KASPERSKY lab

SERVICES DE VEILLE STRATEGIQUE DE KASPERSKY LAB

Aujourd'hui, la cybercriminalité ne connaît pas de frontière et les capacités techniques sur lesquelles elle s'appuie évoluent rapidement : nous assistons à des attaques qui sont de plus en plus sophistiquées. Notre mission est de sauver le monde de tous les types de cyber-menaces. Pour atteindre cet objectif et rendre l'utilisation d'Internet sûre et sécurisée, il est essentiel de partager en temps réel les informations sur les menaces. L'accès rapide à l'information est un élément essentiel de la protection efficace des données et des réseaux.

Eugene Kaspersky
Président et PDG de Kaspersky Lab

INTRODUCTION

De nouvelles cyber-menaces apparaissent tous les jours, prenant des formes différentes et empruntant des vecteurs d'attaque variés.

Il n'existe pas de solution unique qui offre une protection complète. Toutefois, même dans notre monde de big data, savoir où détecter le danger est un élément essentiel de la lutte contre les nouvelles menaces.

En tant que dirigeant d'entreprise, il est de votre responsabilité de protéger votre société contre les menaces d'aujourd'hui et d'anticiper les dangers auxquels elle pourrait être confrontée dans les années à venir. Ceci implique davantage qu'une simple protection opérationnelle intelligente contre les menaces connues ; ceci exige en effet un niveau de veille stratégique en matière de sécurité que très peu d'entreprises ont les ressources de développer en interne.

Chez Kaspersky Lab, nous comprenons qu'il faut établir des relations durables pour assurer la prospérité d'une entreprise sur le long terme.

Kaspersky Lab est un partenaire commercial précieux et toujours disponible pour partager les informations les plus récentes avec votre équipe via différents canaux. Notre large gamme de prestations permet à votre centre de sécurité (Security Operation Center, SOC) d'avoir tous les moyens à disposition pour protéger votre entreprise contre toute menace en ligne.

Même si votre entreprise n'utilise pas les produits Kaspersky Lab, vous pouvez tout de même bénéficier de nos services de veille stratégique.

UNE SÉCURITÉ QUI FAIT TOUTE LA DIFFÉRENCE

La veille en matière de sécurité fait partie intégrante de notre ADN. Elle nous permet de vous proposer le dispositif de protection contre les programmes malveillants le plus puissant du marché et influence tout ce que nous faisons.

Nous sommes, à tous les niveaux, une entreprise axée sur la technologie**, à commencer par notre PDG, Eugène Kaspersky.**

Notre équipe d'analyse et de recherche mondiale (GReAT, Global Research & Analysis Team), composée d'experts en sécurité informatique de haut niveau, a ouvert la voie en détectant de nombreuses menaces de programmes malveillants et d'attaques ciblées parmi les plus dangereuses au monde.

De nombreux organismes de sécurité et d'agences chargées de l'application de la loi parmi les plus respectés au monde, dont Interpol, Europol, CERT ou encore la City of London Police, ont fait appel à nos services**.**

Kaspersky Lab développe et perfectionne toutes ses technologies en interne, ce qui rend ses produits et services de veille naturellement plus fiables et efficaces.

Les sociétés d'analyse les plus respectées du secteur, dont Gartner, Forrester Research et International Data Corporation (IDC), nous considèrent comme un leader dans de nombreux domaines clés de la sécurité informatique.

Plus de 130 fabricants OEM, parmi lesquels Microsoft, Cisco, Blue Coat, Juniper Networks, Alcatel Lucent, intègrent nos technologies dans leurs propres produits et services.

FORMATION À LA CYBER-SÉCURITÉ

Kaspersky Lab vous fait bénéficier de son expérience, de ses connaissances et de son savoir-faire en matière de cyber-sécurité grâce à ces programmes de formation innovants.

La sensibilisation et la formation à la cyber-sécurité sont devenues des impératifs pour les entreprises confrontées à un volume croissant de menaces en constante évolution. Les employés chargés de la sécurité doivent bien maîtriser les techniques de sécurité avancées, qui constituent l'un des éléments clés d'une stratégie efficace de gestion et de réduction des menaces en entreprise. Par ailleurs, tous les employés doivent être sensibilisés aux dangers et aux méthodes de travail sécurisées.

Les formations à la cyber-sécurité de Kaspersky Lab ont été spécialement développées pour les entreprises souhaitant protéger plus efficacement leurs infrastructures et leur propriété intellectuelle.

LES COURS

SENSIBILISATION À LA CYBER SECURITE	FORMATION À LA SÉCURITÉ INFORMATIQUE	
Employés	Niveau 1 - débutant	
PLATEFORME DE FORMATION EN LIGNE	PRINCIPES DE BASE DE LA SÉCURITÉ Connaissances informatiques de base	SENSIBILISATION A LA CYBER-SECURITÉ AVEC APPLICATIONS PRATIQUES Connaissances informatiques de base
Responsables opérationnels	Niveau 2 - intermédiaire	
SERIOUS GAME DE SENSIBILISATION À LA CYBER-SÉCURITÉ	CYBER-DIAGNOSTIC Compétences d'administrateur système requises	ANALYSE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING Compétences en programmation requises
Directeurs administratifs	Niveau 3 - avancé	
ÉVALUATION DU NIVEAU DE CONNAISSANCES EN SECURITE INFORMATIQUE	CYBER-DIAGNOSTIC AVANCÉ Compétences avancées d'administrateur système requises	ANALYSE AVANCÉE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING Compétences d'assembleur requises

SENSIBILISATION À LA CYBER-SÉCURITÉ

Modules de formation interactive en ligne et formation à la cyber-sécurité sous forme de jeu sur site pour tous les employés qui utilisent ou gèrent des ordinateurs ou des appareils mobiles au travail.

Environ 80 % des incidents informatiques sont provoqués par des erreurs humaines. Les entreprises dépensent des millions en programmes de sensibilisation à la cyber-sécurité, mais rares sont les RSSI vraiment satisfaits des résultats. Quel est le problème ?

La plupart des formations de sensibilisation à la cyber-sécurité sont trop longues, trop techniques et foncièrement négatives. Elles n'exploitent pas les principaux points forts des participants, à savoir leurs capacités en termes de prise de décision d'apprentissage, ce qui les rend parfois inefficaces.

C'est pourquoi les entreprises cherchent des approches comportementales plus élaborées (par exemple le développement de la culture d'entreprise), qui offrent un retour sur investissement à la fois mesurable et efficace en matière de sensibilisation à la sécurité.

Les cours de sensibilisation à la cyber-sécurité de Kaspersky Lab reposent sur les points suivants :

- Le changement de comportement, en encourageant les personnes à faire des efforts pour travailler de manière sûre et en créant au sein de l'entreprise une ambiance où « tout le monde se préoccupe de la cyber-sécurité, donc moi aussi ».
- La combinaison d'une approche qui repose sur la motivation avec des techniques d'apprentissage ludiques, des simulations d'attaques et une formation interactive approfondie aux techniques de cyber-sécurité.

COMMENT ÇA MARCHE

Une approche complète mais simple	Grâce à une série d'exercices simples, la formation couvre un large éventail de questions de sécurité, de l'origine des fuites de données aux attaques de programmes malveillants sur Internet, en passant par l'utilisation sécurisée des réseaux sociaux. Nous utilisons des techniques pédagogiques telles que la dynamique de groupe, des modules interactifs, des bandes dessinées et l'apprentissage par le jeu pour rendre le processus d'apprentissage intéressant.
Une motivation soutenue	Nous créons des moments propices à l'enseignement à travers l'apprentissage ludique et des compétitions, puis nous renforçons ces périodes de formation tout au long de l'année par des exercices de simulation d'attaque en ligne, des sessions d'évaluation et des campagnes de formation.
Tordre le cou aux idées reçues	Nous expliquons que ce sont des êtres humains, et non des machines, qui sont les principales cibles des cyber-criminels. Nous montrons comment, en étant plus vigilants dans son travail, il est possible d'éviter d'exposer son lieu de travail à ces attaques et d'en devenir victime personnellement.
Développer dans l'entreprise une culture de la cyber-sécurité	Nous formons les dirigeants à devenir des ambassadeurs de la sécurité ; il est impossible d'instaurer une culture où la cyber-sécurité est une préoccupation naturelle en l'imposant simplement par voie informatique, mais cela devient bien plus facile lorsque la direction s'implique et montre l'exemple.
Une attitude positive et coopérative	Nous démontrons dans quelle mesure les pratiques de sécurité contribuent à améliorer l'efficacité de l'entreprise et encourageons une coopération plus efficace avec d'autres services internes, dont l'équipe de sécurité informatique.
Une approche quantifiable	Nous fournissons des outils pour mesurer les compétences des employés et évaluons l'ensemble de l'entreprise à partir d'une analyse de l'attitude du personnel face à la cyber-sécurité dans le travail au quotidien.

FORMATION DU PERSONNEL INFORMATIQUE A LA SECURITE

Ces cours couvrent un large éventail de thèmes et de techniques de cyber-sécurité et proposent des certifications allant du niveau débutant au niveau expert. Tous les cours sont dispensés soit dans les bureaux locaux ou régionaux de Kaspersky Lab, soit dans ceux de l'entreprise du client, en fonction des possibilités.

Les cours regroupent des enseignements théoriques et des ateliers pratiques. À l'issue de chaque cours, les participants sont invités à passer un examen de validation des connaissances.

DÉBUTANT, INTERMÉDIAIRE OU EXPERT ?

Le programme porte sur de nombreux sujets, des principes de sécurité de base au cyber-diagnostic avancé en passant par l'analyse des programmes malveillants. Il permet aux entreprises d'approfondir leurs connaissances en matière de cyber-sécurité dans trois domaines principaux :

- Connaissances fondamentales du sujet
- Investigations numériques et réaction aux incidents
- Analyse avancée des programmes malveillants et reverse engineering

AVANTAGES DU SERVICE

Atouts de la formation du personnel à la cyber-sécurité :

NIVEAU 1 – Principes de base de la sécurité
Permettre aux administrateurs et aux responsables de la sécurité et de l'informatique de comprendre, de façon élémentaire, les dernières mesures pratiques en matière de sécurité informatique avec l'aide d'un leader du secteur.

NIVEAU 1 - Principes pratiques de base en matière de sécurité
Parvenir à une compréhension approfondie de la sécurité grâce à des exercices pratiques faisant appel à des outils de sécurité modernes.

NIVEAUX 2-3 – Cyber-diagnostic
Améliorer l'expertise de votre équipe interne en matière de cyber-diagnostic et de réaction aux incidents.

NIVEAUX 2-3 – Analyse des programmes malveillants et reverse engineering
Améliorer l'expertise de votre équipe interne en matière d'analyse des programmes malveillants et de reverse engineering.

EXPÉRIENCE CONCRÈTE

Au cours de ces formations, nos experts partagent leur propre expérience de la détection et de la prévention de la cyber-criminalité à son plus haut niveau.

DESCRIPTION DU PROGRAMME

SUJETS	Durée	Compétences acquises
NIVEAU 1 - PRINCIPES DE BASE DE LA SÉCURITÉ		
• Aperçu des cyber-menaces et des marchés souterrains • Spam et phishing, sécurité du courrier électronique • Technologies de protection contre la fraude • Exploitation des failles, menaces persistantes avancées et mobiles • Notions de cyber-diagnostic de base à l'aide d'outils publics basés sur le Web • Sécurisation de votre lieu de travail	2 jours	• Reconnaître les incidents de sécurité et prendre des mesures pour les résoudre • Réduire la charge qui pèse sur les services de sécurité de l'information • Augmenter le niveau de sécurité sur chaque lieu de travail avec des outils supplémentaires • Effectuer des enquêtes simples • Analyser les e-mails de phishing • Reconnaître les sites Internet infectés ou factices

SUJETS	Durée	Compétences acquises
NIVEAU 1 – SENSIBILISATION A LA CYBER-SECURITÉ AVEC APPLICATIONS PRATIQUES		
• Notions de base de la sécurité • Renseignement open-source • Sécurité du réseau d'entreprise • Sécurité des applications et prévention de l'exploitation des failles • Attaques par déni de service distribué et menaces bancaires • Sécurité du réseau LAN sans fil et réseau mobile mondial • Menaces bancaires et mobiles • Réaction aux incidents de sécurité touchant les environnements cloud et virtuels	5 jours	• Effectuer des enquêtes sommaires à l'aide des ressources publiques, des moteurs de recherche spécialisés et des réseaux sociaux • Créer un périmètre réseau sécurisé • Acquérir des compétences de base en matière de tests de pénétration • Surveiller le trafic pour détecter différents types d'attaques • Assurer le développement de logiciels sécurisés • Repérer l'injection de codes malveillants • Procéder au cyber-diagnostic et à l'analyse élémentaire des programmes malveillants
NIVEAU 2 : PRINCIPES GÉNÉRAUX DU CYBER-DIAGNOSTIC		
• Introduction au cyber-diagnostic • Réaction en temps réel et obtention de preuves • Contenu du registre Windows • Analyse des artefacts Windows • Analyse des navigateurs • Analyse des e-mails	5 jours	• Mettre en place un laboratoire de cyber-diagnostic • Recueillir les preuves numériques et les traiter correctement • Reconstruire un incident et utiliser les données d'horodatage. • Détecter des traces d'intrusion grâce aux artefacts dans le système d'exploitation Windows • Trouver et analyser l'historique du navigateur et des e-mails • Être capable d'appliquer les instruments et les outils de cyber-diagnostic
NIVEAU 2 : ANALYSE GÉNÉRALE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING		
• Objectifs et techniques de l'analyse des programmes malveillants et reverse engineering • Système Windows interne, fichiers exécutables, assembleur x86 • Techniques de base d'analyse statique (extraction de données, analyse des importations, aperçu des points d'entrée PE, extraction automatique, etc.) • Techniques de base d'analyse dynamique (débogage, outils de surveillance, interception du trafic, etc.) • Analyse des fichiers .NET, Visual Basic, Win64 • Techniques d'analyse des scripts et non-PE (fichiers batch ; Autoit ; Python ; Jscript ; JavaScript ; VBS)	5 jours	• Construire un environnement sécurisé pour l'analyse des programmes malveillants : déployer sandbox et tous les outils nécessaires • Comprendre les principes d'exécution des programmes Windows • Effectuer l'extraction des objets malveillants, les déboguer et les analyser, identifier leurs fonctions • Détecter les sites malveillants à travers l'analyse des scripts de programmes malveillants • Réaliser une analyse express des programmes malveillants
NIVEAU 3 : CYBER-DIAGNOSTIC AVANCÉ		
• Investigations approfondies dans Windows • Récupération des données • Investigations sur le réseau et le cloud • Investigations sur la mémoire • Analyse chronologique • Exercices d'investigation des attaques ciblées dans le monde réel	5 jours	• Être capable d'effectuer une analyse approfondie du système de fichiers • Être capable de récupérer les fichiers supprimés • Être capable d'analyser le trafic réseau • Détecter des activités malveillantes à partir de vidages de mémoire • Reconstruire la chronologie de l'incident
NIVEAU 3 : ANALYSE AVANCÉE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING		
• Objectifs et techniques de l'analyse des programmes malveillants et reverse engineering • Techniques avancées d'analyse statique et dynamique (extraction manuelle) • Techniques de déobfuscation • Analyse rootkit et bootkit • Analyse des vulnérabilités (.pdf, .doc, .swf, etc.) • Analyse des programmes malveillants hors Windows (Android, Linux, Mac OS)	5 jours	• Mettre en œuvre les meilleures pratiques de reverse engineering du monde • Reconnaître les techniques d'anti-reverse engineering (obfuscation, anti-débogage) • Appliquer des techniques d'analyse avancées des programmes malveillants pour les rootkits/bootkits • Analyser les shellcodes intégrés dans différents types de fichier • Analyser les programmes malveillants hors Windows

SERVICES DE SURVEILLANCE DES MENACES

Le suivi, l'analyse, l'interprétation et la lutte contre les menaces informatiques, en perpétuelle évolution, représentent un travail considérable. Dans tous les secteurs, les entreprises manquent de données actualisées et pertinentes pour gérer les risques liés aux menaces informatiques.

Les services de surveillance des menaces de sécurité de Kaspersky Lab vous donnent accès aux informations nécessaires pour atténuer ces risques, fournies par notre équipe de chercheurs et d'analystes.

Les connaissances et l'expérience approfondies de Kaspersky Lab dans tous les domaines de la cyber-sécurité en font le partenaire de choix des plus grandes autorités de police et administrations au monde, comme INTERPOL et les grands organismes CERT. Votre entreprise peut tirer parti dès aujourd'hui de ces renseignements.

Les services de surveillance des menaces de Kaspersky Lab comprennent les éléments suivants :

- Les flux d'informations sur les menaces
- Le repérage des menaces Botnet
- Les rapports de surveillance des menaces persistantes avancées (APT)

FLUX D'INFORMATION SUR LES MENACES

Renforcez vos outils de défense du réseau, notamment les systèmes SIEM, les pare-feu, les IPS/IDS, les technologies anti-APT et de sandbox/simulation, grâce à des données complètes constamment mises à jour, qui vous offrent un aperçu des cyber-menaces et des attaques ciblées.

Au cours des dernières années, le nombre de familles et de variantes de programmes malveillants a explosé. Chaque jour, Kaspersky Lab détecte environ 325 000 échantillons de programmes malveillants distincts. Pour protéger leurs terminaux contre ces menaces, la plupart des entreprises déploient des mesures de protection classiques, telles que des solutions de lutte contre les programmes malveillants ou des systèmes de prévention des intrusions et de détection des menaces. Dans un environnement en évolution rapide où la cyber-sécurité tente constamment de garder une longueur d'avance sur la cyber-criminalité, ces solutions traditionnelles doivent être renforcées par une veille stratégique sur les menaces mise à jour à la minute près.

Les sources de données sur les menaces de Kaspersky Lab sont conçues pour s'intégrer dans les systèmes de gestion des événements et des informations de sécurité (SIEM) existants pour fournir un niveau de protection supplémentaire. L'intégration de flux d'information sur les menaces permet, par exemple, de corréler les journaux générés par les systèmes SIEM provenant de différents appareils du réseau avec les flux URL provenant de Kaspersky Lab. Une connexion aux systèmes SIEM HP ArcSight est comprise. Des connecteurs pour Splunk et QRadar sont également disponibles.

CAS D'UTILISATION / AVANTAGES DU SERVICE

Les flux d'information sur les menaces de Kaspersky Lab :

- renforcent votre solution SIEM en exploitant les données sur les URL dangereuses. Le système SIEM reçoit une notification de la présence de programmes malveillants, d'URL de phishing et de C&C botnet de la part des journaux qui lui sont envoyés par différents appareils du réseau (ordinateurs des utilisateurs, proxies réseau, pare-feu, autres serveurs).
- renforcent les principales solutions de défense du réseau, telles que les pare-feu, les IPS/IDS, les solutions SIEM, les anti-APT, les technologies de simulation/sandbox, les appliances UTM, etc., grâce à des informations sur les menaces actualisées en permanence.
- améliorent vos capacités de diagnostic en fournissant aux équipes de sécurité des informations utiles sur les menaces et un aperçu de la logique qui sous-tend les attaques ciblées.
- soutiennent vos projets de recherche. Les informations sur les URL dangereuses et les hashes MD5 de fichiers malveillants apportent un soutien précieux aux projets de recherche des menaces.

Kaspersky Lab propose trois types de flux d'informations sur les menaces :

1. URL et masques malveillants
2. Hashes MD5 de base de données d'objets malveillants
3. Flux d'informations sur les menaces mobiles

DESCRIPTION DU FLUX

URL malveillantes – ensemble d'URL couvrant les liens et sites Web dangereux. Des enregistrements avec ou sans masque sont disponibles.
URL de phishing : ensemble d'URL identifiées par Kaspersky Lab comme renvoyant vers des sites de phishing. Des enregistrements avec ou sans masque sont disponibles.
URL C&C Botnet – ensemble d'URL de serveurs de commande et de contrôle (C&C) de botnets et d'objets malveillants connexes.
Hashes de programmes malveillants (ITW) – ensemble de hashes de fichiers et de diagnostics correspondants couvrant les programmes malveillants les plus répandus et les plus dangereux, issus de la surveillance effectuée par KSN.
Hashes de programmes malveillants (système de détection d'urgence) – ensemble de hashes de fichiers détectés par les technologies cloud de Kaspersky Lab via les métadonnées de fichier et les statistiques (sans détenir l'objet lui-même). Cela permet d'identifier les objets malveillants nouveaux et émergents (zero-day) qui ne sont pas détectés par d'autres méthodes.
Hashes de programmes malveillants mobiles – ensemble de hashes de fichiers permettant de détecter les objets malveillants qui infectent les plates-formes mobiles.
Flux d'information sur le cheval de Troie P-SMS – ensemble de hashes de cheval de Troie avec le contexte correspondant permettant de détecter les chevaux de Troie SMS qui génèrent des frais d'appel de numéros surtaxés sur un mobile et permettent à l'agresseur de voler, de supprimer et de répondre à des SMS.
URL C&C Botnet mobiles – ensemble d'URL avec contexte couvrant les serveurs C&C botnet mobiles.

SUIVI D'ACTIVITÉ DES BOTNETS

Services professionnels de suivi et de notification pour identifier les botnets qui menacent vos clients et votre réputation

De nombreuses attaques réseaux sont lancées à l'aide de botnets. Ces attaques peuvent cibler des internautes particuliers, mais elles visent le plus souvent des entreprises spécifiques et leurs clients.

La solution de Kaspersky Lab surveille l'activité des botnets et donne rapidement (en 20 minutes) une notification des menaces associées à des utilisateurs de systèmes bancaires et de paiement en ligne particuliers. Vous pouvez utiliser ces notifications pour alerter votre clientèle, vos fournisseurs de services de sécurité et les autorités locales des menaces en cours. Protégez sans attendre la réputation de votre entreprise et vos clients avec le service de suivi d'activité des botnets de Kaspersky Lab.

CAS D'UTILISATION / AVANTAGES DU SERVICE

- Des alertes proactives sur les menaces venant de botnets qui ciblent vos utilisateurs en ligne vous permettent d'avoir toujours une longueur d'avance sur les attaques
- L'identification d'une liste d'URL des serveurs Command & Control de botnet ciblant vos utilisateurs en ligne vous permet de les bloquer en envoyant des demandes à des CERT ou aux organismes de maintien de l'ordre
- Amélioration de la sécurité en matière d'opérations bancaires et de paiement en ligne grâce à la compréhension de la nature de l'attaque
- Formation de vos utilisateurs en ligne pour les aider à reconnaître et à éviter les pièges d'ingénierie sociale utilisés pour les attaques

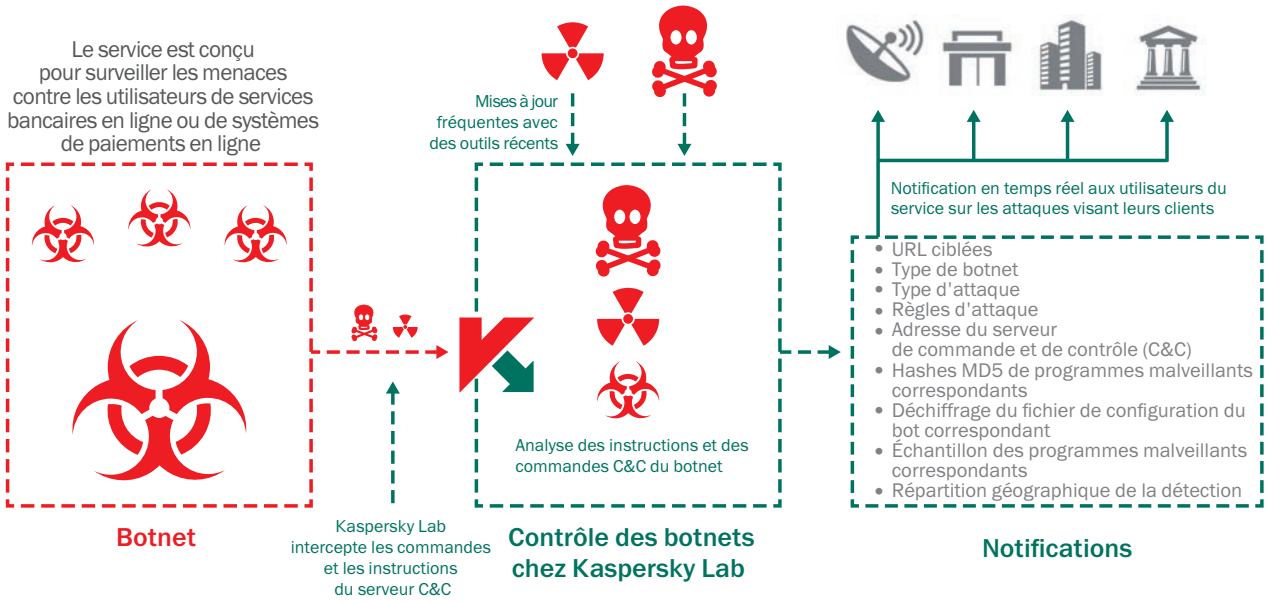
AGISSEZ EN TEMPS RÉEL :

Le service fournit un abonnement à des notifications personnalisées contenant des informations sur des marques et des mots-clés précis dans les botnets surveillés par Kaspersky Lab. Les notifications se font par e-mail ou RSS, soit au format HTML, soit au format JSON, et incluent les éléments suivants :

- **URL ciblée(s) :** les bots malveillants sont conçus pour attendre que l'utilisateur accède aux URL de l'entreprise ciblée pour démarrer l'attaque.
- **Type de botnet** : identifiez précisément le programme malveillant utilisé par le cyber-criminel pour attaquer les transactions de vos clients. Exemples : Zeus, SpyEye et Citadel.
- **Type d'attaque** : déterminez l'objectif des cyber-criminels à l'origine du programme malveillant, par exemple l'injection de données Web, les effacements d'écran, la capture de vidéos ou le transfert d'URL de phishing.
- **Règles d'attaque :** identifiez les règles d'injection de code utilisées, par exemple des requêtes HTML (GET / POST) et les données de page Web avant et après injection.
- **Adresse du serveur de commande et de contrôle (C&C)** : vous permet d'avertir le fournisseur de services Internet du serveur à l'origine de l'attaque, afin de supprimer la menace plus rapidement.
- **Hash des programmes malveillants connexes** : Kaspersky Lab fournit la somme de hash utilisée pour la vérification des programmes malveillants.
- Fichier de configuration déchiffré du bot connexe **: identifie la liste complète des URL ciblées.**
- Échantillon des programmes malveillants connexes **: pour effectuer un reverse engineering approfondi et un cyber-diagnostic de l'attaque.**
- **Répartition géographique de la détection (10 pays principaux)** : données statistiques sur des échantillons de programmes malveillants connexes issus du monde entier.

SUIVI D'ACTIVITÉ DES BOTNETS : ARCHITECTURE

DEPUIS LE SERVEUR C&C



La solution de Kaspersky Lab est proposée en formule standard ou premium pour offrir différentes conditions de services et URL surveillées. Renseignez-vous auprès de Kaspersky Lab ou de votre partenaire revendeur pour déterminer la bonne solution pour votre entreprise.

NIVEAUX D'ABONNEMENT ET CONTENUS

Premium

Notification par e-mail ou au format JSON — **10 URL surveillées**

- Déchiffrage du fichier de configuration du bot correspondant
- Échantillon du programme malveillant correspondant (sur demande)
- Répartition géographique des détections d'échantillons de programmes malveillants

Standard

Notification par e-mail — **5 URL surveillées**

- Ciblage de l'URL (identification de l'URL où le programme de bot cible les utilisateurs)
- Type de botnet (par ex., Zeus, SpyEye, Citadel, Kins, etc.)
- Type d'attaque
- Règles de l'attaque, y compris : injection de données ; capture de vidéo, d'écran, d'URL, etc.
- Adresse C&C
- Hashes MD5 de programmes malveillants correspondants

RAPPORTS DE VEILLE

Soyez plus conscients et mieux informés des attaques de cyber-espionnage de haut vol grâce aux rapports pratiques et complets fournis par Kaspersky Lab.

Grâce aux informations et aux outils fournis dans ces rapports, vous pouvez réagir rapidement face aux nouvelles menaces et vulnérabilités en bloquant les attaques qui passent par des vecteurs connus, en réduisant les dommages causés par les attaques évoluées ainsi qu'en améliorant votre stratégie de sécurité ou celle de vos clients.

Rapports de surveillance des menaces APT

Toutes les menaces persistantes avancées ne sont pas signalées dès leur découverte, et nombre d'entre elles ne sont jamais révélées publiquement. Soyez le premier et le seul à en être informé grâce à nos rapports détaillés de surveillance des menaces APT.

En tant qu'abonné aux rapports de surveillance des menaces APT de Kaspersky Lab, vous avez la possibilité d'accéder à tout moment à nos propres enquêtes et découvertes, y compris à toutes les données techniques disponibles dans une variété de formats sur chaque menace APT telle qu'elle a été découverte, ainsi que sur toutes les menaces qui ne seront jamais rendues publiques.

Nos experts, qui comptent parmi les chasseurs de menaces APT les plus compétents et les plus efficaces du secteur, vous alerteront également immédiatement s'ils constatent une modification dans les stratégies des groupes de cyber-criminels et de cyber-terroristes. De plus, vous aurez accès à tous les rapports des bases de données de menaces APT de Kaspersky Lab, un autre outil de recherche et d'analyse puissant venant compléter l'arsenal de sécurité de votre entreprise.

LES RAPPORTS DE SURVEILLANCE DES MENACES APT DE KASPERSKY LAB COMPRENNENT :

- **Un accès exclusif aux** descriptions techniques des menaces les plus redoutables au cours de l'enquête, avant la publication des résultats.
- **Des informations sur les menaces APT non annoncées publiquement**. Parmi les menaces les plus graves, toutes ne sont pas révélées publiquement. En raison de l'identité des victimes, de la sensibilité des données, de la nature des opérations de correction des vulnérabilités ou des activités de maintien de l'ordre associées, certaines de ces menaces APT ne sont jamais rendues publiques. Néanmoins, toutes sont signalées à nos clients.
- **Une documentation** technique détaillée, des échantillons et des outils, avec notamment une liste complète d'indicateurs de compromission (IOC), disponibles dans des formats standard tels qu'openIOC ou STIX, sans compter l'accès à nos règles Yara.
- **Une surveillance continue des campagnes de menaces APT**. Accès aux informations exploitables au cours de l'enquête (information sur la distribution des menaces APT, les indicateurs IOC, l'infrastructure C&C).
- **Une analyse rétrospective**. Accès garanti à tous les rapports privés précédents durant toute la période de votre abonnement.

RAPPORTS DE VEILLE

Rapports de veille sur les menaces spécifiques au client

Quel est le meilleur moyen d'organiser une campagne d'APT contre votre entreprise ? De quels canaux et informations dispose un pirate qui vous choisirait spécifiquement pour cible ? Une attaque a-t-elle déjà été organisée ou une menace imminente pèse-t-elle sur vous ?

Les rapports de veille sur les menaces spécifiques pour un client en particulier proposés par Kaspersky Lab répondent à toutes ces questions et à d'autres encore grâce au travail de nos experts. Ils permettent un aperçu complet de votre situation actuelle en termes de sécurité, identifient les failles susceptibles d'être exploitées et découvrent les preuves d'attaques passées, actuelles et prévues.

Fort de cette vision d'ensemble unique, vous pouvez concentrer votre stratégie de protection contre les menaces APT sur les points identifiés comme étant des cibles privilégiées pour les cyber-criminels, en prenant des mesures rapides et précises pour repousser les intrus et minimiser le risque qu'une attaque aboutisse.

En s'appuyant sur des méthodes allant du renseignement de sources ouvertes (OSINT) aux systèmes et bases de données spécialisés de Kaspersky Lab, ainsi que sur nos connaissances des réseaux cyber-criminels souterrains, ces rapports couvrent des domaines tels que :

- **L'identification des vecteurs de menace** – Identification et analyse de l'état de toutes les composantes essentielles de votre réseau, y compris des distributeurs automatiques, de la vidéosurveillance et d'autres systèmes utilisant les technologies mobiles, ainsi que des profils de réseaux sociaux et des comptes de messagerie professionnels des employés, qui seraient susceptibles de devenir les cibles potentielles d'une attaque.
- **L'analyse du suivi des activités des logiciels malveillants et des cyber-attaques** – Identification, surveillance et analyse de tous les échantillons, actifs et inactifs, de logiciels malveillants visant votre entreprise, de toutes les activités présentes ou passées des botnets, ainsi que de toutes les activités suspectes liées au réseau.
- **Attaques par des tiers** : preuves de menaces et d'activités des botnets ciblant spécifiquement vos clients, partenaires et abonnés, dont les systèmes infectés pourraient ensuite être utilisés pour vous attaquer.
- **Fuites d'informations** : grâce à la surveillance clandestine de communautés en ligne et de forums souterrains, nous repérons d'éventuelles discussions entre pirates planifiant une attaque contre vous ou, par exemple, des situations dans lesquelles un employé malhonnête vend des informations.
- **Statut d'attaque actuel** : si nous découvrons qu'une attaque APT est actuellement dirigée contre votre infrastructure (et ce type d'attaque peut durer plusieurs années), nous recommandons des mesures correctives efficaces.

DÉMARRAGE RAPIDE - FACILE À UTILISER - AUCUNE RESSOURCE NÉCESSAIRE.

Une fois établis les paramètres (pour les rapports spécifiques au client) et les formats de données à privilégier, aucune autre infrastructure n'est requise pour commencer à utiliser le service de Kaspersky Lab. Les rapports sont transmis sous la forme d'e-mails cryptés.

Les rapports de veille sur les menaces de Kaspersky Lab n'affectent pas l'intégrité et la disponibilité de vos ressources, y compris celles du réseau.

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 cyber-menaces 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 :

- L'investigation sur les incidents
- Les tests de pénétration
- L'évaluation de la sécurité des applications

INVESTIGATION SUR LES INCIDENTS

Cyber-diagnostic | 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 cyber-attaques représentent un danger croissant pour les réseaux des entreprises. Conçues spécifiquement pour exploiter les vulnérabilités de la cible choisie par le cyber-criminel, ces attaques ont souvent pour but de voler ou de détruire des informations confidentielles ou la 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 sur les 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 sur les 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 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 cyber-attaques
- 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 cyber-diagnostic 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.

CYBER-DIAGNOSTIC

Le cyber-diagnostic 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 DU PROGRAMME MALVEILLANT

L'analyse du programme malveillant 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 du programme malveillant fournis par votre entreprise et produisent un rapport détaillé qui comprend :

- **Les propriétés de l'échantillon** : courte description de l'échantillon et diagnostic de classification du programme malveillant
- **Une description détaillée du programme malveillant** : analyse approfondie des fonctionnalités de votre échantillon de programme malveillant ainsi que du comportement et des objectifs de la menace (y compris les indicateurs IOC), vous offrant les informations requises pour neutraliser ses activités
- **Un scénario de mesures correctives** : le rapport proposera des mesures correctives pour protéger pleinement votre entreprise contre ce type de menace

FORMULES PROPRES AUX SERVICES

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 cyber-attaques, 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'accès à n'importe quel cyber-criminel cherchant à contrôler vos systèmes d'information.

Les tests de pénétration servent de démonstration pratique des scénarios d'attaque possibles, où une personne mal intentionnée 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 cyber-attaques,** 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 « expert » 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 phishing, 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
- Communication des 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 cyber-attaques, 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 de 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 de 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 internes 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 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 proactivement 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 exploitations d'éventuelles failles 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 sécurisés, 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 de 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 en matière des 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.


Twitter.com/
Twitter.com/
kasperskyfrance


Facebook.com/
Facebook.com/
kasperskylabfrance


Youtube.com/
Youtube.com/user/
KasperskyFrance

Kaspersky Lab, Moscou, Russie
www.kaspersky.fr

Tout savoir sur la sécurité
sur Internet :
www.viruslist.com/fr

Trouver un partenaire près de chez vous :
http://www.kaspersky.fr/partners/
buyoffline/liste-des-partenaires

Si vous désirez en savoir plus sur les produits et services décrits dans ce catalogue ou bien discuter avec nous pour savoir comment utiliser ces services dans le but d'améliorer la sécurité de votre entreprise, veuillez nous contacter par e-mail à l'adresse Intelligence@kaspersky.com

Veuillez noter que les conditions applicables peuvent varier d'une région à l'autre, notamment, mais sans s'y limiter, en fonction de l'étendue du travail, des échéanciers, de la disponibilité des services au niveau local, de la langue de prestation des services et des coûts.

Catalogue des services de veille stratégique en matière de sécurité, août 2015 GL