Respuesta de ciber IA: Informe de amenazas 2019

Introducción

Los líderes empresariales de la era digital se enfrentan a factores de riesgo extraordinariamente urgentes en una época en la que las ciberamenazas se han automatizado y evolucionan a gran velocidad. Estos riesgos han aumentado espectacularmente en los últimos años a medida que las amenazas se desarrollan y se vuelven más avanzadas, mientras que nuestras empresas digitales siguen creciendo en complejidad, diversidad y escala.

En el pasado, cuando los agentes que lanzaban amenazas estaban menos desarrollados y cuando las redes eran más previsibles, el enfoque tradicional hacia la seguridad a menudo bastaba para mantener a raya las amenazas cibernéticas. Mediante la configuración de herramientas de seguridad combinadas con algunas reglas o firmas, los equipos de seguridad han tratado de detectar amenazas definiéndolas con antelación como 'inofensivas' o 'maliciosas', basándose en representaciones de ataques que han sido concebidos en forma de regla u observados durante su propagación, y que se han analizado mediante técnicas de ingeniería inversa para poder detectarlos en el futuro.

Pese a ello, los cada vez más frecuentes e innovadores ataques externos y amenazas internas, unidos a la complejidad y sutileza de los comportamientos diarios en una empresa, han ido desarmado gradualmente a los equipos de seguridad que aún confían en los controles tradicionales. Las defensas tradicionales no logran detectar las tácticas novedosas ni las técnicas sofisticadas de los ciberdelincuentes, que ahora pueden pasar desapercibidos en la inmensidad de la red y hacer un barrido de grandes y complejas infraestructuras en cuestión de segundos.

El hecho es que las nuevas amenazas logran inevitablemente su propósito, por lo que la atención de la industria se orienta hacía cómo equipar a los responsables de ciberdefensa para que puedan detectar y dar respuesta a las amenazas emergentes que ya han logrado acceder a la empresa pero que aún pueden controlarse antes de que provoquen una crisis. Los líderes empresariales y los equipos de seguridad han recurrido a la inteligencia artificial para responder y ponerse al día.

La exclusiva aplicación de IA de Darktrace aprende el 'patrón de vida' norma de empresas individuales y detecta desviaciones sutiles indicativas de una amenaza, ya sea conocida o desconocida, externa o interna, sutil o que evoluciona a gran velocidad. Al aprender mientras 'trabaja' y adaptándose continuamente a partir de nuevas evidencias, la inteligencia artificial de Darktrace detecta indicadores de ciberamenazas en etapas tempranas que de otra manera habrían pasado desapercibidas, sin depender de reglas, firmas ni conjeturas previas.

Resumen

En este informe se analizan siete casos reales de ataques que fueron interceptados y neutralizados mediante IA de ciberdefensa, incluidos amenazas internas, ransomware y ataques de IoT (internet de las cosas, por sus siglas en inglés).

Aunque todas las situaciones de amenaza eran distintas, unas evolucionaban rápidamente y otras eran lentas y sutiles, los indicadores sutiles de actividad sospechosa solo pudieron detectarse, en todos los casos, empleando la IA de Darktrace, la cual aprende lo que es normal para el entorno empresarial y responde de forma autónoma a los ataques, antes de que inflijan daños.

Contraataque con Darktrace Antigena

A medida que la brecha se ensancha y el volumen y la velocidad de los ataques se elevan, la IA no solo resulta esencial para detectar nuevas amenazas, sino que también se confía en ella para impulsar la primera capa de defensa de una organización. Se trata de una IA que puede contraatacar en tiempo real, permitiendo al equipo de seguridad ganar tiempo para recuperar terreno.

Gracias a una profunda comprensión, que no deja de evolucionar, del 'patrón de vida' normal de cada usuario, dispositivo y grupo de pares asociados de una empresa, la IA de Darktrace no solo puede responder a indicadores de ciberamenazas en etapas tempranas antes de que produzcan daños, sino que además lo hacen de un modo muy selectivo. En lugar de imponer cuarentenas generalistas que solo servirían para provocar más interrupciones, Darktrace Antigena, la solución de ciber IA de respuesta autónoma de Darktrace, aplica quirúrgicamente el 'patrón de vida' normal de un dispositivo infectado o empleado descontento para neutralizar la amenaza en cuestión de segundos y permitir el desarrollo normal de las operaciones.

En su lucha contra ciberdelincuentes avanzados, la ciber IA de Darktrace devuelve el control a los defensores, transformando a una organización compleja y vulnerable en una empresa digital resistente con capacidades de autodefensa.

Amenazas internas

Un empleado escanea la red en busca de vulnerabilidades

Maliciosas y persistentes

La amenaza interna constituye uno de los vectores de ataques más comunes y peligrosos para cualquier empresa, sean maliciosas o no. Los intrusos maliciosos representan una amenaza especialmente significativa para la empresa, ya que su acceso y conocimiento privilegiado sobre la red, les permite llevar a cabo ataques ampliados para extraer o manipular datos críticos sin despertar sospechas.

La IA de Darktrace identificó y neutralizó a uno de estos intrusos maliciosos en una importante firma de inversiones de Sudáfrica. La IA de autoaprendizaje fue capaz de contener una amenaza persistente a través de las distintas etapas de la cadena de ataques, desde el reconocimiento a la escritura hasta ejecución de scripts. Mediante el aprendizaje 'en curso', Antigena se adaptó a la amenaza conforme evolucionaba y la contuvo eficazmente en cada etapa.

Comportamiento sospechoso

La etapa de reconocimiento comenzó con un portátil que enviaba 'pings' a cientos de direcciones IP internas para identificar las que estaban activas. A continuación, realizó un barrido de la red buscando los nombres de las máquinas que respondían y las escanéo para detectar canales de comunicación abiertos. La IA de Darktrace marcó el comportamiento sospechoso como una actividad inusual de escaneo de la red e instantáneamente solicitó a Antigena que interviniera. Sobre la base de la evaluación dinámica de la amenaza, Antigena decidió forzar durante una hora el 'patrón de vida' del grupo de dispositivos, evitando que el portátil se desviara de su comportamiento anterior o del de sus compañeros.

No obstante, pocas horas más tarde, la amenaza regresó. El portátil comenzó a ejecutar comandos en cientos de computadoras internas dentro del rango de las IP que había identificado inicialmente. Esto implicó mover archivos de scripts multipropósito y emplear una herramienta de administración remota. Estos programas podrían haberse aprovechado para localizar documentos e información confidenciales o bien, para abrirle la puerta trasera a un atacante.

> Antigena decidió imponer durante una hora el 'patrón de vida' del grupo de dispositivos

Antigena interviene

Durante este periodo de tiempo no se había detectado ninguna otra acción similar de escritura de archivos, algo que se reveló como sumamente inusual para la IA de Darktrace. Dada su capacidad para comprender paulatinamente la amenaza en el contexto de la red y su anterior respuesta autónoma, Antigena decidió bloquear todas las conexiones salientes utilizando el canal de transferencia de archivos SMB, conteniendo inmediatamente cualquier movimiento lateral a través de la red.

Cuando se neutralizó la amenaza, el equipo de seguridad pudo investigar y confirmar que el portátil pertenecía a un miembro del equipo de TI que había estado utilizando una herramienta de escaneo ilegítima para buscar puntos débiles en la red. Este es un ejemplo especialmente revelador del poder de la IA de Darktrace y de cómo Antigena puede intervenir en las diferentes etapas de una cadena de ataques y neutralizar amenazas persistentes en etapas tempranas.

Troyano de día cero

Descarga y conexiones sospechosas

Nueva cepa de malware

Mientras que las herramientas de seguridad tradicionales pueden identificar amenazas conocidas que ya han sido descubiertas, la IA puede detectar de manera única señales débiles y sutiles de ciberamenazas nunca antes vistas. En los últimos años, esta capacidad se ha convertido an una necesidad a medida que los ciberdelicuentes avanzados continúan desarrollando tácticas, técnicas y procedimiento novedosos, diseñados específicamente para eludir controles que han sido pre-programados con firmas de ataques anteriores.

La capacidad de Darktrace para reaccionar ante estos indicadores sutiles resultó esencial para una empresa norteamericana de controles de IoT industrial que sufrió el ataque de un troyano de día cero.

A las 13.30 horas de un jueves, la IA alertó al director de TI de la empresa de una descarga sospechosa de un archivo llamado 'OfficeActive.bin'. A pesar de que el archivo parecía un producto de Microsoft, Darktrace indicó que estaba siendo descargado desde una fuente no identificada y totalmente extraña para la red.

> A pesar de que el archivo parecía un producto de Microsoft, Darktrace indicó que estaba siendo descargado desde una fuente no identificada

Generando confianza en la respuesta de la IA

En aquel momento, Antigena estaba configurado 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, para permitir que el equipo fuera confiando paulatinamente en la toma de decisiones del sistema. El equipo de TI pudo ver cómo Antigena habría detenido el ataque en una etapa temprana y también el modo en que se adaptó a la nueva amenaza conforme se intensificaba.

Para dar respuesta a un patrón de actividad altamente inusual, Antigena recomendó en primer lugar forzar durante dos horas el 'patrón de vida' del grupo de dispositivos, lo que hubiera detenido la evolución de la amenaza permitiendo el desarrollo normal de las operaciones.

Pero como Antigena observó más descargas sospechosas, intensificó su respuesta forzando durante cinco minutos el 'patrón de vida' individual del dispositivo. De este modo, cuando el dispositivo intentó establecer una nueva conexión externa, Antigena respondió de nuevo, sugiriendo que la IA bloqueara quirúrgicamente durante una hora todas las conexiones salientes del dispositivo.

Solucionando la amenaza

A los pocos minutos de identificar la alerta, el director de TI se había puesto en contacto con el usuario final y había emprendido acciones de emergencia para solucionar la amenaza sobre la máquina. Llevó tan solo 20 minutos completar todo el proceso. Una vez que se neutralizó la amenaza, el director de TI copió la URL del troyano y el nombre de archivo en Virus Total para comprobar si la amenaza se había observado y registrado en otros lugares. Esta búsqueda no ofreció resultados, confirmando así que se trataba sin duda de un troyano de día cero solo descubierto por la IA de Darktrace.

Hackeo de IoT: CCTV

¿Espionaje corporativo?

Cámara de seguridad comprometida

El aumento de la conectividad de los dispositivos de uso cotidiano ha introducido aún más vulnerabilidades en las empresas. Los dispositivos de IoT, a menudo diseñados con controles de seguridad básicos no integrados, son sistemáticamente atacados por agentes que lanzan amenazas y se utilizan como vías de acceso a la red.

En una consultoría de inversiones japonesa, Darktrace descubrió que un sistema de CCTV conectado a Internet había sido infiltrado por atacantes desconocidos. Los autores, por lo tanto, habían accedido a la red y podían ver todas las grabaciones de vídeo de la cámara. La cámara, que se había instalado para vigilar todo el espacio de oficina, desde la oficina del director general a la sala de juntas, se convirtió en un riesgo de seguridad.

> La IA contraatacó a toda velocidad, evitando una brecha grave

Reacción rápida

La IA de Darktrace detectó rápidamente que había un problema. Se observó que se movían volúmenes masivos de datos hacia y desde un servidor de CCTV sin encriptacioón ya que el atacante recopiló datos para preparar la extracción de información confidencial.

En el momento en el que el atacante intentó extraer los datos, Antigena emprendió una acción defensiva rápida y precisa. El sistema decidió bloquear quirúrgicamente el movimiento de datos desde el dispositivo a un servidor externo, aunque sin interrumpir el funcionamiento normal del CCTV.

La IA contraatacó a toda velocidad, evitando una filtración grave de información que podía influir en el mercado. Al emprender una acción proporcionada para contener el ataque en una etapa temprana, Antigena ganó tiempo vital para que el equipo de seguridad pudiera investigar y remediar la amenaza antes de que se ocasionara algun daño.

Hackeo de IoT: Locker inteligente

Ataque dirigido hacia datos confidenciales de clientes

Vulnerabilidad del IoT

En un parque de diversiones norteamericano, alguien intentó robar datos de clientes confidenciales a través de un dispositivo de IoT vulnerable: un locker 'inteligente' empleado por visitantes para guardar pertenencias personales.

Como parte de su configuración predeterminada, el locker inteligente establecía contacto regularmente con la plataforma en línea de terceros del proveedor. El agente responsable de la amenaza identificó el origen de este proceso automatizado y lo secuestró para comprometer el dispositivo.

Ataque 'low and slow'

La IA de Darktrace detectó el ataque poco después de que el locker comenzara a enviar una cantidad inusual de datos sin encriptación a un sitio externo ajeno. Las conexiones se sincronizaron con las comunicaciones regulares del dispositivo con la plataforma del proveedor, sugiriendo que se trataba de un ataque 'low and slow' diseñado específicamente para eludir las defensas de seguridad basadas en reglas.

Mediante un análisis continuo de las comunicaciones en relación al comportamiento anterior del locker y de lockers compañeros, la IA de Darktrace determinó que se requería una respuesta de ciber IA. En cuestión de segundos, Darktrace Antigena emprendió acciones, bloqueando de manera inteligente todas las conexiones salientes desde el dispositivo afectado, dando así tiempo al equipo de seguridad a solucionar la amenaza e impedir la extracción de más datos.

Para este y otros parques de diversiones, la ciber IA de Darktrace ha neutralizado innumerables ataques 'low and slow' en una etapa temprana. Al aprender 'trabajando', el sistema detecta amenazas sutiles que pasarían desapercibidas por otras herramientas. Revisa continuamente su comprensión a partir de nuevas evidencias y emprende acciones autónomas que se adaptan a la amenaza conforme se desarrolla.

Ransomware

Rápido y letal

Extorsión automatizada

A las 19:05 horas de un viernes, un empleado de una gran empresa de telecomunicaciones accede a su correo electrónico personal desde el smartphone de la empresa y fue engañado para descargar un archivo malicioso, que contenía ransomware. Segundos después, el dispositivo comenzó a conectarse a un servidor externo de la red Tor.

La IA de Darktrace respondió casi al instante. Tan solo nueve segundos después del inicio de las actividades de la encriptación SMB, Darktrace lanzó una alerta prioritaria para indicar que esta anomalía requería investigación. Como el comportamiento persistió en los segundos posteriores, Darktrace modificó su decisión y activó Antigena.

Debido a que el equipo de seguridad se había marchado a casa para pasar el fin de semana, Darktrace Antigena intervino de forma autónoma e interrumpió todos los intentos de escribir archivos encriptados en recursos compartidos de la red. Esto neutralizó instantáneamente la amenaza antes de que pudiera propagarse a través de la inmensa infraestructura de telecomunicaciones, dando tiempo al equipo de seguridad para ponerse al día.

Debido a que no dejan de aparecer cepas automatizadas de ransomware en la 'Dark Web' y en redes corporativas de todo el mundo, las empresas necesitan contraatacar con IA para no perder terreno. Tanto en este caso como en otros, la ciber IA de Darktrace se ha convertido en un componente esencial en la lucha, ya que frena ataques que evolucionan rápidamente antes de que tengan tiempo de cifrar datos críticos y provocar un daño irreparable.

'Spear phishing'

Un ataque dirigido a un correo electrónico

Ataque de correo electrónico

Un municipio de EE. UU. fue víctima de un ataque transmitido por correo electrónico. Mientras que muchos de los ataques de 'phishing' son campañas indiscriminadas, esta en concreto presentaba todas las características de un sofisticado delito cibernético coordinado. Todos los correos electrónicos estaban bien diseñados y adaptados al destinatario previsto. El agente responsable de la amenaza también tenía la agenda de direcciones de la ciudad, ya que el ataque se dirigía a los destinatarios por orden alfabético, de la A a la Z.

Aunque cada correo electrónico parecía inofensivo y estaba adaptado al destinatario, todos los mensajes contenían una carga maliciosa oculta tras un botón camuflado de distintas formas como vínculo a Netflix, Amazon y otros servicios de confianza.

> Antigena detectó la campaña en la letra 'A', mientras que las herramientas tradicionales reaccionaron ante la amenaza en la letra 'R'

Enlaces ocultos

La IA de Darktrace fue capaz de analizar estos enlaces ocultos en relación con los patrones de vida 'normales' de los destinatarios en la red. Cuando llegó el primer correo electrónico, Antigena reconoció inmediatamente que ni el destinatario ni nadie de su grupo o del resto del personal de la ciudad, había visitado ese dominio con anterioridad. Antigena activó inmediatamente una alerta de confianza alta y sugirió de manera autónoma bloquear cada enlace conforme accedía a la red.

Curiosamente, el hecho de haber implementado Antigena en 'modo pasivo' pudo demostrar con evidencias claras y concretas la capacidad del sistema para frustrar ataques sutiles que habrían pasado desapercibidos por otras herramientas: mientras que Antigena detectó e intentó neutralizar la campaña en la letra 'A', las herramientas tradicionales del equipo de seguridad reaccionaron a la amenaza en la letra 'R'. En el 'modo activo', Antigena habría neutralizado el ataque antes de que hubiera podido llegar a un solo usuario.

Ataque de la cadena de suministro

Un impostor que se aprovechaba de relaciones de confianza

Cuenta de correo electrónico secuestrada

Algunos de los ciberdelincuentes más ingeniosos han aprendido que la manera más sencilla de introducirse en una empresa es a menudo es a través de la puerta delantera, siempre que se obtenga la confianza de un usuario legítimo. Mediante el secuestro de la información de la cuenta de un compañero de confianza, socio empresarial o proveedor de la cadena de suministro, los agentes que lanzan amenazas pueden engañar a los destinatarios para que hagan clic en un vínculo malicioso o para transferir cantidades enormes de dinero fuera de la empresa.

La IA de Darktrace detectó un ataque de este tipo dirigido a un estudio de producción audiovisual de Los Ángeles, Estados Unidos, después de que la información de la cuenta de un proveedor de confianza hubiera sido comprometida.

La información de una cuenta puede aprovecharse para muchos fines criminales, pero en este caso, el delincuente parece haberla usado para acceder al historial de la correspondencia entre el contacto y un empleado del estudio. Tras revisar conversaciones anteriores entre el contacto y el empleado para comprender el modo en que se comunicaban normalmente, envió una respuesta plausible al último mensaje de correo electrónico del empleado.

> El correo electrónico fue convincente, ya que reflejaba el estilo y tono de escritura del contacto

¿Se lo cree?

El correo electrónico fue convincente, ya que reflejaba el estilo y tono de escritura del contacto, y tenía sentido en el contexto de las relaciones y de conversaciones anteriores. También incluía un enlace malicioso que habría parecido inofensivo a cualquier empleado sensato que recibía un vínculo de un contacto familiar en una empresa familiar. Estos tipos de ataques son cada vez más comunes y muy difíciles de detectar.

La IA de Darktrace reconoció indicadores sutiles que revelaban que este 'contacto de confianza' era una cuenta secuestrada controlada por un atacante. La respuesta de la IA fue informar a la red de que el correo electrónico y su contenido se encontraban fuera del 'patrón de vida' del supuesto remitente. Se alertó al empleado y la carga maliciosa fue neutralizada.

Y lo más importante, la de decisión Antigena se basó en el hecho de que este vínculo concreto habría sido algo extraño tanto para el remitente como para el destinatario, dadas sus comunicaciones previas y los 'patrones de vida' normales del empleado en la red. El equipo de seguridad estaba seguro de su decisión de seguridad ya que sabían que la IA de Darktrace no trataba al destinatario de la red como una mera dirección de correo electrónico. En vez de eso, Antigena reconoce que el alcance completo del 'patrón de vida' de un empleado a menudo se manifiesta en distintos rincones de la red y de un modo que la ciber IA puede correlacionar y analizar de manera correcta.

Contáctenos

Colombia: +57 322 942 6401
España: +34 687 97 2717
Latinoamérica: +55 11 97242 2011
Europa: +44 (0) 1223 394 100
info@darktrace.com | darktrace.com/es
@darktrace