Services de réponse aux incidents de Kaspersky Lab

www.kaspersky.fr
#truecybersecurity

Services de réponse aux incidents de Kaspersky Lab

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.

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.

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.

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.

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

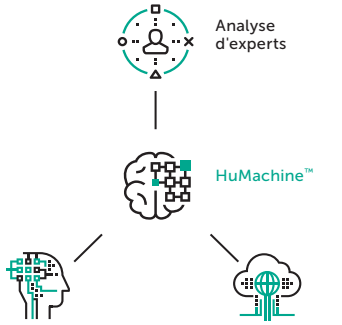
Le cyberdiagnostic peut comprendre l'analyse de programmes malveillants décrite ci-dessus, si un programme malveillant a été découvert au cours de l'investigation. Les experts de Kaspersky Lab rassemblent les éléments de preuve tels que des images HDD, les vidages de mémoire et les traces réseau pour 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.



Solutions de cybersécurité de
Kaspersky Lab pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.fr