Plataforma Cyber AI

Antigena Email

Desarrollo de inmunidad para su bandeja de entrada

Resumen

- **Autoaprendizaje: comprende al humano, no solo la dirección de e-mail**
- **Identifica mensajes de e-mail maliciosos que las herramientas tradicionales dejarían pasar**
- **Eficaz contra todos los ataques de e-mail avanzados, incluyendo la ingeniería social**
- **Implementación rápida y virtual**

Amenazas de e-mail que reconoce Antigena Email

- Spear phishing
- Ingeniería social y suplantación de identidad
- Compromiso del e-mail empresarial
- Robo de cuentas de la cadena de suministro
- Pérdida de datos externos
- Malware nuevo desconocido

> Qudamos sorprendidos con las cosas que nuestras herramientas tradicionales no detectaban y que Antigena Email sí detectó.
>
> **– CTO, Bunim/Murray Productions**

Llegada de nuevas amenazas de e-mail

Los ataques de e-mail son cada vez más sofisticados y en un futuro cercano se espera que IA ofensiva acelere las campañas de ataques de e-mail. Resulta casi imposible distinguir entre los e-mails de spoofing de las comunicaciones genuinas.

Los nuevos ataques eluden constantemente las herramientas de seguridad de e-mail tradicionales, que observan los e-mails individuales de forma aislada y los comparan con reglas y firmas de ataques maliciosos conocidos. Con cadenas de suministro cada vez más complejas y empleados cada vez más distribuidos y móviles, resulta muy necesario un enfoque hacia la seguridad del e-mail basado en el autoaprendizaje impulsado por la IA.

> Ahora más que nunca, la seguridad de e-mail moderno exige innovación y un cambio de mentalidad para combatir el cambiante panorama de amenazas.
>
> **– Gartner**

La primera bandeja de entrada con capacidad de autodefensa del mundo

Antigena Email es la primera solución de ciber AI del mundo para la bandeja de entrada. Mediante el aprendizaje del 'patrón de vida' normal de cada usuario y corresponsal, la tecnología va comprendiendo paulatinamente lo 'humano' de las comunicaciones por e-mail.

Mientras que las defensas tradicionales preguntan si se han observado elementos de un e-mail en ataques históricos, Antigena Email es la única solución que puede preguntar de forma fiable si sería inusual que un destinatario interactuara con un mensaje de e-mail específico en el contexto de su 'patrón de vida' normal, así como si lo sería para sus compañeros y la organización en general.

Este conocimiento contextual permite a la IA tomar decisiones muy precisas y neutralizar toda la gama de ataques de e-mail, desde mensajes 'limpios' que buscan realizar un pago electrónico a intentos sofisticados de spear phishing.

Comprende al humano que hay detrás del mensaje

Inspirado en el sistema inmunológico, Antigena Email utiliza la IA especializada de Darktrace para aprender la 'forma de ser' de cada usuario interno y externo, analizando tanto las comunicaciones entrantes como las salientes, así como las comunicaciones laterales e internas.

Al tratar a los destinatarios como individuos y compañeros dinámicos, Antigena Email identifica de manera única desviaciones sutiles de la 'norma' que revelan que mensajes de e-mail benignos en apariencia son inequívocamente maliciosos.

Caso de uso:
Robo de cuentas de una cadena de suministro

Uno de los ataques más difíciles de detectar es el robo de cuentas externas, en el que un criminal secuestra las credenciales de e-mail de un contacto de confianza y obtiene acceso a su bandeja de entrada.

Una vez dentro, el atacante puede acceder a la correspondencia histórica y producir mensajes muy convincentes, incrustando en la conversación un enlace o archivo adjunto malicioso en el momento adecuado.

Mientras que las defensas tradicionales asumen que se trata de un usuario de confianza, Antigena Email detecta que no lo es. Analiza cada mensaje en el contexto de patrones de vida aprendidos y detecta incluso las desviaciones más sutiles. Estas incluyen (entre otras):

Ubicación de inicio de sesión inusual – Antigena Email puede extraer la dirección IP geolocalizable del remitente auténtico y determinar si esto es raro en relación con el patrón de vida histórico del contacto de confianza. Aunque es posible que una ubicación de inicio de sesión rara no pueda por sí sola activar una alerta o una respuesta autónoma, se tendrá en cuenta en el cálculo general del sistema y en la puntuación de anomalías.

Rareza del enlace – La gente comparte a menudo enlaces a los sitios Web que visitan y en los que confían. Al observar estos enlaces en el correo lateral, Antigena Email puede determinar qué enlaces y dominios son raros en el contexto de la organización. Esto también resulta útil en otros escenarios de amenazas para poder determinar si se ha observado el dominio de e-mail de un remitente determinado en enlaces internos compartidos.

Destinatarios inusuales – Antigena Email modela las relaciones basadas en gráficos entre usuarios y compañeros internos y externos, y comprende sus relaciones a un nivel más detallado. Si el atacante envía varios mensajes de e-mail a una serie de destinatarios de la organización, Antigena Email puede estimar la probabilidad de que este grupo concreto reciba un mensaje de e-mail de la misma fuente.

Anomalías de comportamiento – Con el tiempo, Antigena Email aprende el modo en que los distintos remitentes construyen sus mensajes de e-mail, analizando tanto los metadatos ocultos del mensaje de e-mail como los patrones del cuerpo del mensaje. Al aplicar la IA a cada mensaje de e-mail entrante, Darktrace identifica cambios sutiles que podrían indicar que el mensaje de e-mail ha sido enviado por alguien que no es el verdadero titular de la cuenta.

Al correlacionar estos indicadores débiles, Antigena Email puede realizar rápidamente una puntuación de anomalías completa, determinando con confianza que el e-mail es malicioso y neutralizando el ataque antes de que pueda provocar daños.

Descubra Antigena Email en su propio entorno con una prueba gratuita de 30

Agende una demostración, ahora