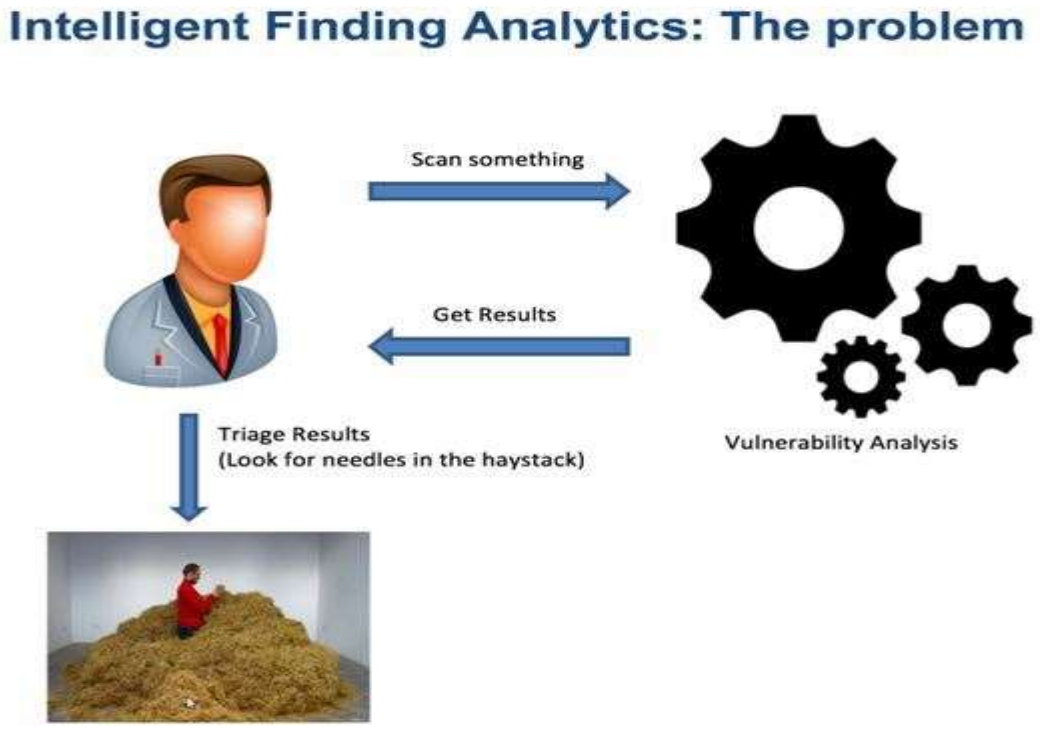
Intelligent Finding Analytics : votre expert en sécurité des applications grâce à l'informatique cognitive

14 octobre 2016 | Par David Marshak et Kris Duer (co-auteur)

Il y a deux ans, IBM® s'est lancé dans des recherches pour déterminer comment l'informatique cognitive pourrait créer des outils d'analyses de détection intelligente pour résoudre les problèmes complexes liés à la compréhension et à la réduction des risques de la sécurité des applications. Les entreprises qui utilisent des analyses statiques (SAST) pour comprendre et réduire ce type de risque sont confrontées à un casse-tête : doivent-elles se concentrer sur la vitesse de signalement des vulnérabilités aux développeurs ou sur la précision des analyses des résultats pour identifier, prioritiser et résoudre ces problèmes ? Normalement, la précision nécessite un personnel expert pour vérifier les vulnérabilités à haut risque et éliminer les faux positifs qui peuvent empêcher une équipe de sécurité d'atteindre son objectif de rendement. Dit plus simplement, on ne pouvait pas avoir les 2. C'était encore vrai hier !

Aiguille et botte de foin

Prenons l'exemple de l'aiguille dans la botte de foin. Comme la meilleure approche SAST consiste à examiner les flux des données dans une application, le scanner SAST a tendance à générer un volume de résultats important. Imaginez tous les résultats possibles. Et vous avez votre botte de foin proverbiale.



Pour trouver des aiguilles dans cette botte de foin, les équipes de sécurité peuvent choisir une des deux approches suivantes :

Réduire la taille de la botte de foin

Vous devez pour cela choisir un scanning plus léger des applications, qui génèrera moins de résultats, qui seront néanmoins les plus importants, ou du moins vous l'espérez. La vitesse est le principal avantage de cette approche. Au risque de filer trop loin notre métaphore, plus la botte de foin est petite plus vite vous aurez séparé le grain de l'ivraie. Les équipes de sécurité peuvent alors fournir des résultats plus rapides aux développeurs. Mais l'inconvénient est important et ne peut pas être ignoré : certaines aiguilles restent invisibles aux yeux des équipes de sécurité. En d'autres termes, ce processus ne garantit pas que le risque de sécurité des applications sera réduit au strict minimum.

Recruter plus d'employés

La deuxième approche consiste à recruter plus d'employés pour examiner les résultats et chercher les aiguilles à la main. Cette approche a l'avantage d'être exhaustive. Les aiguilles ne se perdent pas dans le processus des tests et les experts peuvent identifier les résultats nécessitant des corrections. L'inconvénient est évidemment lié à l'inefficacité en termes de compétences, de coûts et de temps plus particulièrement. Plus la botte de foin sera grande, plus les experts devront être nombreux. Et ces experts sont rares et coûteux ! L'extraction des résultats peut nécessiter des heures, des jours ou même des semaines, générant des retards inacceptables pour les développeurs ou pour la continuité de la production. Confrontées à la pénurie des compétences, certaines entreprises ont décidé d'externaliser la totalité du processus. Cette approche comble l'écart des compétences à court terme, mais elle augmente considérablement les coûts et la durée. L'externalisation élimine les charges liées au recrutement et à la formation, mais elle implique aussi une certaine perte de contrôle en termes de prioritisation des tâches et de gestion du temps.

Intelligent Finding Analytics

Face à ce choix et compte tenu des succès remportés par d'autres efforts cognitifs, les experts IBM ont imaginé une troisième possibilité. C'est ainsi qu'est né l'Intelligent Finding Analytics (IFA) d'IBM, actuellement en instance de brevet. Initialement, l'IFA était un projet de recherche visant à déterminer si la vitesse, principal avantage de la première approche SAST, pourrait être préservée avec la précision (avantage de la deuxième approche), sans leurs inconvénients respectifs. Il s'agissait donc d'utiliser les mêmes fonctions cognitives qui forment la base d'IBM Watson et de les faire fonctionner comme un groupe d'experts pour trier la botte de paille.

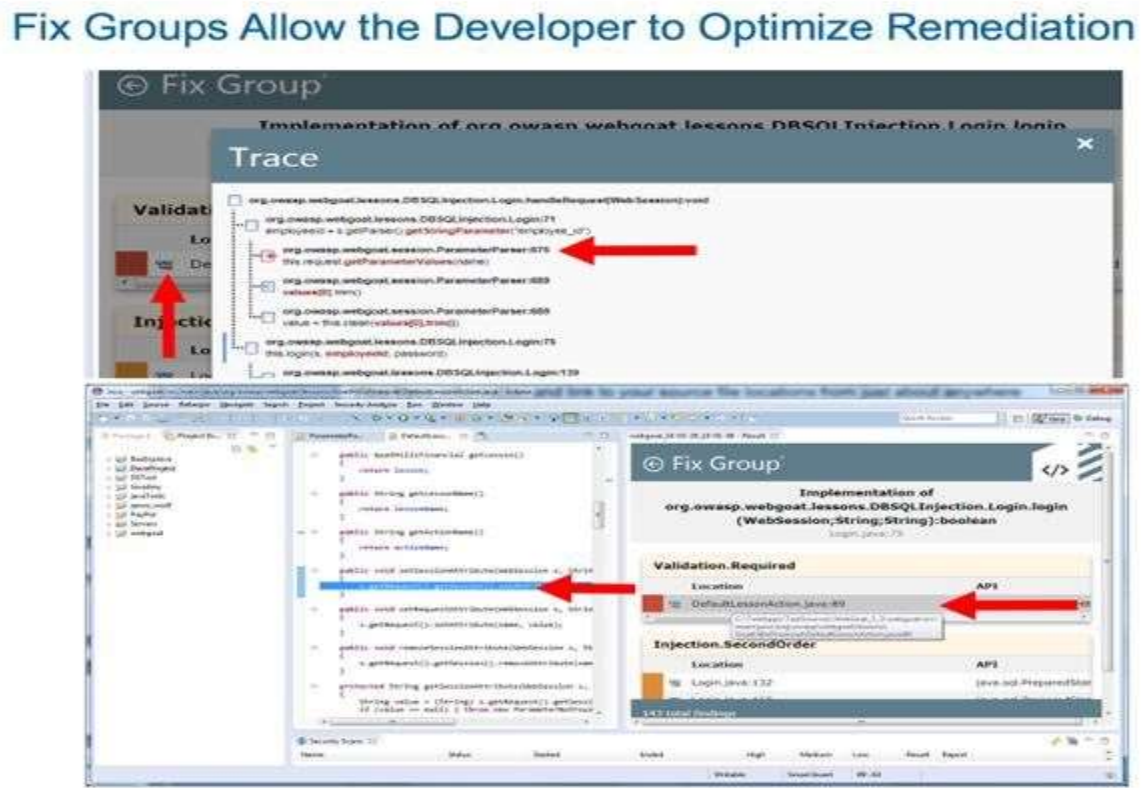
Des chiffres incroyables

L'année dernière, les résultats ont été encore plus déterminants que prévus. Au niveau de l'utilisation client réelle, en éliminant les faux positifs et le bruit, les bottes de résultats ont été réduites de plus de 90 %. Grâce aux fonctions d'apprentissage d'IFA, la précision de la suppression des faux positifs a dépassé 98 %. En octobre 2016, la réduction réelle des faux positifs et du bruit sur tous les scans clients de la sécurité des applications dans le cloud a même atteint 98,91 % !

Comme nous l'avons indiqué, cette réduction n'a en rien affecté la précision. Avec un taux de 98 %, la précision de l'IFA est presque identique à celle d'experts de la sécurité des applications compétents et expérimentés. Dans de nombreux cas, les résultats de l'IFA sont en réalité supérieurs à ceux des experts humains. Il est probable que cette différence soit due à la fatigue, bien naturelle après des heures de chasse aux aiguilles dans des bottes de foin… ! Les résultats de l'IFA apparaissent après quelques minutes de travail, parfois des secondes, au lieu d'heures ou de journées entières pour les experts humains qui analysent des applications lourdes. Cette vitesse permet aux équipes de la cybersécurité d'envoyer les résultats aux développeurs avec une rapidité suffisante pour tenir la cadence des menaces persistantes et assurer la continuité de la production. Les développeurs peuvent alors scanner plus tôt, plus souvent, éliminer des vulnérabilités dès leur apparition, au lieu d'attendre leur manifestation indésirable.

Groupes de corrections et résultats réels

Mais l'IFA fait bien plus que résoudre le dilemme de la vitesse et de la précision. Il aide les développeurs à progresser en efficacité parce qu'ils peuvent maintenant traiter des résultats et résoudre des problèmes directement dans le code qu'ils écrivent. En exploitant des techniques cognitives, l'IFA réduit le volume des résultats et des groupes de corrections. Avec les groupes de corrections, les développeurs savent exactement où se trouvent les problèmes de sécurité dans le code, ce qui leur permet de résoudre plusieurs problèmes simultanément. Ils peuvent maintenant prévoir entre cinq et dix groupes de corrections pour plusieurs centaines de problèmes de sécurité. Avec l'IFA, les développeurs peuvent tous les corriger dans un seul environnement de développement intégré (IDE).



Avec de telles capacités, comment l'IFA aide-t-il les entreprises à résoudre les challenges de la sécurité des applications au quotidien ? Prenons trois exemples de résultats clients réels :

		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

Dans l'application No. 1, les scans en profondeur ont identifié plus de 12 000 vulnérabilités potentielles. L'IFA a réduit ce chiffre à 1 000 environ, et identifié 35 points (groupes de corrections) dans le code pour corriger la totalité de ces 1 000 vulnérabilités. Dans l'application No. 2, les scans en profondeur ont identifié près de 250 000 vulnérabilités potentielles. Ici encore, l'IFA les a réduites à 1 000 et a identifié dans le code 103 groupes de corrections pour les résoudre. Dans l'application No. 3, les scans en profondeur ont identifié près de 750 000 vulnérabilités potentielles. L'IFA les a réduites à seulement 483 résultats réels et identifiés 42 groupes de corrections.

Après plus d'une année d'expérience, l'IFA démontre qu'il peut apporter un soutien efficace à une équipe de développement, quelle que soit la taille de l'application. Pour les équipes de sécurité, il élimine la nécessité de passer des heures à rechercher et à corriger des problèmes de sécurité, ou dans certains cas, de jeter l'éponge face à la taille colossale de la tâche. Ces entreprises ont donc pu améliorer de plus de 98 % leur efficacité à réduire les risques de sécurité dans leurs applications.

Exploiter l'IFA

Après tout ce travail théorique, l'apprentissage machine continu et l'expérience client réelle, que peut vous apporter l'IFA ? En termes très simples, l'IFA permet de :

- Accélérer vos tests de sécurité et de les intégrer à votre processus de développement continu.
- Réduire la charge de travail de votre équipe de sécurité.
- Aider vos développeurs à produire du code sécurité avec une plus grande efficacité.

Et ce n’est pas tout. Les fonctions IFA IBM sont maintenant disponibles avec nos solutions Application Security on Cloud et IBM Security AppScan Source. Utilisez le replay de notre webinaire ci-dessous pour savoir comment exploiter la puissance de la technologie cognitive dans votre entreprise. La courte vidéo présente de manière divertissante nos outils IFA et Intelligent Code Analytics (ICA) pour la sécurité des applications dans le cloud.