ARQUITECTURA DE SEGURIDAD ADAPTATIVA

Es un modelo de seguridad con la capacidad de monitorear todo lo que ocurre en un computador o en una red, analizando los datos obtenidos y realizando acciones que le permitan mantener su uso eficiente, con mecanismos de respuesta de manera automática e inmediata para estar constantemente buscando contener amenazas activas y neutralizar vectores de ataques.

PRINCIPIOS

- Autopreservación
- Compartimentación
- Mínimos Privilegios
- Defensa en profundidad
- Proporcionalidad

PILARES

Capacidad preventiva

Este es el conjunto de políticas, herramientas y procesos que buscan prevenir la ocurrencia de ataques exitosos. Para eso se necesitan modelos de prevención zero trust, como la microsegmentación definida por software, que aumenten la seguridad sin aumentar los costos.

Capacidades de detección

Son los controles concebidos para identificar ataques que evadieron de forma exitosa las medidas preventivas. Además de la simple correlación de eventos incorporando algoritmos de analítica de datos, aprendizaje automático, detección de estándares y comportamientos que estén fuera de la normalidad de las operaciones usuales, etc.

Capacidades de respuesta

Proporcionan una forma de responder a la amenaza, sea encogiendo la superficie de ataque, disminuyendo su velocidad, actuando en su remediación, entre otros aspectos.

Capacidades predictiva

Son aquellas que permiten a la organización prever ataques, analizar tendencias y pasar de una postura de seguridad reactiva a una proactiva. Es fundamental una combinación eficaz de las técnicas de detección avanzadas con una sofisticada red de inteligencia de amenazas.