KASPERSKY lab

SERVICES KASPERSKY SECURITY INTELLIGENCE. SERVICES D'EXPERTS

www.kaspersky.fr

SERVICES D'EXPERTS

Les services d'experts de Kaspersky Lab sont, comme leur nom l'indique, des services proposés par nos experts internes, qui, pour la plupart, font autorité dans leur domaine au niveau mondial et dont les connaissances et l'expérience jouent un rôle essentiel dans notre réputation de leader mondial en matière de veille stratégique.

Chaque infrastructure informatique est unique et les cybermenaces les plus redoutables sont conçues sur mesure pour exploiter les vulnérabilités spécifiques à chaque organisation, c'est pourquoi nos experts proposent également des services sur mesure. Les services décrits dans les pages suivantes font partie de notre boîte à outils professionnelle. Ils pourront être utilisés, en partie ou en totalité, lors de notre collaboration avec vous.

Notre objectif premier est de travailler avec vous individuellement pour vous fournir des conseils spécialisés afin de vous aider à évaluer vos risques, renforcer votre sécurité et atténuer les effets des futures menaces.

Les services d'experts comprennent les éléments suivants :

- Investigation des incidents
- Tests de pénétration
- Évaluation de la sécurité des applications

INVESTIGATION DES INCIDENTS

Cyberdiagnostic | Analyse des programmes malveillants

Aide personnalisée à l'investigation sur les incidents pour aider votre organisation à identifier et à résoudre les incidents de sécurité.

Les cyberattaques représentent un danger croissant pour les réseaux des entreprises. Conçues spécifiquement pour exploiter les vulnérabilités de la cible choisie par le cybercriminel, ces attaques ont souvent pour but de voler ou de détruire des informations confidentielles ou de propriété intellectuelle, de saper les opérations, d'endommager les installations industrielles ou encore de voler de l'argent.

Il est de plus en plus difficile de protéger une entreprise contre ces attaques bien planifiées et sophistiquées. Il peut même être difficile de déterminer de façon certaine si votre entreprise est victime d'une attaque.

Les services d'investigation des incidents de Kaspersky Lab peuvent aider les entreprises à élaborer des stratégies de défense en fournissant des analyses approfondies des menaces et en offrant des conseils sur les mesures appropriées à mettre en œuvre pour résoudre les incidents.

AVANTAGES DU SERVICE

Les services d'investigation des incidents de Kaspersky Lab vous aident à résoudre les problèmes de sécurité en temps réel et à comprendre les comportements des programmes malveillants ainsi que leurs conséquences, en vous conseillant sur les mesures correctives à mettre en œuvre. Cette approche aide indirectement à :

- réduire les coûts liés à la résolution des problèmes générés par les cyberattaques
- arrêter les fuites d'informations confidentielles susceptibles de découler d'ordinateurs infectés
- réduire les risques liés à la réputation causés par les processus opérationnels affectés par des attaques
- restaurer le fonctionnement normal des ordinateurs endommagés par les attaques

Les investigations de Kaspersky Lab sont menées par des analystes expérimentés disposant d'une expertise pratique dans le cyberdiagnostic et l'analyse de programmes malveillants. À l'issue des investigations, un rapport détaillé vous est remis avec les résultats complets des investigations numériques et des propositions de mesures correctives.

CYBERDIAGNOSTIC

Le cyberdiagnostic est un service d'investigation visant à produire une image détaillée de l'incident. Celle-ci peut comprendre l'analyse de programmes malveillants décrite ci-dessus si un programme malveillant a été découvert au cours de l'investigation. Les experts de Kaspersky Lab rassemblent les éléments de preuve tels que des images HDD, les vidages de mémoire et les traces réseau pour comprendre ce qui se passe exactement. Ils parviennent ainsi à une explication détaillée de l'incident.

En tant que client, vous amorcez le processus en recueillant des éléments de preuve et en fournissant une description de l'incident. Les experts de Kaspersky Lab analysent les symptômes de l'incident, identifient les programmes malveillants binaires (le cas échéant) et analysent les programmes malveillants afin de générer un rapport détaillé préconisant des mesures correctives.

ANALYSE DES PROGRAMMES MALVEILLANTS

L'analyse des programmes malveillants permet de comprendre intégralement le comportement et les objectifs des programmes malveillants spécifiques ciblant votre entreprise.

Les experts de Kaspersky Lab réalisent une analyse approfondie des échantillons de programme malveillant fournis par votre entreprise et produisent un rapport détaillé qui comprend :

- **Propriétés de l'échantillon** : courte description de l'échantillon et diagnostic de classification du programme malveillant
- **Description détaillée des programmes malveillants** : analyse approfondie des fonctionnalités de votre échantillon de programme malveillant ainsi que du comportement et des objectifs de la menace (y compris les IOC), ce qui vous offre les informations requises pour neutraliser ses activités
- **Scénario de mesures correctives** : le rapport proposera des mesures correctives pour protéger pleinement votre entreprise contre ce type de menace

FORMULES DU SERVICE

Les services d'investigation de Kaspersky Lab sont disponibles :

- par abonnement, sur la base d'un nombre d'incidents prédéterminé
- en réaction à un incident unique

SERVICES DE TEST DE PÉNÉTRATION

Toutes les entreprises sont confrontées à la difficulté de protéger entièrement leur infrastructure informatique contre d'éventuelles cyberattaques, mais cette tâche s'avère d'autant plus compliquée pour les grandes entreprises avec plusieurs milliers d'employés, des centaines de systèmes d'information et plusieurs sites dans le monde entier.

Votre équipe informatique et vos spécialistes en sécurité travaillent d'arrache-pied pour s'assurer que toutes les composantes du réseau sont protégées contre les intrusions tout en restant entièrement disponibles pour les utilisateurs légitimes ; cependant, il suffit d'une seule vulnérabilité pour offrir une porte d'entrée à n'importe quel cybercriminel cherchant à contrôler vos systèmes d'information.

Les tests de pénétration servent de démonstration pratique des scénarios d'attaque possibles, où une personne malintentionnée tenterait de contourner les contrôles de sécurité de votre réseau d'entreprise afin d'obtenir des privilèges élevés dans des systèmes importants.

Le service de test de pénétration de Kaspersky Lab vous permet de mieux comprendre les failles de sécurité de votre infrastructure, en révélant les vulnérabilités, en analysant les conséquences possibles des différents types d'attaque, en évaluant l'efficacité de vos mesures de sécurité actuelles et en proposant des améliorations et des mesures correctives.

Les tests de pénétration de Kaspersky Lab vous aident, vous et votre entreprise, à :

- **Identifier les principales vulnérabilités de votre réseau** pour que vous puissiez décider, en toute connaissance de cause, des points sur lesquels vous devez concentrer votre attention et vos investissements afin de réduire les risques à venir.
- **Éviter les dommages financiers, opérationnels et liés à la réputation causés par les cyberattaques,** en les empêchant de se produire grâce à la détection proactive des vulnérabilités et à leur correction.
- **Respecter les normes gouvernementales, industrielles et internes de l'entreprise** qui imposent ce type d'évaluation de sécurité (par exemple dans le cadre de la norme PCI DSS (paiement sécurisé par carte bancaire)).

FORMULES ET ÉTENDUE DES SERVICES

En fonction de vos besoins et de votre infrastructure informatique, vous pouvez faire appel à l'ensemble ou à une partie seulement des services de test de pénétration suivants :

- **Tests de pénétration externe** : évaluation de sécurité effectuée via Internet par un « pirate » n'ayant aucune connaissance préalable de votre système.
- **Tests de pénétration interne** : scénarios basés sur une attaque de l'intérieur, par exemple par un visiteur bénéficiant seulement d'un accès physique à vos bureaux ou par un sous-traitant disposant d'un accès limité aux systèmes.
- **Tests d'ingénierie sociale** : évaluation du niveau de sensibilisation de votre personnel aux questions de sécurité en simulant des attaques d'ingénierie sociale, telles que le hameçonnage, les faux liens malveillants dans les e-mails, les pièces jointes suspectes, etc.
- **Évaluation de la sécurité des réseaux sans fil** : nos experts effectuent une visite de votre site et analysent les contrôles de sécurité wifi.

Vous pouvez appliquer nos tests de pénétration à n'importe quelle partie de votre infrastructure informatique, mais nous vous recommandons fortement de tester l'ensemble du réseau ou ses principales composantes, car les tests donnent toujours des résultats plus probants lorsque nos experts travaillent dans les mêmes conditions qu'un intrus potentiel.

RÉSULTATS DES TESTS DE PÉNÉTRATION

Le service de test de pénétration est conçu pour révéler les failles de sécurité susceptibles d'être exploitées pour accéder sans autorisation aux composantes essentielles d'un réseau. Les failles potentielles concernent notamment les aspects suivants :

- Une architecture réseau vulnérable, une protection insuffisante du réseau
- Des vulnérabilités permettant d'intercepter et de rediriger le trafic du réseau
- Des niveaux d'authentification et d'autorisation insuffisants dans différents services
- Des données d'identification utilisateur à faible sécurité
- Des défauts de configuration, notamment des privilèges excessifs accordés aux utilisateurs
- Des vulnérabilités provenant d'erreurs dans le code d'application (injection de code, traversée de chemin, vulnérabilités côté client, etc.)
- Des vulnérabilités causées par l'utilisation de matériel et de logiciels obsolètes ne bénéficiant pas des dernières mises à jour de sécurité
- La divulgation d'informations

Les résultats sont présentés dans un rapport final, qui comprend des informations techniques détaillées sur le déroulement du test, les résultats, les vulnérabilités révélées et les mesures correctives préconisées, le tout accompagné d'un résumé analytique décrivant les résultats du test et illustrant les vecteurs d'attaque. Sur demande, nous pouvons également fournir des vidéos et des présentations destinées à votre équipe technique ou à la direction.

À PROPOS DE L'APPROCHE ADOPTÉE PAR KASPERSKY LAB POUR LES TESTS DE PÉNÉTRATION

Les tests de pénétration simulent de véritables cyberattaques, mais restent étroitement contrôlés ; ils sont effectués par les experts en sécurité de Kaspersky Lab en préservant entièrement la confidentialité, l'intégrité et la disponibilité de vos systèmes et dans le plus strict respect des normes internationales et des bonnes pratiques, telles que :

- La norme en matière d'exécution des tests de pénétration (PTES)
- Les publications spéciales 800-115 du NIST - Guide technique des tests et des évaluations de la sécurité des informations
- Le Manuel méthodologique des tests de sécurité open source (OSSTMM)
- Le Cadre d'évaluation de la sécurité des systèmes d'information (ISSAF)
- La classification des menaces établie par le consortium WASC (Web Application Security Consortium)
- Le Guide des tests du projet OWASP (Open Web Application Security Project)
- Le système de notation des vulnérabilités CVSS (Common Vulnerability Scoring System)

L'équipe du projet est composée de professionnels expérimentés bénéficiant de connaissances pratiques approfondies et actuelles dans ce domaine ; ce sont des conseillers en sécurité reconnus par les plus grandes entreprises du secteur, dont Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens et SAP.

FORMULES DES SERVICES :

En fonction du type de service d'évaluation de sécurité, des spécificités de vos systèmes et de vos habitudes de travail, nous pouvons procéder à l'évaluation de votre sécurité à distance ou sur place. La plupart des services peuvent être réalisés à distance et les tests de pénétration interne peuvent même être effectués via un réseau VPN, tandis que d'autres, tels que l'évaluation de sécurité des réseaux sans fil, exigent une présence sur place.

SERVICES D'ÉVALUATION DE LA SÉCURITÉ DES APPLICATIONS

Que vous développiez vos applications d'entreprise en interne ou les achetiez à des tiers, vous savez qu'une seule erreur de codage peut créer une vulnérabilité qui vous expose aux attaques et entraîne des dommages financiers considérables tout en portant sérieusement atteinte à votre réputation. De nouvelles vulnérabilités peuvent également apparaître pendant le cycle de vie d'une application, lors de la mise à jour de logiciels, au cours d'une configuration de composants non sécurisée ou encore suite à l'apparition de nouvelles méthodes d'attaque.

Les services d'évaluation de la sécurité des applications de Kaspersky Lab permettent d'identifier les vulnérabilités de toutes sortes d'applications : vastes solutions reposant sur le Cloud, systèmes ERP, services bancaires en ligne et autres applications professionnelles spécialisées ou encore applications mobiles et embarquées sur différentes plates-formes (iOS, Android et autres).

Grâce à leurs connaissances pratiques et à leur expérience en matière de bonnes pratiques internationales, nos experts détectent les failles de sécurité pouvant exposer votre organisation à différentes menaces, dont :

- le détournement de données confidentielles
- l'infiltration et la modification de données et de systèmes
- le lancement d'attaques par déni de service
- l'implication dans des activités frauduleuses

En suivant nos recommandations, vous pouvez corriger les vulnérabilités identifiées dans les applications et empêcher ainsi ces attaques.

AVANTAGES DU SERVICE

Les services d'évaluation de la sécurité des applications de Kaspersky Lab aident les propriétaires et les développeurs d'applications à :

- **Éviter les dommages financiers, opérationnels et liés à la réputation**, en détectant et corrigeant de manière proactive les vulnérabilités exploitées dans les attaques contre les applications.
- **Réduire les coûts des mesures correctives** en repérant les vulnérabilités des applications encore au stade de développement et de test, avant leur entrée dans l'environnement utilisateur, où leur correction peut entraîner des perturbations et des frais considérables.
- **Favoriser un cycle de développement de systèmes sécurisé** (S-SDLC) permettant de créer et de maintenir des applications fiables.
- **Se conformer aux normes gouvernementales, industrielles et internes de l'entreprise** en matière de sécurité des applications, telles que les normes PCI DSS ou HIPAA.

FORMULES ET ÉTENDUE DES SERVICES

Parmi les applications pouvant être évaluées figurent les sites Internet officiels et les applications métiers, classiques ou basées sur le Cloud, y compris les applications mobiles et embarquées.

Adaptés à vos besoins et aux spécificités des applications, les services peuvent comprendre :

- **Le test de la boîte noire** : simule une attaque externe
- **Le test de la boîte grise** : simule l'attaque par des utilisateurs légitimes présentant différents profils
- **Le test de la boîte blanche** : procède à une analyse avec un accès complet à l'application, y compris aux codes source ; cette approche est la plus efficace pour révéler de nombreuses vulnérabilités
- **L'évaluation de l'efficacité du pare-feu d'application** : les applications sont testées avec le pare-feu activé et désactivé de façon à repérer des vulnérabilités et à vérifier si les failles éventuelles sont bloquées

RÉSULTATS

Vulnérabilités pouvant être identifiées par les services d'évaluation de la sécurité des applications de Kaspersky Lab :

- Failles dans l'authentification et l'autorisation, y compris l'authentification multi-facteurs
- Injection de code (injection SQL, OS Command, etc.)
- Vulnérabilités logiques à l'origine de fraudes
- Vulnérabilités côté client (script intersite, falsification de requête intersite, etc.)
- Utilisation d'une cryptographie insuffisante
- Vulnérabilités dans les communications client-serveur
- Transfert ou stockage de données non sécurisées, par exemple avec un masquage insuffisant du numéro de compte principal dans les systèmes de paiement
- Défauts de configuration, y compris ceux à l'origine d'attaques de gestion de session
- Divulgation d'informations sensibles
- Autres vulnérabilités d'applications Web les exposant aux menaces énumérées dans la classification des menaces v2.0 du WASC et dans la liste des 10 menaces les plus importantes d'après l'OWASP

Les résultats sont présentés dans un rapport final, qui inclut des informations techniques détaillées sur le déroulement du test, les résultats, les vulnérabilités révélées et les mesures correctives préconisées, le tout accompagné d'un résumé analytique expliquant les implications en matière de gestion. Sur demande, nous pouvons également fournir des vidéos et des présentations destinées à votre équipe technique ou à la direction.

À PROPOS DE L'APPROCHE DE L'ÉVALUATION DE LA SÉCURITÉ DES APPLICATIONS DE KASPERSKY LAB

La sécurité des applications est évaluée par les experts en sécurité de Kaspersky Lab aussi bien manuellement qu'avec des outils automatisés dans le respect le plus total de la confidentialité, de l'intégrité et de la disponibilité de vos systèmes et conformément aux normes internationales et aux bonnes pratiques, telles que :

- La classification des menaces établie par le consortium WASC (Web Application Security Consortium)
- Le Guide des tests du projet OWASP (Open Web Application Security Project)
- Le Guide de tests de la sécurité mobile d'OWASP
- D'autres normes, en fonction du secteur d'activité et de la localisation de votre entreprise

L'équipe du projet est composée de professionnels expérimentés bénéficiant de connaissances pratiques actuelles et approfondies dans le domaine, notamment concernant différentes plates-formes, langages de programmation, infrastructures, vulnérabilités et méthodes d'attaque. Ils interviennent dans les plus grandes conférences internationales et sont consultés pour des questions de sécurité par les principaux fournisseurs d'applications et de services Cloud, tels qu'Oracle, Google, Facebook, Apple et PayPal.

FORMULES DES SERVICES :

En fonction du type de service d'évaluation de sécurité, des spécificités des systèmes concernés et de vos exigences en matière de conditions de travail, nous pouvons fournir nos services d'évaluation de sécurité à distance ou sur place. La plupart de ces services peuvent être réalisés à distance.

KASPERSKY lab