



<http://diarioti.com/las-actuales-soluciones-de-seguridad-son-insuficientes/100619>

“Las actuales soluciones de seguridad son insuficientes”

26/09/16



## “Las actuales soluciones de seguridad son insuficientes”

Según Wedge Networks, las amenazas avanzadas son actualmente tan evasivas, que las tecnologías existentes han demostrado ser insuficientes y no confiables, en la lucha contra el malware.

Diario TI 26/09/16 10:08:59

En el marco de la cumbre global organizada por [NetEvents](#) para prensa y analistas de TI en Silicon Valley, Estados Unidos, Diario TI conversó con Frank Wiener, vicepresidente de marketing en [Wedge Networks](#),

sobre el panorama actual de seguridad informática y, en particular, sobre la forma en que el sector TI está reaccionando frente a amenazas como ransomware y spear phishing.

Wiener comentó que las empresas se han visto forzadas a cambiar su estrategia de seguridad, de la prevención a la detección y mitigación de amenazas en tiempo real, principalmente debido a la incapacidad de los sistemas actuales para detectarlas y bloquearlas. A esto se suma el abrumador volumen de datos generado por cada incidente de ataque a las redes. “El personal de seguridad se ve en la necesidad de determinar cuáles son las amenazas más críticas, con el fin de poder concentrar sus recursos”, comentó Wiener, agregando que las nuevas amenazas son altamente evasivas, lo que dificulta aún más su detección.

La solución de Wedge ante estos retos ha sido utilizar inteligencia artificial en combinación con otras tecnologías probadas, con el fin de detectar y bloquear las amenazas que pasan desapercibidas para otras empresas de seguridad informática. Durante la cumbre tecnológica de NetEvents, [Wedge presentó su solución WedgeAMB](#), que incorpora la solución de seguridad basada en inteligencia artificial de Cylance. Wiener explicó que WedgeAMB coloca las amenazas en un motor lógico centralizado de funcionalidad analítica, que convierte el gran volumen de datos complejos en información intuitiva y accionable que permite al personal de seguridad concentrar sus esfuerzos en la mitigación de las amenazas más importantes.

Las aspiraciones de Wedge no son modestas. “Con WedgeAMB esperamos proporcionar la prevención más eficaz de la industria contra este tipo de amenazas”, explicó Frank Wiener, agregando que el sistema virtualizado es instalado detrás del NGFW o UTM. “WedgeAMB bloquea el malware, ransomware y virus convencionales utilizando una combinación de DCI en tiempo real, y reconstrucción total de contenidos y análisis múltiple, en sistemas operando a 100 Mbps, 1 Gbps y 10 Gbps”.

El sistema opera en combinación con WedgeIQ, motor de analítica que consolida los datos obtenidos por los sistemas WedgeAMB distribuidos en la empresa, generando un panorama de amenazas en tiempo real, que abarca toda la red. WedgeIQ utiliza técnicas avanzadas de visualización y analítica, que mapean parámetros multi dimensionales de amenazas en un formato intuitivo e interactivo.

WedgeAMB incluye sandbox opcional, que permite el envío automático de contenidos inseguros a un sandbox para detonación y evaluación. La funcionalidad sandbox no ha sido diseñada para detectar amenazas adicionales, sino para eliminar potenciales falsos positivos y proporcionar una caracterización adicional de malware nuevo.

Al pedirle mayores detalles sobre la cooperación con [Cylance](#), que Wiener define como asociación tecnológica, el ejecutivo puso de relieve que [Cylance es una de las empresas más exitosas y de más rápido crecimiento en la protección de endpoints](#), basada en su sistema de aprendizaje automático e inteligencia artificial que desarma contenidos con código ejecutable, al realizar el equivalente de un análisis de ADN de miles de atributos. “Después de haber evaluado millones de ejemplos de malware, el motor de inteligencia artificial de Cylance ha desarrollado la inteligencia necesaria para analizar, detectar patrones y pronosticar la presencia de malware en milisegundos, con un grado de exactitud sin precedentes”.

Wiener explicó que Wedge ha licenciado la tecnología de inteligencia artificial de Cylance, incorporándola en sus productos, para la inspección profunda de paquetes y de contenidos, con reconstrucción de contenidos en tiempo real. “Nuestra solución es una orquestación de la tecnología de Cylance, que acabo de describir, con múltiples tecnologías de seguridad”, concluyó señalando Frank Wiener, vicepresidente de marketing en Wedge Networks.



Frank Wiener, vicepresidente de marketing en Wedge Networks, conversa con Diario TI en Saratoga, California, Estados Unidos.

**Fotografías: Diario TI**