DETECCIÓN DE ATAQUES DIRIGIDOS CON DETECCIÓN DE CONTEXTO AMPLIO™

REPORTE TÉCNICO

F-Secure

INTROCUCIÓN

La seguridad cibernética se encuentra en medio de un cambio de paradigma. Los ataques dirigidos están superando los mecanismos de prevención y detección que tienen las empresas. Las soluciones de protección de punto final no pueden detectar ataques sin archivos definidos por el comportamiento y el uso de herramientas legítimas del sistema operativo, en lugar de que un programa malicioso se instale en una máquina. Las tecnologías de detección ciertamente detectan eventos sospechosos, pero con demasiada frecuencia no logran filtrar el ruido de incidentes críticos,
generando un número abrumador de alertas que no tienen esperanza de ser procesadas.

De acuerdo con un estudio de la EMA de 2017, 1). 79% de los equipos de seguridad informaron estar abrumados por un alto número de alertas de amenazas. Y no es de extrañar: por ejemplo, un estudio realizado por Ovum encontró que el 37% de los bancos reciben más de 200,000 alertas por día y el 61% recibe más de 100,000 2). El Instituto Ponemon informa que casi la mitad de todas las alertas de seguridad son falsos positivos 3). Del resto, una gran parte es intrascendente y fácil de remediar.

Con la posibilidad de examinar solo una pequeña fracción de las alertas, los equipos de seguridad sobrecargados se ven obligados a dejar que la mayoría de las alertas activadas a diario se desplacen sin atención. Los equipos se quedan frustrados. El EMA encontró que el 52% del personal de operaciones siente altos niveles de estrés, y el 21% de ellos declara que "no contar con suficiente personal" es un factor de estrés. la escasez de habilidades de seguridad cibernética empeoró e impactó al 70% de las organizaciones.

Así que aquí estamos en 2018, con alta seguridad cibernética en nuestra conciencia colectiva, y las empresas todavía están luchando contra las vulneraciones. Se informa que el tiempo de permanencia promedio de la brecha es de 100 días, o más, dependiendo de la industria y el estudio 5). Las empresas aún están siendo sorprendidas con la guardia baja por vulneraciones que exponen sus redes y sus clientes.

Mientras tanto, los intrusos continúan, ocultos por un mar de alertas.

Cómo se ve un verdadero ataque dirigido: Case Gothic Panda

Para demostrar un ataque cibernético avanzado y dirigido, usamos el ejemplo del grupo de amenazas persistentes avanzadas (APT) conocido como Panda Gótico de la base de conocimiento y modelo de Tácticas, Técnicas y Conocimiento Común (ATT & CK ™) de MITRE para el comportamiento de adversario cibernético. 6) Los adversarios en este ejemplo de ataque están interesados en la exfiltración de documentos y propiedad intelectual, a menudo de naturaleza industrial.

El proceso de Gothic Panda se puede dividir en tres fases principales, como se muestra arriba. En la fase inicial de compromiso, los atacantes pretenden lograr la ejecución exitosa del código y el control de un sistema dentro del entorno objetivo. El objetivo de la segunda fase, la propagación de la red, es identificar y pasar a los sistemas deseados dentro del entorno de destino con la intención de descubrir credenciales y documentos para la exfiltración. En la fase final de exfiltración, el objetivo es recopilar los datos, comprimirlos en un paquete fácil de transmitir mientras se encuentra en el entorno de destino y luego proceder a la exfiltración ocultándose en otro tráfico de red saliente. Dependiendo de la configuración defensiva, la exfiltración puede ser mucho más ruidosa y más perceptible que tratar de esconderse en el ruido con herramientas de disposición de la tierra.

Desde un punto de vista de detección, la fase más importante es, naturalmente, la primera, antes de que el atacante gane persistencia y se mueva a sistemas de alto valor dentro del entorno objetivo. Las organizaciones bien preparadas utilizan una capa preventiva como las plataformas de protección de endpoints para bloquear las amenazas de malware de productos básicos, como el ransomware, que evita la ejecución de código malicioso en el entorno de destino. Sin embargo, los atacantes avanzados pueden permanecer sin ser detectados mediante el uso de ataques lentos y bajos, y al final encuentran una forma de evitar la capa preventiva. Es entonces cuando la detección y la respuesta entran en escena.

EL CONTEXTO ES TODO

En todo. En la vida y en la seguridad cibernética. Una llave gira la cerradura de la puerta de su casa. Importa si la persona que tiene la llave es su cónyuge o un ladrón. Una persona emerge de una tienda por departamentos que lleva una bolsa grande de mercadería. Importa si esa persona ha completado o no una transacción de pago antes de hacerlo. Un comando Powershell complicado se ejecuta desde la máquina de un usuario. Importa si se ejecuta como parte del mantenimiento del sistema o por Microsoft Word.

La falta de contexto, a la inversa, es falta de una fuente, casi todo lo que se necesita saber para emitir un juicio. Sin contexto, los eventos aislados aislados carecen de significado. Solo cuando se conectan los puntos entre eventos relacionados puede surgir una imagen completa.

La falta de contexto es un contribuyente principal para alertar la fatiga. Muchos sistemas de detección de intrusos en la actualidad todavía producen alertas aisladas que son en sí mismas anómalas, pero cuando se conectan con otros eventos relacionados, se consideran inocuas. Por lo tanto, las falsas alarmas abarrotan la fila, lo que aumenta la carga de trabajo para los equipos de seguridad que ya están agotados al máximo, y disminuye la probabilidad de que se descubran los incidentes reales.

HOMBRE Y MÁQUINA

Desde una perspectiva de mentalidad, debemos dejar de lado la noción de que la seguridad cibernética es sobre productos y servicios. Se trata de habilidades. Experiencia. Competencia. Independientemente de los productos y soluciones que tenga, todo se reduce a gestionar de forma proactiva un entorno altamente complejo y cambiante y un panorama de amenazas. Eso requiere habilidades. Desafortunadamente, la disponibilidad de las habilidades necesarias es escasa, y esta escasez será cada vez más apremiante a medida que las capacidades digitales se conviertan en una parte más importante de la creación de valor para todos.

Pero quizás aún más importante es que las habilidades por sí solas no son suficientes. Al igual que la tecnología ha aumentado nuestras capacidades cuando se trata de todo, desde el trabajo de productividad hasta la ingeniería, debemos desarrollar tecnologías que aumenten nuestras habilidades y nos ayuden a escalar nuestros esfuerzos cuando se trata de seguridad cibernética. Debemos desarrollar tecnologías que puedan aprender a hacer lo que hacen los analistas de seguridad humana, solo que a la velocidad de la luz: conectar los puntos, ubicar los eventos en una imagen general adecuada para hacer un juicio preciso.

Uniendo los hechos como un detective

Detectar en un contexto más amplio quizás se explique más fácilmente para personas no técnicas en un lenguaje sencillo con una analogía del mundo real. Imagina que se encuentra un coche estrellado en la base de un acantilado. ¿Fue un accidente, o fue un crimen involucrado? ¿Había alguien en el coche? Estas son preguntas importantes que se deben contestar para comprender cómo responder al descubrimiento.

Se llama a los investigadores forenses a la escena del accidente. Estudian el sitio para reconstruir la secuencia de eventos que condujeron al accidente. Estudian las huellas de los neumáticos en la parte superior del acantilado para determinar si el automóvil aceleró o si se aplicaron los frenos. Verifican el velocímetro para ver si pueden determinar qué tan rápido viajaba el auto. Verifican la temperatura del motor para tratar de determinar cuánto tiempo ha estado allí el automóvil. Realizan una verificación de la matrícula para averiguar a nombre de quién está registrado el automóvil y rastrear el sitio en busca de cualquier rastro de un ser humano. Analizan los eventos que ocurrieron en las semanas anteriores, tales como si el propietario del vehículo recibió llamadas telefónicas sospechosas o si su historial de navegación revela una búsqueda de servicio de mapas alrededor del acantilado, para eliminar anomalías en el comportamiento normal.

Por sí solos, cada uno de estos factores (velocímetro, temperatura del motor, eventos de semanas previas al accidente, etc.) parecería no tener sentido, pero cuando se ubica en el contexto adecuado, surgirá una historia que ayudará a los investigadores a determinar qué ha ocurrido y si se ha cometido un delito.

CAMBIO DE JUEGO

Desde el punto de vista del defensor, este cambio de paradigma cambia el juego. No es una opción dar un impulso a una solución de protección de punto final existente y comercializarla como una nueva tecnología. Los proveedores de seguridad cibernética deben crear nuevas soluciones desde el principio específicamente dirigidas a la nueva era y los nuevos problemas que enfrentamos. Esto significa un cambio desde las detecciones de un solo disparo, las detecciones de puntos y las respuestas binarias de activación / desactivación, a las detecciones basadas en contexto y de flujo de eventos, y las respuestas multifacéticas basadas en el riesgo.

Para dar un poco de perspectiva de la enormidad de este cambio, en el mundo tradicional de protección de endpoints, nuestros sistemas backend analizan más de un millón de muestras cada día para decidir si las muestras son maliciosas o no. Este es un número impresionante, gracias a que ya contamos con decenas de millones de clientes enpoint que envían estas muestras.

Sin embargo, en la nueva era de intentar detectar actividades maliciosas y ocultas de atacantes de los pequeños eventos individuales que los atacantes activan cuando ejecutan sus tácticas, técnicas y procedimientos, el juego es totalmente diferente. En un entorno de cliente mediano, con 1.300 endpoints, tenemos que analizar 70 millones de eventos de comportamiento al día.

La inteligencia artificial y el aprendizaje automático son, obviamente, la única solución escalable que se puede aplicar. Pero de nuevo, la IA sola no es la respuesta; por sí misma, la IA es poco más que un generador glorificado de falsos positivos. Más bien, lo que se necesita es la combinación perfecta de expertos en ciencia de datos y seguridad cibernética.

TOMANDO LA FORMA

La idea de una tecnología adaptada al contexto y adaptada por expertos surgió después de las discusiones con nuestros clientes. Les preguntamos qué les faltaba en su organización. Nos dijeron que tienen sistemas implementados para detener los archivos de malware que conforman el 99.9% del volumen de amenazas que enfrenta una organización. Lo que necesitaban era una herramienta para detener el otro .1% de las amenazas que utilizan medios no tradicionales para infiltrarse en una organización.

Estas son las amenazas que causan el mayor daño, las amenazas sin archivos que generan eventos que son casi imposibles de distinguir de los eventos que generaría un usuario común. Solo mediante la conexión de los puntos entre los eventos surge un patrón malicioso. Conectar los puntos es el punto donde el analista de seguridad generalmente se necesita para intervenir.

Nuestro Servicio de Detección y Respuesta Rápida, lanzado hace dos años, pone a nuestros expertos de seguridad cibernética de clase mundial al servicio de las organizaciones. Trabajando desde nuestro Centro de Respuesta y Detección Rápida, monitorean los entornos de nuestros clientes las 24 horas del día, los 7 días de la semana. Cuando se detecta una anomalía, nuestros expertos la investigan y una vez que determinan que es una amenaza real, alertan al cliente dentro de los 30 minutos posteriores a la detección.

Hay un solo problema con este servicio: estos expertos altamente calificados son de suministro limitado. Nos dimos cuenta de que necesitábamos encontrar una manera de llevar el conocimiento y las habilidades de nuestros expertos del Centro de Detección Rápida a cualquier compañía. Entonces, nos pusimos a trabajar en tecnología que se acerque lo más posible a lo que hacen nuestros expertos humanos: investigar el contexto de una alerta para determinar si es un incidente real.

El resultado es algo que llamamos Broad Context Detection ™, Detección de Contexto Amplio

INNOVACIÓN EN SU MEJOR EXPRESIÓN

Detectar el uso indebido del uso adecuado, es como buscar una aguja en un pajar. Se requiere recolectar grandes cantidades de eventos de comportamiento. Broad Context Detection ™ está diseñado para tomar este mar de eventos y filtrarlo a una serie de incidentes significativos.

Por ejemplo, una organización mediana con 650 sensores usualmente genera aproximadamente mil millones de eventos cada mes, pero solo alrededor de diez detecciones requieren acciones de contención y remediación. El papel de Broad Context Detection ™ es permitirnos concentrarnos en los pocos incidentes que importan. Lo hace analizando innumerables eventos, marcando los sospechosos, luego relacionando eventos similares y clasificando eventos relacionados en un grupo que pertenece a un incidente. Luego, Broad Context Detection ™ muestra los eventos del grupo en una línea de tiempo cronológica para ofrecer una imagen completa del incidente que ha ocurrido. Con Broad Context Detection ™, a medida que la puntuación de riesgo aumenta con cada detección basada en las acciones del adversario, se revelarán los eventos de comportamiento capturados del compromiso inicial y se alertará al administrador del entorno objetivo. El contexto más amplio del ataque se vuelve instantáneamente visible en una línea de tiempo que muestra todos los hosts afectados y eventos relevantes, junto con las acciones de respuesta recomendadas.

Como resultado, el atacante puede aislarse de la red antes de propagarse a la red y filtrar los datos de los servidores que almacenan datos personales, documentos comerciales confidenciales y propiedad intelectual.

Como resultado, el atacante puede aislarse de la red antes de propagarse a la red y filtrar los datos de los servidores que almacenan datos personales, documentos comerciales confidenciales y propiedad intelectual.

COMO FUNCIONA

Cuando la detección de incidentes se basa en proporcionar alertas, no es de extrañar que la tasa de falsos positivos sea tan alta. Broad Context Detection ™ de F-Secure lleva la tecnología de detección más lejos que nunca, al filtrar las alertas en incidentes reales. Usando el contexto, reducimos una larga lista de alertas en una lista más corta de detecciones, luego las reducimos a una lista aún más corta de incidentes reales que sean claros y prácticos para que los especialistas de seguridad respondan.

Primero, los eventos simples se transmiten a nuestro complejo motor de procesamiento de eventos, que controla el comportamiento sospechoso y mueve los procesos a un monitoreo más detallado. En esta etapa de monitoreo, tomamos en cuenta el contexto más amplio, lo que nos permite identificar eventos que serían demasiado propensos a falsas alarmas si se analizaran por sí mismos. Ahora podemos identificar el comportamiento sospechoso y hostil de manera confiable e ignorar el comportamiento que es aceptable.

Detección de contexto amplioTM en acción

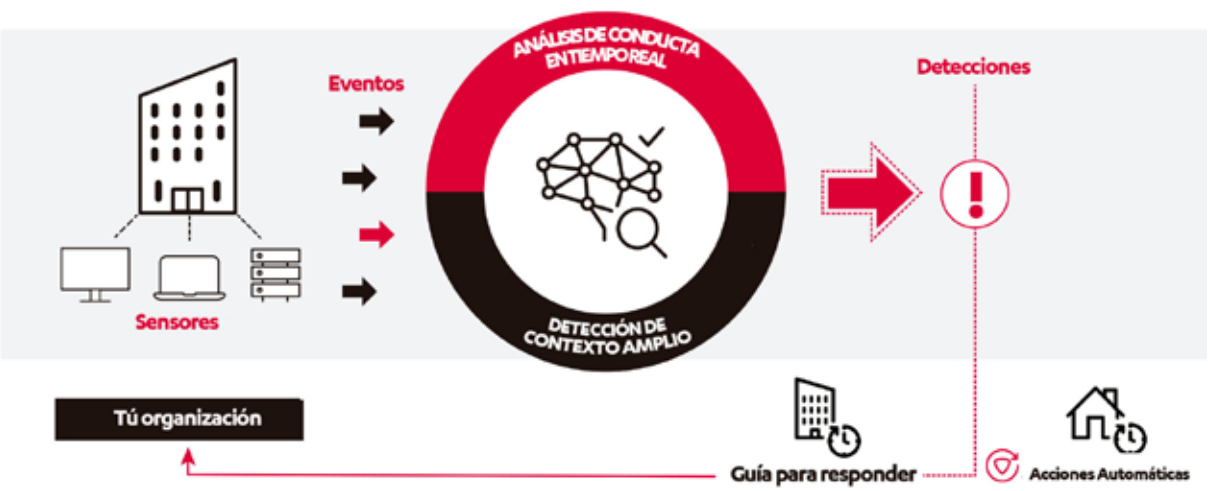
En una instalación de 325 nodos, de un cliente, nuestros sensores recolectaron alrededor de 500 millones de eventos en un período de un mes. El análisis de datos sin procesar en nuestros sistemas de back-end filtró ese número hasta 225,000 eventos sospechosos.
Nuestros mecanismos de Detección de Contexto Amplio analizaron aún más los eventos sospechosos para reducir el número de detecciones a solo 24. Finalmente, esas 24 detecciones fueron revisadas a detalle por expertos humanos y solo 7 fueron confirmadas como amenazas reales.
Enfocarse en un menor número de detecciones y en detecciones de alta precisión permite que la respuesta sea más rápida y efectiva cuando se está bajo un ataque real.

El flujo de alertas luego ingresa a un motor de agregación de alertas, que comienza a construir la imagen contextual agrupando múltiples alertas relacionadas. Sobre la base de la imagen más completa que se forma cuando se agrupan las alertas, se realizan juicios para las detecciones reales, con una probabilidad de falsos positivos cercana a cero. Finalmente, estas detecciones se transmiten a un motor de detección de incidentes que confirma incidentes reales. Una vez más, la tasa de falsos positivos está cerca de cero.

A partir de la lista de detecciones, ahora mucho más manejable y sin embargo más completa, se construye una línea de tiempo, que coloca las detecciones cronológicamente para que los analistas puedan ver el conjunto completo de circunstancias que rodean el incidente. Las detecciones también tienen prioridad según la severidad de acuerdo con el nivel de riesgo, la criticidad del huésped y el panorama de amenazas prevaleciente.

Con este enfoque, los equipos de TI reciben una lista relativamente corta de detecciones confirmadas. cada uno marcado con distintos niveles de prioridad y acciones de respuesta recomendadas. Así que no solo los equipos saben en qué concentrarse primero, sino que también saben cómo responder y pueden hacerlo de manera rápida y decisiva.

Rápida Detección y Respuesta F-Secure



1. Los sensores livianos monitorean las actividades de los puntos finales y transmiten eventos de comportamiento a nuestra nube en tiempo real.

2. El análisis de datos de comportamiento en tiempo real procesa los eventos, marca y monitorea los procesos y otros comportamientos de los usuarios que han desencadenado los eventos.

3. Los mecanismos de Broad Context Detection ™ reducen aún más los datos, colocan los eventos relacionados en contexto entre sí, identifican rápidamente los ataques reales y los priorizan con respecto al nivel de riesgo, la criticidad del host y el panorama de amenazas prevaleciente.

4. Tras una detección confirmada, la solución guía a los equipos de TI y de seguridad a través de los pasos necesarios para contener y remediar la amenaza.

DETECCIONES Y COMPORTAMIENTOS

Broad Context Detection ™ señala las indicaciones de posibles infracciones al alertar a los administradores de tácticas, técnicas y procedimientos (TTP) utilizados en ataques dirigidos. Por ejemplo, esto puede incluir las siguientes acciones posiblemente sospechosas:

- Actividad anormal de los programas estándar
- Llamadas a procesos en ejecución desde ejecutables no estándar
- Ejecución de scripts inesperados
- Ejecución inesperada de herramientas del sistema desde procesos estándar

El Broad Context Detection ™ marca los TTP utilizados para lograr los siguientes objetivos:

- Persistencia
- Escalamiento de privilegios
- Evasión de defensa
- Acceso a credenciales
- Descubrimiento
- Movimiento lateral
- Ejecución
- Exfiltración
- Comando y control

El Broad Context Detection ™ facilita la comprensión del alcance de un ataque dirigido por medio de:

1. Combinar el análisis de comportamiento, reputación y big data en tiempo real con el aprendizaje automático.

2. Tener en cuenta los niveles de riesgo, la criticidad del huésped afectado y el panorama de amenazas prevaleciente para proporcionar una visión completa de un incidente y su gravedad

3. Presentar solo detecciones relevantes con visualización accionable para respuestas multifacéticas y basadas en el riesgo

---

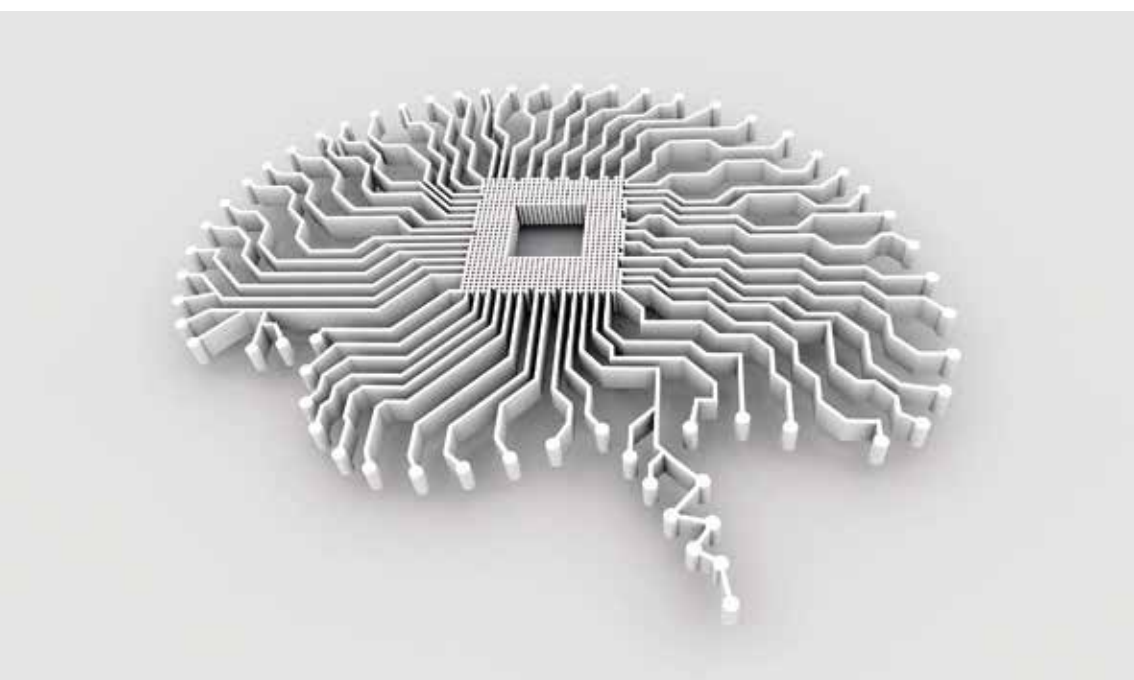
EMPUJANDO EL APRENDIZAJE AUTOMÁTICO AL MÁXIMO

El uso del aprendizaje automático y la IA que los expertos humanos ajustan constantemente significa que nuestros sistemas siguen siendo cada vez más inteligentes. A diferencia de los enfoques tradicionales de simplemente entrenar a la máquina acerca de cómo se ve el mal comportamiento, nuestro enfoque básico se centra en el modelo de atipicidad. Es decir, capacitamos a nuestros sistemas sobre el comportamiento normal y "bueno" y luego marcamos todo lo que es diferente de lo que esperamos. Esto nos permite estar abiertos a una gama mucho más amplia de posibles comportamientos maliciosos.

Este enfoque significa que no estamos limitados a los métodos típicos de detección de ataques, que se basan en factores como los permisos inusualmente altos y el rápido patrón de operaciones. Los atacantes competentes se han dado cuenta, optando por emplear permisos mínimos y llamados ataques "bajos y lentos", lo que significa que llevan a cabo ataques de forma gradual, en pasos paulatinos a lo largo del tiempo. De esta manera, pueden volar bajo el radar de las herramientas de monitoreo convencionales, porque estos ataques no coinciden con los patrones que se usaron para enseñar las herramientas.

La ventaja del aprendizaje automático es que podemos entrenar máquinas para aprender de todo, incluso de sus propios errores. (Eso es algo que ni siquiera los humanos hacen siempre). Cuando la máquina señala una alerta que resulta ser un falso positivo, la máquina descubre por qué fue un falso positivo y toma esto en cuenta la próxima vez, asegurándose de no marcar el mismo tipo de alerta. Esta es una de las razones por las que nuestra tasa de falsos positivos es tan baja.

Si bien la detección en tiempo real es la base de nuestra solución, a veces es necesario detectar algo después del hecho. Con el aprendizaje automático, podemos fácilmente adoptar nuevas reglas para las detecciones que nuestros expertos acaban de identificar y aplicarlas a datos antiguos, retomando las actividades que pueden haberse pasado la primera vez.



CONCLUSIÓN

La seguridad cibernética se trata de habilidades y experiencia. Pero el dilema del defensor nos recuerda que necesitamos tener los recursos para estar vigilantes todo el tiempo, mientras que nuestros adversarios pueden atacar a voluntad. Y con la actual escasez de expertos entrenados, los adversarios están ganando el juego.

Lo que es más, las habilidades y la experiencia por sí solas no son suficientes. Se necesita tecnología para aprovechar esa experiencia para monitorear una red organizativa completa y detectar las pequeñas pistas que indican que un ataque está en marcha. Y se necesita una tecnología superior para hacerlo con precisión, sin activar alertas innecesarias que consumen tiempo y recursos que los equipos de seguridad deberían dedicar a incidentes reales.

Broad Context Detection ™ es una característica central de la solución Rapid Detection & Response de F-Secure, que brinda a las empresas las capacidades avanzadas que necesitan para defenderse de los ataques dirigidos. Con el poder del aprendizaje automático entrenado y mejorado constantemente por los expertos en seguridad cibernética de élite, Broad Context Detection ™ garantiza que las soluciones de F-Secure identifiquen solo los incidentes que sí importan. Es la combinación perfecta de hombre y máquina, lo que pone a la defensa cibernética de clase mundial al alcance de todas las organizaciones.

Con Broad Context Detection ™, su empresa puede detectar ataques dirigidos que anteriormente no se detectaban. Ahora vaya a luchar para ganar.

Para ver un video sobre Broad Context Detection ™, vaya a www.f-secure.com/RDR

Probando nuestros propios productos

Nuestro sistema está siendo constantemente ajustado y analizado por nuestros expertos. El hecho de que sea el mismo motor que usamos para proporcionar el servicio Premium de detección y respuesta administrado de F-Secure significa que no es solo un análisis de datos a ciegas basado en datos de aprendizaje. Usamos el sistema para proporcionar servicios premium a los clientes, y luego incorporamos constantemente los aprendizajes de esos entornos de clientes a la solución para proporcionar una solución mucho más alta calidad y mejor ajustada que el proveedor típico que solo produce la solución. Nosotros mismos somos los principales usuarios de muchas instalaciones, lo que hace que nuestra motivación sea la satisfacción del cliente, pero más: el sistema también forma parte de nuestras operaciones diarias.

Más información sobre el servicio de Detección y Respuesta administrado de F-Secure en www.f-secure.com/RDS

1 Enterprise Management Associates. A Day in the Life of a Cyber Security Pro (2017).
2 Ovum. Closing the Cybersecurity Gaps in Financial Services (2017).
3 Ponemon Institute. The 2017 State of Endpoint Security Risk Report (2017).
4 ISSA/ESG. The Life and Times of Cyber Security Professionals (2017).
5 Ponemon Institute for HPE. Cybersecurity Trend Report (2016).
6 The MITRE Corporation. Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) knowledge base (2018).

Nadie conoce la seguridad cibernética como F-Secure. Durante tres décadas, F-Secure ha impulsado innovaciones en seguridad cibernética, defendiendo a decenas de miles de empresas y millones de personas. Con una experiencia sin igual en la protección de puntos finales, así como en la detección y respuesta, F-Secure protege a las empresas y los consumidores contra todo, desde ataques cibernéticos avanzados y violaciones de datos hasta infecciones generalizadas de ransomware. La sofisticada tecnología de F-Secure combina el poder del aprendizaje automático con la experiencia humana de sus laboratorios de seguridad de renombre mundial para un enfoque singular llamado Live Security. Los expertos en seguridad de F-Secure han participado en más investigaciones europeas sobre la escena del crimen cibernético que cualquier otra compañía en el mercado, y sus productos se venden en todo el mundo a través de más de 200 operadores de banda ancha y móviles y miles de revendedores. Fundada en 1988,
F-Secure cotiza en NASDAQ OMX Helsinki Ltd.

F-Secure.