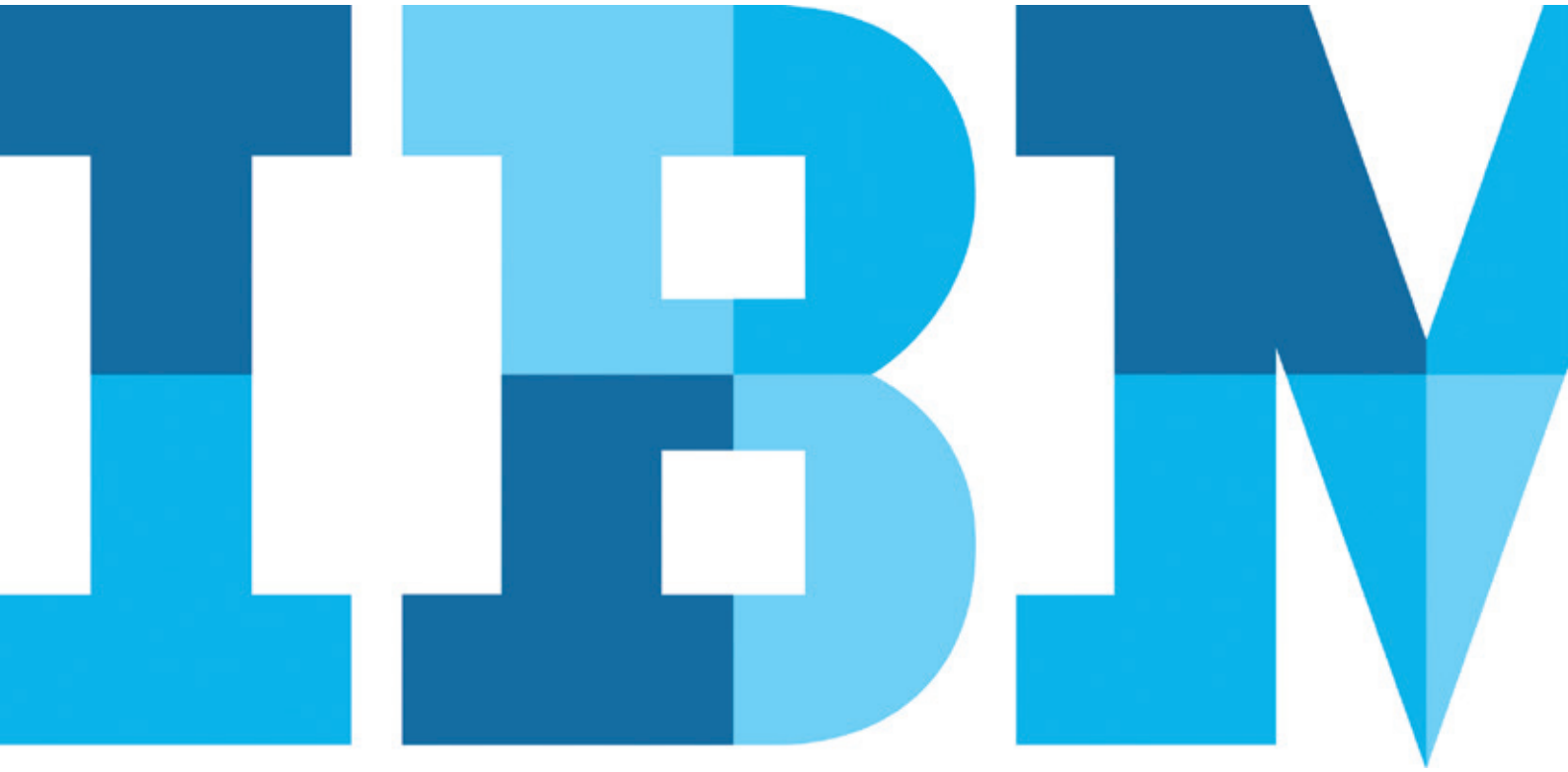
Décembre 2017

Gérer les risques de sécurité de vos applications pour protéger les données stratégiques de votre entreprise

Les solutions complètes IBM de test de la sécurité des applications aident à identifier les failles et à réduire les risques



IBM

Analyse de la sécurité des applications

De nombreuses entreprises s'appuient sur des applications logicielles pour exécuter leurs processus stratégiques, mener à bien leurs transactions avec les fournisseurs et proposer des services sophistiqués aux clients. Etonnamment, même si leurs activités dépendent de ces applications, rares sont celles qui investissent de manière à assurer une sécurité adaptée. Ces entreprises comprennent les technologies de sécurité classiques pour les tâches de routine sur le réseau et au sein des opérations, par exemple pour gérer des procédures telles que le contrôle de l'accès et l'authentification, mais elles peinent souvent à mettre en œuvre, à gérer et à soutenir des programmes dédiés à la sécurité des applications. Cependant, le niveau de menace actuel exige de mettre la barre plus haut. Etant donné que les applications peuvent compromettre la sécurité de l'ensemble de l'entreprise, leur sécurité doit devenir une priorité absolue.

Les conséquences d'une sécurité incomplète des applications peuvent être terribles. Les failles introduites accidentellement au cours du développement peuvent permettre aux pirates informatiques de déstabiliser les applications et d'obtenir un accès libre aux informations confidentielles de la société ou aux données privées des clients. Ce type de perte de données risque d'affecter la réputation de la marque, d'entraîner une perte de confiance des clients, de perturber les activités, d'interrompre la chaîne d'approvisionnement et de causer des poursuites et/ou des sanctions judiciaires; soit tout un ensemble de conséquences préjudiciables à la rentabilité.

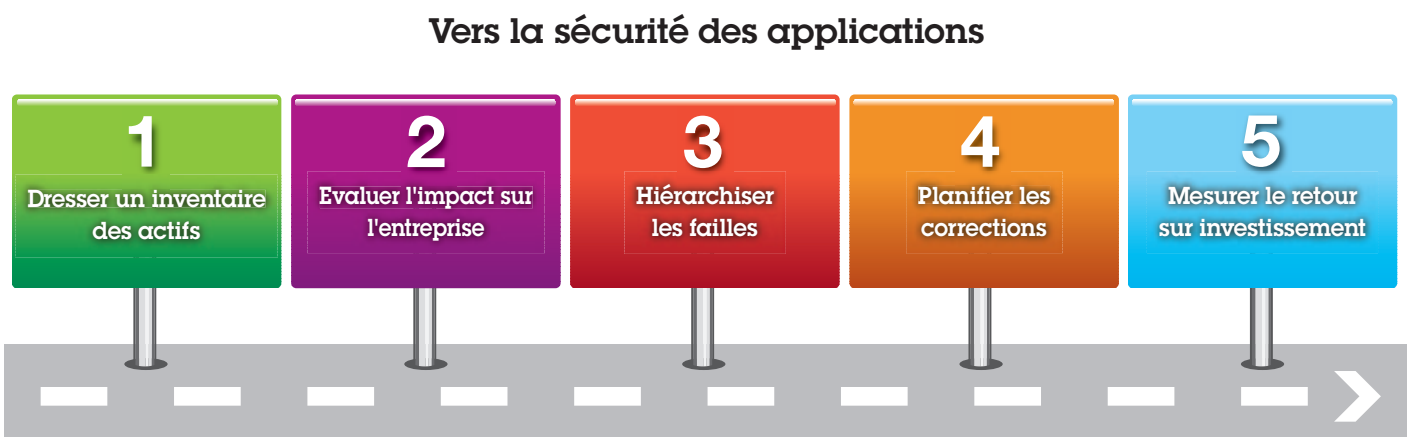
Assurer la sécurité des applications peut s'avérer un défi. Les grandes entreprises gèrent des milliers d'applications et leur sécurité repose généralement sur les épaules d'une équipe restreinte et surchargée. Pour se protéger contre ces conséquences potentielles, les entreprises telles que la vôtre doivent mettre en place une gestion de la sécurité des applications basée sur le risque. Vous avez besoin de solutions qui offrent une visibilité nette de l'ensemble de l'infrastructure ; identifient et hiérarchisent les applications en fonction de leur impact stratégique ; évaluent la vulnérabilité des applications ; remettent les failles en contexte pour déterminer leur niveau de risque ; et atténuent les risques en implémentant les correctifs nécessaires dans le code ou en déployant les politiques appropriées. La première étape tangible est d'adopter une stratégie de sécurité capable de protéger les applications Internet et mobiles à chaque étape de leur cycle de vie.

Adopter une stratégie de gestion de la sécurité des applications

Rares sont les entreprises qui hiérarchisent la sécurité des applications, ce qui les expose aux risques. Selon une étude menée par le Ponemon Institute, seules 25 % des personnes interrogées évaluent la capacité de leur entreprise à contrer ou limiter les failles de sécurité des applications comme « hautement efficace », et seules 44 % des personnes interrogées déclarent réaliser des tests de sécurité.[1] Une autre étude indique que seules 39 % des personnes sondées déclarent que leurs applications mobiles sont testées en production.[2] Répartissez-vous correctement votre budget dédié à la sécurité pour répondre à cette évolution des risques ?

L'efficacité de la sécurité dépend clairement de la gestion des risques. Vous devez absolument comprendre, gérer et atténuer les risques sur vos actifs les plus stratégiques. Pour sécuriser efficacement vos applications, veillez à :

1. **Dresser un inventaire des actifs :** Identifiez vos actifs et déterminez ceux qui sont les plus stratégiques. Plutôt que d'essayer de sécuriser directement toutes vos applications, concentrez-vous d'abord sur les plus stratégiques.
2. **Evaluer l'impact stratégique :** Une fois que vous avez hiérarchisé vos actifs, procédez à une analyse de leurs failles. Evaluez les risques entraînés par chaque application en fonction de son impact stratégique et de la gravité de ses failles.
3. **Hiérarchiser les failles :** Une fois que vous avez évalué les risques de chaque application, concentrez-vous sur celles qui présentent les dangers les plus importants et corrigez d'abord les failles les plus graves.
4. **Planifier les corrections :** L'atténuation des risques peut impliquer la correction d'erreurs de code, la création de correctifs virtuels via le pare-feu d'une application Internet ou, dans certains cas, le retrait temporaire des applications.
5. **Evaluer le retour sur investissement :** Les différentes statistiques peuvent vous aider à surveiller l'état de la sécurité des applications et à évaluer l'efficacité de votre programme. Une étude récente menée par une société d'analyse leader a révélé qu'un client IBM atteignait un retour sur investissement à trois chiffres grâce à sa solution IBM Security AppScan Source.[3]



La gestion de la sécurité des applications implique d'envisager les risques sous cinq angles clés.

Découvrir la gestion intégrée de la sécurité des applications d'IBM

Mener une initiative relative à la sécurité des applications dans une grande entreprise peut relever du défi. La sécurisation des milliers d'applications conçues par les développeurs repose souvent sur une équipe restreinte chargée de la sécurité. IBM fournit des fonctions intégrées de gestion de la sécurité des applications qui permettent aux équipes de corriger les failles détectées au quotidien. Le portefeuille inclut des options sur site et dans le cloud ajustées à vos besoins spécifiques.

Comme décrit ci-dessus, les programmes de test de la sécurité des applications les plus efficaces se concentrent sur l'atténuation du risque. Les entreprises novices dans ce domaine peuvent justifier leur besoin de test en menant un DAST (Dynamic Application Security Testing) sur leurs applications les plus importantes afin d'identifier les failles les plus graves. Le DAST leur permet également de contrer les risques les plus élevés dans leur portefeuille d'applications et de prouver rapidement leur réussite. De nos jours, chaque entreprise doit déterminer si sa première préoccupation est d'identifier les failles applicatives les plus graves ou d'établir une culture de rédaction de code sécurisé et d'appliquer les meilleures pratiques. Le DAST aide les développeurs à améliorer les pratiques de rédaction de code dans le temps et à mettre en place des tests de sécurité des applications. Le SAST (Static Application Security Testing) représente souvent un effort plus stratégique visant utiliser les meilleures pratiques en rédaction de code et à atténuer potentiellement les risques avec l'amélioration de la qualité du code.

Solutions sur site

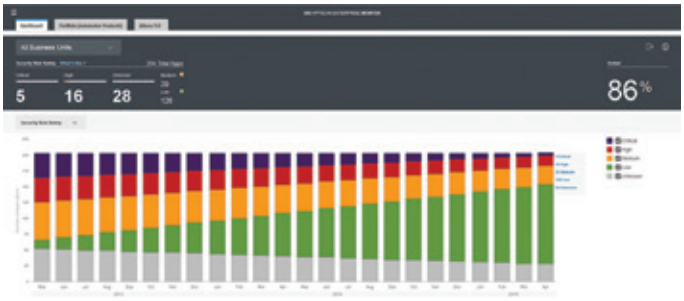
Les solutions IBM Security AppScan fournissent des composants spécialement conçus pour les responsables de la sécurité des applications et les équipes de développement des entreprises de toute taille. Solutions sur site :

- **IBM Security AppScan Standard :** Permet de réduire le risque d'attaques sur les applications Internet et les violations de données en automatisant les tests à la recherche de failles de sécurité et en tirant parti de fonctions DAST avancées

- **IBM Security AppScan Source :** Aide à réduire les coûts et l'exposition aux risques en intégrant le SAST dans l'automatisation des DevOps afin de tester les applications plus tôt dans le cycle de développement et d'éliminer les failles avant le déploiement

Le logiciel AppScan Source fournit des synthèses d'évaluation qui cartographient les risques des applications et apportent des perspectives sur les failles.

- **IBM Security AppScan Enterprise :** Permet aux entreprises de réduire les risques de sécurité des applications tout en se conformant aux exigences réglementaires. De même, elle aide les équipes en charge de la sécurité et du développement à dresser des inventaires de leurs applications, à les classer en fonction de leur impact stratégique, et à hiérarchiser et à corriger les failles tout au long du cycle de vie.



Les fonctions de gestion de la sécurité des applications AppScan permettent aux équipes de corriger les failles détectées au quotidien.

IBM Application Security on Cloud facilite grandement les tests sur les applications mobiles, Internet et de bureau. Il suffit aux utilisateurs de choisir le type d'applications qu'ils souhaitent analyser.

Solutions cloud

IBM Application Security on Cloud contribue à sécuriser les applications Internet et mobiles de votre entreprise en détectant des douzaines de types de failles actuelles et fréquemment exploitées. IBM Application Security on Cloud intègre le DAST, le MAST (Mobile Application Security Testing), le SAST et l'Open Source Analyser pour détecter les failles des applications avant la mise en production et le déploiement. Des rapports pratiques et détaillés vous permettent de corriger efficacement les risques de sécurité des applications afin de proposer une expérience plus sécurisée aux utilisateurs.

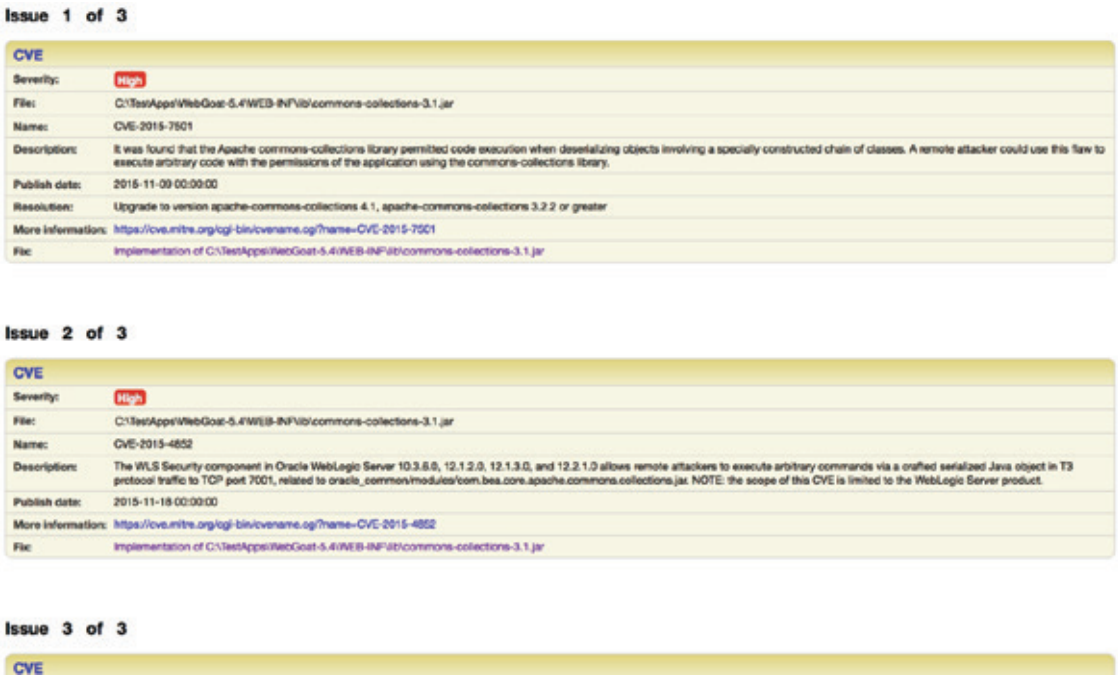
Fonctions cognitives d'IBM Application Security on Cloud :

- Intelligent Finding Analytics, qui s'appuie sur l'apprentissage automatique pour interpréter les résultats, réduire intelligemment les faux-positifs et écourter considérablement les temps d'analyse demandant une validation des experts de la sécurité des applications
- Intelligent Code Analytics, qui automatise l'analyse de tous les cadres de rédaction de code utilisés par les équipes de développement, éliminant ainsi les révisions manuelles onéreuses et les faux négatifs tout en contribuant à l'automatisation complète du test des DevOps.

Caractéristiques des solutions

Les solutions IBM pour le test des applications, notamment AppScan et IBM Application Security on Cloud, permettent aux entreprises de gérer la sécurité tout au long du cycle de vie. Principales fonctionnalités :

- **Evolutivité des tests de sécurité des applications** - Ce qui vous permet de sélectionner la solution la mieux adaptée à votre entreprise et d'ajouter des composants pour la personnaliser au gré de l'évolution de votre programme de sécurité des applications
- **Visibilité importante** - Tableau de bord offrant une visibilité à l'échelle de l'entreprise du niveau de sécurité et des risques de conformité des applications et des processus
- **Stratégie sécurisée pour les DevOps** - S'intègre aux environnements clés et aux environnements de développement intégrés afin de proposer des tests transparents et une correction rapide et ciblée de vos applications
- **Groupes de réparation** - Localise et collecte les résultats concernant un ou plusieurs emplacements ou croisements dans des groupes afin de faciliter la consultation et la correction, et, donc, de réduire le travail des développeurs, d'accélérer les DevOps et de renforcer la sécurité des applications en cours de déploiement
- **Gestion des exigences réglementaires** - Permet aux utilisateurs de choisir parmi plus de 40 rapports pré-définis et de cartographier les résultats d'analyse en fonction des principales normes de conformité réglementaires et industrielles, pour que les entreprises puissent répondre aux exigences concernant leurs applications Internet
- **Gouvernance des tests de sécurité** - Vous permet de créer, valider et faire appliquer des politiques de sécurité cohérentes, utiles dans toute l'entreprise, en vous appuyant sur des règles de test et des modèles d'analyse
- **Correction des problèmes** - Etablit une liste entièrement hiérarchisée des failles détectées à chaque analyse afin que les problèmes les plus importants soit résolus en priorité
- **Intelligence au service de la sécurité** - S'intègre aux autres solutions IBM Security pour optimiser l'évaluation des menaces et la hiérarchisation des problèmes de sécurité.



IBM Open Source Analyser affiche les failles dans des groupes de réparation afin de faciliter leur consultation et leur correction.

Test avancé des applications

Etant donné qu'il existe de multiple façons d'envisager la sécurité des applications, le logiciel AppScan utilise toute une variété de techniques de test complémentaires afin d'automatiser les tests approfondis dès le début des processus DevOps. La détection précoce offre aux équipes de développement un meilleur retour sur investissement car elles corrigent les failles avant que l'application ne soit déployée en production.

Les solutions de test de la sécurité des applications d'IBM offrent des fonctions DAST, SAST et open source pour que les utilisateurs gardent une avance sur les dernières menaces et qu'ils obtiennent des résultats précis et exploitables. Les méthodes de test AppScan comprennent également :

- **Une analyse interactive :** Positionne des agents d'exécution sur la machine où se trouvent les applications et analyse les applications. En associant les aspects de l'analyse dynamique et de l'analyse statique lors de l'exécution, vous pouvez détecter davantage de failles avec une précision accrue
- **Une analyse hybride :** Associe l'analyse statique à l'analyse dynamique pour corréler et vérifier les résultats. Assure la traçabilité des problèmes détectés dans l'analyse dynamique jusqu'à la ligne de code en question et valide les problèmes identifiés au cours de l'analyse statique avec un test externe
- **IBM Application Security Open Source Analyser :** Aide à sécuriser et à gérer vos composants open source en automatisant les tests de sécurité et en configurant l'analyse spécifiquement pour les failles open source. Vous permet de gagner en contrôle et en visibilité sur le risque open source en identifiant les composants logiciels défaillants en temps réel
- **Analyse JavaScript™ côté client :** Vous aide à analyser le code téléchargé sur le client. Plus les fonctions exécutées côté client sont nombreuses, plus le potentiel de défaillance côté client est important.

Qui peut tirer parti des solutions IBM de test de la sécurité des applications ?

Les solutions de test de la sécurité des applications d'IBM® sont conçues pour profiter à trois groupes principaux :

- Directeur métier ou directeur de la sécurité informatique : Ces personnes sont chargées de la sécurité des applications et, donc, responsables des conséquences en cas de protection inadaptée. Grâce à ces solutions, elles peuvent mieux comprendre les risques de sécurité de l'entreprise et son niveau de conformité général
- Equipe chargée de la sécurité des applications : L'équipe chargée de gérer et de renforcer la sécurité des applications de l'entreprise peut être avantagée par le fait de connaître exactement les actifs dont elle dispose, leur importance par priorité, leur niveau de sécurité et les failles les plus critiques
- Equipe chargée du développement des applications : Les développeurs d'applications peuvent profiter de l'intégration des tests de sécurité au processus DevOps afin de mieux détecter les failles dès le début du cycle de développement.

Création de solutions de sécurité de bout en bout

La sécurité des applications ne se limite pas uniquement à l'analyse et à la détection de failles ; il s'agit également de gérer le risque. Le déploiement de solutions intégrées et automatisées pour la sécurité des applications permet d'aboutir à des résultats plus rationalisés, plus rentables et plus fiables. L'intégration permet d'adopter une approche basée sur les risques, susceptible d'aider votre entreprise à gérer l'impossibilité de protéger immédiatement toutes les applications. Par exemple, l'intelligence de la sécurité est nécessaire pour hiérarchiser les applications et déterminer celles qui doivent être corrigées, à quel moment et selon quelles modalités.

C'est la raison pour laquelle les solutions de test de la sécurité des applications d'IBM sont conçues pour s'intégrer à des offres IBM Security complémentaires. Les entreprises voient ainsi la sécurité de leurs applications renforcée et disposent de capacités pour mieux évaluer les menaces et hiérarchiser les failles en fonction des risques qu'elles présentent. Ces offres incluent :

- **IBM QRadar Security Intelligence Platform,** qui intègre la sécurité des informations et la gestion des événements, la gestion des journaux, la détection et la configuration des anomalies et la gestion des failles pour une meilleure détection des menaces, une simplicité d'utilisation accrue et une réduction du coût de revient
- **IBM Security Guardium,** qui offre une plateforme complète pour la sécurité des données avec tout un éventail de fonctions : depuis la découverte et la classification des données sensibles jusqu'à l'évaluation de la vulnérabilité des données et fichiers afin de les protéger par la surveillance, les masques, le chiffrement, le blocage, les alertes et la mise en quarantaine
- **Solutions de sécurité mobile IBM,** qui intègrent les fonctions de test de la sécurité des applications mobiles d'IBM Application Security on Cloud pour vous aider à corriger les failles potentielles de manière proactive et à augmenter l'efficacité opérationnelle
- **Solutions de sécurité cloud IBM,** qui fournissent des ressources informatiques à la demande sur Internet avec paiement à l'utilisation, qu'il s'agisse d'applications ou de centres informatiques.

Synthèse

L'importance de la sécurité des applications est claire et les défis sont complexes. Sans la visibilité nécessaire sur l'infrastructure et les solutions de sécurité adaptées, la protection de votre entreprise peut sembler insurmontable. IBM a défini une feuille de route concrète pour la sécurité des applications, vous éclairant ainsi sur les démarches cruciales que votre entreprise peut accomplir en vue de créer un programme de test fructueux et efficace.

Grâce à ses tests de sécurité avancés et à sa plateforme de gestion des risques des applications, AppScan est conçu pour aider les entreprises à mettre en œuvre et à gérer plus facilement les stratégies de sécurité les plus récentes. Cette solution apporte l'expertise en sécurité et les intégrations à la gestion du cycle de vie des applications dont vous avez besoin pour identifier les failles et réduire globalement les risques.

De même, au fur et à mesure que votre entreprise évolue en matière de sécurité des applications, vous pouvez personnaliser les solutions de test IBM avec les composants les mieux adaptés à vos besoins spécifiques.

Pour accéder dès aujourd'hui à un essai complémentaire AppScan, veuillez consulter la page Internet AppScan.

Pour accéder à une version d'essai complémentaire IBM Application Security on Cloud, veuillez consulter la page Internet IBM Application Security Analyser.

Complément d'information

Pour en savoir plus sur les solutions de test de la sécurité des applications d'IBM ou sur les offres complémentaires d'IBM Security, veuillez contacter votre représentant ou partenaire commercial IBM. Vous pouvez également consulter le site :
ibm.com/security/application-security/appscan/

Pour consulter les pré-requis système de chaque solution de test de la sécurité des applications, veuillez cliquer sur les liens suivants :

- AppScan Standard
- AppScan Source
- AppScan Enterprise
- IBM Application Security on Cloud

[1] « How to Make Application Security a Strategically Managed Discipline » (« Comment transformer la sécurité des applications en discipline gérée et stratégique »), *Ponemon Institute*, parrainé par IBM Security, mars 2016. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGL03106USEN&attachment=WGL03106USEN.PDF

[2] « 2017 Study on Mobile and Internet of Things Application Security », (« Etude 2017 sur la sécurité des applications mobiles et de l'Internet des Objets ») *Ponemon Institute*, parrainé par IBM Security et Arxan Technologies, janvier 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03136USEN&

[3] Neil Jones, « Recently Released Industry Research Study Reveals Triple-Digit ROI for IBM Application Security Testing Solution », (« Une étude récente de l'industrie montre un retour sur investissement à trois chiffres pour la solution de test de la sécurité des applications IBM »), *SecurityIntelligence*, 19 juillet 2016. https://securityintelligence.com/recently-released-industry-research-study-reveals-triple-digit-roi-for-ibm-application-security-testing-solution/

IBM United Kingdom Limited (are we talking about France?)
17 avenue de
l'Europe 92275
Bois-Colombes
Cedex France

IBM Ireland Limited (are we talking about France?)
Oldbrook House
24-32 Pembroke Road
Dublin 4 (are we talking about France?)

IBM France est enregistrée en France.
La page d'accueil d'IBM est accessible à l'adresse suivante : **ibm.com**/fr

WGB03009-FRFR-06