ÉVALUATION D'APPLICATION

Les organisations étant bien informées comprennent que leurs applications représentent bien plus qu'un simple service d'informations. Ces applications représentent également l'image de l'entreprise auprès de leurs clients et du public. Si une application est amenée à être désactivée en raison d'une atteinte à la sécurité, cela peut entraîner une perte d'informations, de réputation, de confiance et de revenus. Avoir l'assurance que vos applications puissent dissuader la plupart des menaces vous garantira la continuation de vos services auprès de vos clients et ce, sans perdre de temps, ni d'argent nécessaires pour répondre à un problème de perte ou de disponibilité des données.

LES ÉVALUATIONS D'APPLICATION D'HITACHI SYSTEMS SECURITY SONT CONÇUES POUR:

- **Identifier les vulnérabilités et l'impact potentiel au niveau de l'infrastructure, des applications et des opérations**
- **Vous fournir une vision d'ensemble précise de votre posture de sécurité**
- **Vous fournir des recommandations sur la façon de réduire le risque à des niveaux d'affaires acceptables**
- **Déterminer le niveau de risque commercial réel pour vos auditeurs, vos cadres, votre personnel de sécurité et vos professionnels de l'infrastructure**
- **Vous assurer que vous êtes conforme aux exigences, règlements et normes**

QU'EST-CE QU'UNE L'ÉVALUATION D'UNE APPLICATION?

L'évaluation des applications entreprise par Hitachi Systems Security aide les compagnies à bien comprendre les vulnérabilités de leurs applications, qu'il s'agisse d'un site Web public desservant des clients, d'une interface de fournisseur tiers dans un outil de la gestion de la relation client de l'entreprise ou même d'applications autonomes.

Grâce à une **évaluation des vulnérabilités des applications Web** ou à u**n test d'intrusion des applications**, vous pourrez comprendre la posture de sécurité de votre entreprise. Cette évaluation vous fournira également des recommandations pratiques sur la façon de corriger les vulnérabilités découvertes au sein de votre environnement, notamment les correctifs requis, les modifications de code et les ajustements d'accès.

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, bureau 244, Blainville, QC J7C 5J6 Canada Tél: +1 450-430-8166/ +1 866-430-8166 (sans frais) Fax: +1 450-430-1858
www.hitachi-systems-security.com

ÉLÉMENTS DE SERVICE

Dans le cadre d'une évaluation complète des applications, Hitachi Systems Security Inc.:

- **Définira la portée du projet** – Comprendre l'objectif d'affaires de la ou des applications, de comprendre les menaces potentielles et de définir l'approche de test ainsi que l'environnement à évaluer.
- **Réalisera la collecte de renseignements** – Déterminer ce que l'on sait de l'application(s) ou de la compagnie qui peut être utilisée au cours du test.
- **Cartographiera les applications** – Comprendre les conventions de dénomination, la taille de l'application, le type de technologie utilisée ainsi que le contenu et la structure de l'application.
- **Analysera les applications et déterminera les vulnérabilités** – Saisir les points de contrôle de sécurité, la gestion des sessions utilisateur, les points d'entrée de données et les messages d'erreur.
- **Testera les vulnérabilités techniques** – tester les contrôles d'application, les mécanismes d'authentification, les contrôles d'accès, les faiblesses de l'infrastructure et des applications.
- **Préparera le rapport** – Inclure les vulnérabilités identifiées, classées par ordre de priorité en fonction de leur impact respectif sur votre entreprise. Le rapport comprendra également des recommandations pour la correction desdites vulnérabilités.

LIVRABLES

Une fois l'évaluation complétée, vous recevrez un **rapport détaillé**, comprenant:

- Un sommaire exécutif indiquant les éléments nécessitant une attention immédiate, en mettant l'accent sur l'impact ou le risque d'affaires, plutôt qu'une explication technique détaillée des défauts exacts
- Une section sur l'aspect technique, décrivant les activités ayant été réalisées pour déterminer les vulnérabilités
- Une liste détaillée des vulnérabilités découvertes, répertoriées par ordre de criticité
- Des recommandations pour optimiser la protection des actifs identifiés par les évaluations de vulnérabilité, en tenant compte des coûts résultant de l'opération et l'entretien des investissements de capitaux, du personnel et du temps consacré
- Des annexes reflétant les résultats, les captures d'écran ou autres données d'outils qui permettent de préciser le contexte ou clarifier les vulnérabilités détectées
- Un résumé tactique décrivant les prochaines étapes possibles, y compris un ensemble de solutions temporaires ou à long terme qui pourrait être amené à être intégré à plus grande envergure ou faire l'objet d'une enquête.

RÉSULTATS

- ✓ **Bien comprendre la posture de sécurité de vos applications**
- ✓ **Identifier les failles, les vulnérabilités et les risques auxquels vos applications sont soumises et ce, en fonction de leur niveau de gravité et de leur probabilité d'occurrence**
- ✓ **Mettre en place des activités de correction pour protéger vos applications**
- ✓ **Former votre personnel sur la façon de remédier aux vulnérabilités afin de réduire le risque global**