SERVICES DE VEILLE STRATÉGIQUE 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 cybermenaces. 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.

Eugène Kaspersky
Président et PDG de Kaspersky Lab

INTRODUCTION

Chaque jour, de nouvelles cybermenaces apparaissent sous des formes différentes et à travers une grande variété de vecteurs d'attaque.

Il n'existe aucune solution unique capable d'offrir une protection complète. Toutefois, même dans notre univers dominé aujourd'hui par l'échange de données volumineuses, il est essentiel de savoir d'où le danger peut provenir pour lutter efficacement contre les nouvelles menaces.

En tant que gérant 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 la nécessité d'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 éventail de services permet à votre centre de sécurité (Security Operation Center, SOC) et/ou votre équipe de sécurité informatique 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 toujours bénéficier de nos services de veille stratégique.

UNE SÉCURITÉ QUI FAIT TOUTE LA DIFFÉRENCE

Nous disposons de l'un des meilleurs services de veille en matière de sécurité monde. Il fait partie intégrante de notre ADN, il nous permet de nous aide à 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'analystes et de chercheurs au niveau mondial (GReAT, Global Research & Analysis Team), composée d'experts de sécurité informatique de haut niveau, a ouvert la voie en détectant de nombreux programmes malveillants et attaques ciblées parmi les plus dangereuses au monde.

De nombreux organismes de sécurité et agences chargées de l'application de la loi parmi les plus respectés au monde, dont Interpol, Europol, des 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.

PROGRAMME DE FORMATION À LA CYBERSÉCURITÉ

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

La sensibilisation et la formation à la cybersécurité 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.

Le programme de formation à la cybersécurité de Kaspersky Lab a été spécialement développé pour les entreprises souhaitant protéger plus efficacement leurs infrastructures et leur propriété intellectuelle. Tous les cours sont proposés en anglais (les cours de sensibilisation à la cybersécurité sont disponibles dans plus de 10 langues (dont le français).

LES COURS

	SENSIBILISATION DES EMPLOYÉS NON SPÉCIALISTES DE L'INFORMATIQUE	FORMATION À LA SÉCURITÉ INFORMATIQUE	
Employés	PLATE-FORME DE FORMATION DÉDIÉE AUX EMPLOYÉS Compétences en matière de cyberhygiène	Débutant	PRINCIPES DE BASE DE LA SÉCURITÉ Formation en ligne sur les connaissances informatiques de base
			SENSIBILISATION À LA CYBERSÉCURITÉ AVEC APPLICATIONS PRATIQUES Connaissances informatiques de base
Responsables opérationnels	SERIOUS GAME DE SENSIBILISATION À LA CYBERSÉCURITÉ	Intermédiaire	CYBERDIAGNOSTIC Compétences d'administrateur système requises
			ANALYSE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING Compétences en programmation requises
Cadres supérieurs et responsables de la sécurité des systèmes d'information (RSSI)	KASPERSKY INTERACTIVE PROTECTION (KIPS) Stratégie et assistance aux entreprises	Avancé	CYBERDIAGNOSTIC AVANCÉ Compétences avancées d'administrateur système requises
			ANALYSE AVANCÉE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING Compétences d'assembleur requises
Directeurs administratifs	ÉVALUATION DU NIVEAU DE CONNAISSANCE EN SÉCURITÉ INFORMATIQUE	Responsables de la réponse aux incidents et analystes en sécurité	RÉPONSE AUX INCIDENTS ET RÈGLES YARA

SENSIBILISATION À LA CYBERSÉCURITÉ

Programmes de formation interactive permettant d'instaurer un cyberenvironnement sûr au sein d'une entreprise. En combinant une approche ludique à une expertise approfondie en cybersécurité, les produits Kaspersky Security Awareness apportent savoir-faire et motivation aux employés non spécialisés en informatique.

Plus de 80 % des cyberincidents sont dus à des erreurs humaines. Les entreprises perdent des millions pour se remettre d'incidents provoqués par le personnel, mais l'efficacité des programmes de formation traditionnels visant à prévenir ces problèmes est limitée et, bien souvent, ils ne réussissent pas à susciter la motivation et le comportement escompté.

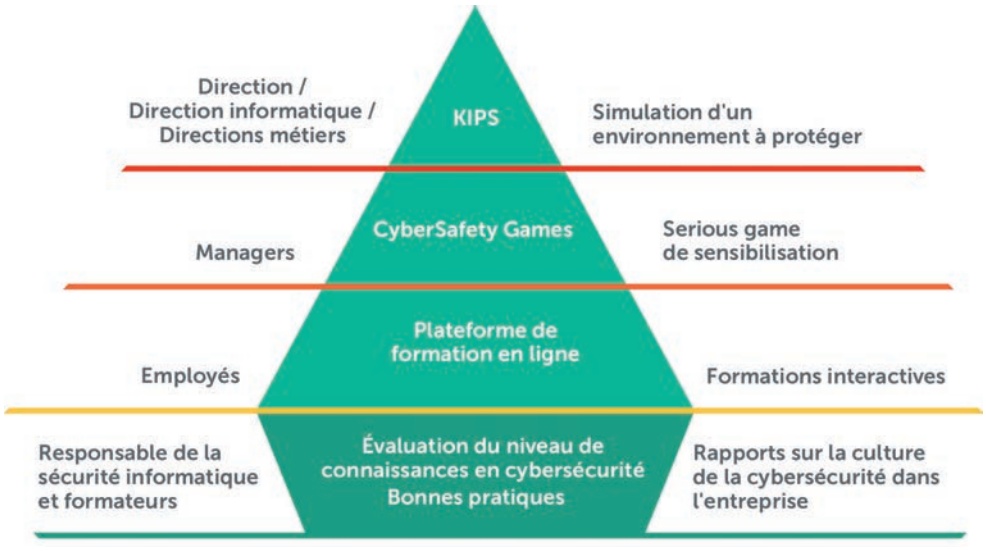
Kaspersky Lab a lancé une gamme de produits de formation sur ordinateur qui s'appuient sur des techniques d'apprentissage modernes et conviennent à tous les niveaux de la structure de l'entreprise. Notre programme de formation a déjà prouvé son efficacité, à la fois auprès de nos clients et de nos partenaires Kaspersky Lab dans la mesure où il :

- **Permet de développer un comportement et ne se limite pas à transmettre des connaissances** : la méthode d'apprentissage inclut le jeu, l'apprentissage par la pratique, la dynamique de groupe, la simulation d'attaques, des parcours pédagogiques, etc. De ce fait, les habitudes comportementales sont renforcées et les améliorations en termes de cybersécurité sont durables.
- **Instaure une culture de la cybersécurité** : « tout le monde se préoccupe de la cybersécurité, donc moi aussi ». Tous partagent des valeurs, des habitudes et des attitudes qui contribuent à maintenir un certain niveau de sécurité.
- **Porte ses fruits** : jusqu'à 90 % d'incidents en moins, risque financier associé aux cybermenaces réduit de 50-60 %, jusqu'à 93 % de chances de voir les employés utiliser leurs connaissances au quotidien.

COMMENT ÇA MARCHE

La formation aborde un large éventail de questions de sécurité : fuite de données, ransomware, attaques de programmes malveillants sur Internet, utilisation sécurisée des réseaux sociaux et sécurité des appareils mobiles.

La méthodologie d'apprentissage continu permet de renforcer les compétences de manière constante et de susciter la motivation au sein de l'entreprise.



Le fait d'adapter les formations aux différents niveaux et fonctions de l'entreprise favorise une culture de la cybersécurité collaborative, partagée par tous et pilotée par la direction.

La formation inclut des outils de reporting et d'analyse qui évaluent les compétences et la progression de l'apprentissage des employés, ainsi que l'efficacité des programmes au niveau de l'entreprise.

FORMATION DES PROFESSIONNELS DE LA SÉCURITÉ

Ces cours couvrent un large éventail de thèmes et de techniques de cybersécurité et proposent des certifications allant du niveau débutant au niveau expert. Tous les cours sont dispensés soit dans les bureaux 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 formation, 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 base de la sécurité au cyberdiagnostic avancé en passant par l'analyse des programmes malveillants. Il permet aux entreprises d'approfondir leurs connaissances en matière de cybersécurité dans trois domaines principaux :

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

AVANTAGES DU SERVICE

Principes de base de la sécurité
Permettre 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.

Cyberdiagnostic
Améliorer l'expertise de votre équipe interne en matière de cyberdiagnostic et de réponse aux incidents.

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.

Réponse aux incidents
Améliorer l'expertise de votre équipe interne en matière de réponse aux incidents.

Formation Yara
Améliorer l'expertise de votre équipe de réponse aux incidents pour qu'elle soit en mesure d'identifier des menaces jusque-là indétectables.

EXPÉRIENCE CONCRÈTE

Travaillez et apprenez aux côtés de nos experts mondiaux qui inspirent les participants en partageant leur propre expérience de la détection et de la prévention de la cybercriminalité à son plus haut niveau.

DESCRIPTION DU PROGRAMME

SUJETS	Durée	Compétences acquises
PRINCIPES DE BASE DE LA SÉCURITÉ		
• Aperçu des cybermenaces et des marchés souterrains • Spam et phishing, sécurité du courrier électronique • Technologies de protection contre la fraude • Failles, menaces persistantes avancées et mobiles • Notions de cyberdiagnostic de base à l'aide d'outils publics basés sur le Web • Sécurisation de votre lieu de travail	En ligne	• 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
PRINCIPES GÉNÉRAUX DU CYBERDIAGNOSTIC		
• Introduction au cyberdiagnostic • 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 cyberdiagnostic • 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 cyberdiagnostic
ANALYSE GÉNÉRALE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING		
• Objectifs et techniques de l'analyse des programmes malveillants et du 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 une 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
CYBERDIAGNOSTIC AVANCÉ		
• Investigations approfondies dans Windows • Récupération des données • Investigations sur le réseau et dans 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
ANALYSE AVANCÉE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING		
• Objectifs et techniques de l'analyse des programmes malveillants et du reverse engineering • Techniques avancées d'analyse statique (analyse statique de shellcodes, analyse d'en-tête PE, TEB, PEB, chargement de fonctions par différents algorithmes de hachage) • Techniques avancées d'analyse dynamique (structure PE, extraction manuelle et avancée, extraction d'outils de compression malveillants qui stockent le fichier exécutable sous forme chiffrée) • Reverse engineering d'APT (couvre un scénario d'attaque APT, des e-mails de phishing aux cas les plus complexes) • Analyse des protocoles (analyse des protocoles de communication chiffrés C2, décryptage du trafic) • Analyse des rootkits et des bootkits (débogage de secteur de démarrage en utilisant Ida et VMWare, débogage de noyau en utilisant 2 machines virtuelles, analyse des échantillons de rootkit)	5 jours	• Être en mesure de suivre les bonnes pratiques de reverse engineering tout en reconnaissant les techniques d'anti-reverse engineering (obfuscation, anti-débogage) • Être en mesure d'appliquer une analyse avancée des programmes malveillants pour décortiquer les rootkits/ bootkits • Être en mesure d'analyser les shellcodes intégrés dans les différents types de fichiers et les programmes malveillants ciblant des systèmes autres que Windows
RÉPONSE AUX INCIDENTS		
• Introduction à la réponse aux incidents • Détection et analyse préliminaire • Cyberdiagnostic • Élaboration de règles de détection (Yara, Snort, Bro)	5 jours	• Distinguer les menaces persistantes avancées (APT) des autres types de menaces • Comprendre les techniques des différents cybercriminels et la structure des attaques ciblées • Appliquer des méthodes de surveillance et de détection spécifiques • Suivre le processus de réponse aux incidents • Reconstruire l'historique et la logique des incidents • Élaborer des règles de détection et des rapports
FORMATION YARA		
• Brève introduction sur la syntaxe des règles Yara • Conseils et astuces pour élaborer des règles courtes mais efficaces • Rédacteurs des règles Yara • Recherche de faux positifs au moyen de tests des règles Yara • Recherche de nouveaux échantillons non encore détectés sur VT • Utilisation de modules dans Yara pour une recherche efficace • Recherche d'anomalies • Multiples exemples concrets • Exercices pour améliorer vos compétences Yara	2 jours	• Élaborer des règles Yara efficaces • Tester les règles Yara • Faire en sorte que votre équipe soit capable d'identifier des menaces jusque-là indétectables

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 Kaspersky Lab vous donnent accès aux informations nécessaires pour atténuer ces risques. Ils sont fournis par notre équipe de chercheurs et d'analystes de niveau mondial.

Les connaissances et l'expérience approfondies de Kaspersky Lab dans tous les domaines de la cybersécurité 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 :

- Informations sur les menaces interprétables par une machine
- Suivi d'activité des botnets
- Rapports de veille stratégique
- Rapports personnalisés
- Kaspersky Threat Lookup
- Kaspersky Managed Protection

INFORMATIONS SUR LES MENACES INTERPRÉTABLES PAR UNE MACHINE

Renforcez vos outils de défense du réseau, notamment les systèmes SIEM, les pare-feux, 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 cybermenaces 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 cybersécurité tente constamment de garder une longueur d'avance sur la cybercriminalité, ces solutions traditionnelles doivent être renforcées par une veille stratégique sur les menaces mise à jour à la minute près.

Les informations sur les menaces interprétables par une machine de Kaspersky Lab combinent des flux d'informations sur les menaces et des outils intégrables aux plate-formes SIEM les plus répandues dans le monde (y compris IBM QRadar, HP ArcSight et Splunk). Cette combinaison offre aux entreprises un tout nouvel aperçu du paysage des menaces, et fournit aux centres de supervision de la sécurité les indicateurs de compromission nécessaires pour identifier et bloquer le plus rapidement possible une multitude de cyberattaques.

CAS D'UTILISATION/AVANTAGES DU SERVICE

Les flux d'informations 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 de 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 (SHA1 et SHA256) de fichiers malveillants apportent un soutien précieux aux projets de recherche des menaces.

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

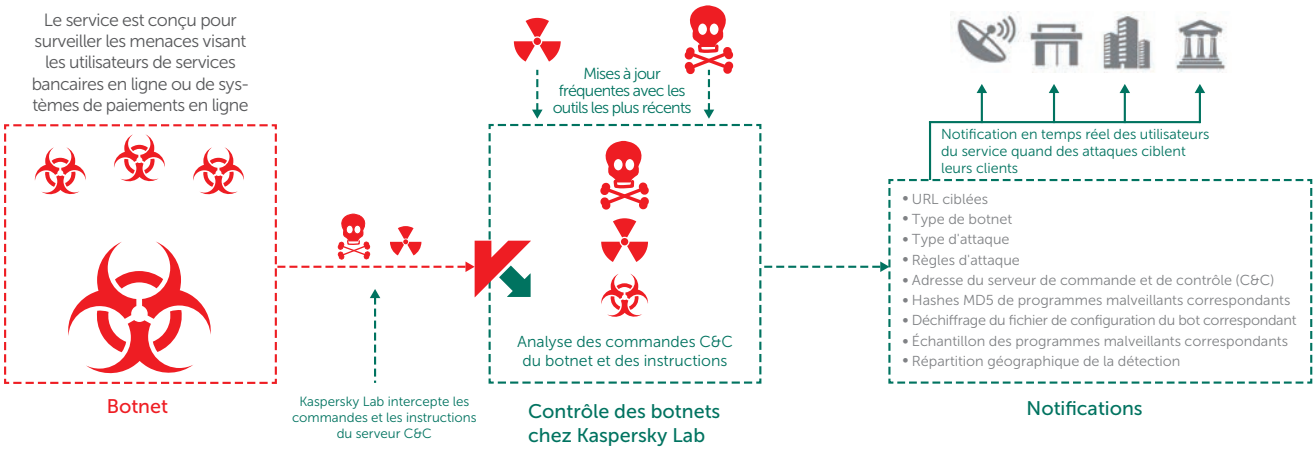
1. URL et masques malveillants
2. Hashes MD5 (SHA1 et SHA256) de base de données d'objets malveillants
3. Flux d'informations sur les menaces mobiles
4. Hashes MD5 (SHA1 et SHA256) de base de données d'objets authentiques
5. Adresses IP malveillantes

DESCRIPTION DU FLUX

Informations sur la réputation des adresses IP : un ensemble d'adresses IP avec des données sur les hôtes suspects et malveillants.
URL malveillantes : ensemble d'URL couvrant les liens et sites Web dangereux. Des enregistrements masqués et non masqués sont disponibles.
URL de phishing : ensemble d'URL identifiées par Kaspersky Lab comme renvoyant vers des sites de phishing. Des enregistrements masqués et non masqués sont disponibles.
URL C&C de botnet : ensemble d'URL de serveurs de commande et de contrôle (C&C) de botnets et d'objets malveillants connexes.
Sources de hashes malveillants : couvrant les nouveaux programmes malveillants les plus répandus et les plus dangereux.
Hashes de programmes malveillants mobiles : ensemble de hashes de fichiers permettant de détecter les objets malveillants qui infectent les plates-formes mobiles.
Flux d'informations sur le cheval de Troie P-SMS : ensemble de hashes de chevaux 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 de botnet mobiles : ensemble d'URL avec contexte couvrant les serveurs C&C de botnet mobiles.
Flux d'informations de listes blanches : ensemble de hashes de fichiers fournissant des connaissances détaillées des logiciels authentiques.

SUIVI D'ACTIVITÉ DES BOTNETS

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



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 aux 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 À L'AIDE DE CONTENUS EN TEMPS RÉEL :

Le service fournit un abonnement à des notifications personnalisées contenant des informations sur les marques correspondantes en suivant les mots-clés dans les botnets surveillés par Kaspersky Lab. Les notifications peuvent être livrées 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 cybercriminel pour atteindre vos clients. Exemples : Zeus, SpyEye et Citadel.
- **Type d'attaque** : déterminez l'objectif des cybercriminels 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.
- **Hashes MD5 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 cyberdiagnostic de l'attaque.
- **Répartition géographique de la détection (10 principaux pays)** : données statistiques sur des échantillons de programmes malveillants connexes issus du monde entier.

ÉLÉMENTS LIVRABLES

Notification par e-mail ou au format JSON

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

Notification par e-mail

- 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 STRATÉGIQUE

Soyez plus conscient et mieux informé des attaques de cyberespionnage les plus sophistiquées grâce aux rapports pratiques et complets fournis par Kaspersky Lab.

Grâce aux informations et aux outils fournis dans ces rapports, vous pouvez réagir rapidement 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 APT

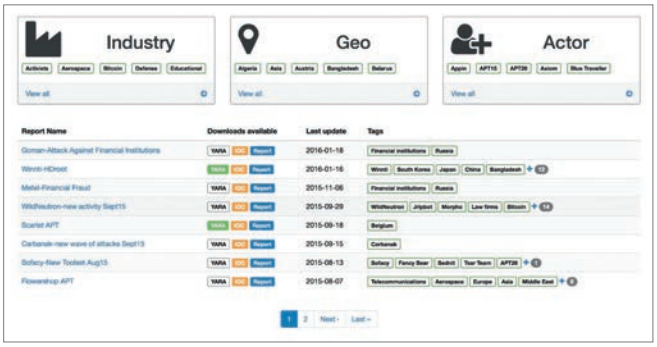
Toutes les APT ne sont pas signalées dès leur découverte, et nombre d'entre elles ne sont jamais révélées publiquement. Soyez le premier et le seul à en être informé grâce à nos rapports de surveillance des APT détaillés et exploitables.

En tant qu'abonné aux rapports de surveillance des 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 différents formats sur chaque 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 d'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 cybercriminels et de cyberterroristes. De plus, vous aurez accès à tous les rapports des bases de données d'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 APT DE KASPERSKY LAB PROPOSENT :

- **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 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 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 standards tels qu'openIOC ou STIX, sans compter l'accès à nos règles Yara.
- **Une surveillance continue des campagnes APT**. Accès aux informations exploitables au cours de l'enquête (information sur la distribution des 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.
- **Portail de surveillance des APT**. Ce portail, qui permet de consulter l'ensemble des rapports (y compris les tout derniers rapports sur les indicateurs IOC), offre à nos clients une expérience utilisateur transparente.



REMARQUE – RESTRICTION APPLIQUÉE AUX ABONNÉS

En raison du caractère sensible et spécifique de certaines informations contenues dans les rapports fournis par ce service, nous sommes tenus de limiter les abonnements aux organisations gouvernementales, publiques et privées de confiance.

RAPPORTS PERSONNALISÉS SUR LES MENACES

Rapports sur les menaces spécifiques au client

Quel est le meilleur moyen d'organiser une attaque 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 sur les menaces spécifiques au client proposés par Kaspersky Lab répondent à toutes ces questions et à d'autres encore grâce au travail de nos experts. Ils offrent 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 sur les points identifiés comme étant des cibles privilégiées pour les cybercriminels, en prenant des mesures rapides et précises pour repousser les intrus et minimiser le risque qu'une attaque aboutisse.

Développés à l'aide de l'outil de renseignement de sources ouvertes (OSINT), d'une analyse profonde des systèmes et bases de données spécialisés de Kaspersky Lab et de nos connaissances des réseaux souterrains de cybercriminels, ces rapports abordent les domaines suivants :

- **L'identification des vecteurs de menaces :** 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 personnels des employés, qui seraient susceptibles de devenir les cibles potentielles d'une attaque.
- **L'analyse du suivi des activités des programmes malveillants et des cyberattaques** : identification, surveillance et analyse de tous les échantillons, actifs et inactifs, des programmes malveillants visant votre entreprise, de toutes les activités présentes ou passées des botnets, ainsi que de toutes les activités suspectes liées au réseau.
- **Les 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.
- **Les fuites d'informations** : grâce à la surveillance discrète de communautés et de forums en ligne 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.
- **La situation actuelle en matière de sécurité** : les attaques d'APT peuvent rester inaperçues pendant de nombreuses années. Si nous détectons une attaque qui affecte votre infrastructure, nous vous donnons des conseils vous permettant de prendre des mesures correctives efficaces.

DÉMARRAGE RAPIDE - FACILE À UTILISER - AUCUNE RESSOURCE NÉCESSAIRE

Une fois les paramètres (pour les rapports spécifiques au client) et les formats de données personnalisés établis, aucune infrastructure supplémentaire n'est nécessaire pour commencer à utiliser ce service Kaspersky Lab.

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

Rapports sur les menaces spécifiques à un pays

La cybersécurité d'un pays comprend la protection de l'ensemble de ses institutions et organisations principales. Les APT visant les autorités gouvernementales peuvent affecter la sécurité nationale ; d'éventuelles cyberattaques contre les industries, le transport, les télécommunications, les banques et d'autres secteurs essentiels peuvent provoquer des dommages importants au niveau national, comme des pertes financières, des accidents de production, le blocage des communications réseau et le mécontentement de la population.

En cas d'attaques de programmes malveillants et de pirates informatiques ciblant votre pays, disposer d'une vue d'ensemble sur les surfaces d'attaque et les tendances actuelles vous permet de concentrer votre stratégie de défense sur des zones ayant été identifiées comme les cibles principales des cybercriminels, ce qui vous donne la possibilité d'agir rapidement et avec précision pour repousser les intrus et minimiser le risque de succès de ces attaques.

En s'orientant vers des approches allant du renseignement issu de sources ouvertes (OSINT) à l'analyse approfondie des systèmes et bases de données spécialisés de Kaspersky Lab, ainsi que sur nos connaissances des réseaux cybercriminels souterrains, les rapports sur les menaces spécifiques pour chaque pays couvrent des domaines tels que :

- **L'identification des vecteurs de menaces** : identification et analyse de l'état des ressources informatiques essentielles du pays disponibles en externe, y compris les applications gouvernementales vulnérables, les équipements de télécommunications, les composants des systèmes de contrôle industriel (SCADA, PLC, etc.), les distributeurs automatiques, etc.
- **L'analyse du suivi des activités des programmes malveillants et des cyberattaques** : identification et analyse des campagnes d'APT, des échantillons, actifs et inactifs, des programmes malveillants, de toutes les activités présentes ou passées des botnets et d'autres menaces importantes ciblant votre pays, en nous basant sur les données disponibles de nos propres ressources de surveillance interne.
- **Les 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 certaines entreprises. Nous découvrons également des comptes compromettants importants, qui pourraient représenter des risques pour les organisations et les institutions visées (par exemple, les comptes appartenant aux employés des agences gouvernementales disponibles dans l'attaque contre Ashley Madison, qui pourraient être utilisés à des fins de chantage).

Les rapports de veille sur les menaces de Kaspersky Lab n'affectent pas l'intégrité et la disponibilité des ressources du réseau inspectées. Le service repose sur des méthodes de reconnaissance de réseau non intrusives et sur l'analyse des informations disponibles en open sources et dans les ressources dont l'accès est limité.

À la conclusion du service, vous recevrez un rapport contenant la description des menaces importantes pour les différentes industries et institutions d'État, ainsi que des informations supplémentaires sur les résultats détaillés de l'analyse technique. Les rapports sont transmis sous la forme d'e-mails cryptés.

Le service peut être fourni de manière ponctuelle ou périodique, dans le cadre d'un abonnement (trimestriel, par exemple).

COMMENT BÉNÉFICIER DU SERVICE DE RAPPORTS SUR LES MENACES SPÉCIFIQUES À UN PAYS

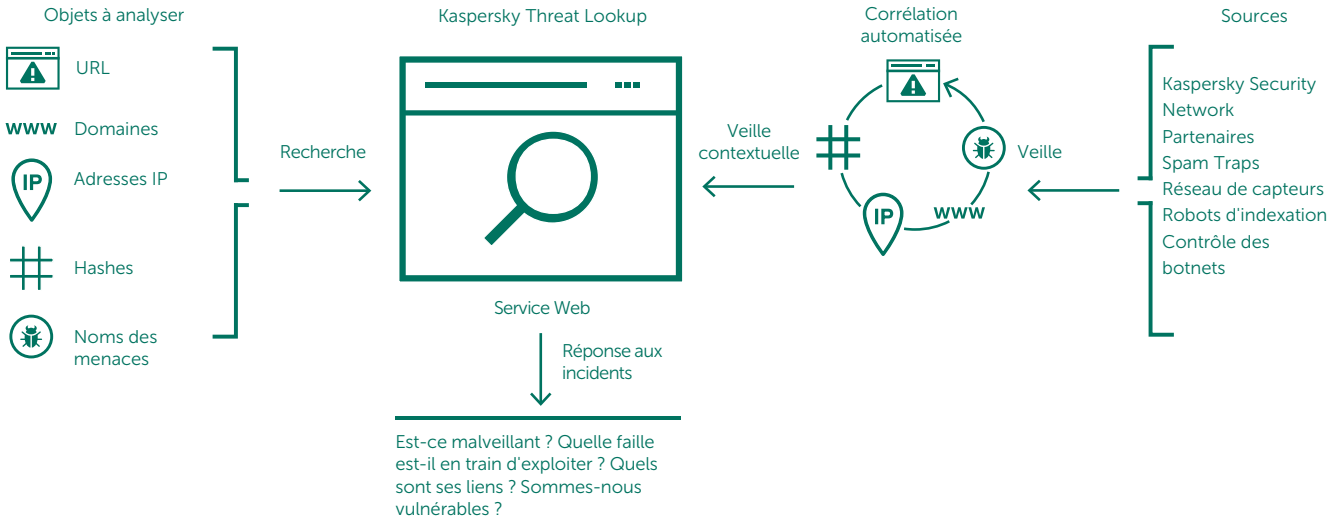
Si vous souhaitez obtenir des rapports sur les menaces spécifiques à un pays, veuillez contacter votre responsable régional Kaspersky Lab ou envoyer un e-mail à l'adresse information-services@kaspersky.fr. En fonction des informations que vous nous communiquerez en termes d'étendue, de conditions et de calendrier prévisionnel, nous préparerons une offre de service spécifique à votre pays.

KASPERSKY THREAT LOOKUP

Aujourd'hui, la cybercriminalité ne connaît pas de frontières et les capacités techniques sur lesquelles elle s'appuie évoluent rapidement : nous assistons à des attaques qui sont de plus en plus sophistiquées, les cybercriminels ayant recours à des ressources du Dark Web pour menacer leurs cibles. La fréquence, la complexité et l'obfuscation des cybermenaces ne cessent de croître. Et les cybercriminels utilisent de nouveaux moyens pour affaiblir vos défenses. Chaînes de frappe complexes et TTP (Tactiques, Techniques et Procédures) personnalisées font désormais partie de leurs méthodes pour paralyser votre activité, dérober vos ressources et attaquer vos clients.

Kaspersky Threat Lookup fournit instantanément des informations fiables sur les cybermenaces et les objets authentiques, ainsi que sur leurs liens et indicateurs. Ces informations sont enrichies d'un contexte exploitable, ce qui vous permet d'informer les membres de votre entreprise ou vos clients sur les risques et implications associés. Vous êtes désormais en mesure d'atténuer les menaces, d'y répondre plus efficacement, et de vous défendre contre les attaques avant même qu'elles ne soient lancées.

Kaspersky Threat Lookup repose sur toutes les connaissances acquises par Kaspersky Lab sur les cybermenaces et leurs liens, regroupées dans un service Web unique et efficace. Le but est de fournir à vos équipes de sécurité autant d'informations que possible, afin de contrer les cyberattaques avant qu'elles n'aient un impact sur votre entreprise. La plateforme récupère les dernières informations détaillées relatives à la surveillance des menaces sur les URL, les domaines, les adresses IP, les hashes de fichiers, les noms des menaces, les données statistiques/comportementales, les données WHOIS/DNS, etc. Le résultat est une visibilité globale sur les menaces nouvelles et émergentes qui vous permet de sécuriser votre entreprise et d'améliorer la réponse aux incidents.

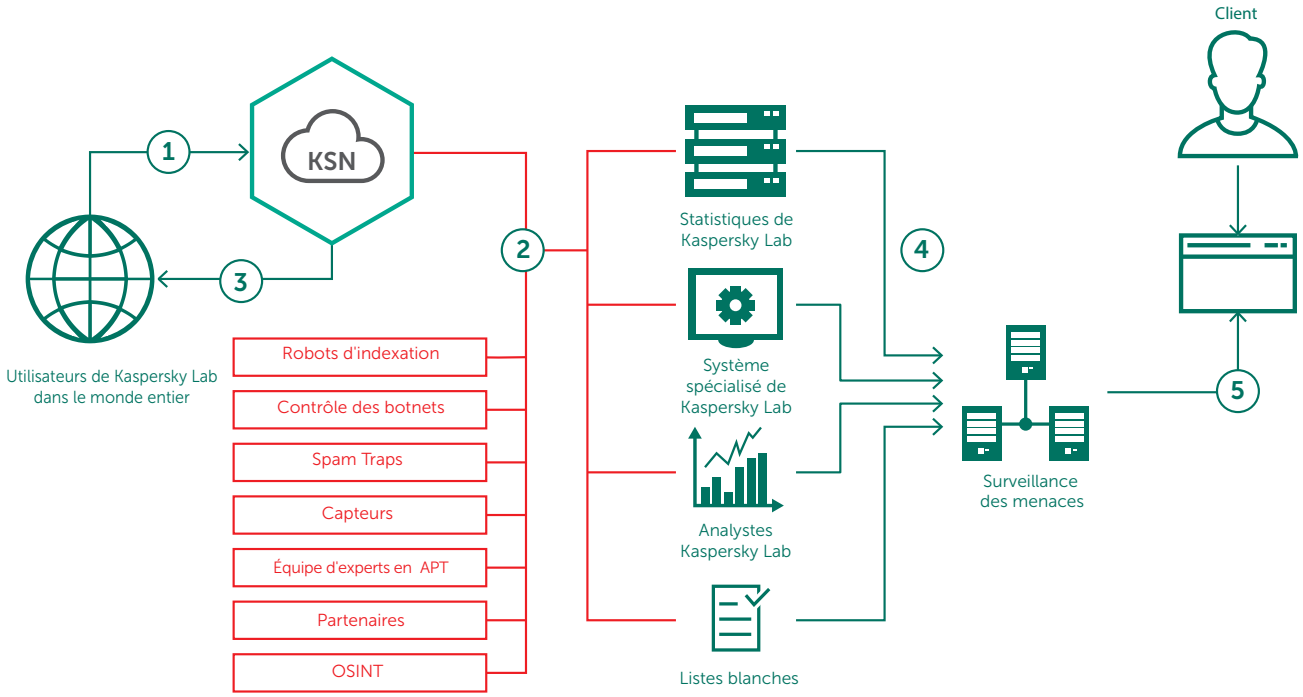


FONCTIONNALITÉS

- **Informations de confiance** : un des principaux atouts de Kaspersky Threat Lookup est la fiabilité de nos données sur la surveillance des menaces, enrichies d'un contexte exploitable, ce qui peut donner lieu à des actions. Les produits de Kaspersky Lab arrivent en tête dans les tests anti-malware[1] et démontrent la qualité de nos renseignements en offrant les taux de détection les plus élevés, avec un nombre de faux positifs quasi nul.
- **Niveaux élevés de couverture en temps réel :** les informations sur les menaces sont générées en temps réel et de manière automatique, en fonction de résultats obtenus dans le monde entier (grâce à la solution Kaspersky Security Network qui permet une visibilité sur une proportion considérable de l'ensemble du trafic Internet et sur tous les types de données, couvrant des dizaines de millions d'utilisateurs finaux dans plus de 213 pays), afin de garantir des niveaux élevés de couverture et une bonne précision.

1 http://www.kaspersky.fr/top3

- **Recherche de menaces** : faites preuve de proactivité dans la prévention, la détection et la réaction face aux attaques afin de minimiser leur impact et leur fréquence. Suivez et éliminez avec fermeté les attaques le plus tôt possible. Plus tôt vous détectez une menace, moins il y a de dommages et plus rapides sont les réparations ainsi que le retour à la normale des opérations de réseau.
- **Richesse des données** : la surveillance des menaces offerte par Kaspersky Threat Lookup couvre de nombreux types de données différents, dont les hashes, les URL, les adresses IP, les données whois, pDNS, GeoIP, les attributs de fichier, les données statistiques et comportementales, les chaînes de téléchargement, les horodatages et bien plus encore. Grâce à ces données, vous pouvez examiner les diverses menaces de sécurité auxquelles vous avez affaire.
- **Disponibilité permanente** : la surveillance des menaces est générée et surveillée par une infrastructure hautement tolérante aux pannes, assurant une disponibilité permanente et des performances constantes.
- **Examen continu par des experts en sécurité** : des centaines d'experts, y compris des analystes en sécurité du monde entier, des experts en sécurité appartenant à notre équipe GReAT et réputés mondialement, ainsi que nos équipes de R&D à la pointe de la technologie, tous contribuent à générer des informations utiles et concrètes sur la surveillance des menaces.
- **Analyse des sandboxes** :[2] détectez les menaces inconnues en exécutant des objets suspects dans un environnement sécurisé et examinez l'étendue complète du comportement de la menace et des artefacts grâce à des rapports faciles à lire.
- **Large éventail de formats d'exportation** : exportez les indicateurs de compromission (IOC) ou le contexte actionnable dans des formats de partage largement utilisés et mieux organisés, lisibles par machine, tels que STIX, OpenIOC, JSON, Yara, Snort ou même CSV, afin de profiter pleinement des avantages de la surveillance des menaces, d'automatiser les processus d'opérations, ou de les intégrer dans des contrôles de sécurité tels que SIEM.



2 Cette fonctionnalité devrait être disponible à partir du premier semestre 2017.

- **Interface Web conviviale ou API compatible REST** : vous pouvez choisir d'utiliser le service en mode manuel par l'intermédiaire d'une interface Web (avec un navigateur Web) ou d'y accéder via une simple API compatible REST.

PRINCIPAUX AVANTAGES

- **Améliorez et accélérez votre processus de réponse aux incidents et vos capacités de diagnostic** en fournissant aux équipes de sécurité/SOC des informations utiles sur les menaces et un aperçu global de la logique qui sous-tend les attaques ciblées. Diagnostiquez et analysez plus efficacement les incidents de sécurité qui frappent les hébergeurs et le réseau, et hiérarchisez les signaux émis par les systèmes internes face à des menaces inconnues afin de réduire le délai d'intervention et de perturber la chaîne de frappe avant que des données et des systèmes critiques ne soient compromis.
- **Examinez de manière approfondie les indicateurs de menace** (adresses IP, URL, domaines, hashes de fichiers) dotés d'un contexte hautement validé afin de hiérarchiser les attaques, de prendre de meilleures décisions concernant la dotation en personnel et l'affectation des ressources, et de mettre l'accent sur l'atténuation des menaces les plus dangereuses pour votre entreprise.
- **Limitez les attaques ciblées**. Optimisez vos infrastructures de sécurité grâce à une veille tactique et stratégique contre les menaces et à des stratégies de défense et de lutte adaptées.

SOURCES D'INFORMATIONS SUR LA SURVEILLANCE DES MENACES

La surveillance des menaces fusionne des sources hétérogènes et extrêmement fiables, dont Kaspersky Security Network (KSN) et nos propres robots d'indexation, notre service de contrôle des botnets (surveillance des botnets, de leurs cibles et activités 24/7/365), les spam traps, les équipes de recherche, les données de partenaires et d'autres données d'historiques sur des objets malveillants recueillies par Kaspersky Lab depuis plus de deux décennies. Ensuite, toutes les données agrégées sont soigneusement inspectées et affinées en temps réel, en utilisant différentes techniques de prétraitement, telles que les critères statistiques, les systèmes et bases de données spécialisés de Kaspersky Lab (sandboxes, moteurs heuristiques, outils de similarité, profil de comportement, etc.), la validation par les analystes et la vérification des listes blanches.

MAINTENANT, C'EST POSSIBLE

- Rechercher des indicateurs de menace via une interface Web ou une API compatible REST.
- Comprendre en quoi un objet particulier doit être considéré comme malveillant.
- Vérifier si l'objet en question est répandu ou unique.
- Examiner les informations détaillées (certificats, noms couramment utilisés, chemins d'accès aux fichiers, URL associées) pour identifier de nouveaux objets suspects.

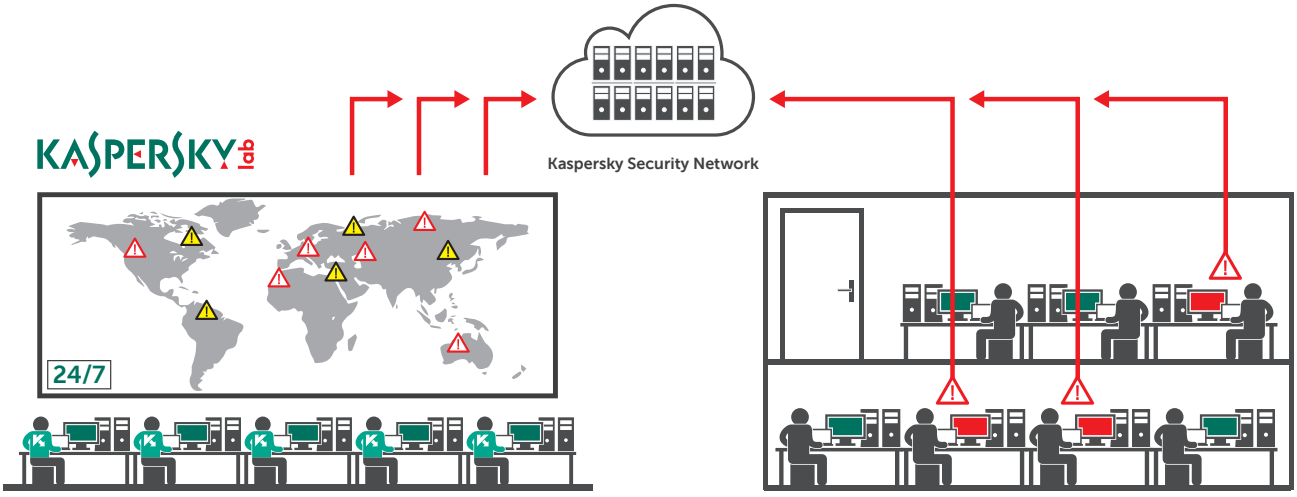
Et la liste est encore longue. Il existe de nombreuses façons d'exploiter cette abondante base de données utiles et granulaires.

Apprenez à distinguer vos amis de vos ennemis. En identifiant les fichiers, URL et adresses IP non malveillants, vous pouvez accélérer le processus d'investigation. Chaque seconde compte. Ne perdez pas votre temps à analyser des objets fiables.

Notre mission est de sauver le monde de tous les types de cybermenaces. Pour atteindre cet objectif et faire d'Internet un environnement sûr et sécurisé, il est essentiel de partager les informations sur les menaces et d'y accéder en temps réel. L'accès rapide à l'information est un élément essentiel de la protection efficace de vos données et réseaux. Aujourd'hui, Kaspersky Threat Lookup facilite et optimise plus que jamais cet accès.

KASPERSKY MANAGED PROTECTION

Le service Kaspersky Managed Protection offre aux utilisateurs de Kaspersky Security for Business et de la plate-forme Kaspersky Anti Targeted Attack une combinaison unique de mesures techniques avancées permettant de détecter et de prévenir les attaques ciblées. Ce service inclut un contrôle 24 h/24, 7 jours sur 7 par des experts de Kaspersky Lab et une analyse constante des données de cybermenaces (veille stratégique contre les cybermenaces) offrant une détection en temps réel des campagnes de cyberespions et de cybercriminels – aussi bien nouveaux que notoires – visant les systèmes d'information critiques.



LES POINTS FORTS DU SERVICE

- Un haut niveau de protection contre les attaques ciblées et les programmes malveillants et une assistance 24h/24 et 7j/7 de la part des analystes de Kaspersky Lab.
- Des informations sur les cybercriminels, et plus précisément sur leurs mobiles, leurs méthodes et leurs outils, ainsi que sur les dommages éventuels qu'ils pourraient provoquer, le tout contribuant à l'élaboration d'une stratégie de protection efficace et parfaitement étayée.
- La détection des attaques d'origine non malveillante, des attaques impliquant des outils jusqu'alors inconnus ou des attaques exploitant des vulnérabilités zero-day.
- L'analyse rétrospective des incidents et la « chasse aux menaces ».
- La réduction du coût total relatif à la sécurité, associée à une protection de meilleure qualité. Il s'agit d'un service hautement professionnel proposé par le leader mondial en matière d'analyse des cyberattaques (y compris l'analyse des méthodes et technologies employées par les auteurs de menaces). Il est beaucoup plus rentable de faire appel à un service extérieur pour obtenir un tel niveau de renseignement que de recruter des spécialistes au domaine de compétence restreint.
- Approche intégrée. Grâce à sa large gamme de solutions intégrées (Kaspersky Security for Business), Kaspersky Lab offre tous les services et technologies nécessaires à la mise en œuvre d'un cycle complet de protection contre les attaques ciblées : Préparation – Détection – Investigation – Analyse de données – Protection automatisée.

AVANTAGES DU SERVICE

- Détecte rapidement les incidents.
- Collecte suffisamment d'informations pour permettre d'effectuer une classification (faux positifs ou vraies menaces).
- Permet de déterminer si les artefacts collectés sont courants et si l'attaque est unique.
- Lance le processus de réponse à un incident touchant la sécurité des informations.
- Lance les mises à jour de bases de données antivirus nécessaires pour empêcher la propagation des menaces.

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 est de 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 :

- Services de test de pénétration
- Services d'évaluation de la sécurité des applications
- Évaluation de la sécurité des DAB/points de vente
- Évaluation de la sécurité des réseaux de télécommunications

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 wi-fi** : nos experts effectuent une visite de votre site et analysent les contrôles de sécurité wi-fi.

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 wi-fi, 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 : solutions 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 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 dans 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'un chiffrement insuffisant
- 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 menant à des attaques sur les sessions.
- 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.

ÉVALUATION DE LA SÉCURITÉ DES DAB/POINTS DE VENTE

Les DAB et les terminaux de points de vente ne sont plus seulement vulnérables aux attaques physiques (par ex., cambriolage de distributeur ou piratage et clonage de carte). Suite à l'évolution des mesures de protection prises par les fournisseurs de DAB/terminaux de point de vente, les criminels passent eux aussi à la vitesse supérieure et leurs attaques sont de plus en plus sophistiquées. Les pirates informatiques exploitent les vulnérabilités des applications et de l'infrastructure des DAB/points de vente afin de créer des programmes malveillants sur mesure. Les services d'évaluation de la sécurité des DAB/points de vente de Kaspersky Lab vous aident à identifier les failles de sécurité de vos DAB et/ou terminaux de points de vente et à limiter le risque qu'ils soient compromis.

Cette évaluation consiste en une analyse complète de vos DAB et/ou terminaux de points de vente. Elle permet de repérer les éventuelles vulnérabilités que les criminels pourraient exploiter pour leurs activités frauduleuses, par exemple : un retrait ou des transactions non autorisé(es), la récupération des données de cartes de paiement de vos clients ou encore une attaque par déni de service. Ce service 1) mettra en évidence la moindre vulnérabilité dans l'infrastructure de vos DAB/points de vente susceptible d'être exploitée pour différents types d'attaque, 2) précisera les conséquences possibles d'une telle exploitation, 3) évaluera l'efficacité de vos mesures de sécurité actuelles, et 4) vous aidera à établir un plan d'action pour corriger les failles identifiées et renforcer votre protection.

AVANTAGES DU SERVICE

Les services d'évaluation de la sécurité des DAB/points de vente de Kaspersky Lab permettent aux fournisseurs et aux établissements financiers :

- **De comprendre les vulnérabilités** de leurs DAB et/ou terminaux de points de vente et d'optimiser les processus de sécurité correspondants.
- **D'éviter les dommages financiers, opérationnels et liés à la réputation** qui peuvent être occasionnés par une attaque, en détectant et corrigeant de manière proactive les vulnérabilités susceptibles d'être exploitées par les criminels.
- **De se conformer aux normes gouvernementales, industrielles et internes de l'entreprise** qui imposent des évaluations de sécurité, (par exemple la norme PCI DSS (paiement sécurisé par carte bancaire)).

ÉTENDUE DES SERVICES

Ce service inclut une analyse complète des DAB/points de vente, notamment un « fuzzing » et des démonstrations d'attaques dans un environnement de test. Cette analyse peut porter sur un seul DAB et/ou terminal de point de vente, ou bien sur tout un réseau. Nous vous recommandons, aux fins de cette évaluation, de choisir le type de DAB et/ou de terminal de point de vente le plus utilisé au sein de votre entreprise, ou le plus critique (par exemple un appareil qui a déjà fait l'objet d'incidents) dans sa configuration classique.

APPROCHE DE L'ÉVALUATION DE LA SÉCURITÉ DES DAB/POINTS DE VENTE DE KASPERSKY LAB

Au cours de l'analyse, nos experts ne se contenteront pas de rechercher et d'identifier les éventuels défauts de configuration et vulnérabilités dans les logiciels obsolètes. Ils examineront en détail la logique qui sous-tend les processus exécutés par vos DAB et/ou terminaux de points de vente, et réaliseront une recherche en sécurité dans le but de repérer toute nouvelle vulnérabilité de type « zero-day » au niveau des composants. S'ils découvrent des vulnérabilités susceptibles d'être exploitées par un criminel (et conduisant, par exemple, à un retrait non autorisé), nos experts pourront vous fournir une démonstration des scénarios d'attaque possibles au moyen d'outils ou d'appareils d'automatisation spécialement conçus à cet effet.

Bien que l'évaluation de la sécurité des DAB/points de vente implique la simulation de véritables cyberattaques en vue de mesurer concrètement l'efficacité de votre système de défense, cette méthode est parfaitement sûre et non invasive. Ce service est fourni par les experts en sécurité de Kaspersky Lab qui s'attacheront à préserver la confidentialité, l'intégrité et la disponibilité de vos systèmes, dans le plus strict respect des normes internationales et des bonnes pratiques. Si nous découvrons une nouvelle vulnérabilité dans le DAB/point de vente d'un client, nous nous engageons à appliquer une politique d'information responsable, c'est-à-dire à avertir le fournisseur concerné et à lui recommander des mesures correctives.

Kaspersky Lab fournit ses services d'évaluation de la sécurité des DAB/points de vente conformément aux normes internationales et aux bonnes pratiques ci-dessous :

- Les normes sectorielles relatives aux cartes de paiement
  - La norme sur la sécurité des données
  - La norme sur la sécurité des données des applications de paiement
  - La norme sur la sécurité des transactions nécessitant la saisie d'un code PIN
- Le Manuel méthodologique des tests de sécurité open source (OSSTMM)
- Le Cadre d'évaluation de la sécurité des systèmes d'information (ISSAF)
- Le système de notation des vulnérabilités CVSS (Common Vulnerability Scoring System)
- D'autres normes applicables, selon les besoins, à des modèles d'activité et des zones géographiques spécifiques

L'équipe de projet est composée de professionnels de la sécurité très expérimentés bénéficiant de connaissances pratiques approfondies dans un domaine qu'ils ne cessent de parfaire. Régulièrement, ceux-ci conseillent les fournisseurs de DAB/points de vente en matière de sécurité et présentent les résultats de leurs recherches dans le cadre de conférences phares sur la sécurité des informations (comme la conférence Black Hat).

RÉSULTATS DE L'ÉVALUATION DE LA SÉCURITÉ DES DAB/POINTS DE VENTE

Les services d'évaluation de la sécurité des DAB/points de vente doivent permettre d'identifier un certain nombre de vulnérabilités, parmi lesquelles :

- Une architecture réseau vulnérable et une protection insuffisante du réseau.
- Des vulnérabilités permettant à un cybercriminel de contourner le mode kiosque et d'obtenir un accès non autorisé au système d'exploitation.
- Des vulnérabilités dans les logiciels de sécurité tiers permettant aux éventuels cybercriminels de contourner les contrôles de sécurité.
- Une protection insuffisante des appareils d'entrée/sortie (lecteurs de cartes, distributeurs, etc.), ainsi que des vulnérabilités dans les communications desdits appareils, susceptibles de favoriser l'interception et la modification des données transférées.
- Des vulnérabilités provenant d'erreurs dans le code de l'application ou causées par l'utilisation de matériels et de logiciels obsolètes (dépassement de la mémoire tampon, injection de code, etc.).
- La divulgation d'informations.

Au terme de l'évaluation, vous recevrez un rapport contenant 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 nos conclusions au vu des résultats du test et illustrant les différents vecteurs d'attaque. Sur demande, nous pouvons également fournir à votre équipe technique ou à la direction des présentations et des vidéos de démonstration d'attaques.

SERVICES D'ÉVALUATION DE LA SÉCURITÉ DES RÉSEAUX DE TÉLÉCOMMUNICATIONS

PRÉSENTATION DES SERVICES

L'infrastructure informatique d'une entreprise de télécommunications est constituée d'un certain nombre de réseaux interconnectés reposant sur diverses fonctionnalités et technologies. En règle générale, elle comprend un réseau d'entreprise incluant des éléments de gestion, un réseau radio central (GSM/UMTS/LTE) fournissant un accès Internet haut débit aux abonnés, des canaux dédiés à grande vitesse de type « trunk », ainsi que des services d'hébergement et de Cloud. Chaque composante de cette infrastructure est essentielle à l'entreprise et doit être parfaitement protégée contre les cyberattaques pour réduire les risques en termes financiers, opérationnels et de réputation. Vous pouvez atteindre cet objectif grâce aux services d'évaluation de la sécurité des réseaux de télécommunications de Kaspersky Lab qui, après avoir identifié les vulnérabilités de vos systèmes, les éliminent ou les corrigent en instaurant des contrôles.

En ce qui concerne la sécurité des réseaux de télécommunications, Kaspersky Lab propose les services d'évaluation suivants :

- Test de pénétration de l'infrastructure informatique
- Évaluation de la sécurité au niveau de la configuration de l'infrastructure informatique
- Évaluation de la sécurité des réseaux GSM/UMTS/LTE
- Évaluation de la sécurité des applications (fournissant divers services : IPTV, portail client libre-service, etc.)
- Évaluation de la sécurité du service voix sur IP (VoIP)
- Évaluation de la sécurité des équipements de télécommunications

RÉSULTATS

Au terme de chaque évaluation de sécurité, vous recevrez un rapport contenant des informations techniques et détaillées sur les failles de sécurité de vos réseaux de télécommunications, ainsi que nos conclusions quant à l'efficacité de vos contrôles de sécurité. Vous pourrez utiliser ces résultats pour renforcer la sécurité de vos réseaux et, ce faisant, limiter les risques en termes financiers, opérationnels et de réputation associés aux menaces sur la sécurité des informations.

Le rapport contiendra les éléments suivants :

- Des conclusions détaillées sur le niveau de sécurité actuel de vos réseaux de télécommunications
- Une description de la méthodologie et du processus appliqués par le service
- Une description détaillée des vulnérabilités détectées, y compris leur degré de gravité et de complexité, leurs répercussions éventuelles sur le système considéré et les preuves de leur existence (dans la mesure du possible)
- Des recommandations pour éliminer ces vulnérabilités (modification de la configuration, mises à jour, modification des codes source ou encore mise en place de contrôles de compensation lorsqu'il est impossible d'éliminer une vulnérabilité)

SERVICES DE DÉTECTION ET DE RÉPONSE AUX INCIDENTS

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. Personne n'est à l'abri. L'absence de contrôles de sécurité efficaces pourrait faire de vous une victime.

Les services de détection et de réponse aux incidents répondent à plusieurs objectifs : 1) déterminer si vous êtes en train de subir une cyberattaque et, si oui, pour quelle raison, 2) localiser les éventuelles sources de l'attaque, 3) établir un plan d'action, et 4) vous aider à éviter toute attaque similaire à l'avenir.

Les experts de Kaspersky Lab vous aideront à résoudre les problèmes de sécurité en temps réel et à comprendre les comportements des programmes malveillants ainsi que leurs conséquences, tout en vous conseillant sur les mesures correctives à mettre en œuvre, et ce à travers deux services :

- **Détection des attaques ciblées**
- **Réponse aux incidents**
- **Analyse des programmes malveillants**
- **Cyberdiagnostic**

Détection des attaques ciblées

Si vous craignez des attaques visant votre secteur, si vous avez constaté des comportements potentiellement suspects au sein de vos systèmes ou si votre entreprise est tout simplement consciente des avantages qu'elle peut tirer de contrôles préventifs réguliers, faites appel aux services Kaspersky Targeted Attack Discovery. Vous saurez ainsi :

- Si vous êtes en train de subir une attaque et, si oui, quelles en sont les caractéristiques et qui en est l'auteur
- En quoi cette attaque affecte vos systèmes et quelles sont les possibilités qui s'offrent à vous
- Comment éviter au mieux d'autres attaques

FONCTIONNEMENT DU SERVICE

Nos experts indépendants mondialement reconnus identifieront et analyseront tous les incidents, menaces APT et attaques de cybercriminalité et de cyberespionnage affectant votre réseau. Ils vous aideront à repérer les éventuelles activités malveillantes, à comprendre quelles peuvent être les sources des incidents et à planifier les mesures correctives les plus efficaces.

Notre approche consiste à :

- Analyser les sources d'informations sur les menaces afin de comprendre le paysage de menaces propre à votre entreprise
- Étudier en détail votre infrastructure informatique et vos données (telles que les fichiers journaux) afin de repérer d'éventuels signes de compromission
- Analyser vos connexions réseau sortantes à la recherche d'une quelconque activité suspecte
- Découvrir les sources probables de l'attaque et d'autres systèmes susceptibles d'être compromis

LES RÉSULTATS

Nos conclusions sont regroupées dans un rapport détaillé incluant :

Nos découvertes générales : confirmation de l'existence ou de l'absence de signes de compromission dans votre réseau.

Une analyse approfondie : analyse des données recueillies sur la surveillance des menaces et des indicateurs de compromission mis en évidence.

Une description détaillée : description des vulnérabilités exploitées, des sources potentielles de l'attaque et des composantes du réseau affectées.

Les mesures correctives préconisées : mesures suggérées pour atténuer les répercussions de l'incident détecté et protéger vos ressources contre des attaques similaires à l'avenir.

À PROPOS DU SERVICE

Le service Kaspersky Targeted Attack Discovery se compose de plusieurs activités, à savoir :

Collecte et analyse d'informations sur la surveillance des menaces. L'objectif consiste à obtenir un instantané de votre surface d'attaque, c'est-à-dire des menaces et attaques de cybercriminalité et de cyberespionnage visant potentiellement ou activement vos ressources. Nous puiserons dans les sources d'informations externes comme internes, y compris les communautés souterraines de fraudeurs et les systèmes de surveillance internes de Kaspersky Lab. L'analyse de ces informations nous permettra par exemple d'identifier des faiblesses de grand intérêt pour les cybercriminels dans votre infrastructure, ou encore des comptes compromettants.

Collecte de données sur place et réponse rapide aux incidents. Parallèlement à la surveillance des menaces réalisée dans nos propres laboratoires, les experts de Kaspersky Lab collecteront sur place des artefacts réseau et système, ainsi que toutes les informations SIEM disponibles. Nous pourrons également effectuer une rapide évaluation des vulnérabilités afin de mettre en évidence les failles de sécurité les plus critiques et de les corriger sans attendre. Au cas où un incident se serait déjà produit, nous réunirons des éléments de preuve pour procéder à une investigation. À ce stade, nous vous exposerons les mesures correctives à court terme que nous préconisons.

Analyse de données. Pour nous permettre de comprendre exactement ce qui se passe dans votre système, les artefacts réseau et système collectés seront analysés en laboratoire au moyen de la base de connaissances Kaspersky Lab sur les indicateurs de compromission, des listes noires de serveurs C&C, des technologies de sandbox, etc. Si, à cette étape, nous identifions par exemple un nouveau programme malveillant, nous vous conseillerons et vous fournirons les bons outils (c'est-à-dire les règles Yara) pour le détecter immédiatement. Nous resterons en contact tout au long du processus et travaillerons à distance sur vos systèmes le cas échéant.

Création de rapports. Enfin, nous rédigerons un rapport formel exposant nos résultats sur la détection d'attaques ciblées et les mesures correctives que nous préconisons.

SERVICES COMPLÉMENTAIRES

Vous pouvez également demander à nos experts d'analyser les symptômes d'un incident, de réaliser un cyberdiagnostic approfondi de certains systèmes, d'identifier un programme malveillant binaire (le cas échéant) ou encore d'analyser les programmes malveillants. Ces services optionnels donnent lieu à des rapports distincts contenant des recommandations supplémentaires en matière de mesures correctives.

Nous pouvons par ailleurs, sur demande, déployer la **plate-forme Kaspersky Anti Targeted Attack** sur votre réseau, de façon permanente ou à titre de démonstration. Cette plate-forme combine les technologies les plus récentes à des solutions d'analyse mondiales dans le but de détecter des attaques ciblées, d'y répondre rapidement et de les contrer à toutes les étapes du cycle de vie de votre système

Réponse aux incidents

Il est de plus en plus difficile d'éviter les incidents liés à la sécurité des informations. S'il n'est pas toujours possible de stopper une attaque avant qu'elle ne pénètre votre périmètre de sécurité, nous sommes cependant tout à fait en mesure de limiter les dommages qui en résultent et d'éviter sa propagation.

L'objectif principal du service de réponse aux incidents est de réduire l'impact d'une violation de sécurité ou d'une attaque sur votre environnement informatique. Ce service couvre le cycle complet d'investigation sur les incidents, depuis l'acquisition sur place des éléments de preuve à l'identification d'indications supplémentaires de compromission, et comprend la conception d'un plan de résolution ainsi que l'élimination complète de la menace pour votre entreprise.

Notre approche consiste à :

- Identifier les ressources compromises
- Isoler la menace
- Empêcher que l'attaque ne se propage
- Trouver et recueillir des éléments de preuve
- Analyser les éléments de preuve et reconstruire l'historique et la logique de l'incident
- Analyser le programme malveillant utilisé dans l'attaque (lorsqu'un programme malveillant est détecté)
- Découvrir les sources de l'attaque et d'autres systèmes susceptibles d'être compromis (si possible)
- Effectuer des analyses assistées par outil de votre infrastructure informatique pour révéler d'éventuels signes de compromission
- Analyser les connexions sortantes entre votre réseau et les ressources externes pour détecter tout élément suspect (tels que d'éventuels serveurs de commande et de contrôle)
- Éliminer la menace
- Recommander d'autres mesures correctives à prendre

Selon que vous ayez ou non votre propre équipe de réponse aux incidents, vous pouvez demander à nos experts d'exécuter un cycle complet d'investigation, de simplement identifier et isoler les machines compromises et d'empêcher la diffusion de la menace, ou de réaliser des analyses de programmes malveillants ou des cyberdiagnostics.

Les services de réponse aux incidents de Kaspersky Lab sont fournis par des analystes et des chercheurs chevronnés dans la détection de cyberintrusions. Toute la force de notre expertise mondiale en matière de cyberdiagnostic et d'analyse de programmes malveillants peut être mise à contribution pour résoudre votre incident de sécurité.

ANALYSE DES PROGRAMMES MALVEILLANTS

L'analyse des programmes malveillants permet de comprendre pleinement le comportement et les objectifs des programmes malveillants spécifiques ciblant votre entreprise. Les experts de Kaspersky Lab réalisent une analyse approfondie des échantillons de programmes malveillants que vous fournissez 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 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 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.

CYBERDIAGNOSTIC

Le cyberdiagnostic 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 élucidation 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.

FORMULES DES SERVICES

Les services de réponse aux incidents de Kaspersky Lab sont disponibles :

- Par abonnement
- En réponse à un incident ponctuel

Ces deux options reposent sur le temps que nos experts consacrent à la résolution de l'incident, tel que nous le négocions ensemble avant la signature du contrat. Vous pouvez préciser le nombre d'heures de travail à fournir ou bien suivre les recommandations de nos experts en fonction de l'incident en question et de vos besoins.

REMARQUES

REMARQUES


Twitter.com/
KasperskyFrance


Facebook.com/
KasperskyLabFrance


Youtube.com/
KasperskyFrance

AO Kaspersky Lab France, 2 rue Joseph Monier, 92859 Rueil Malmaison www.kaspersky.fr

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

Trouver un partenaire près de chez vous : https://www.kaspersky.fr/small-to-medium-business-security/how-to-buy

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 2016 GL