KASPERSKY lab

FAIRE VIVRE UN SOC : MÉTHODOLOGIE ET CONSEILS

www.kaspersky.fr

Tandis que les entreprises apprennent à mieux se protéger, les criminels élaborent dans le même temps des techniques toujours plus sophistiquées pour franchir leurs murs de sécurité. Attirés par les possibilités de gain sans précédent que les cyberattaques peuvent générer, les auteurs de menaces toujours plus nombreux cherchent et ciblent activement les failles de sécurité auparavant inconnues.

« Les centres de supervision de la sécurité doivent être conçus pour la surveillance et adopter une architecture de sécurité évolutive afin qu'ils soient sensibles au contexte et basés sur la veille stratégique. Les responsables de la sécurité doivent comprendre la manière dont les SOC basés sur la veille stratégique utilisent les outils, les processus et les stratégies pour se protéger contre les nouvelles menaces. »

Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, novembre 2015

De plus en plus de centres de supervision de la sécurité (SOC) sont mis en place pour lutter contre les problèmes de sécurité à mesure qu'ils se présentent, fournissant ainsi une réponse et une résolution dans les plus brefs délais.

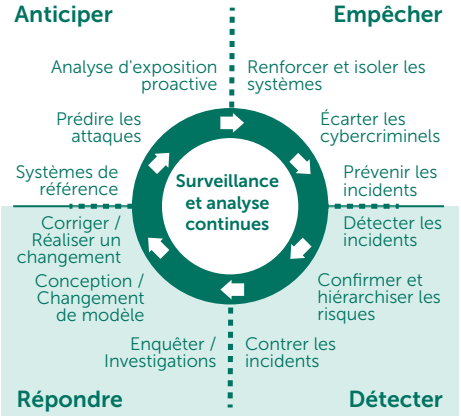
LE SOC EST UNE FONCTION CENTRALISÉE POUR LA SURVEILLANCE ET L'ANALYSE DES MENACES EN CONTINU, AINSI QUE POUR L'ATTÉNUATION ET LA PRÉVENTION DES INCIDENTS DE CYBERSÉCURITÉ

Une enquête menée récemment par B2B International (à paraître fin 2016), impliquant plus de 4 000 entreprises dans 25 pays, émet le constat suivant :

- **38 %** des entreprises interrogées ont connu de graves **problèmes liés à des virus et des logiciels malveillants** au cours des 12 mois précédents, entraînant une perte de productivité.
- **21 %** ont subi **une perte/exposition de données en raison d'attaques ciblées**.
- Environ 40 % des entreprises interrogées ont insisté sur ces problèmes jugés particulièrement préoccupants.
- **17 %** des entreprises ont été victimes d'une **attaque DDoS** au cours des 12 derniers mois, souvent plus d'une fois.
- **42 %** de tous les sondés ayant été la cible **d'attaques par phishing** étaient des entreprises.
- **26 %** de la totalité des événements de sécurité **n'ont pas été détectés** pendant des semaines et n'ont été découverts que grâce à des audits de sécurité externes.
- Pour une entreprise ayant subi au moins un piratage de données, **l'impact financier moyen** était de **891 000 dollars** (ceci inclut les rémunérations supplémentaires du personnel interne, les baisses de cotes de solvabilité/primes d'assurance, les affaires manquées, les efforts supplémentaires en matière de relations publiques pour réparer les dommages en termes d'image de marque et l'emploi de consultants externes).
- Les **répercussions** chiffrées pour les entreprises **variaient de 393 000 à 1,1 million de dollars**, selon le moment où le piratage avait été détecté, une identification rapide entraînant des coûts moins élevés pour l'entreprise.
- Le nombre total de dossiers sensibles de clients/employés compromis était également dépendant de ce moment, de 9 000 en cas de détection quasiment instantanée (système de détection en place) à 240 000 en cas de piratage non repéré pendant plus d'un an.

Selon le modèle d'architecture de sécurité évolutive de Gartner, si les équipes des SOC souhaitent lutter efficacement contre la cybercriminalité dans l'environnement de menace actuel, elles doivent être préparées à :

- ANTICIPER
- DÉTECTER
- EMPÊCHER
- RÉAGIR



Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014, Foundational January 2016

QUATRE ÉLÉMENTS ESSENTIELS

Quatre éléments essentiels, associés à des processus clairement définis et à des technologies pertinentes, doivent être mis en place pour soutenir cette approche reconnue par le secteur :

- **LA GESTION DES CONNAISSANCES.** Le personnel (les membres de l'équipe SOC) doit être bien formé aux techniques de cyberdiagnostic, d'analyse des programmes malveillants et de réponse aux incidents afin de pouvoir prévenir des attaques de plus en plus sophistiquées et y répondre.
- **LA SURVEILLANCE DES MENACES**, recueillies auprès de nombreuses sources différentes (plus il y en a, mieux c'est), est essentielle pour détecter en temps opportun les nouvelles menaces :
  1. Données relatives aux menaces internes
  2. Renseignements tirés de sources ouvertes (OSINT)
  3. CERT du secteur
  4. Fournisseurs internationaux de solutions de protection contre les programmes malveillants
- **LA RECHERCHE DES MENACES** permet de rechercher de façon proactive les menaces non détectées par des systèmes de sécurité traditionnels, comme les pare-feu, les solutions de prévention et de détection des intrusions, SIEM, etc.
- **UN CADRE DE RÉPONSE AUX INCIDENTS** mis en œuvre pour limiter les dommages et réduire les coûts liés aux actions correctives.

Ces éléments sont tous d'égale importance et méritent une attention particulière.

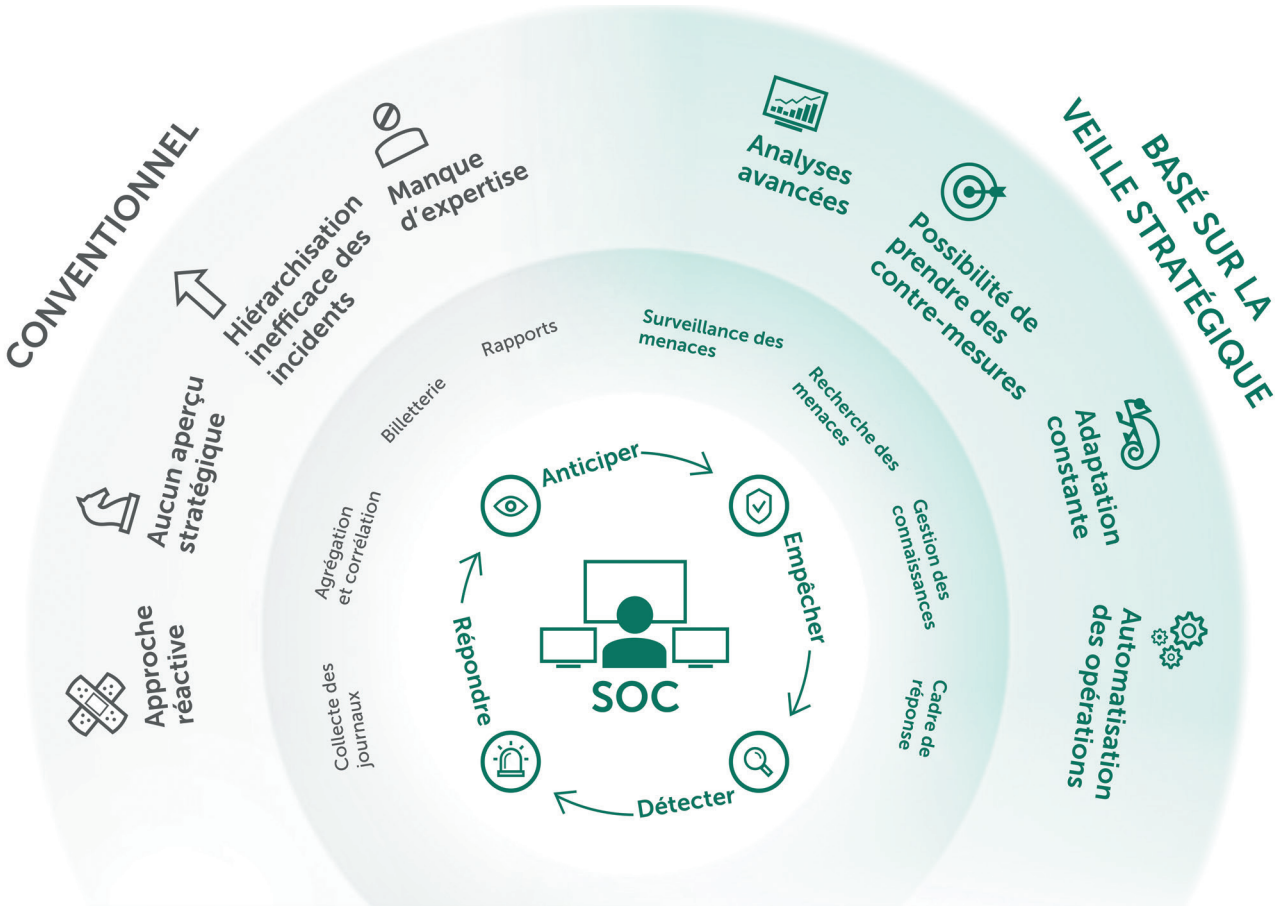


Figure 1 :
Les quatre éléments essentiels du SOC

GESTION DES CONNAISSANCES

Le SOC doit fournir un ensemble de connaissances pratiques et l'expertise suffisante pour analyser une grande quantité d'informations et identifier où de nouvelles investigations sont nécessaires.

Les budgets limités rendent difficile la dotation en personnel du SOC.

Le marché connaît actuellement une pénurie de professionnels correctement formés dans la cybersécurité, ce qui conduit à une augmentation des coûts de recrutement et d'emploi.

Un membre d'une équipe de SOC doit disposer des aptitudes suivantes :

- Curiosité d'esprit et capacité à élaborer une idée générale intégrée à partir de fragments d'informations dispersées.
- Capacité à rester concentré dans la durée, tout en résistant à des niveaux de stress élevés.
- Bonne connaissance générale de l'informatique et de la cybersécurité, avec de préférence beaucoup d'expérience pratique.

Lorsque vous cherchez à pourvoir un poste dans un SOC, que ce soit par recrutement externe ou par promotion interne, trouver le membre d'équipe ayant les compétences souhaitées et prêtes à l'emploi n'est pas facile. Une formation continue sera nécessaire, non seulement pour combler les écarts entre les compétences actuelles et celles requises, mais aussi pour préparer les membres de l'équipe à gérer des technologies de sécurité et un environnement de menace en constante évolution.

Des compétences en matière de réponse aux incidents, de cyberdiagnostic et d'analyse de programmes malveillants sont indispensables.

GESTION DES INCIDENTS ET CYBERDIAGNOSTIC	ANALYSE DES PROGRAMMES MALVEILLANTS
• Répondre de manière rapide et précise en cas d'incident • Analyser les éléments de preuve (images hdd, vidages de mémoire, traces d'activité réseau), et reconstruire l'historique et la logique de l'incident • Découvrir les sources présumées de l'attaque et d'autres systèmes susceptibles d'être compromis (si possible) • Comprendre la cause fondamentale de l'incident afin de prévenir tout incident similaire	• Obtenir une bonne compréhension de l'échantillon de logiciel suspect et de ses capacités • Préciser s'il s'agit en effet d'un programme malveillant ou non • Déterminer l'impact potentiel de l'échantillon sur les systèmes compromis au sein de l'entreprise • Élaborer un plan de résolution détaillé en se basant sur ce que le comportement du logiciel malveillant a révélé

Kaspersky Lab propose les solutions suivantes : Services de formation à la cybersécurité

Depuis plus de 17 ans, l'expertise en cybersécurité de Kaspersky Lab a évolué et progressé de manière continue (détection des menaces, recherche des programmes malveillants, reverse engineering et cyberdiagnostic inclus). Nos experts savent comment gérer de la meilleure façon les menaces que représentent les 325 000 échantillons de programmes malveillants que nous découvrons chaque jour et comment transmettre ces connaissances et cette expérience pratique aux entreprises confrontées aux nouveaux dangers de la cyberréalité contemporaine.

Notre programme de formation sur la sécurité a été conçu et développé par les génies de la sécurité qui ont contribué à la création des laboratoires anti-virus de Kaspersky Lab et qui inspirent et conseillent aujourd'hui la nouvelle génération d'experts internationaux.

Les cours regroupent des enseignements théoriques et pratiques (ateliers). À la fin de chaque cours, les étudiants sont invités à valider leurs connaissances en passant une évaluation.

Les cours de formation sont adaptés aux professionnels de l'informatique qui possèdent des compétences générales ou avancées en administration de systèmes et en programmation. Tous les cours sont dispensés soit dans les locaux de Kaspersky Lab, soit dans ceux de l'entreprise du client, en fonction des possibilités.

DESCRIPTION DU PROGRAMME

SUJETS	DURÉE	COMPÉTENCES ACQUISES
CYBERDIAGNOSTIC		
• Présentation du 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 • Appliquer les outils et les techniques de cyberdiagnostic en toute confiance
ANALYSE 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

SUJETS	DURÉE	COMPÉTENCES ACQUISES
CYBERDIAGNOSTIC AVANCÉ		
• Investigations approfondies dans Windows • Récupération des données • Investigations sur le réseau et le Cloud • Investigations au niveau de 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		
• 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 qui stockent le fichier exécutable sous forme chiffrée) • Reverse engineering des menaces APT (couvre un scénario d'attaque APT, des e-mails de phishing aux cas les plus complexes) • Analyse des protocoles (analyse chiffrée des protocoles de communication C2, décryptage du trafic) • Analyse des rootkits et des bootkits (débogage du secteur de démarrage en utilisant Ida et VMWare, débogage du 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 pièges d'anti-engineering (obfuscation, anti-débogage) • Être en mesure d'appliquer une analyse avancée des logiciels malveillants pour décortiquer les rootkits/bootkits • Être en mesure d'analyser les shellcodes intégrés dans les différents types de fichiers et les programmes malveillants autres que Windows
RÉPONSE AUX INCIDENTS		
• Présentation de 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

Les outils évoluent avec le temps, mais les bases et les méthodes de travail restent cohérentes. Cela permet aux participants de recevoir un ensemble d'outils et d'instructions, mais également de comprendre les principes et fonctionnalités essentiels. Tous les travaux pratiques sont dans la mesure du possible basés sur des cas réels, en respectant la confidentialité du client.

SURVEILLANCE ET RECHERCHE DES MENACES

À l'origine, le SOC a été conçu pour fournir :

- La gestion des appareils de sécurité, la maintenance du périmètre et des technologies de sécurité préventive telles que les solutions IPS/IDS, les pare-feu, les proxies, etc.
- La surveillance des événements de sécurité via un système de gestion des événements et des informations de sécurité (SIEM).
- Le diagnostic et la résolution des incidents.
- La conformité interne ou réglementaire (par ex : PCI-DSS).

De nombreuses entreprises envisagent à présent d'accroître la visibilité des menaces en établissant leurs propres SOC. Cependant, certaines entreprises disposant déjà d'un SOC estiment qu'elles rencontrent toujours les mêmes problèmes.
Les raisons à cela sont multiples :

- Mauvaise définition des priorités, ce qui signifie que les menaces réelles disparaissent parmi les milliers d'alertes de sécurité sans importance reçues et analysées chaque jour.
- Résolution des incidents sans une réelle compréhension des TTP (Tactiques, Techniques et Procédures) des auteurs de menaces impliqués. Par conséquent, des attaques avancées sont négligées.
- Faux négatifs en raison de l'absence de données sur les menaces correspondantes.
- Approche réactive face aux incidents, au lieu d'une « chasse » proactive des menaces non découvertes mais pourtant actives au sein de l'entreprise.
- Absence d'une vue d'ensemble stratégique sur le paysage des menaces actuel et d'une prise en compte des attaques contre des entreprises similaires et des contre-mesures disponibles.

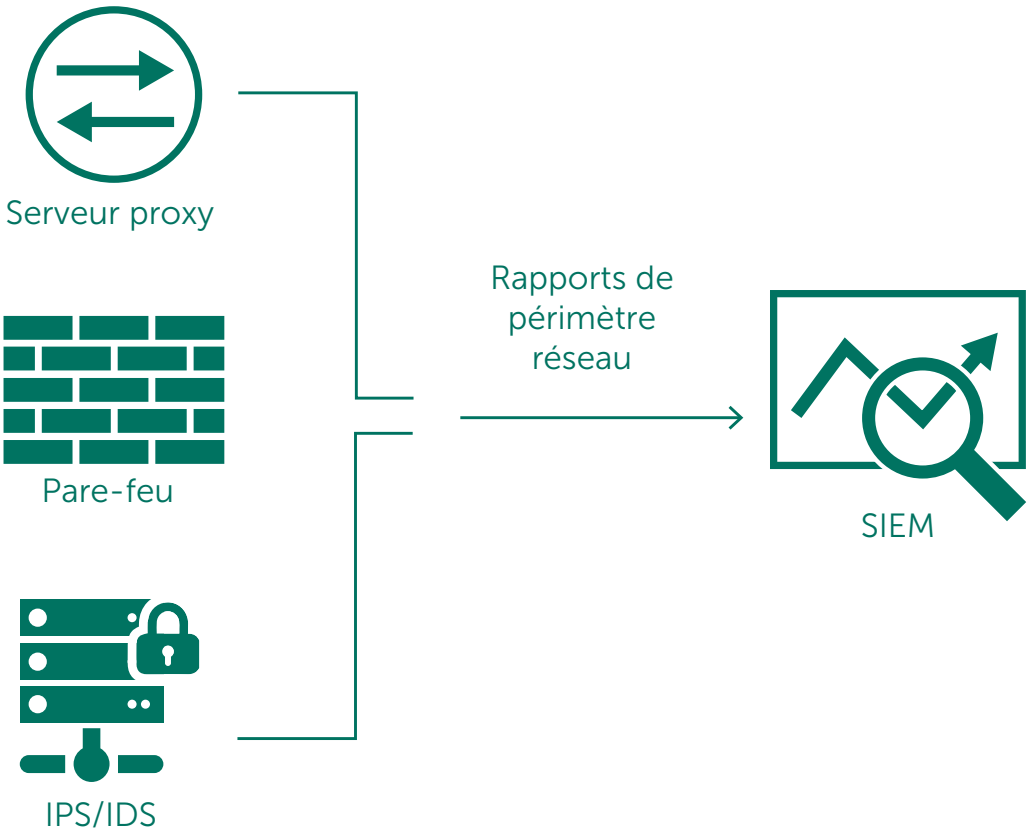


Figure 2 :
Un SOC conventionnel

- Difficultés en interne à attirer des investissements adéquats dans des technologies de sécurité spécifiques, en raison de difficultés à transmettre des informations sur les risques que représentent les violations de sécurité sur les processus métier aux hauts responsables n'ayant pas d'expertise technique.

Gartner définit la surveillance des menaces ainsi :
« Les connaissances fondées sur des données empiriques, telles que le contexte, les mécanismes, les indicateurs, les implications et les conseils pratiques sur les menaces existantes et nouvelles ou sur un risque pour les ressources, peuvent être utilisées pour éclairer les décisions concernant la réaction du sujet face à cette menace ou à ce risque. »

Gartner, How Gartner Defines Threat Intelligence, February 2016

À partir de ces considérations, les responsables de sécurité seraient bien avisés de suivre une approche de SOC reposant sur la veille stratégique. Pour que le SOC soit efficace, il doit continuellement s'adapter aux nouvelles technologies et aux nouveaux moyens de contrôle, en fonction des changements radicaux qui se produisent dans l'environnement de menace actuel.

Combiner les données relatives aux menaces internes et les informations recueillies à partir de différentes sources (par ex : OSINT ou fournisseurs de solutions de protection contre les programmes malveillants) permet de comprendre les techniques d'attaque et leurs indicateurs potentiels. Ceci permet également aux entreprises de développer des stratégies de défense efficaces contre les attaques primaires ou avancées ciblant des entreprises spécifiques.

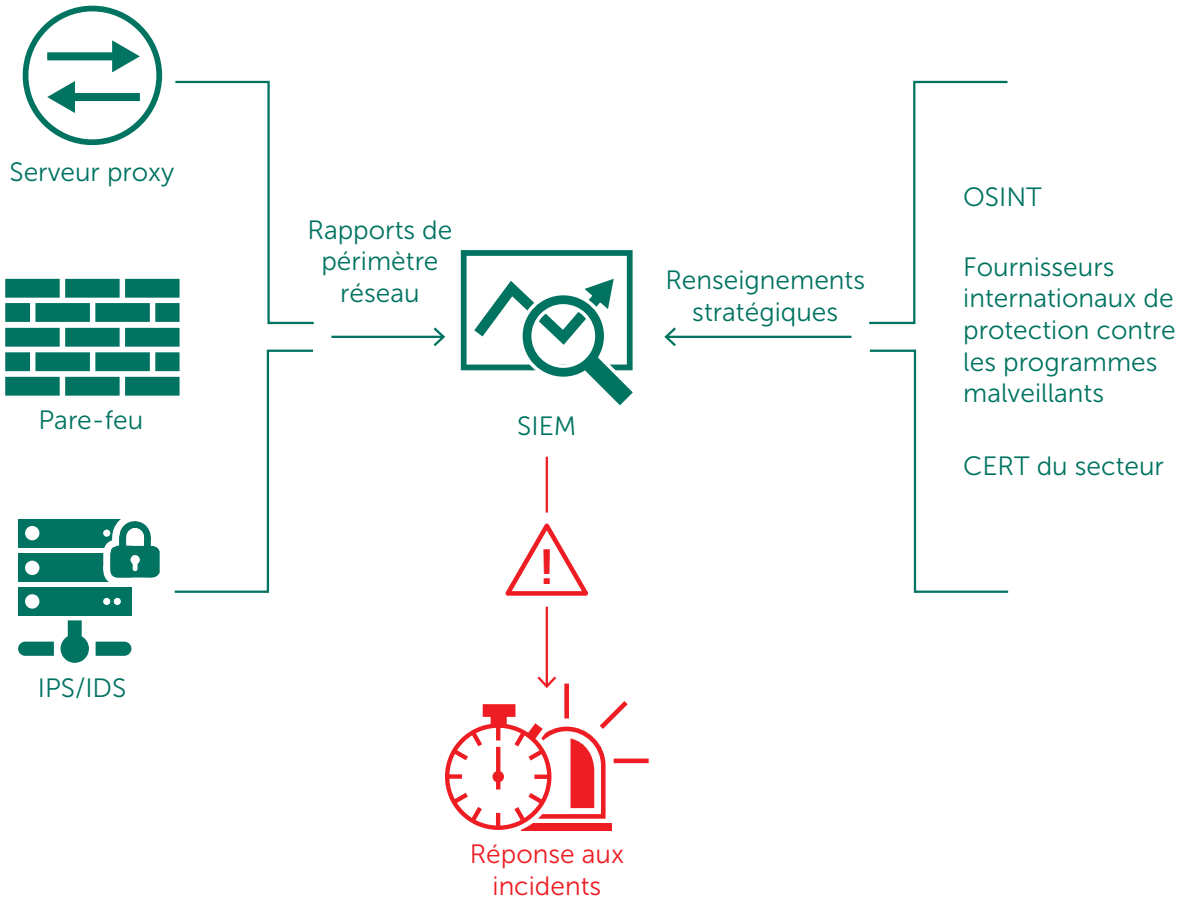


Figure 3 :
Le SOC basé sur la veille stratégique

Les sources de renseignements doivent être soigneusement sélectionnées. Il existe une corrélation directe entre la qualité des informations utilisées et l'efficacité des décisions prises en fonction de ces informations. Si vous vous appuyez sur des informations non pertinentes, inexactes ou qui ne correspondent pas à vos objectifs commerciaux, ou encore si les informations sur les menaces ne sont pas reçues rapidement, la qualité du processus décisionnel de votre entreprise peut être sérieusement compromise.

Des données brutes sans contexte ne fourniront pas la pertinence requise pour que les équipes de SOC soient pleinement efficaces. Par exemple, savoir qu'une URL spécifique est malveillante est très différent que de savoir qu'elle est utilisée pour exploiter une faille ou un type de programme malveillant particulier. Ce surcroît d'informations indique à vos experts en sécurité ce à quoi il faut prêter attention lorsqu'ils explorent une machine infectée.

Ce qu'il faut rechercher dans les sources externes d'informations sur les menaces :

- Des informations ayant une portée internationale, procurant une grande visibilité sur les attaques
- Un fournisseur ayant de l'expérience dans le repérage précoce de nouveaux indicateurs de menace
- Des renseignements riches en contexte et pouvant être utilisés immédiatement
- Des formats de livraison et des mécanismes permettant une intégration simplifiée dans les systèmes de contrôle de sécurité existants

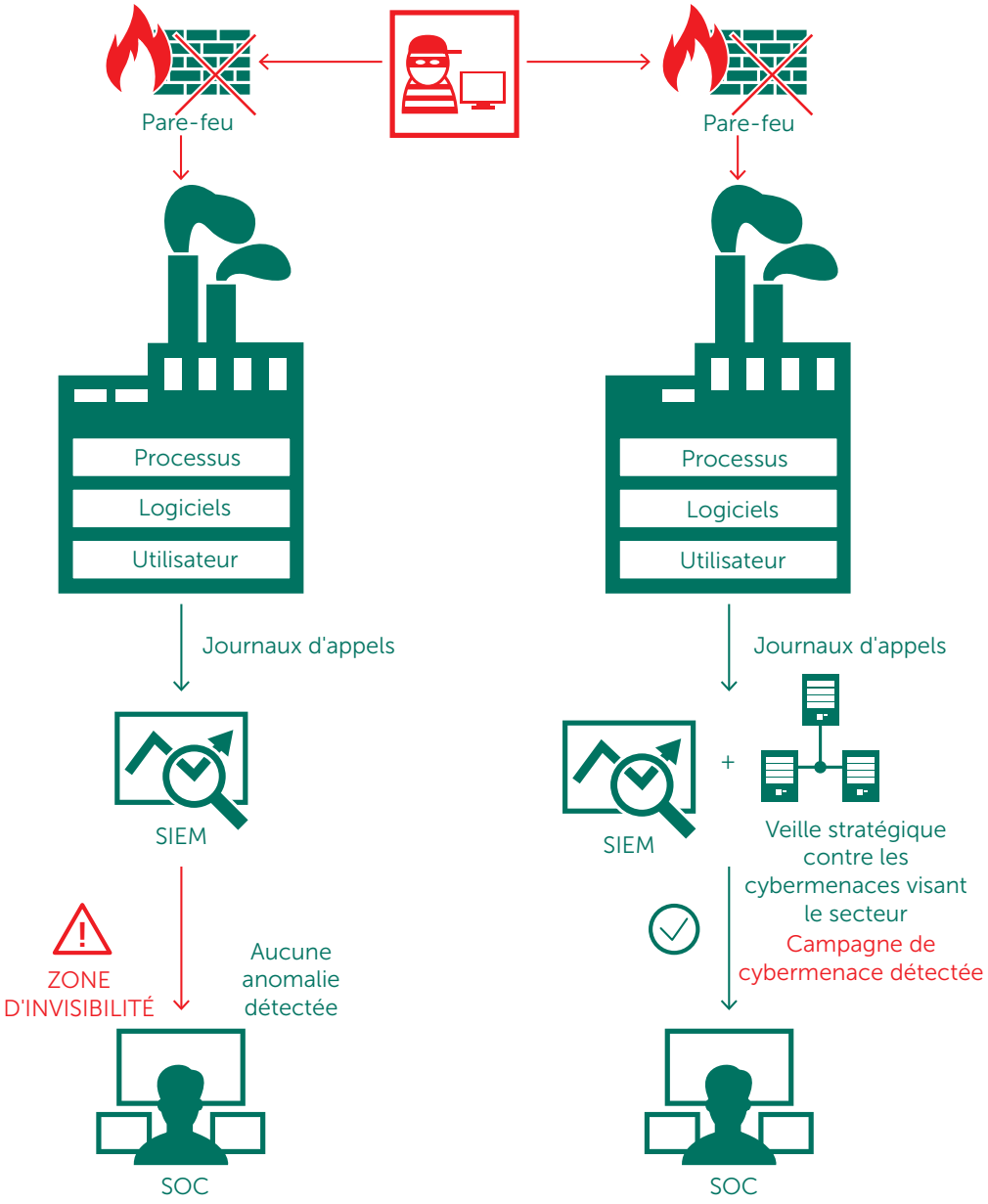


Figure 4 :
Modèle de veille stratégique

La recherche des menaces est également un élément important des opérations quotidiennes du SOC. Ce n'est pas un concept nouveau. La détection des menaces inconnues et avancées repose sur l'intervention manuelle fastidieuse des analystes en charge de la sécurité, plutôt que sur des règles automatisées ou des mécanismes de détection basés sur les signatures.

Ce processus implique de rassembler différentes techniques (comme l'analyse statistique, l'apprentissage automatique et la visualisation) et de les appliquer à toutes les données disponibles obtenues à partir de terminaux, de réseaux, de contrôles de sécurité mis en œuvre, de systèmes d'authentification, etc. L'objectif est de confirmer une hypothèse existante à propos du piratage potentiel. Parmi les technologies de recherche des menaces auxquelles l'analyste peut avoir recours figurent les systèmes déjà mentionnés, comme les solutions SIEM, OSINT, les plates-formes de surveillance des menaces et d'autres sources de données.

L'analyste en charge de la recherche de données consulte des indicateurs de compromission (IOC) récupérés en externe et applique des outils spécialisés pour rechercher ces artefacts (sous la forme d'adresses IP, de hashes de fichiers, d'URL, etc.) sur les hôtes de l'entreprise. Dès la détection d'un signe évident d'atteinte à la sécurité, des procédures de réponse aux incidents peuvent être appliquées.

La recherche et l'identification, au sein d'importants volumes de données, d'artefacts que des mesures automatisées n'ont pas réussi à détecter constituent une tâche qui s'adresse à des professionnels expérimentés et hautement qualifiés.

Kaspersky Lab propose les solutions suivantes : Flux d'informations sur la surveillance des menaces

Kaspersky Lab propose en permanence des flux d'informations mis à jour sur la surveillance des menaces afin d'informer votre équipe SOC sur les risques et implications associés aux cybermenaces, vous aidant ainsi à atténuer les menaces plus efficacement et à vous défendre contre les attaques avant même qu'elles ne soient lancées.

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 données de listes blanches : ensemble de hashes de fichiers fournissant des solutions et des services tiers avec des connaissances détaillées des logiciels authentiques.

Sources de hashes malveillants : couvrant les nouveaux programmes malveillants les plus répandus et les plus dangereux.

Sources de hashes malveillants mobiles : ensemble de hashes de fichiers permettant de détecter les objets malveillants qui infectent les plateformes mobiles.

Flux d'informations 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 de botnet mobiles : ensemble d'URL avec contexte couvrant les serveurs C&C de botnet mobiles.

LES POINTS FORTS DU SERVICE

- Les flux d'informations sont générés en temps réel et de manière automatique, en fonction de résultats obtenus dans le monde entier (Kaspersky Security Network permet une visibilité sur une proportion considérable de l'ensemble du trafic Internet, couvrant des dizaines de millions d'utilisateurs dans plus de 200 pays), afin de garantir un taux de détection élevé et une bonne précision.
- Pour tous les flux de données, chaque dossier est enrichi de contexte pouvant donner lieu à des actions (noms des menaces, horodatages, géolocalisation, adresses IP résolues de ressources Web infectées, hashes, popularité, etc.). Les données contextuelles permettent de mettre en évidence la situation globale, étayant et soutenant ainsi une large utilisation des données. Les données mises en contexte peuvent être plus facilement utilisées pour répondre aux questions telles que qui, quoi, où et quand, ce qui vous permet d'identifier vos adversaires, vous aidant à prendre des décisions opportunes, ainsi qu'à adopter des mesures qui protégeront votre entreprise en particulier.
- L'utilisation de formats de diffusion simples et légers (JSON, CSV, OpenIoC, STIX) faisant appel au protocole HTTPS ou à des mécanismes de distribution ad hoc simplifie l'intégration des flux dans les solutions de sécurité.
- Les informations sur les menaces sont générées et surveillées par une infrastructure hautement tolérante aux pannes, assurant une disponibilité permanente et des performances constantes.
- La solution propose une intégration prête à l'emploi avec HP ArcSight, IBM QRadar, Splunk et d'autres produits.

Kaspersky Threat Lookup

Kaspersky Threat Lookup fournit toutes les connaissances acquises par Kaspersky Lab sur les cybermenaces et leurs relations, regroupées au sein d'un service Web unique et efficace. Le but est de fournir à vos équipes de SOC 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 de 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.

LES POINTS FORTS DU SERVICE

- Informations de confiance : un des principaux atouts de Kaspersky Threat Lookup est la fiabilité de nos données sur la surveillance des menaces, qui sont enrichies d'un contexte pouvant donner lieu à des actions. Les produits de Kaspersky Lab arrivent en tête dans les tests anti-malware[1] et démontrent la qualité inégalée de nos renseignements sur la sécurité en offrant les taux de détection les plus élevés, avec un nombre de faux positifs quasi nul.
- Niveaux élevés de couverture en temps réel : la surveillance des menaces est générée en temps réel de manière automatique, en fonction de résultats obtenus dans le monde entier et elle est prise en charge par Kaspersky Security Network.
- 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.

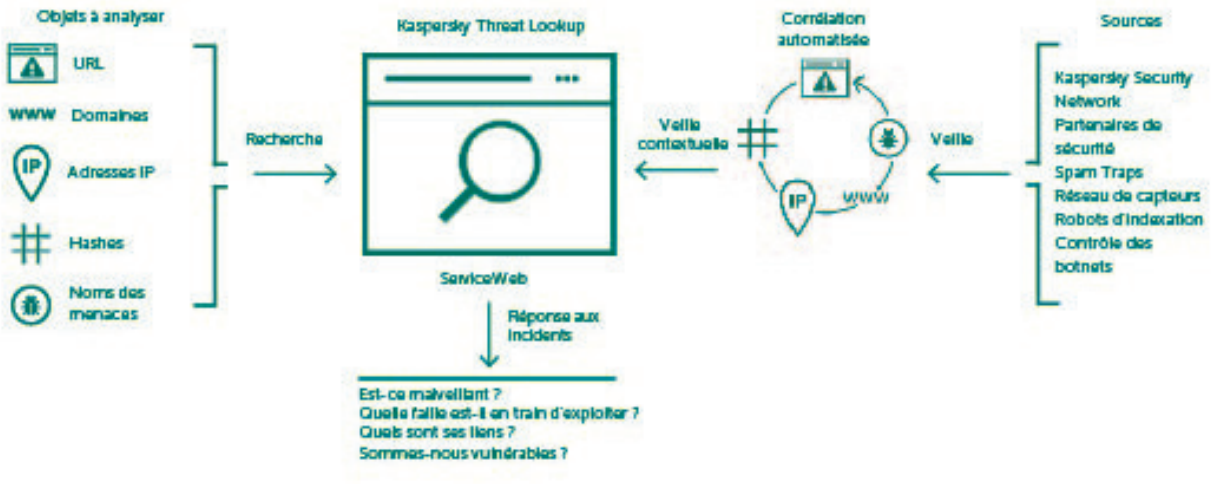
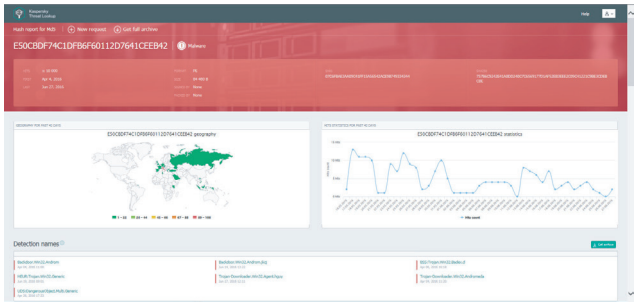
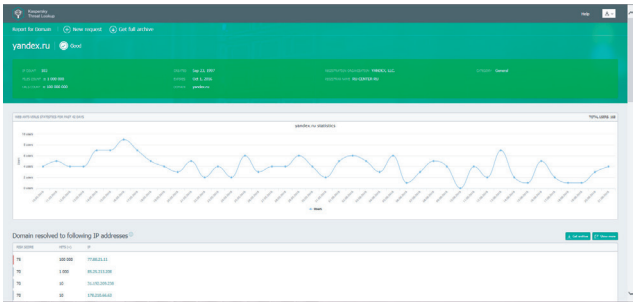


Figure 5 :
Kaspersky Threat Lookup

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

- Analyse des sandboxes : 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 pouvant donner lieu à des actions 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.
- 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.





Rapports de surveillance des menaces persistantes avancées (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 à découvrir nos recherches les plus récentes grâce à notre rapport de surveillance sur les APT exclusif, détaillé et pouvant donner lieu à des actions.

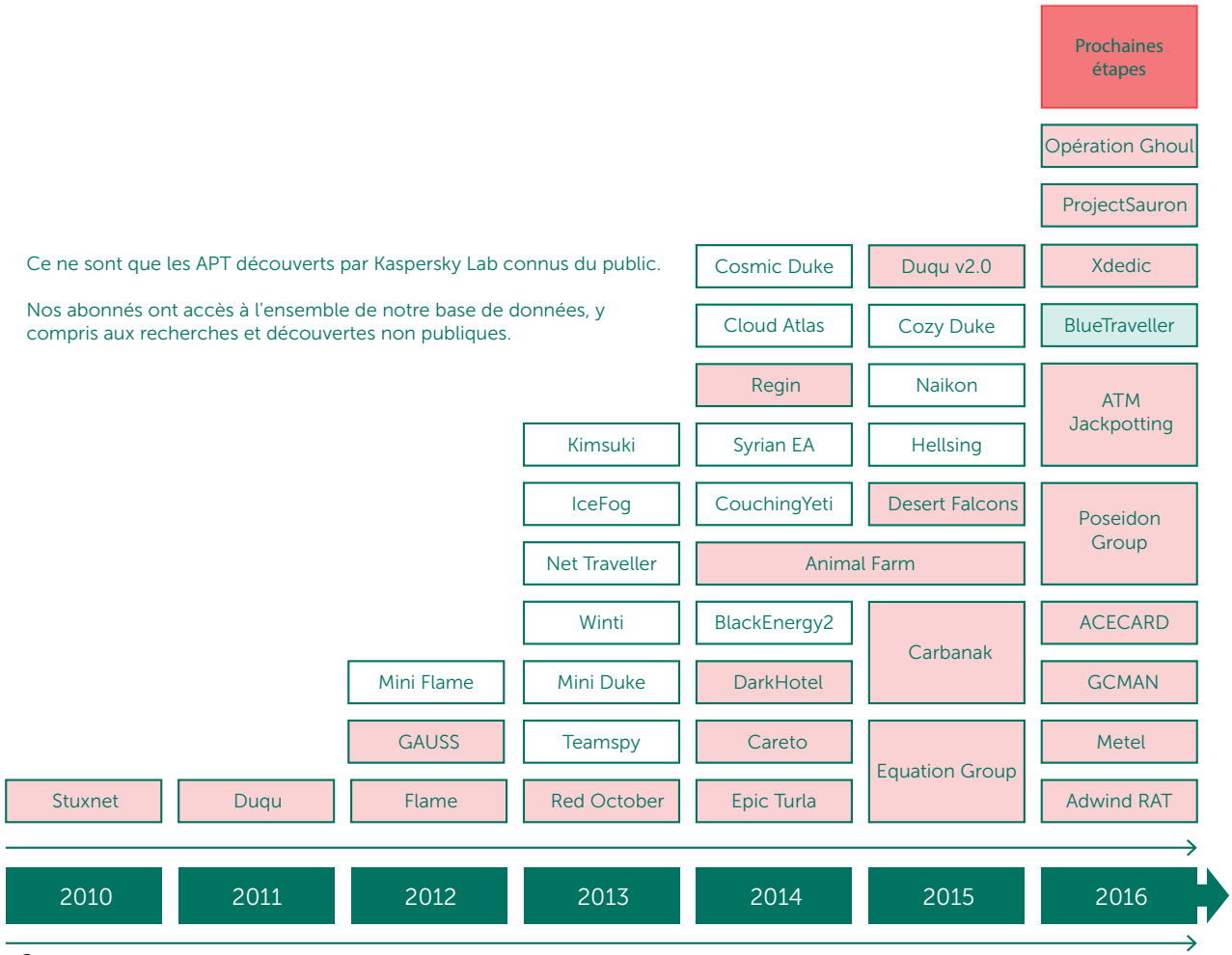


Figure 6 :
Menaces APT découvertes par Kaspersky Lab

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 différents formats sur chaque menace APT découverte et 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 cybercriminels et de cyberterroristes. 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 POINTS FORTS DU SERVICE

- 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 le format openIOC, 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).
- Analyse rétrospective : accès garanti à tous les rapports privés précédents durant toute la période de votre abonnement.

D'un point de vue pratique, les indicateurs de compromission constituent la partie la plus utile du rapport pour les experts d'un SOC. Ces informations structurées sont fournies pour utilisation ultérieure avec des outils automatisés spécifiques qui aident à contrôler les signes d'infection sur votre infrastructure.
Tous les rapports sont fournis via le portail de surveillance des menaces APT, comme illustré ci-dessous.

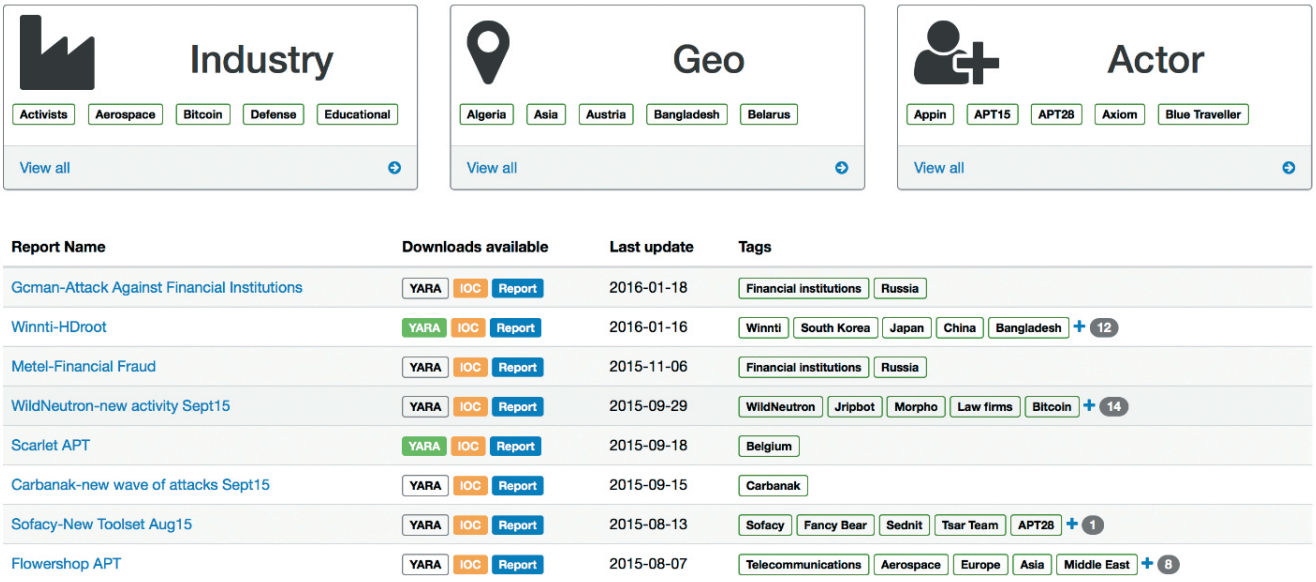


Figure 7 :
Portail de surveillance des menaces APT

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, qui 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 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 personnels des employés, qui seraient susceptibles de devenir les cibles potentielles d'une attaque.
- **L'analyse du suivi des activités des logiciels 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 APT peuvent rester cachées 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 menaces APT contre 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 à l'extérieur, y compris les applications gouvernementales vulnérables, les équipements de télécommunication, les composants des systèmes de contrôle industriel (SCADA, PLC, etc.), les guichets automatiques, etc.
- **L'analyse du suivi des activités des logiciels malveillants et des cyberattaques** : identification et analyse des campagnes APT, des échantillons, actifs et inactifs, de logiciels 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 et susceptibles d'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 d'accès 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).

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.

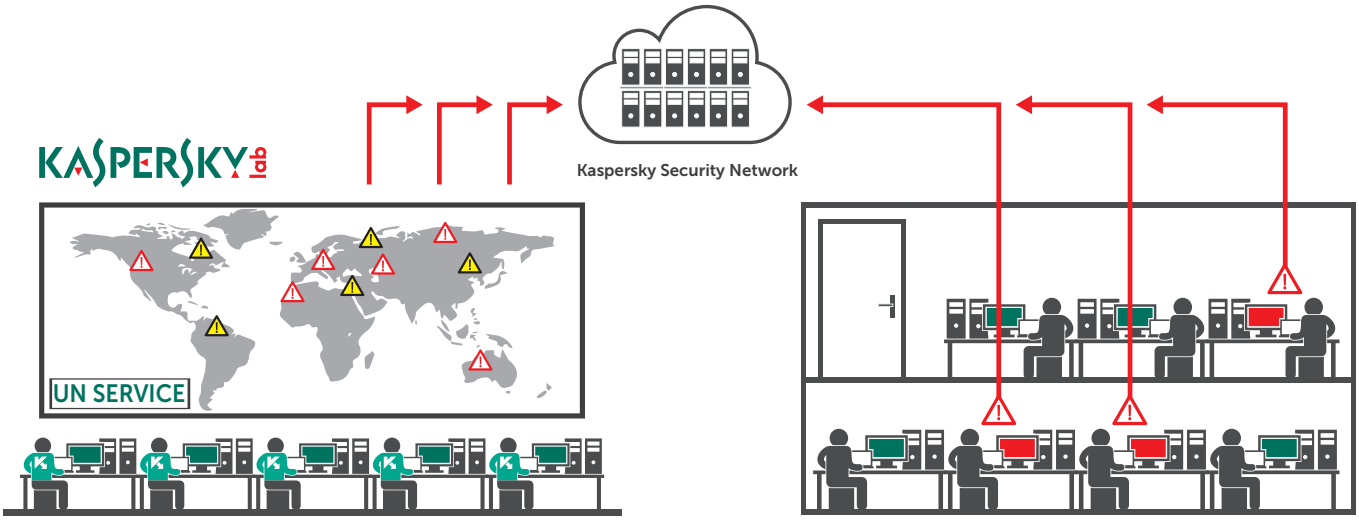


Figure 8 :
Kaspersky Managed Protection

LES POINTS FORTS DU SERVICE

- Un niveau élevé 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 de type « zero-day ».
- L'analyse rétrospective des incidents et la recherche des 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.
- Une 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 concernant la sécurité des informations.
- Lance les mises à jour de bases de données antivirus nécessaires pour empêcher la propagation des menaces.

En savoir plus sur les sources d'informations concernant les menaces de Kaspersky Lab

La surveillance des menaces constitue un ensemble issu du mélange de 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 que vous disposez d'un personnel compétent et formé de manière appropriée, d'informations sur la surveillance des menaces acquises auprès de sources fiables et mises en œuvre dans les contrôles de sécurité existants, il est temps de vous pencher sur votre capacité de réaction aux incidents.

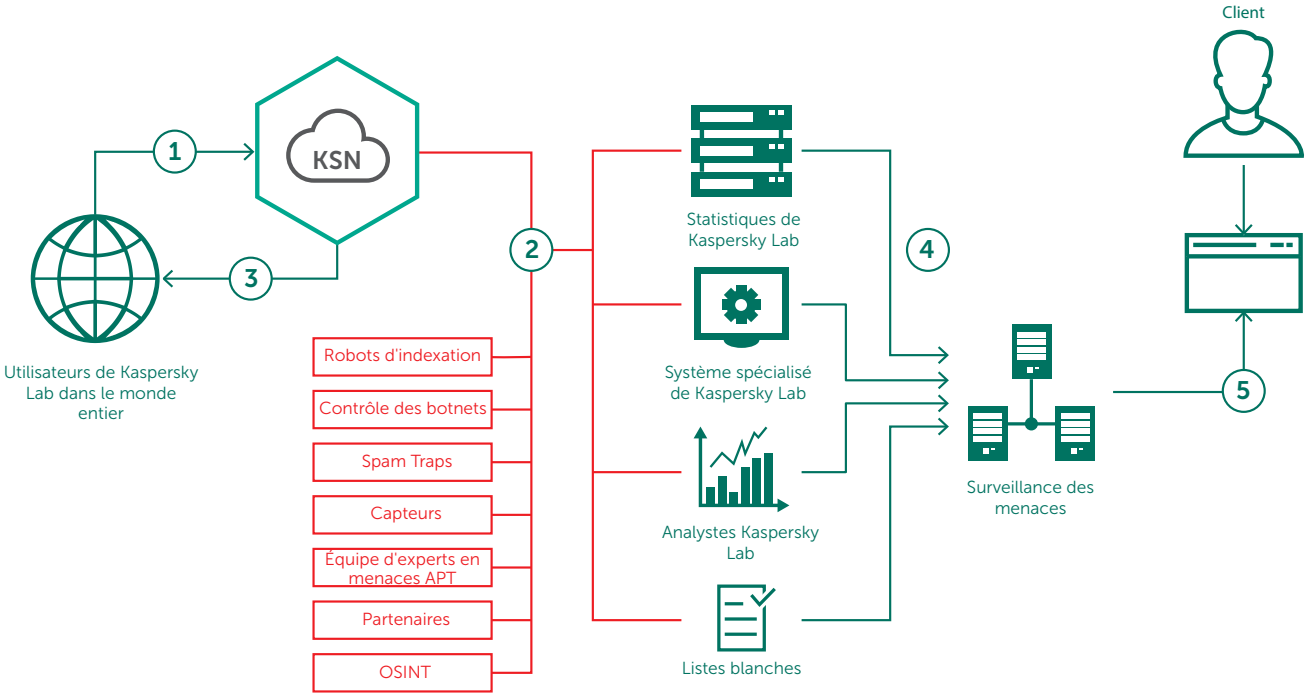


Figure 9 :
Sources d'informations sur les menaces de Kaspersky Lab

PROCÉDURE DE RÉPONSE AUX INCIDENTS

En cas d'incident, le diagnostic et la réponse nécessitent l'affectation de ressources internes considérables avec un délai d'annonce très court ou sans notification préalable. Des spécialistes compétents dotés d'une grande expérience pratique dans la lutte contre les cybermenaces devront agir rapidement pour identifier, isoler et bloquer les activités malveillantes. La rapidité est essentielle pour minimiser les conséquences et les coûts d'actions correctives.

Maîtriser ce niveau d'expertise dans un délai très court peut être difficile, même pour une équipe de SOC bien établie : peu d'entreprises ont suffisamment de ressources internes disponibles pour arrêter une attaque avancée dans sa course. Il peut de plus y avoir des cas (par exemple, des menaces complexes commanditées par un État ou des menaces APT) où l'équipe du SOC manque d'expertise en ce qui concerne les approches et les tactiques spécifiques utilisées par les acteurs impliqués dans l'APT.

Dans des cas comme ceux-ci, il peut être plus rentable et productif de collaborer avec un fournisseur tiers de solution de réponse aux incidents ou avec une entreprise de conseil, qui sera en mesure d'appliquer une réponse rapide et pleinement éclairée.

Un cadre de réponse aux incidents complet doit inclure :

- **Identification de l'incident**
  Analyse initiale de l'incident et mise à l'écart des systèmes infectés
- **Acquisition d'éléments de preuve**
  Selon le type d'incident, différentes sources devront être inspectées pour obtenir les éléments de preuve nécessaires
- **Analyses criminalistiques (si nécessaire)**
  À ce stade, une image détaillée de l'incident peut être établie
- **Analyses de programmes malveillants (si nécessaire)**
  Afin de mieux comprendre les capacités de logiciels malveillants donnés
- **Plan des actions correctives à mettre en place**
  Élaboration d'un plan visant à éradiquer la cause fondamentale du problème et toutes traces du code malveillant
- **Enseignements tirés**
  Vérification et mise à jour des contrôles de sécurité existants pour éviter des incidents similaires

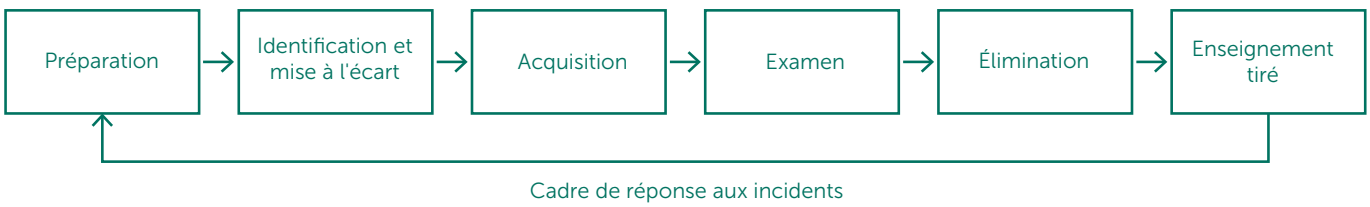


Figure 10 :
Cadre de réponse aux incidents

Kaspersky Lab propose les solutions suivantes : Services de réponse aux incidents

Le service de réponse aux incidents est un service haut de gamme : il 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. Les enquêtes de Kaspersky Lab sont menées 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.

Les objectifs suivants doivent être atteints lors de la mise en œuvre du service :

- Identifier les ressources compromises.
- Isoler la menace.
- Empêcher la propagation de l'attaque.
- 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 de votre infrastructure informatique à l'aide d'outils pour identifier 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.

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

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 DU SERVICE

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

- Par abonnement
- En réponse à un incident ponctuel

Ces deux options dépendent du temps que nos experts consacrent à la résolution de l'incident. Ceci est négocié avec le client avant la signature du contrat. Le client peut inclure à sa guise autant d'heures de travail qu'il le juge nécessaire ou suivre les recommandations de nos experts adaptées à chaque cas particulier.

POURQUOI KASPERSKY LAB ?

Parce nous avons :

- Des partenariats avec des organismes du maintien de l'ordre du monde entier, notamment Interpol et de nombreux CERT
- Des outils basés dans le Cloud assurant le suivi en temps réel de millions de cybermenaces dans le monde entier
- Des équipes internationales chargées de l'étude et de l'analyse de cybermenaces de toutes sortes

Parce que nous sommes :

- Le plus grand éditeur indépendant de logiciels de sécurité au monde, axé sur la surveillance des menaces et le leadership technologique
- Le leader incontestable en matière de résultats aux tests indépendants de détection de programmes malveillants
- Reconnus comme un leader par Gartner, Forrester et IDC

À propos de Kaspersky Lab

Kaspersky Lab est le plus grand éditeur privé mondial de solutions de protection des terminaux. La société fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité pour utilisateurs de terminaux. Depuis plus de 18 ans, Kaspersky Lab fait figure de précurseur dans le domaine de la sécurité informatique, fournissant des solutions de sécurité numérique efficaces aux entreprises, PME et particuliers. Ayant sa holding enregistrée au Royaume-Uni, Kaspersky Lab opère actuellement dans près de 200 pays et territoires du monde entier et propose une protection à plus de 350 millions d'utilisateurs.


Twitter.com/
kasperskyfrance


Facebook.com/
kasperskylabfrance


Youtube.com/
Kaspersky

Kaspersky Lab
www.kaspersky.fr

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

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

KASPERSKY lab