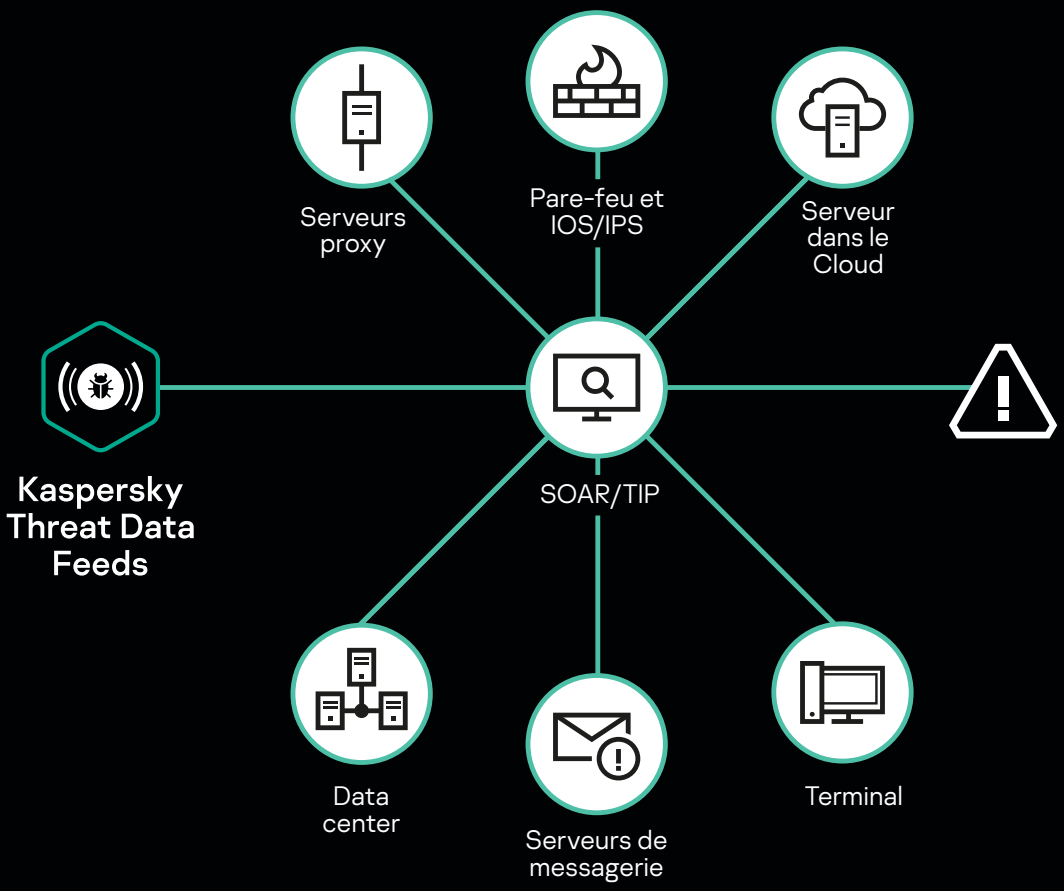
kaspersky BRING ON THE FUTURE

Pourquoi avons-nous besoin de plateformes de Threat Intelligence et comment les sélectionner ?

Les avantages de l'intégration des flux de Threat Intelligence dans les processus et systèmes de sécurité de l'information existants sont évidents. Ils fournissent une liste constamment mise à jour d'indicateurs de compromission actifs (IoC) (le plus souvent des adresses IP malveillantes, des URL ou des hachages d'objets malveillants) avec un contexte supplémentaire qui peut être utilisé pour améliorer la détection de diverses menaces et la réponse à celles-ci.

Si une entreprise ne surveille que les événements qui se produisent à l'intérieur de son réseau et n'utilise pas de données externes sur les IoC, qui sont par exemple actifs dans la zone géographique ou le secteur d'activité de l'entreprise, celle-ci court un plus grand risque de passer à côté d'une activité malveillante se produisant sur le réseau ou de ne pas y réagir. Cela peut être dû, par exemple, au fait qu'elle ne dispose d'aucune information lui permettant de déterminer si une adresse IP particulière avec laquelle un hôte du réseau a établi une connexion est malveillante.



Défis liés à l'opérationnalisation des flux de Threat Intelligence

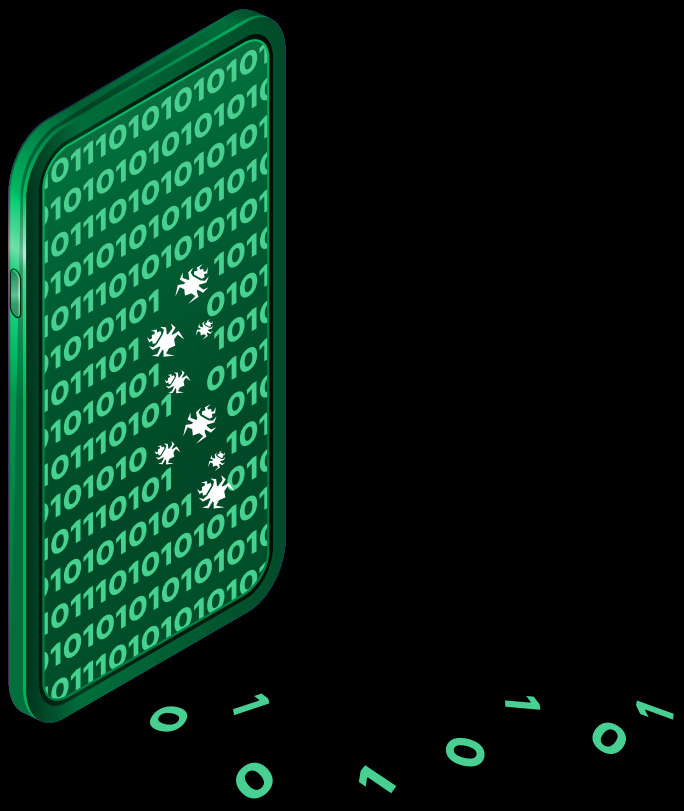
Si les avantages sont évidents, pour pouvoir exploiter efficacement ces avantages liés à l'utilisation des flux de renseignements sur les menaces, plusieurs problèmes doivent avoir été résolus.

Plateformes de Threat Intelligence

Au fur et à mesure que ces problèmes s'accumulaient, il est devenu évident qu'un produit était nécessaire pour les résoudre. Les plateformes de Threat Intelligence (TIP) vous permettent d'utiliser simultanément de nombreux flux différents, de les analyser, puis d'intégrer des IoC déjà vérifiés dans le SIEM afin de détecter l'activité suspecte associée et d'accélérer la suite de la réponse si un incident est confirmé. Toutefois, ces produits présentent également leurs propres nuances.

Tout d'abord, ils sont assez lents. L'importation et l'exportation d'un million d'IoC seulement peuvent prendre plusieurs heures. Or, compte tenu de la vitesse à laquelle les pirates informatiques peuvent modifier leurs infrastructures, ce délai est inacceptable.

Par exemple, un site Web compromis proposant des explications fiscales, lu par votre comptable et des centaines d'autres comptables dans d'autres organisations, peut infecter les ordinateurs des utilisateurs lorsqu'ils le visitent. Une fois qu'ils auront réussi leur attaque, les cybercriminels retireront rapidement la charge malveillante du site Web, qui redeviendra alors tout à fait authentique. Par conséquent, si vous n'êtes pas informé à temps que le site a été infecté, vous risquez de passer à côté de l'incident.



Deuxièmement, s'il est nécessaire de vérifier rétrospectivement les journaux d'événements à l'aide de données sur les menaces nouvellement reçues pour détecter des incidents qui n'avaient pas été détectés auparavant, les plateformes de Threat Intelligence ne seront pas utiles non plus, car elles ne sont pas adaptées à ce type d'opérations. Ils n'offrent également qu'un contrôle limité sur la durée de vie de l'indicateur, tandis que l'utilisation d'indicateurs obsolètes entraînera bien entendu une augmentation du nombre de faux positifs.

Mise en correspondance des données entrantes

L'un des principaux inconvénients de la plupart des plateformes de Threat Intelligence est qu'elles s'appuient sur les mécanismes intégrés au SIEM pour faire correspondre les flux avec les indicateurs contenus dans les journaux d'événements. Pourquoi est-ce un inconvénient ? Tout d'abord, parce que les systèmes SIEM ne sont pas conçus pour gérer autant d'IoC et le contexte qui les accompagne. Si nous chargeons des millions d'indicateurs dans le SIEM, ses performances s'en trouveront fortement réduites. Mais surtout, leur logique de correspondance intégrée et le manque de normalisation des données entrantes laisseront échapper des incidents. Les pirates informatiques utilisent désormais activement des techniques de brouillage pour dissimuler les activités malveillantes dans les journaux d'événements. Et il existe de nombreuses techniques de ce type.

Par exemple, voici un indicateur :

github.com@520966948

De quel type d'indicateur s'agit-il ? Il est impossible de le dire d'emblée, n'est-ce pas ? En fait, il se présentait au départ sous la forme http://31.13.83.36/ et constitue en fait un lien vers https://www.facebook.com. Nous avons présenté l'adresse IP sous forme décimale, ajouté une fausse chaîne d'autorisation et le tour est joué. Le SIEM ne le détectera plus.

Conclusion

Les flux de Threat Intelligence pertinents provenant de sources fiables apportent une réelle valeur ajoutée, tandis que les plateformes de Threat Intelligence peuvent aider à surmonter les problèmes liés à leur gestion et à leur intégration dans les processus de sécurité existants. Toutefois, les clients doivent sélectionner ces produits avec soin afin d'éviter les pièges potentiels. Voici quelques éléments à prendre en compte lors du choix d'une plateforme de Threat Intelligence :

- Assurez-vous qu'elle permet d'importer et d'exporter rapidement les données de Threat Intelligence
- Comprenez où les opérations de mise en correspondance des données ont lieu : sur le SIEM ou du côté de la plateforme de Threat Intelligence
- Précisez si le fournisseur de plateforme de Threat Intelligence exploite les dernières connaissances en matière de techniques de brouillage utilisées par les acteurs de la menace pour dissimuler leur activité dans les journaux
- Assurez-vous que la plateforme prend en charge l'analyse des journaux en masse si vous souhaitez l'utiliser à des fins de recherche rétrospective des menaces

En savoir plus

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : https://www.kaspersky.fr/blog/category/business/
Sécurité informatique pour les PME : https://www.kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : https://www.kaspersky.fr/enterprise-security
Portail de Threat Intelligence : opentip.kaspersky.com
Interactive Portfolio Tool (outil de catalogue interactif) : https://media.kaspersky.com/fr/business-security/enterprise/KL-Enterprise-Catalogue.pdf

www.kaspersky.fr