

¿Qué es Threat Hunting y por qué es necesario?

Threat Hunting es un proceso proactivo de búsqueda y detección de amenazas informáticas con el objetivo de encontrar y neutralizar ataques maliciosos antes de que causen daños significativos. La búsqueda de amenazas se basa en el análisis de datos y en la investigación para identificar patrones y comportamientos sospechosos que indican la presencia de una amenaza. Esto puede incluir la revisión de registros de seguridad, la detección de anomalías en el tráfico de red y el análisis de la actividad del usuario. El objetivo es detectar y responder a las amenazas que no han sido detectadas por los sistemas de seguridad automatizados.

El threat hunting se realiza mediante una combinación de técnicas automatizadas y manuales, mediante el uso de herramientas de inteligencia artificial, aprendizaje automático y análisis de comportamiento para identificar patrones sospechosos. Es una técnica especialmente útil para detectar ataques avanzados persistentes (APT) y otros tipos de ciberataques que pueden evadir las defensas tradicionales.