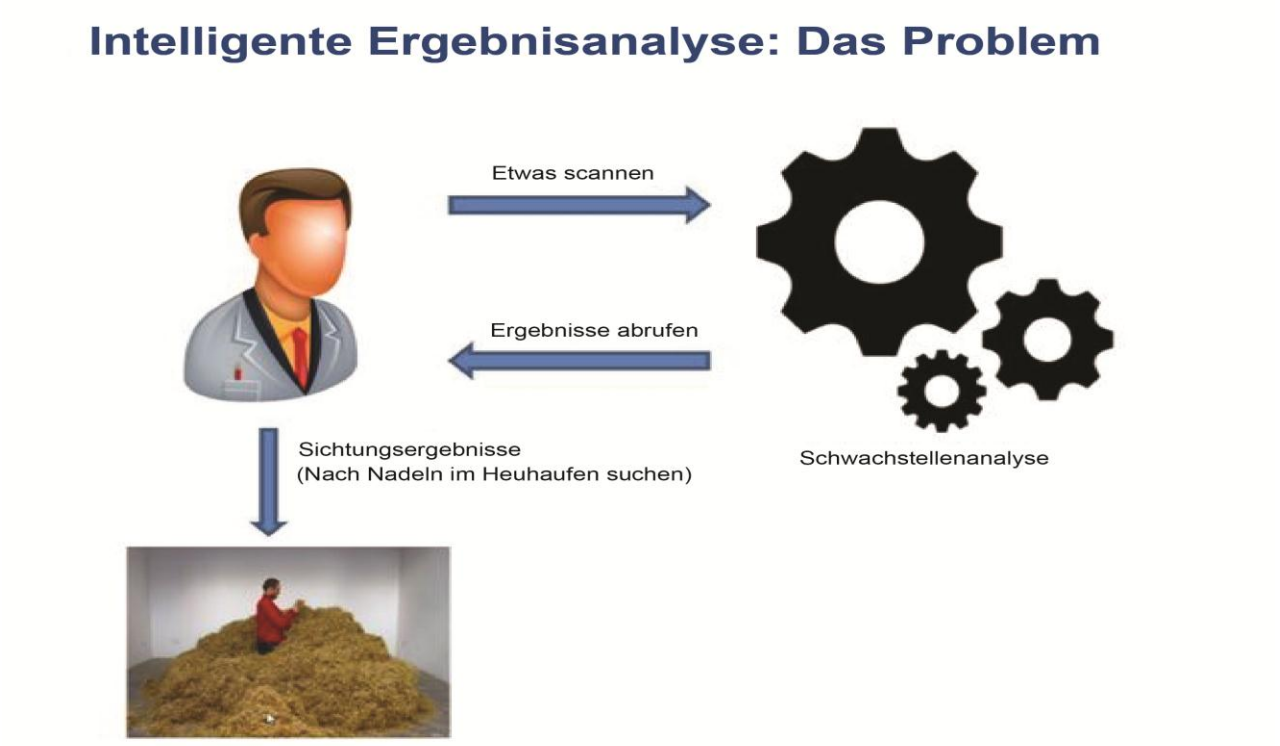
Intelligente Ergebnisanalyse: Ihr Experte für Anwendungssicherheit im Bereich kognitives Computing

14. Oktober, 2016 | Von David Marshak Mitverfasser Kris Duer

Vor zwei Jahren begann IBM® zu untersuchen, wie kognitives Computing eine intelligente Ergebnisanalyse erzeugen kann, um schwierigere Probleme zu lösen, mit denen Unternehmen konfrontiert sind, wenn sie das Sicherheitsrisiko von Anwendungen verstehen und reduzieren möchten. Unternehmen, die statische Anwendungssicherheitsprüfungen (SAST) einsetzen, um dieses Anwendungssicherheitsrisiko zu verstehen und zu reduzieren, stehen vor der Frage: Sollen sie sich auf die Geschwindigkeit konzentrieren, mit der sie Entwicklern Schwachstellen melden, oder auf die Genauigkeit, mit der sie Ergebnisse analysieren, um diese Probleme zu identifizieren, zu priorisieren und anzugehen? In der Regel müssen für die letztgenannte Zielgenauigkeit Experten eingesetzt werden, um Hochrisikoschwachstellen zu überprüfen und Falschmeldungen zu eliminieren, die Sicherheitsteams daran hindern können, die bisherige Zielgeschwindigkeit zu erreichen. Um es einfach auszudrücken, man konnte nicht beides haben. So war das zumindest bisher.

Nadeln und Heuhaufen

Nehmen wir das Beispiel eines Heuhaufens. Da der beste Ansatz für SAST darin besteht, die tatsächlichen Datenflüsse innerhalb einer Anwendung zu analysieren, liefert der SAST-Scanner tendenziell zahlreiche Ergebnisse. Betrachten Sie diese als alle möglichen Ergebnisse. Das ist der sprichwörtliche Heuhaufen.



Um die Nadeln in diesem Heuhaufen zu finden, können Sicherheitsteams einen von zwei möglichen Ansätzen wählen:

Die Größe des Heuhaufens verkleinern

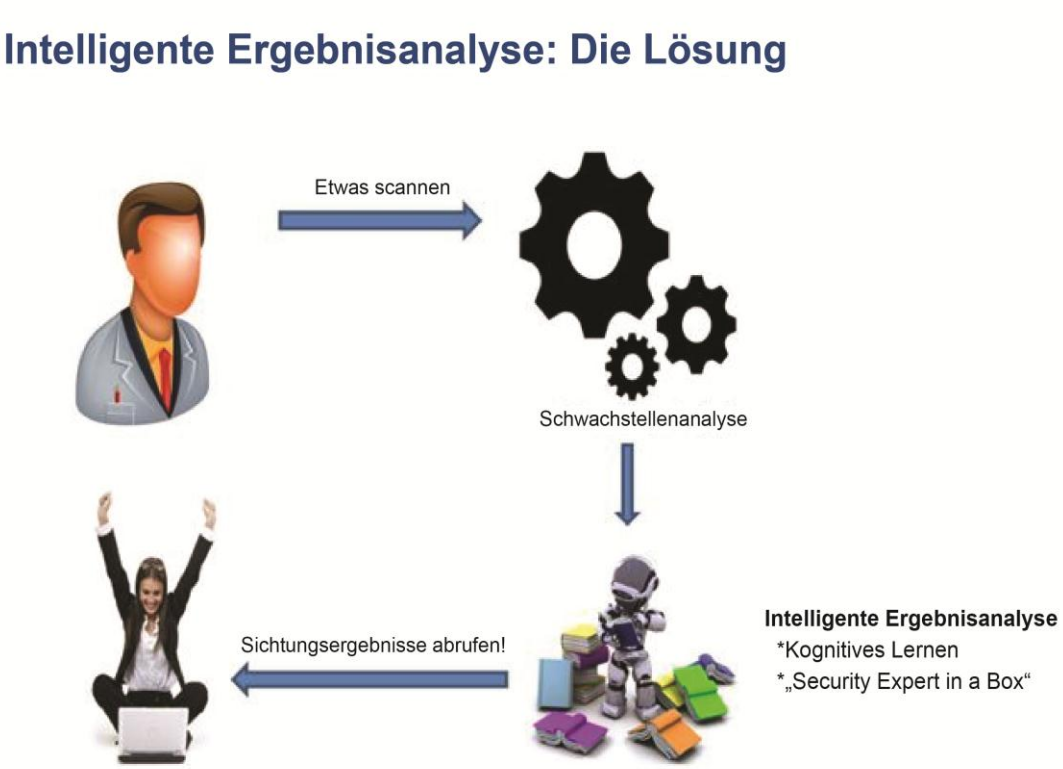
Dazu wird normalerweise ein leichterer Ansatz zum Scannen von Anwendungen gewählt, der weniger Ergebnisse liefert, aber hoffentlich die wichtigsten. Der große Vorteil dieses Ansatzes ist die Geschwindigkeit. Auf die Gefahr hin, unsere Metaphern zu vermischen, kann mit den wenigen Ergebnissen schnell die Spreu vom Weizen getrennt werden. So können Sicherheitsteams den Entwicklern schnell Ergebnisse liefern. Der Nachteil sollte aber auch nicht unterschätzt werden, denn: Sicherheitsteams finden vielleicht nie die Nadeln, nach denen sie suchen. Mit anderen Worten, der Prozess kann nicht garantieren, dass das allgemeine Anwendungssicherheitsrisiko eines Unternehmens reduziert wird.

Mehr Hilfe rekrutieren

Der zweite Ansatz besteht darin, mehr Mitarbeiter einzustellen, um die Ergebnisse zu analysieren und die Nadeln manuell zu finden. Der Vorteil dieses Ansatzes ist seine Vollständigkeit. Die Nadeln gehen bei der Prüfung nicht verloren, und Experten können die Ergebnisse identifizieren, bei denen Handlungsbedarf besteht. Der Nachteil ist natürlich die Ineffizienz in Bezug auf Qualifikation, Kosten und vor allem Zeit. Je größer der Heuhaufen, desto mehr Experten benötigt das Projekt. Diese Experten sind knappe und teure Ressourcen. Die Analyse der Ergebnisse kann Stunden, Tage oder sogar Wochen dauern, weshalb es praktisch unmöglich ist, den Entwicklern zeitnah Ergebnisse zu liefern oder ein kontinuierliches Engineering zu gewährleisten. Aufgrund des Fachkräftemangels entscheiden sich einige Unternehmen, den gesamten Prozess auszulagern. Dies kann die kurzfristige Qualifikationslücke schließen, erhöht aber die Kosten und Prozesszeit erheblich. Outsourcing befreit Unternehmen von Einstellungen und Schulungen, bedeutet aber auch, dass sie keine Kontrolle darüber haben, wie sie ihre Zeit priorisieren.

Intelligente Ergebnisanalyse

Angesichts dieser Optionen und des Erfolgs anderer kognitiver Bemühungen stellten IBM-Experten fest, dass es eine dritte Alternative geben muss. Damit war die zum Patent angemeldete intelligente Ergebnisanalyse (IFA) von IBM geboren. Die IFA war ursprünglich ein Forschungsprojekt, um festzustellen, ob der große Vorteil des ersten SAST-Ansatzes - Geschwindigkeit - mit dem Vorteil des zweiten Ansatzes - Genauigkeit - ohne die jeweils damit verbundenen Nachteile erreicht werden konnte. Ziel war es, die gleichen kognitiven Fähigkeiten, die IBM Watson zugrunde liegen, zu nutzen, um hauptsächlich als eine Gruppe von Experten zu agieren, die sich durch den Heuhaufen wühlen.



Verblüffende Zahlen

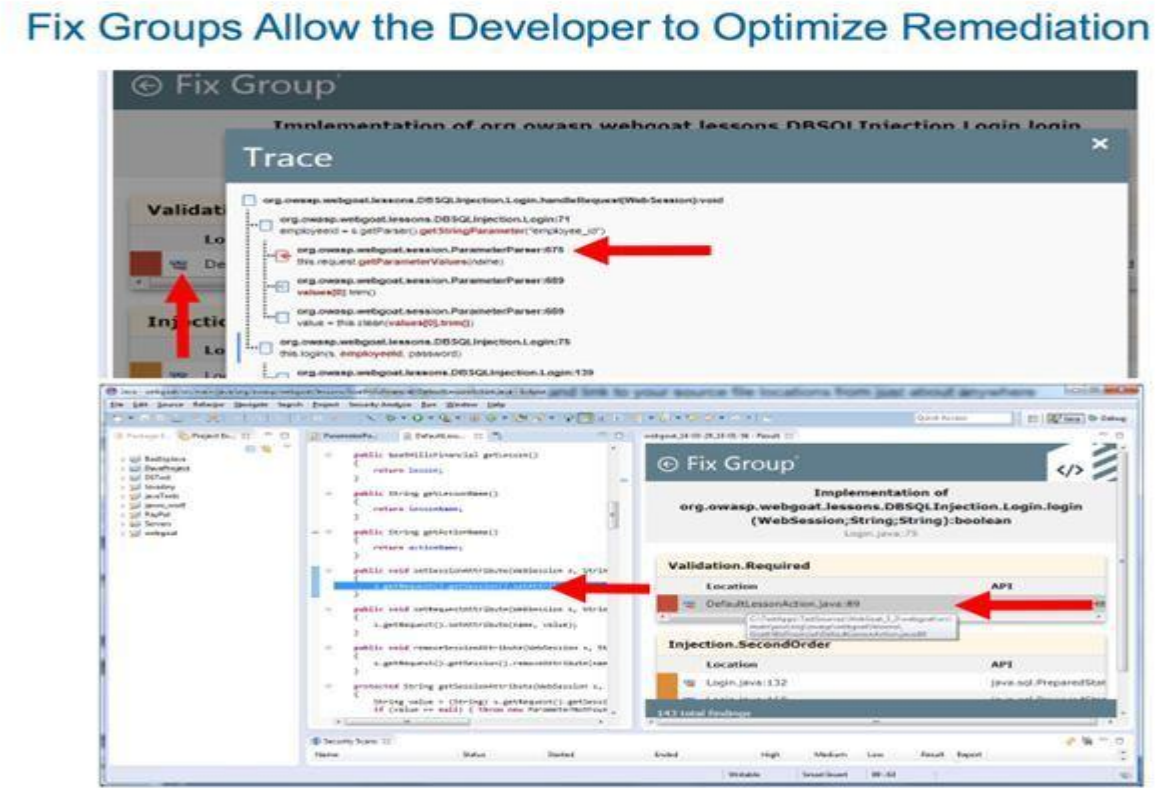
Im vergangenen Jahr waren die Ergebnisse noch aussagekräftiger als ursprünglich erwartet. Im realen Kundeneinsatz wurde durch die Beseitigung von Falschmeldungen und Ungenauigkeiten die Größe des Heuhaufens kontinuierlich um über 90 Prozent reduziert. Dank der Lernfähigkeiten der IFA liegt die Genauigkeit bei der Entfernung von Falschmeldungen bei über 98 Prozent. Die tatsächliche Reduzierung von Falschmeldungen und Ungenauigkeiten beträgt ab Oktober 2016 in der Summe aller Kundenscans bei Application Security on Cloud sagenhafte 98,91 Prozent!

Wie wir festgestellt haben, geht diese Reduzierung nicht zu Lasten der Genauigkeit, denn die 98-prozentige Genauigkeit der IFA ist nahezu identisch mit der von kompetenten und erfahrenen Experten für Anwendungssicherheit. In vielen Fällen sind die Ergebnisse der IFA sogar besser als die von menschlichen Experten. Höchstwahrscheinlich ist dies auf die Ermüdung der Menschen nach stundenlanger Jagd auf Nadeln zurückzuführen. Die IFA liefert ihre Ergebnisse in Minuten, wenn nicht gar Sekunden, verglichen mit Stunden oder Tagen, die menschliche Experten für die Analyse umfangreicher Anwendungen benötigen. Dank dieser Geschwindigkeit können Cybersicherheitsteams Entwicklern schnell genug Erkenntnisse liefern, damit diese mit den anhaltenden Bedrohungen Schritt halten und einen kontinuierlichen Engineering-Modus aufrechterhalten können. Dies ermöglicht es Entwicklern, häufig und frühzeitig zu scannen und Schwachstellen gleich bei ihrem Auftreten zu beheben, anstatt darauf zu warten, dass sie später ihr Unwesen treiben.

Problemgruppen und Ergebnisse in der Praxis

Doch die IFA geht nicht nur Heuhaufen und Nadeln an. Sie hilft Entwicklern auch dabei, effizienter Erkenntnisse zu gewinnen und Probleme direkt im von ihnen geschriebenen Code

zu beheben. Durch die Anwendung kognitiver Techniken reduziert die IFA mithilfe von Problemgruppen die Menge der Erkenntnisse. Problemgruppen zeigen Entwicklern genau an, an welchen Stellen sich Sicherheitsprobleme im Code befinden, sodass sie mehrere Probleme gleichzeitig beheben können. Entwickler sehen jetzt fünf bis zehn Problemgruppen anstatt von Hunderten von Sicherheitsproblemen. Die IFA ermöglicht es Entwicklern, alle Probleme in einer integrierten Entwicklungsumgebung (IDE) zu beheben.



Wie kann die IFA Unternehmen dabei helfen, die täglichen Herausforderungen im Bereich Anwendungssicherheit zu bewältigen? Schauen wir uns drei reale Kundenergebnisse an:

		Nach-IEA-Ergebnisse	
	Vor-IEA-Scanergebnisse	Schwachstellen	Gruppenempfehlungen festlegen
Anwendung 1	12.480	1.057	35
Anwendung 2	247.350	1.271	103
Anwendung 3	746.979	483	42

In der Anwendung Nr. 1 identifizierten die Ergebnisse des Deep-Scans mehr als 12.000 potenzielle Schwachstellen. Die IFA reduzierte diese Zahl auf etwa 1.000 und identifizierte 35 Stellen (Problemgruppen) im Code, um alle 1.000 Probleme anzugehen. In der

Anwendung Nr. 2 identifizierten die Ergebnisse des Deep-Scans fast 250.000 potenzielle Schwachstellen. Auch hier reduzierte die IFA die Sicherheitslücke auf etwa 1.000 Schwachstellen und identifizierte 103 Problemgruppen im Code. In der Anwendung Nr. 3 identifizierten die Ergebnisse des Deep-Scans fast 750.000 potenzielle Schwachstellen. Erstaunlicherweise reduzierte die IFA diese auf nur 483 reale Ergebnisse und identifizierte 42 Problemgruppen.

Mit mehr als einem Jahr Erfahrung zeigt die IFA, dass sie einem Entwicklungsteam bei der Entwicklung von Anwendungen jeder Größe helfen kann. Sie sorgt dafür, dass Sicherheitsteams nicht mehr Stunden für die Identifizierung von Problemen bei der Anwendungssicherheit und deren Behebung verbringen müssen, und in einigen Fällen, dass Teams nicht angesichts der gewaltigen Herausforderung frustriert aufgeben. Stattdessen haben Unternehmen jetzt die Effizienz, mit der sie Anwendungssicherheitsrisiken angehen, um mehr als 98 Prozent gesteigert.

Lassen Sie die IFA die Arbeit machen

Nach der ganzen wissenschaftlichen Arbeit, dem ständigen maschinellen Lernen und der praktischen Kundenerfahrung, was kann die IFA für Sie tun? Ganz einfach gesagt können Sie mit der IFA:

- Ihre Sicherheitstests beschleunigen, um sie in Ihren kontinuierlichen Entwicklungsprozess zu integrieren.
- Die Belastung für Ihr begrenztes Sicherheitspersonal reduzieren.
- Ihre Entwickler dabei unterstützen, sicheren Code effektiver bereitzustellen.

Und dies ist nur der Anfang. Die IFA-Fähigkeiten von IBM sind ab sofort in unseren Lösungen Application Security on Cloud und IBM Security AppScan Source verfügbar. Sehen Sie sich unser Webinar-Replay an, um zu erfahren, wie Sie die leistungsstarken kognitiven Technologien in Ihrem Unternehmen entfesseln können. Das kurze Video zeigt Ihnen einen unterhaltsamen Überblick über unsere IFA- und ICA-Funktionen (Intelligent Code Analytics) für Application Security on Cloud.