensa de la infraestructura multinube desde una vista unificada
- Necesidad imperativa de garantizar la tecnología de ciudad inteligente basada en el IoT

Resultados

- Implementación de la IA de Darktrace para detección de amenazas y respuesta autónoma en tiempo real
- Visibilidad total de toda la infraestructura de nube híbrida y de la red industrial
- Capacidad para neutralizar de forma autónoma ataques basados en la nube en tiempo real
- Protección de infraestructura crítica contra amenazas nunca vistas

Antecedentes

En los últimos años, Las Vegas se ha convertido en una ciudad inteligente prototípica. Mientras los pasajeros a bordo del primer transporte completamente autónomo jamás implementando en una vía pública recorren el Strip de las Vegas, es muy probable que no vean basura en las aceras. Esto se debe a que las cámaras de vigilancia de la ciudad transmiten imágenes a un servicio de IA que dirige a los equipos de limpieza hacia los puntos en que se acumula la basura. Cuando se acerca la hora punta, sus pasajeros pueden estar seguros de que una matriz de sensores conectados ayudan a agentes de tráfico a anticipar atascos en intersecciones de mucho tráfico.

Pero mientras la infraestructura inteligente permite a Las Vegas alcanzar nuevas cotas de eficacia, las herramientas de seguridad convencionales están en gran medida mal preparadas para defender la nube híbrida y las redes industriales en las que se basa esta infraestructura. Estos entornos diversos atraen cada vez más a ciberdelincuentes sofisticados con intenciones de interrumpir servicios públicos o extraer datos confidenciales. Debido a la gran complejidad de la red a defender, la vanguardista ciudad de Las Vegas reconoció la necesidad de ciberdefensas igualmente innovadoras.

> La IA del Enterprise Immune System de Darktrace puede detectar y responder a amenazas transmitidas por correo electrónico, ataques basados en la nube y nuevas cepas de malware que pasarían desapercibidas para otras herramientas.
>
> **Michael Sherwood, director de tecnología e innovación, Las Vegas, Estados Unidos**

Desafío

Al emprender sus iniciativas de ciudad inteligente, la ciudad de Las Vegas tenía por objetivo apostar por la innovación sin comprometer la seguridad de sus 650 mil habitantes y 42 millones de turistas anuales. Sin embargo, las autoridades locales saben que la infraestructura conectada a Internet a menudo es vulnerable a ataques en línea dirigidos, que siguen dificultando la distinción entre las amenazas digitales y las físicas.

El malware automatizado actual a menudo ataca a la velocidad de la máquina, lo que provoca una preocupación justificada de los funcionarios municipales en caso de que el ataque –incluso si se trata de la violación de un solo dispositivo inteligente– pueda moverse lateralmente para cifrar o secuestrar toda su red en cuestión de minutos.

Además de los ataques externos a los que se enfrenta la infraestructura crítica de Las Vegas, la ciudad también corrió peligro por amenazas internas a sus datos privados e información de los contribuyentes. La mayoria de los incidentes globales relacionados con la ciberseguridad son producto de empleados maliciosos o negligentes, y debido a que el equipo de seguridad de la ciudad depende de herramientas tradicionales que no proporcionan visibilidad del tráfico de la red interna, no había manera de detectar estas amenazas. De hecho, debido a las limitaciones de personal, el equipo de seguridad estaba mal preparado para contrarrestar cualquier tipo de ciberataque que evolucionara rápidamente en tiempo real antes de que infringiera daños.

Pero el mayor desafío defensivo al que se enfrentó Las Vegas fueron los ataques nunca vistos. Las herramientas de seguridad tradicionales funcionan usando reglas y firmas fijas para predefinir el aspecto de una amenaza, evitando que detecten amenazas nunca antes vistas. Desde correos electrónicos de spear phishing haciéndose pasar por contactos confiables, hasta nuevos ataques que intentan infiltrarse a través del entorno multinube de la ciudad, Las Vegas buscó una herramienta de seguridad única capaz de ir al compás del panorama de amenazas en constante evolución.

Solución

La búsqueda por parte de la ciudad de una solución de seguridad adaptativa, les llevó a implementar la IA de Darktrace en todas sus redes empresariales, de nube e industriales. Sobre la base de la Inteligencia Artificial líder mundial, Darktrace comenzó inmediatamente un proceso de autoaprendizaje del 'patrón de vida' único de cada empleado y dispositivo de Las Vegas. Y lo más importante de todo es que la IA de Darktrace no predefine qué constituye una amenaza para la ciudad; más bien, detecta las anomalías sutiles de comportamiento asociadas con cualquier ataque, ya sea conocido o desconocido. Para defenderse de ataques automatizados en tiempo real, la ciudad también implementó Darktrace Antigena, la primera herramienta de respuesta de ciber IA que neutraliza las amenazas de forma autónoma emprendiendo acciones quirúrgicas inteligentes.

Antigena funciona confinando los dispositivos infectados en su 'patrón de vida' típico en menos de dos segundos, conteniendo amenazas significativas sin interrumpir las operaciones municipales centrales. Estas operaciones dependen en gran medida de la arquitectura multinube de Las Vegas, que incluye Amazon Web Services, Microsoft Azure y Office 365. Mientras que el enfoque descontextualizado convencional para asegurar estos servicios carece de un contexto vital, Darktrace analiza flujos de datos de toda la infraestructura digital de la ciudad, lo que permite que la respuesta de ciber IA de Antigena neutralice los ataques independientemente de su de origen.

> Darktrace representa una nueva frontera en la ciberdefensa basada en IA. Nuestro equipo tiene ahora cobertura completa en tiempo real a través de nuestras infraestructuras en la nube, empresarial e industrial.
>
> **Michael Sherwood, director de tecnología e innovación, Las Vegas, Estados Unidos**

Ventajas

Darktrace ya ha detectado y respondido a numerosos ataques contra la ciudad de Las Vegas, entre los que se incluye una campaña de spear phishing dirigida que eludió los controles de correo electrónico nativos de la ciudad. Los sofisticados atacantes, que habían obtenido la libreta de direcciones de la ciudad, enviaban mensajes de correo electrónico aparentemente inofensivos, pero que contenían una carga maliciosa, a los destinatarios por orden alfabético, de la 'A' a la 'Z'. A pesar de la naturaleza enmascarada de este ataque, Antigena marcó inmediatamente como anómalo el dominio vinculado en los correos electrónicos para los empleados de Las Vegas, una acción solo posible gracias a la paulatina comprensión de la 'forma de ser' que aprende la IA de Darktrace.

En aquel momento, Antigena se implementó en 'modo pasivo', el modo inicial que restringe la IA a comunicar qué habría hecho para dar respuesta a la amenaza, sin emprender ninguna acción. Curiosamente, esto sirvió para demostrar su capacidad para detener ataques que habrían pasado desapercibidos para otras herramientas. Mientras que Darktrace detectó la campaña en la letra 'A', el conjunto de herramientas tradicionales de ciudad reaccionó ante la amenaza en la letra 'R' En el 'modo activo', Antigena habría neutralizado el ataque antes de que hubiera llegado a un solo usuario. La IA de Darktrace ha transformado fundamentalmente la postura defensiva de la ciudad, brindando a sus líderes la confianza para adoptar tecnologías inteligentes y servicios en la nube por igual.

Contacto

Norteamérica: +1 (415) 229 9100

Latinoamérica: +55 11 97242 2011

Europa: +44 (0) 1223 394 100

Asia-Pacífico: +65 6804 5010

info@darktrace.com

darktrace.com