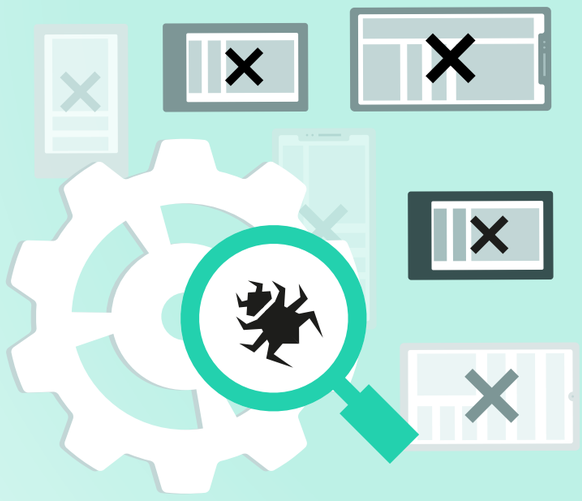
Les 4 mythes de la réponse à incidents

Mythe n °1 :

La réponse prend fin avec l'endiguement de la menace

Mythe Ou le piège de la pensée à court terme. La réponse à incidents, au sens le plus strict, consiste à gérer les conséquences d'une faille de sécurité. Malheureusement, la portée des « conséquences » est souvent sous-estimée. Entre autres, elle devrait inclure une investigation approfondie, une chronologie complète de l'incident et une reconstruction logique.

Solution **Ne vous précipitez pas pour vous remettre en selle dès que vous avez traité un problème causé par un incident. Effectuez une investigation approfondie pour mieux comprendre les causes profondes afin de pouvoir éviter les incidents similaires à l'avenir avec un minimum de perturbations.**



Mythe n °2 :

Les succès se mesure au nombre d'incidents résolus

Mythe La sécurité informatique au XXIème siècle est une activité stimulante, risquée et haletante, qui implique des équipes d'experts rendant compte à une myriade de parties prenantes, dont le PDG, les actionnaires et les organismes de réglementation. Elle constitue également un secteur d'élite ultra-complexe. Il n'est donc guère surprenant que les experts en sécurité informatique mesurent souvent l'efficacité en termes de « tableau de chasse » des cyberincidents.

Solution **Mesurez la valeur des processus de réponse à incidents au moyen des indicateurs de temps moyen de détection et de réponse et prenez en compte des indicateurs plus larges tels que les économies et le niveau de dommage évité (réputation et opérationnel).**

Mythe n °3 :

Vous ne pouvez compter que sur vous-même

Mythe Au lieu de limiter la question de l'externalisation de la réponse aux incidents à « devons-nous répondre en interne OU recruter en externe pour nous aider ? », optez pour une approche combinée. Votre équipe interne compte les experts les plus aptes à gérer la situation, mais vous pouvez recourir à des services externes de réponse aux incidents.

Solution **Recherchez des services de réponse aux incidents qui complètent les efforts de votre équipe en interne. Les services de réponse aux incidents sont l'un des outils les plus indispensables que vos experts peuvent utiliser pour se protéger contre les incidents complexes.**

Mythe n° 4 :

Si vous avez besoin de services de réponse à incidents, vous avez forcément fait quelque chose d'incorrect

Mythe Cela aurait pu être vrai pour les très grandes entreprises matures sur le plan informatique il y a vingt ans, mais c'est loin d'être le cas aujourd'hui en raison de la complexité des menaces et de la nécessité de bénéficier d'une Threat Intelligence mondiale et d'un vaste écosystème de cybersécurité.

Solution **Optimisez la capacité de cybersécurité de votre équipe avec une technologie performante qui lui permettra d'appliquer ses propres processus de réponse à incidents tout en les renforçant par ceux de l'expertise externe si nécessaire.**

Chez Kaspersky, nous comprenons les défis inhérents à la protection contre les APT et les attaques complexes. Kaspersky Expert Security permet à votre équipe d'éliminer les menaces sophistiquées et les attaques de type APT. Conçue à partir d'une plateforme XDR, cette solution inclut des fonctionnalités qui augmentent les superpouvoirs internes de votre équipe de sécurité, avec la Threat Intelligence, la formation et les conseils d'experts.

go.kaspersky.com/expert-fr

kaspersky