#TrueCybersecurity

Plate-forme Kaspersky Anti Targeted Attack

Réduire le risque d'attaques ciblées et de menaces avancées

Bénéfices

- Réduire les dommages financiers et opérationnels causés par la cybercriminalité
- Limiter les interruptions des processus métiers stratégiques
- Éviter les actions en justice coûteuses ainsi que les problèmes de réglementation et de conformité
- Éviter les coûts des mesures correctives (comme les formations supplémentaires, la dotation en personnel ou le renforcement du système)

VOTRE ORGANISATION EST-ELLE CIBLÉE ?

Les techniques développées pour cibler les grandes entreprises sont en constante évolution. Pourtant, bien trop d'organisations persistent à utiliser des technologies de sécurité obsolètes pour se protéger contre la cybercriminalité actuelle. La clé de la détection des attaques ciblées repose sur la capacité à détecter les changements subtils dans les comportements des systèmes, signes d'une faille de sécurité. Dès lors qu'une menace est détectée, l'atténuation doit aller de pair avec l'analyse des menaces. Ainsi, l'expérience et les connaissances acquises permettent d'affiner constamment votre stratégie de sécurité.

VOTRE SÉCURITÉ EST-ELLE SUFFISANTE ?

Les attaques ciblées fructueuses ont généralement recours à de nombreuses techniques et exploitent plusieurs zones de vulnérabilité différentes. Comprendre les outils et techniques de votre adversaire est essentiel pour renforcer et affûter la stratégie de sécurité de votre entreprise. Si vous ne savez pas comment réagir à une attaque et comment ajuster votre stratégie en conséquence, la détection en elle-même devient alors presque inutile. Quelle que soit la qualité des technologies dont vous disposez, les problèmes persisteront tant que vous n'aurez pas élaboré une stratégie de sécurité fiable et évolutive.

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

« La solution de Kaspersky Lab a remarquablement bien fonctionné lors du cycle de test : elle est parvenue à détecter 99,44 % des menaces auparavant inconnues et a montré une redoutable efficacité en matière de détection des menaces face à près de 550 menaces nouvelles ou peu connues »

–Rapport sur les tests de certification de défense contre les menaces avancées, ICSA, quatrième trimestre 2016

Une protection avancée dépend d'une détection avancée

Grâce à l'association unique de technologies et de services consolidés par l'un des meilleurs services de veille stratégique au monde, Kaspersky Lab aide les entreprises à atténuer les risques, à détecter plus rapidement les attaques ciblées, à gérer les menaces en temps réel et à améliorer leur protection contre de futures attaques.

La plate-forme Kaspersky Anti Targeted Attack utilise un système de détection des menaces multi-niveaux dit « détection avancée », destiné à protéger les entreprises contre les attaques les plus sophistiquées. Cette détection avancée comprend notamment une évaluation granulaire des activités survenant sur le réseau de l'entreprise. Elle est également renforcée par une détection des hôtes associés aux attaques ciblées, grâce à une base de données continuellement mise à jour des serveurs actifs de commande et de contrôle, des sites Web nocifs et des points de distribution de programmes malveillants. Ces données issues de la veille de l'équipe GReaT* de Kaspersky Lab permettent même la détection des menaces les plus récentes.

*Global Research and Analysis Team : *équipe internationale Kaspersky Lab de chercheurs et analystes*

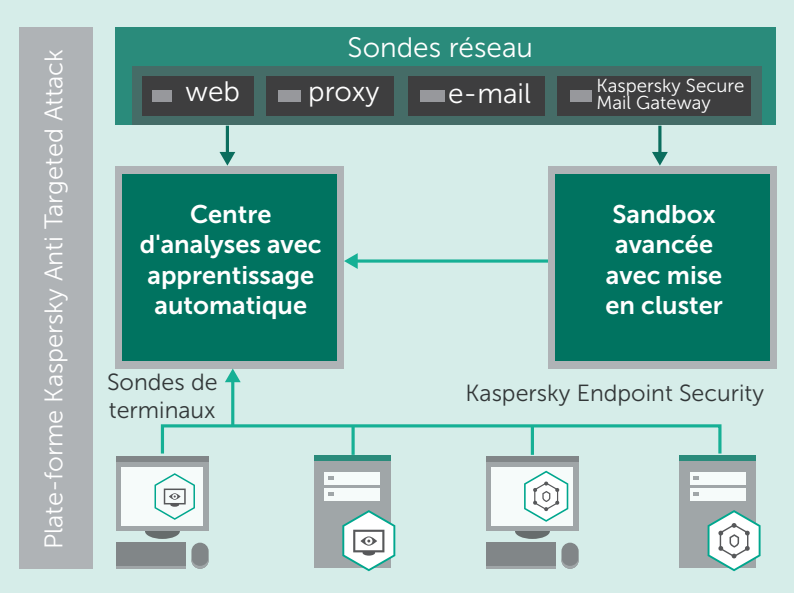
Nouveautés de la plate-forme Kaspersky Anti Targeted Attack

- Intégrée à Kaspersky Secure Mail Gateway – empêchez les cybercriminels de pénétrer dans votre périmètre
- Interface Web simplifiée – un flux de travail sans effort et une meilleure visibilité
- Notification rapide des menaces – soyez immédiatement alerté des incidents de gravité élevée
- Rapports personnalisés – ils pourront être intégrés aux présentations faites à votre direction
- Suivi personnel VIP pour les systèmes critiques – bénéficiez d'analyses prioritaires
- Contrôle d'accès basé sur les rôles – des scénarios à l'échelle de l'entreprise pour protéger les données sensibles
- Performances et flexibilité améliorées grâce à une sandbox avec mise en cluster et une prise en charge de l'environnement ESXi
- Corrélation d'événements améliorée et reconstitution de la chaîne de frappe – connectez les événements entre eux pour avoir une vision toujours plus claire

Architecture de la solution

La plate-forme Kaspersky Anti Targeted Attack combine une analyse dynamique basée sur une sandbox avec des capacités d'apprentissage automatique avancées pour vous protéger contre un large éventail de menaces. La plate-forme comprend :

- **une architecture de sondes multi-niveaux pour vous donner une visibilité à 360 degrés**
  Grâce à une combinaison de sondes réseau, Web et messagerie électronique, ainsi que de sondes de terminaux, la plate-forme Kaspersky Anti Targeted Attack fournit une détection avancée à chaque niveau de l'infrastructure informatique de votre entreprise.
- **une sandbox avancée pour évaluer les nouvelles menaces**
  Issue d'une élaboration continue de plus de 10 ans, notre sandbox avancée offre un environnement isolé et virtuel où les objets suspects peuvent être exécutés en toute sécurité, afin d'en observer le comportement.
- **des moteurs d'analyse puissants pour des diagnostics rapides et moins de faux positifs**
  Notre analyseur d'attaques ciblées évalue les données du réseau et des terminaux saisies par les sondes, puis génère rapidement un rapport de détection des menaces destiné à votre équipe de sécurité.



Une approche stratégique de la sécurité avancée pour les entreprises

La plate-forme Kaspersky Anti Targeted Attack offre une nouvelle approche plus stratégique pour détecter les attaques ciblées. Complétée par nos technologies et solutions de prévention multi-niveaux, ainsi que par un large portefeuille de services de veille stratégique pour la réaction et la prévision, Kaspersky Lab offre une approche réellement intégrée et stratégique de la détection et de la réaction aux attaques ciblées et aux menaces.

Ces technologies et services facilitent les stratégies de sécurité d'entreprise les plus efficaces ainsi que les architectures qui les soutiennent, notamment celles construites sur les piliers que représentent la prévision, la prévention, la détection et la réaction.

Plate-forme Kaspersky Anti Targeted Attack/Janvier 2017/Mondial

KASPERSKY lab