INFO & INSIGHTS

LA EFECTIVIDAD DE LA SEGURIDAD A NIVEL ENDPOINT:

LAS 3 MÉTRICAS QUE SI IMPORTAN

Las organizaciones podrían elegir las soluciones de seguridad que proveen un valor superior de seguridad no solo en términos monetarios si no en términos de efectividad. La efectividad de la seguridad es medida por la capacidad de la tecnología para cumplir con estas tres capacidades básicas, como mínimo:

1 PERFORMANCE DE LA FUNCIÓN PREVISTA: ¿TU SOLUCIÓN TECNOLÓGICA PROPORCIONA LA FUNCIÓN DE SEGURIDAD QUE SE PRETENDE Y QUÉ SE ESPERA QUE REALICE?

En pocas palabras, ¿Cumple con lo prometido? Existen dos vectores de ataque principales utilizados para comprometer todos los equipos endpoint o de punto final**: Ejecutables maliciosos (malware) y vulnerabilidades.**

Una solución tecnológica para la seguridad endpoint que realmente sea efectiva debe evitar que el malware y las vulnerabilidades comprometan los puntos finales y los servidores.

También debe evitar las variantes conocidas y desconocidas de cada malware y exploit.

2 Persistencia Inherente: ¿TU SOLUCIÓN TECNOLÓGICA EVITA QUE LOS ATACANTES Y USUARIOS PASEN POR ALTO SUS FUNCIONES DE SEGURIDAD?

Ninguna herramienta o tecnología de seguridad de protección para equipos endpoint, está construida con la intención de ser fácilmente anulada o sufrir un bypass. Si un atacante y / o usuarios finales son capaces de eludir la función pretendida de la tecnología, entonces la solución no está cumpliendo su propósito final.

Una plataforma de seguridad para endpoint efectiva no debe permitir que los atacantes pasen por alto la función de seguridad, además de causar problemas de rendimiento que resultarían en que los usuarios inhabilitaran los componentes.

3 Flexibilidad: ¿TU SOLUCIÓN TECNOLÓGICA EVOLUCIONA PARA ACOMODAR Y PROTEGER NUEVAS APLICACIONES, SISTEMAS Y PLATAFORMAS?

La frecuencia de los ataques cibernéticos hace varias décadas era baja, al igual que la sofisticación del malware y los métodos de ataque, en este escenario las herramientas de seguridad para Endpoint eran diseñadas para evitar que los virus infectaran un sistema.

Sin embargo, actualmente el panorama de amenazas es radicalmente diferente y ha relegado herramientas de seguridad para endpoint como el antivirus, a herramientas de detección y respuesta reactivas.

Los productos de seguridad necesitan adoptar un enfoque proactivo para asegurar adecuadamente los equipos endpoint, hoy en día es necesario centrarse en la prevención a fin de reducir la frecuencia y el impacto de las infracciones cibernéticas.

Es un hecho que hoy las organizaciones deben seleccionar productos de seguridad que proporcionen un valor de seguridad significativo medido por la efectividad de la capacidad de sus soluciones tecnológicas de seguridad para cumplir con los tres requisitos anteriores.

Si quieres conocer cómo puedes defenderte de las amenazas protegiendo de forma eficaz tus equipos endpoint, se parte del Entrenamiento de Defensa Integral Hands On con Grupo Smartekh y Palo Alto Networks.

IMPLEMENTAR UNA ESTRATEGIA DE PROTECCIÓN A NIVEL ENDPOINT VALE LA PENA

Para todas las organizaciones. No se trata sólo de detectar riesgos para tu negocio, se trata de reducir la superficie de ataque para que las amenazas se ejecuten en tu negocio.