VirusTotal, el popular servicio de escaneo multi antivirus propiedad de Google, anunció recientemente nuevas capacidades para la detección de amenazas con la ayuda de una compañía de seguridad cibernética israelí.

VirusTotal ofrece un servicio gratuito en línea que analiza archivos sospechosos y URL para detectar malware y los comparte de forma automática con la comunidad de seguridad.

Debido a los nuevos tipos de malware, los investigadores confían en el rápido descubrimiento y uso compartido proporcionado por VirusTotal para mantener a sus compañías a salvo de ataques.

VirusTotal se basa en un flujo continuo de nuevos descubrimientos de malware para proteger a sus miembros de daños significativos.

Cynet, el creador de la plataforma autónoma de protección contra violaciones, ahora integró su motor de detección de Cynet en VirusTotal.

Entre los beneficios de esta asociación, se encuentra que Cynet proporciona a la red de socios de VirusTotal inteligencia de amenazas de vanguardia de su motor de detección basado en ML (CyAI) que protege activamente a los clientes de la compañía en todo el mundo.

CyAI es un modelo de detección en constante aprendizaje y evolución que aporta información de forma rutinaria sobre nuevas amenazas que no están disponibles en VirusTotal. Aunque muchos proveedores están utilizando modelos AI/ML, la capacidad de los modelos para detectar nuevas amenazas varía mucho.

Cynet supera habitualmente a las plataformas de detección de terceros y de código abierto, y frecuentemente, se confía en los casos de respuesta a incidentes cuando las amenazas subyacentes permanecen ocultas de otras soluciones.

Por ejemplo, Cynet realizó recientemente un compromiso de respuesta a incidentes para un

gran proveedor de telecomunicaciones y descubrió varios archivos maliciosos que no aparecían en la base de datos de VirusTotal.

Contribuir con información sobre estos archivos recién descubiertos ayuda a toda la industria a desempeñarse mejor y proteger a las empresas contra ataques cibernéticos.

Por otro lado, Cynet aprovechará la inteligencia en VirusTotal para informar su modelo CyAI con el fin de mejorar continuamente sus capacidades de detección y precisión.

CynetAI está en constante evolución, aprendiendo nuevos conjuntos de datos para mejorar su precisión y disminuir su relación de falsos positivos que ya es baja. La comparación de los archivos que CyAI considera maliciosos con los archivos que otros proveedores también consideran maliciosos ayuda a validar rápidamente los hallazgos de Cynet.