Qué es el Threat Hunting, la estrategia de cacería de hackers y ciberataques

Ciudad de México, 17-09-2021 | Autor: Agencia NotiPress

Cuáles son las ventajas de Threat Hunting y cómo pueden ayudar a una organización a evitar ciberataques

Dentro del mundo de la ciberseguridad, siempre aparecen nuevos conceptos, uno de ellos es el Threat Hunting, una función dentro del proceso de detección de amenazas de ciberseguridad. Es indispensable entender que el Threat Hunting es un proceso de búsqueda interactiva-proactiva en redes para detectar y aislar amenazas informáticas avanzadas que suelen evadir sistemas de seguridad existentes.

En otras palabras, es un cazador de amenazas informáticas que rastrean los movimientos de las ciberamenazas determinando su entorno para reducir los ciberataques. En el ecosistema de la informática, el Threat Hunting se posiciona como una de las tendencias más importantes en cuestión de ciberseguridad corporativa en los últimos cinco años.

De acuerdo con Ernesto Rosales, director de servicios administrativos en Data Warden, explicó a NotiPress que las amenazas cada vez son más complejas y sofisticadas. Por tanto, las empresas deben adoptar un marco de gestión de ciberseguridad más fuerte que contenga protección, detección y respuesta. Rosales subrayó, estos tres puntos son vitales para salvar una organización: "Debes proteger tu negocio u organismo, es básico, sobre todo porque si dejas la puerta abierta las amenazas se vuelven un enorme problema".

Aunque el Threat Hunting parece un concepto nuevo, la realidad es que es un compendio de múltiples metodologías con nuevas herramientas en un mundo lleno de datos e información de piezas. Entre sus principales misiones está ayudar a los usuarios a cazar mejor y encontrar las amenazas cibernéticas las cuales atentan contra la integridad del hardware.

Los expertos en Data Warden detallan, el Threat Hunting primero conoce el entorno, después identifica la forma de interactuar de las herramientas, aprovecha el conocimiento externo. Después crea una hipótesis (determina si el sistema fue hackeado o no), luego analiza y genera conocimientos a largo plazo a fin de aprender y evolucionar en procesos de cacería para futuras amenazas.

Después, el cazador de amenazas dirige las investigaciones paso a paso buscando el origen del problema, toma una respuesta inmediata, lleva a cabo su plan y reduce las probabilidades de algún ataque. Su método para cazar ciberataques es muy parecido al machine learning, un tipo de entrenamiento para software donde el sistema aprende por medio de prueba y el error mejorando su autonomía.

Mientras sigue aprendiendo, va descubriendo nuevos patrones de ataque mediante la identificación automática de anomalías en el acoplamiento de cada usuario, proceso y máquina. Además, cada nuevo patrón de ataque se convierte también en una comportamiento de detección de amenazas para detener a futuros hackers antes de producir algún tipo de daño.

No obstante, en un inicio puede tener algunos problemas, pero conforme pasa el tiempo, su estructura de aprendizaje puede mejorar y optimizar los procesos para detectar amenazas informáticas más agresivas. A pesar de ello, el Threat Hunting puede ser un método de seguridad costoso, pero efectivo a la hora de anular los ciberataques.

Cabe señalar, expertos en Data Warden detallan que el modelo de Threat Hunting está dirigido para cualquier organización en cualquier sector sin importar la posición dentro del organigrama de una compañía. Encima, el Threat Hunting se posiciona como una solución de ciberseguridad para retail, manufactura y finanzas con el fin de proteger la información sensible sin importar el tipo de organización.