INTELLIGENT-DATA

Cada minuto hay 2.645 invasiones a redes. Es hora de tomar la ofensiva.

Sin embargo, hoy en día la detección es un post-evento. Incluso la información de seguridad y gestión de eventos en los centros de operaciones sigue sucediendo posterior al evento, y apenas ayuda a prevenir futuros ataques basados en el pasado. **Pero hay un cambio de paradigma al utilizar Inteligencia Artificial y "White Hat Robots"**.

Detección continua, automática y autónoma - Disponible Ya.

Los ataques de hoy provienen de múltiples ecosistemas: socios de segundo y tercer nivel (quizás incluso aquellos que usan su logotipo), aplicaciones SaaS y plataformas (IaaS) utilizadas fuera de su propia red.

Soluciones disponibles – Hay tres rutas típicamente utilizadas:

I Realizar un **análisis de vulnerabilidad** de la red - esto descubre rutas abiertas para un ataque a través de múltiples factores: puertos abiertos, dispositivos que requieren parches, etc.

II Ejecutar un **PEN TEST (prueba de penetración)** - esto requiere un pirata informático experto con algún conocimiento previo de la red al que se deja intentar entrar en la red.

III Contratar a un **Hacker Ético Certificado (CEH),** permitirle ingresar a su red para informar los resultados. Generalmente, son contratados por tiempo limitado.

Por supuesto, puede tercerizar el servicio, pero todos los proveedores solicitan algún permiso. Esta nunca es una opción que tendría a un pirata y, por lo tanto, ese tipo de pruebas ya conllevan un sesgo.

TODAS las pruebas de vulnerabilidad y TODOS los PEN TEST requieren información sobre su red, permisar a priori, o colocar activos (virtuales/in situ) para realizar la prueba.

El Reto: ¿Cómo tomar la ofensiva en esta guerra de ciberseguridad 24 x 7 x 365?

Un enfoque radicalmente nuevo para la detección del "Shadow Risk".

- **CYCOGNITO** NO requiere agentes en la red. No solicitamos NINGUNA información sobre su red. **Los resultados son 100% imparciales**.
- **CYCOGNITO** utiliza I.A. automatizada. Robots en más de 100 países que nunca descansan. **Su red está sujeta de forma continua y autónoma a ataques simulados que NO causan daño ni activan falsas alarmas.** Podrá ver cada vector fuera de su superficie de ataque, identificando todos los activos conocidos y desconocidos.
- **CYCOGNITO** a través de un panel de control, permite monitorear todas las actividades, activos y eventos, priorizando los vectores basados en el camino de menor resistencia. Los pasos de corrección con enlaces de información sobre cada riesgo le ayudan a manejar la amenaza.

Su Próximo Paso: Intelligent-Data puede brindarle más información sobre cómo CYCOGNITO puede ayudarlo a detectar y predecir sus vulnerabilidades en la red. No necesitamos información sobre su red (al igual que malhechor) y nuestros robots actuará a través de todos los ecosistemas de Internet.

Haremos una prueba de concepto (POC) para que la evalúe con un team de **CYCOGNITO**. **Entramos a su red** – sin crear falsas alarmas – y le decimos cómo lo hicimos, sin costo alguno. **Luego usted decide.**

bobr@intelligent-data.com **Boston Hqt.(Northeast) or** daniel@intelligent-data.com **Miami Hqt. / LATAM**