Tests Interactifs de Sécurité des Applications (IAST)

En quoi les Tests Interactifs de Sécurité des Applications (IAST) consistent-ils ?

Les tests de sécurité des applications englobent les diverses approches mises en œuvre par les entreprises pour identifier et éliminer les vulnérabilités de leurs applications. Également appelé AppSec et AST, ce processus consiste à tester, analyser et produire des rapports sur le niveau de sécurité d'une application au cours du cycle de vie de son développement (SDLC).

Pourquoi sont-ils importants ?

Les tests interactifs de sécurité des applications (IAST) combinent les techniques statiques (SAST) et dynamiques (DAST) pour une approche optimale de la sécurité applicative. Grâce à leur interactivité, les tests IAST couvrent plus de code, produisent de meilleurs résultats et balaient un plus large spectre de règles de sécurité que ne le font individuellement les outils SAST ou DAST, avec en outre une rapidité accrue.

Approche en continu ou instantané ?

Selon une étude de Gartner, 84 % des violations exploitent des vulnérabilités de la couche applicative. Puisque les SAST, les DAST et les tests de pénétration ne fournissent qu'une image prise à l'instantané, ils ne sont pas adaptés à l'agilité qui caractérise aujourd'hui le cycle de vie du développement d'une application, ni à l'évolution constante des menaces. Ce qui signifie que les équipes développement, les opérations et la sécurité ont toujours un temps de retard lorsqu'elles conçoivent, testent et lancent les applications en production.

La puissance de l'IAST

Les solutions de sécurité IAST, en revanche, déploient des agents et capteurs qui surveillent et analysent les applications en continu durant leur exécution. Puisqu'elles sont auto-apprenantes, elles produisent des analyses applicatives en temps réel, à mesure du développement et des tests. Elles sont donc idéalement

adaptées aux environnements Agile, DevOps et DevSecOps, car elles permettent d'identifier et de corriger les failles de sécurité plus en amont dans le SDLC, quand il est encore facile et peu coûteux d'y remédier.

Imaginez que vous puissiez identifier les vulnérabilités à la vitesse DevOps, en arrêtant les attaques avant qu'elles se produisent, et en prévenant les problèmes avant qu'ils puissent causer de réels dommages. Contrast sort du cadre des outils traditionnels avec une solution de sécurité IAST innovante et automatisée, Contrast Assess, qui dote les applications de capacités d'évaluation des vulnérabilités permettant d'identifier les failles de sécurité automatiquement et en temps réel quel que soit le lieu d'exécution.

Fonctionnement des tests interactifs de sécurité des applications

Contrast Assess est une solution IAST révolutionnaire intégrant la sécurité au sein de l'application elle-même. Celle-ci se trouve alors dotée de capacités d'évaluation des vulnérabilités permettant d'identifier les failles de sécurité en temps réel. Solution embarquée (au travers d'un agent unifié), évolutive et continue, s'adaptant avec fluidité aux environnements de développement et de production, Contrast Assess accélère, simplifie et intègre la sécurité des applications pour les équipes développement, les opérations et la sécurité. Elle utilise les capteurs Contrast pour assurer une télémétrie en temps réel des vulnérabilités et attaques tout au long du flux de travail – amélioration indéniable par rapport aux approches traditionnelles.

7 Avantages de l'IAST par rapport aux tests SAST et DAST

Objectivement, en termes d'avantages, l'IAST laisse loin derrière elle les tests SAST et DAST sur les sept points suivants.

1. **Faux positifs :** Ceux-ci constituent la plus grande faiblesse des outils de sécurité traditionnels, constituant plus de 50 % des résultats des tests. Ce qui entraîne une surcharge de travail pour des ressources déjà rares, et complique l'identification des failles les plus critiques. L'IAST, en revanche, produit des informations en temps réel et procure la visibilité continue nécessaire à la détection et à la correction des vulnérabilités en ne générant pratiquement aucun faux positif ou faux négatif.

2. **Couverture des vulnérabilités :** L'analyse interactive conjugue les avantages des tests statiques et dynamiques. Non seulement les tests interactifs se concentrent sur les failles les plus courantes et les plus dangereuses des applications, mais permettent en outre d'établir des règles personnalisées pour adapter la couverture aux besoins spécifiques de l'entreprise.

3. **Couverture du code :** Les tests statiques et dynamiques passent à côté d'énormes portions de la plupart des applications. Les tests SAST ne balaient pas les bibliothèques ou les frameworks, ce qui limite considérablement l'analyse des vulnérabilités. Et les tests DAST ne peuvent analyser que la surface exposée d'une application. La solution IAST, pour sa part, observe l'application depuis l'intérieur – en incluant les bibliothèques et les frameworks. Il en résulte une bien meilleure couverture de toute la base de code.

4. **Évolutivité :** Les outils statiques et dynamiques ne brillent guère par leur évolutivité. Leur configuration et leur exécution nécessitent généralement le savoir-faire d'un expert, de même que l'interprétation de leurs résultats. En revanche, les tests interactifs n'ont que faire de la

taille ou de la complexité d'une application, et sont capables de traiter sans aucune difficulté des applications extrêmement volumineuses.

5. **Retour d'information instantané :** Les outils statiques et dynamiques étant exécutés de manière périodique, des semaines, voire des mois, peuvent s'écouler entre l'erreur et la détection de la vulnérabilité. L'IAST permet un retour d'information instantané, dans les secondes qui suivent le codage et le test du nouveau code. Grâce à l'IAST, les développeurs sont sûrs de ne soumettre que du code « propre ».

6. **Pas besoin d'experts :** Quand vous achetez quelque chose, vous voulez pouvoir l'utiliser aussitôt. Avec les outils interactifs IAST, oubliés les mois de configuration, de réglage et de personnalisation. L'application est testée dès qu'elle est lancée – en continu et automatiquement.

7. **Zéro perturbation des processus :** Pour les entreprises, le délai de mise sur le marché est essentiel. Les stratégies Agile et DevOps permettent de réduire la durée des tests. Puisque l'analyse interactive se superpose en toute transparence aux tests habituels d'assurance qualité ou unitaires, les processus ne sont en rien perturbés. L'IAST s'intègre harmonieusement aux tests de sécurité existants.

L'atout Contrast

L'approche unique en son genre appliquée par Contrast pour garantir la sécurité des applications modernes produit des informations en temps réel et assure une visibilité continue, ce qui permet de détecter et de corriger les vulnérabilités avec 99 % de faux positifs en moins. Misant sur une méthodologie bien connue, l'instrumentation de sécurité profonde, Contrast Assess agit avec discrétion pendant le développement et les tests des applications web ou des API. Cette approche passive élimine le besoin d'analyses de sécurité statiques longues et inefficaces. Par ailleurs, l'évaluation continue des vulnérabilités assurée par Contrast Assess s'intègre parfaitement au cycle de vie du développement logiciel (SDLC). Contrast Assess s'adapte également à l'ensemble du portefeuille d'applications, ce qui le rend idéal pour les environnements Agile, DevOp et DevSecOps.

- L'instrumentation de sécurité utilisée par Contrast Assess produit continuellement des analyses précises.

- La sécurité des applications devient intégrée, les développeurs reçoivent des informations sur lesquelles ils peuvent agir immédiatement.

- Adaptabilité à l'ensemble du portefeuille d'applications.

- Évaluation des vulnérabilités en continu, intégration parfaite au SDLC et aux outils utilisés habituellement.

En outre, Contrast SCA assure une gestion automatisée des risques liés aux composants open source, du développement à la production. Contrast est la seule solution capable d'identifier les composants open source vulnérables, de déterminer comment ils sont réellement utilisés par l'application et d'empêcher leur fonctionnement durant l'exécution, le tout via une plateforme unifiée.

Comment expliquer une telle efficacité ?

Voici 8 grandes raisons expliquant l'efficacité remarquable des outils IAST, Contrast Assess et Contrast SCA :

1. Ils ont été pensés dès le départ pour interagir avec les développeurs lorsqu'ils écrivent et testent les applications web et les API.

2. Ils conjuguent les éléments les plus efficaces des approches IAST, SAST et DAST aux analyses de configuration et de sécurité des logiciels libres, en les intégrant directement aux applications.

3. Ils évaluent la sécurité à mesure des changements de code.

4. Ils embarquent des agents pour surveiller le code et rendent des rapports depuis l'intérieur de l'application.

5. Les failles de sécurité sont automatiquement identifiées, tant durant le développement que tout au long du SDLC.

6. Les développeurs disposent des éléments dont ils ont besoin pour corriger les vulnérabilités, sans nécessiter d'experts en sécurité.

7. Ils produisent des résultats en temps réel pour identifier et corriger les failles de sécurité en amont, quand il est encore facile et peu coûteux d'y remédier.

8. Ils peuvent s'adapter à l'ensemble du portefeuille d'applications.

Caractéristiques principales

Contrast Assess et Contrast SCA sont des solutions de sécurité d'un nouveau type, adaptées aux applications modernes.

- Couverture étendue des vulnérabilités : Contrast assure une couverture étendue des risques de sécurité les plus courants, y compris ceux du Top 10 de l'OWASP.

- Conseils de correctifs au niveau du code : Le traçage innovant de Contrast localise précisément les vulnérabilités du code et leur déploiement. Contrast « parle la langue des développeurs », et fournit des correctifs faciles à comprendre et à mettre en œuvre.

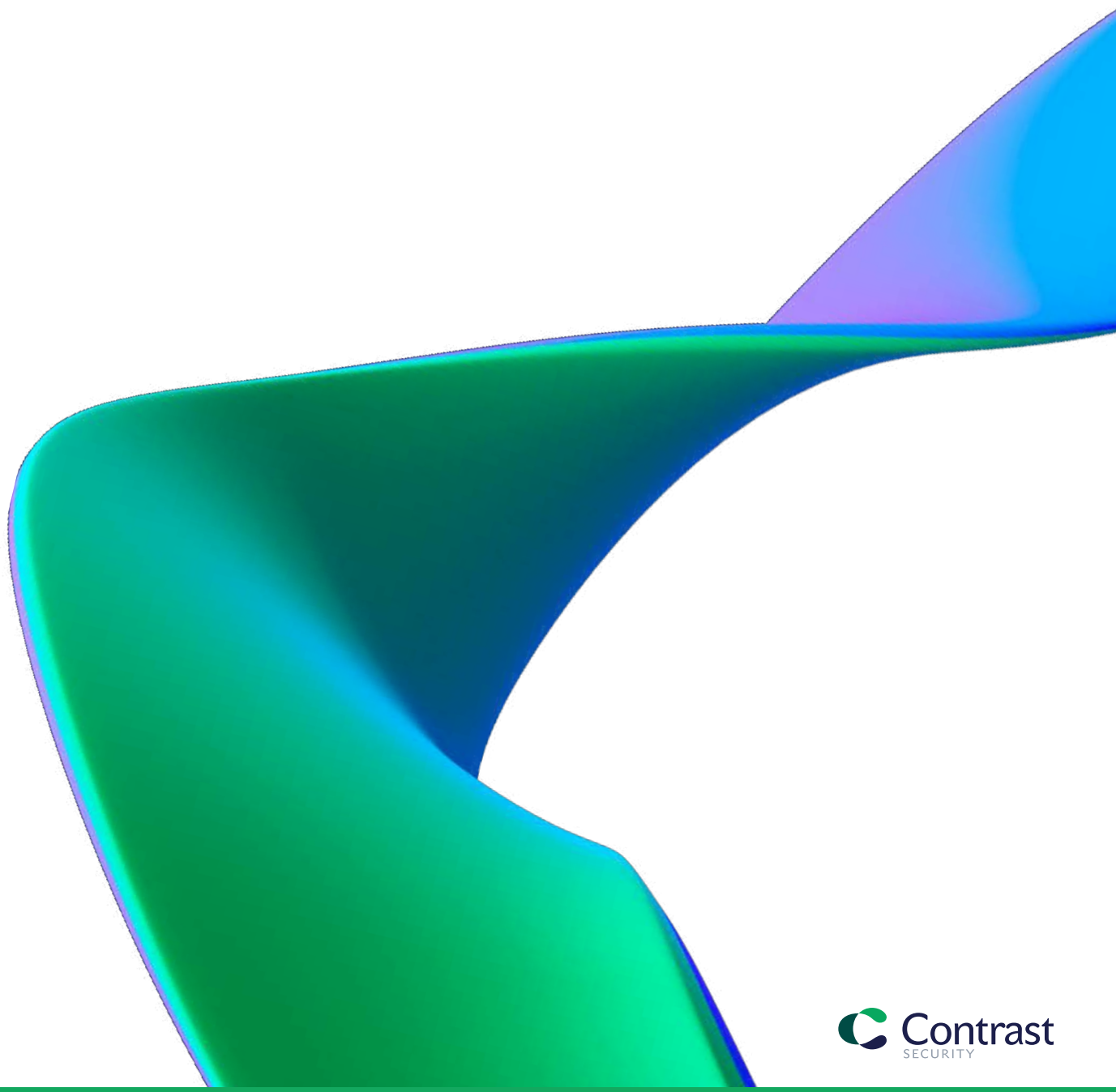
- Analyse des composants open source : Les applications modernes sont comme des icebergs – leur code se cache à 80 % « sous la surface », dans des bibliothèques, des frameworks et d'autres composants. Les applications comportent souvent plus d'une cinquantaine de bibliothèques, soit des millions de lignes de code potentiellement vulnérables.

- Inventaire des applications : Il est impossible de protéger l'invisible. Aujourd'hui, les organisations peuvent posséder des centaines ou des milliers d'applications, de microservices et d'API – sous de multiples versions, car installées au fil du développement et de l'assurance qualité, et en constante évolution. Contrast trace et documente en continu les services web internes et externes et leurs

relations dans une application, pour fournir un inventaire de sécurité unifié et une nomenclature constamment à jour.

- Architecture de l'application en direct : Contraste génère automatiquement des diagrammes simples illustrant les principaux composants de l'architecture de l'application. Ces informations aident le développeur à identifier rapidement la signification d'une vulnérabilité et à prendre des mesures décisives.

Pour toutes ces raisons et bien d'autres encore, Contrast Security vous souhaite la bienvenue dans le monde merveilleux des logiciels autoprotégés - de manière automatisée et en temps réel.



Contrast Security est leader du marché de sécurité des applications grâce à une approche moderne qui intègre l'analyse du code et la prévention des attaques au cœur même des applications. Sa technologie d'instrumentation brevetée Deep Security bouscule totalement les approches traditionnelles par son observabilité intégrée et complète en fournissant une évaluation très précise et en assurant une protection continue du portefeuille d'applications tout entier. Ainsi, plus besoin de disposer d'infrastructures gourmandes en performances et d'experts spécialisés en sécurité. La plateforme de sécurité des applications Contrast accélère les cycles de développement, augmente l'efficacité, réduit les coûts et permet un déploiement rapide tout en protégeant les applications contre les menaces connues et inconnues.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com