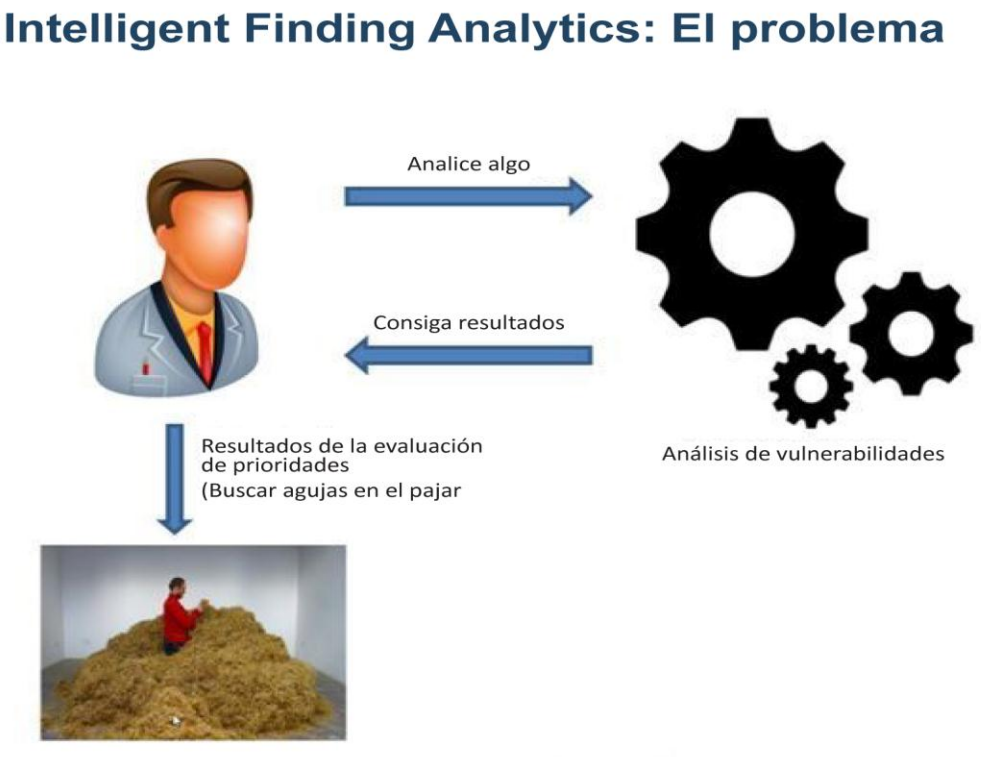
Intelligent Finding Analytics: Su experto en seguridad de las aplicaciones de computación cognitiva

14 de octubre de 2016 | Por David Marshak en colaboración con Kris Duer

Hace dos años, IBM® comenzó a investigar cómo la computación cognitiva: podría producir analítica con resultados inteligentes para abordar algunos de los problemas más peliagudos a los que hacen frente las empresas que tratan de comprender y reducir los riesgos para la seguridad de sus aplicaciones. Las empresas que utilizan comprobación de la seguridad de las aplicaciones: (SAST) estática para comprender y reducir los riesgos de seguridad de las aplicaciones se encuentran ante un dilema: ¿Deben centrarse en la velocidad con la que informan de las vulnerabilidades a los desarrolladores o en la precisión con la que analizan los resultados para identificar, priorizar y abordar estos problemas? Generalmente, la precisión de este último objetivo conlleva recurrir a personal especializado para verificar las vulnerabilidades de elevado nivel de riesgo y eliminar falsos positivos que pueden impedir que el equipo de seguridad alcance la velocidad deseada. En pocas palabras, no podían tener las dos cosas. Hasta ahora.

Agujas y pajares

Utilicemos el ejemplo de un pajar. Como el mejor enfoque para SAST es examinar los flujos de datos reales en la aplicación, el analizador de SAST tiende a ofrecer abundantes resultados. Considere que estos son todos los resultados posibles. Es el pajar del proverbio.



Para encontrar las agujas en este pajar, los equipos de seguridad pueden adoptar uno de los dos enfoques posibles:

Reducir el tamaño del pajar

Esto suele conseguirse adoptando un enfoque menos exhaustivo para el análisis de aplicaciones que producirá menos resultados, idealmente, los más significativos. La principal ventaja de este enfoque es la velocidad. A riesgo de confundir las metáforas, la pequeña cantidad de resultados permite separar la paja del trigo. Esto permite a los equipos de seguridad: ofrecer rápidamente resultados a los desarrolladores. Pero también hemos de destacar la desventaja: Es posible que los equipos de seguridad no hallen nunca las agujas que buscan. En otras palabras, no es posible garantizar que el proceso reduzca el riesgo general para la seguridad de las aplicaciones de la organización.

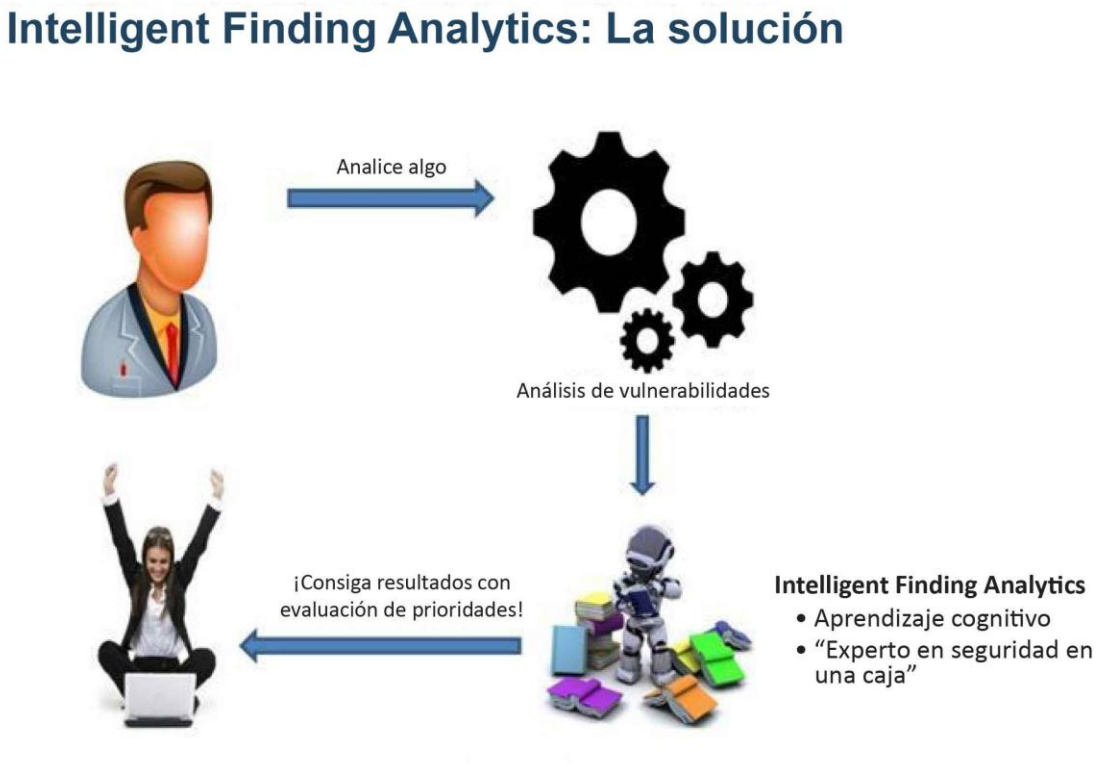
Contratar más personal

El segundo enfoque implica contratar más empleados para revisar los resultados y encontrar las agujas a mano. La ventaja de este enfoque es la exhaustividad. No se pierden agujas en el proceso de comprobación y los expertos pueden determinar qué resultados precisan alguna acción. La desventaja es, evidentemente, la ineficiencia en términos de destreza, costes y, sobre todo, tiempo. Cuanto más grande sea el pajar, más expertos precisará el proyecto. Estos expertos son un recurso escaso y costoso. Revisar los resultados puede llevar horas, días o incluso semanas, lo que hace prácticamente imposible ofrecer resultados a los desarrolladores de forma puntual o garantizar un proceso continuado. Debido a la escasez de personal especializado, algunas empresas deciden externalizar todo el proceso. Esto puede resolver la falta de personal a corto plazo, pero aumenta de forma significativa el coste y el tiempo del proceso. La externalización alivia a las empresas de la carga de contratar y formar personal, pero también supone una pérdida de control a la hora de priorizar su tiempo.

Intelligent Finding Analytics

Ante estas dos opciones y el éxito de otros esfuerzos cognitivos, los expertos de IBM consideraron que debería haber una tercera alternativa. Este fue el origen de la Intelligent Finding Analytics (IFA) de IBM, con patente en trámite. Inicialmente, IFA fue un proyecto de investigación para ver si era posible lograr la principal ventaja del primer enfoque de SAST, la velocidad, a la vez que la ventaja del segundo enfoque, la precisión, sin los inconvenientes que conllevaba cada uno de ellos. La meta era utilizar las mismas capacidades cognitivas en las que se basa IBM Watson para funcionar como un grupo de

expertos examinando el pajar.



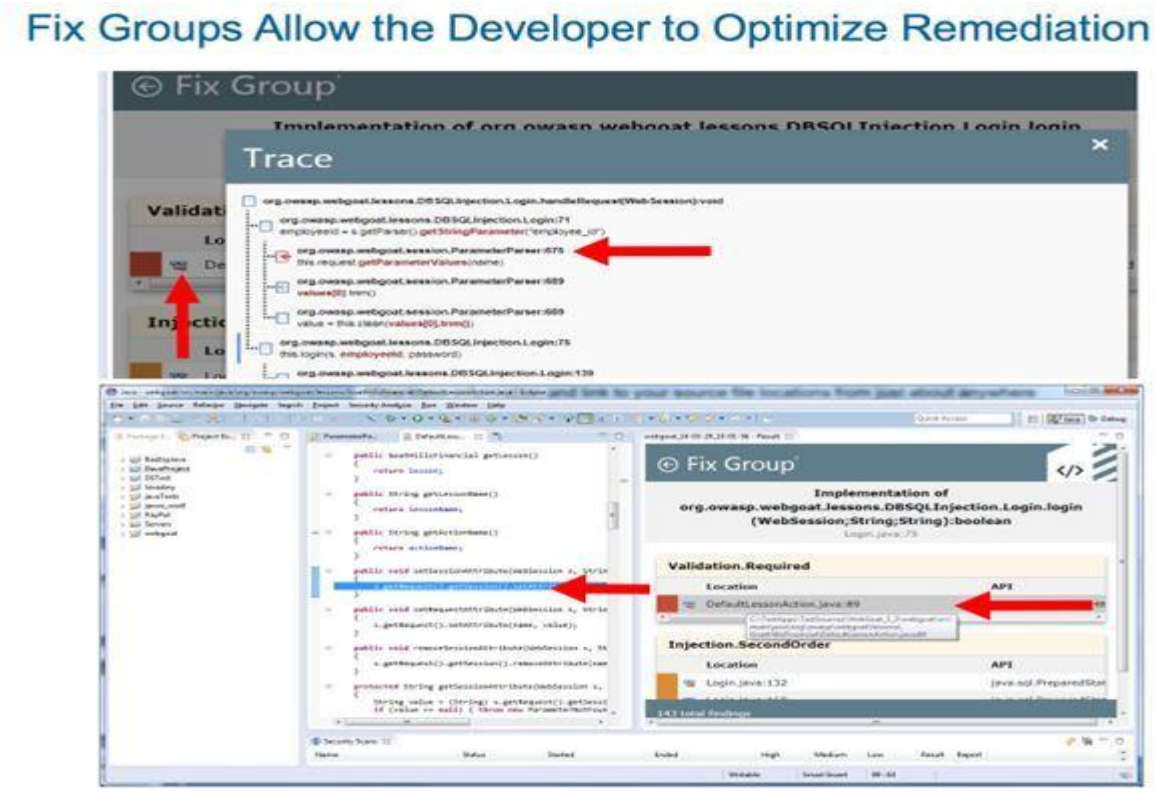
Cifras asombrosas

A lo largo del último año, los resultados han sido aún más significativos de lo previsto inicialmente. En el uso real por parte de los clientes, al eliminar ruido y falsos positivos, los pajares de resultados se han reducido de forma continuada en más del 90 por ciento. Las capacidades de aprendizaje de IFA consiguen una precisión en la eliminación de falsos positivos de más del 98 por ciento. De hecho, la reducción real de falsos positivos y ruido en el total de análisis de clientes en seguridad de las aplicaciones: en el cloud alcanzó en octubre de 2016 la increíble cifra del 98,91 por ciento.

Como hemos indicado,esta reducción no se produce a expensas de la precisión, ya que el 98 por ciento de precisión de IFA es casi idéntico al conseguido por expertos en seguridad con elevado nivel de preparación y experiencia. En muchos casos, los resultados de IFA son en realidad mejores que los de los expertos humanos. Es muy probable que esto sea atribuible a la fatiga de las personas tras horas de búsqueda de agujas. IFA ofrece los resultados en cuestión de minutos o incluso segundos, en comparación con las horas o días que precisan los expertos humanos para analizar grandes aplicaciones. Esta velocidad permite a los equipos de ciberseguridad ofrecer resultados a los desarrolladores con rapidez suficiente como para seguir el ritmo de las amenazas persistentes y mantener un modo de ingeniería continuo. Así, los desarrolladores pueden realizar análisis frecuentes y tempranos, y corregir vulnerabilidades en el momento que se introducen en lugar de esperar a que aparezcan.

Grupos de correcciones y resultados para el mundo real

Pero IFA no se limita a abordar el problema del pajar y las agujas. También ayuda a los desarrolladores a aumentar su eficiencia al poner los hallazgos y soluciones directamente en el código que están creando. La aplicación de técnicas cognitivas permite a IFA reducir el conjunto de resultados con grupos de correcciones. Los grupos de correcciones muestran a los desarrolladores el lugar exacto del código en el que se encuentran los problemas de seguridad y permiten remediar múltiples problemas simultáneamente. Los desarrolladores ven ahora entre cinco y 10 grupos de correcciones para cientos de problemas relacionados con la seguridad. IFA permite a los desarrolladores corregirlos todos en un mismo entorno integrado de desarrollo (IDE).



Con estas capacidades, ¿cómo ayuda IFA a las empresas a hacer frente a los desafíos cotidianos a la seguridad de las aplicaciones? Veamos tres resultados reales de clientes:

		Post- IFA Results	
	Pre-IFA Scan Findings	Vulnerabilities	Fix Group Recommendations
Application #1	12,480	1,057	35
Application #2	247,350	1,271	103
Application #3	746,979	483	42

En la aplicación nº 1, los hallazgos de análisis en profundidad identificaron más de 12,000 vulnerabilidades potenciales. IFA redujo esta cifra a alrededor de 1000 e identificó 35 puntos (grupos de correcciones) en el código para corregirlas todas. En la aplicación nº 2, los hallazgos de análisis en profundidad identificaron casi 250,000 vulnerabilidades potenciales. De nuevo, IFA redujo la cifra de vulnerabilidades a alrededor de 1000 e identificó 103 grupos de correcciones en el código para abordarlas. En la aplicación nº 3, los hallazgos de análisis en profundidad identificaron casi 750,000 vulnerabilidades potenciales. Sorprendentemente, IFA redujo esta cifra a solo 483 resultados reales e identificó 42 grupos de correcciones.

Con más de un año de experiencia, IFA está demostrando su capacidad para ayudar a los equipos de desarrollo con aplicaciones de todos los tamaños. Para los equipos de seguridad, eliminó la necesidad de pasar horas buscando y corrigiendo problemas de seguridad de las aplicaciones: o, en algunos casos, dejando la tarea por imposible. En vez de ello, estas empresas han aumentado su eficiencia para hacer frente a los riesgos de seguridad de las aplicaciones: en más del 98 por ciento.

IFA a pleno rendimiento

Después de todo este trabajo académico, aprendizaje automático continuado y experiencia real en clientes, ¿cómo puede ayudarle IFA a usted? De forma muy simplificada, IFA ofrece una forma de:

- Acelerar sus pruebas de seguridad integrándolas en su proceso de desarrollo continuado
- Reducir la carga de su personal de seguridad, necesariamente limitado
- Ayudar a sus desarrolladores a entregar código seguro de forma más eficaz

Y esto sólo es el comienzo. Las capacidades de IBM IFA ya están disponibles en nuestras soluciones Application Security on Cloud e IBM Security AppScan Source. Reproduzca el seminario web en el siguiente enlace para aprender a liberar la potencia de la tecnología cognitiva en su organización. Este breve vídeo ofrece una interesante visión general de las capacidades de IFA e Intelligent Code Analytics (ICA) para Application Security on Cloud.