FIREEYE™

FICHE PRODUIT

Bilan de sécurité et d'architecture cloud

Améliorez vos configurations et architectures cloud pour renforcer vos cyberdéfenses

PRINCIPAUX AVANTAGES

- **Identification** des menaces spécifiques à l'architecture de votre environnement cloud
- **Élimination** des erreurs de configuration généralement exploitées sur les architectures cloud
- **Réduction** de votre exposition aux techniques d'exploitation courantes
- **Meilleure visibilité** sur les principaux risques de sécurité associés aux configurations existantes
- **Amélioration** du suivi, de la visibilité et des capacités de détection dans le cloud
- **Priorisation** des mesures de renforcement de votre environnement cloud

Pourquoi choisir FireEye Mandiant ?
Depuis 2004, FireEye Mandiant agit en première ligne sur le front de la cybersécurité et de la Cyber Threat Intelligence (CTI). Nos experts de la réponse à incident opèrent sur les violations de sécurité les plus complexes et les plus médiatisées qui soient. Ils possèdent une connaissance approfondie des auteurs de menaces établis et émergents dont ils suivent l'évolution constante des modes opératoires.

Présentation
Pour réduire leurs coûts et gagner en évolutivité, les entreprises migrent de plus en plus de leurs ressources vers le cloud. En réponse, les attaquants réalignent leurs tactiques et techniques (ingénierie sociale, exploitation des erreurs de configuration, etc.) pour cibler les environnements cloud.

Le bilan FireEye Mandiant de sécurité et d'architecture cloud évalue l'état actuel de votre sécurité et recommande des mesures de renforcement prioritaires pour les grandes plateformes cloud : Microsoft Azure, Amazon Web Services, Google Cloud Platform, etc.

Ce bilan aide votre entreprise à cerner les menaces spécifiques et déterminer les contrôles de sécurité à mettre en place dans son environnement cloud. Détection, investigation, réponse… vous améliorerez vos capacités d'action à chaque étape du cycle d'une attaque et renforcerez votre sécurité contre les menaces ciblées.

Ces services ont été conçus pour les utilisateurs de solutions IaaS (Infrastructure as a Service) et PaaS (Platform as a Service), deux modèles reposant sur une responsabilité partagée entre le fournisseur de services cloud et le client pour la protection contre les cyber-incidents. Notre bilan met donc l'accent sur la part de responsabilité du client dans la mise en place de mesures de renforcement de sa sécurité.

Notre méthodologie

Le bilan se déroule en quatre étapes au cours desquelles des experts Mandiant cartographient votre environnement cloud existant et évaluent l'efficacité de votre programme de sécurité.

Semaine 1 – Revue initiale de la documentation (stratégies de migration, diagrammes d'architecture, mesures de renforcement, standards et politiques de gestion des accès, playbooks / procédures standard d'exploitation, standards de journalisation, etc.) avec les acteurs concernés côté client.

Semaine 2 – Ateliers sur site visant à explorer votre environnement cloud, le modèle de sécurité en place, ainsi que les mesures et contrôles de sécurité nécessaires pour répondre à vos besoins métiers.

Semaines 3 et 4 – Examen des configurations de la plateforme cloud pour vérifier la présence de contrôles de sécurité adaptés et appliquer les connaissances acquises lors des ateliers pour l'identification des failles exploitables par les attaquants.

Semaine 5 – Génération d'un rapport comportant des recommandations techniques pratiques pour renforcer la sécurité de l'environnement cloud et améliorer la visibilité, les processus et les capacités de détection, avec à la clé une réduction du risque de compromission.

LIVRABLES

Le rapport rédigé par Mandiant en fin de mission comprend :

- Un état des lieux de votre environnement cloud, avec détails de l'architecture et des contrôles de sécurité existants
- Des mesures de sécurité pour des services cloud spécifiques, en phase avec vos configurations et processus opérationnels en place
- Des conseils pratiques pour améliorer la visibilité et les capacités de détection
- Des recommandations détaillées et priorisées pour renforcer la sécurité de votre infrastructure cloud

Des rapports techniques et exécutifs sont disponibles sur demande.

Principaux domaines d'évaluation

Gouvernance, risque et mise en conformité

- Services et gouvernance du cloud
- Standards et politiques cloud
- Évaluation des risques de menace
- Gestion des vulnérabilités
- Exigences de conformité réglementaire

Réseau et architecture de sécurité

- Architecture cloud et contrôles de sécurité
- Segmentation du réseau et intégration des environnements sur site
- Connectivité et gestion des systèmes distants
- Reprise d'activité
- Containers, configurations et contrôles de sécurité

Gestion des identités et des accès

- Infrastructure d'authentification dans le cloud, y compris les connexions à l'environnement sur site (par ex. ADFS)
- Gestion des identités
- Gestion des privilèges d'accès
- Contrôle des accès basé sur les rôles

Protection des données et des secrets commerciaux

- Protection et prévention contre la perte de données
- Sécurité des bases de données
- Gestion des clés et des certificats
- Chiffrement

DevOps

- Configurations des pipelines
- Déploiement des systèmes et des applications
- Cycle de développement logiciel sécurisé
- Contrôles de sécurité sur les référentiels de code

Détection et réponse aux menaces

- Journalisation des systèmes, bases de données et applications
- Centralisation et journalisation de la sécurité
- Contrôles de sécurité sur le réseau et les terminaux
- Processus de réponse aux incidents dans le cloud

Pour en savoir plus, rendez-vous sur **www.fireeye.fr**

FireEye, France
Nextdoor Cœur Défense
110 Esplanade du Général de Gaulle
92931 Paris La Défense Cedex 92974
+33 1 70 61 27 26
france@FireEye.com | www.FireEye.fr
FireEye, Inc.
601 McCarthy Blvd.
Milpitas, CA 95035
+1 408 321 6300 | info@FireEye.com

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Cyber Threat Intelligence (CTI). Prolongement naturel et évolutif des opérations de sécurité des clients, la plate-forme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.

FIREEYE™