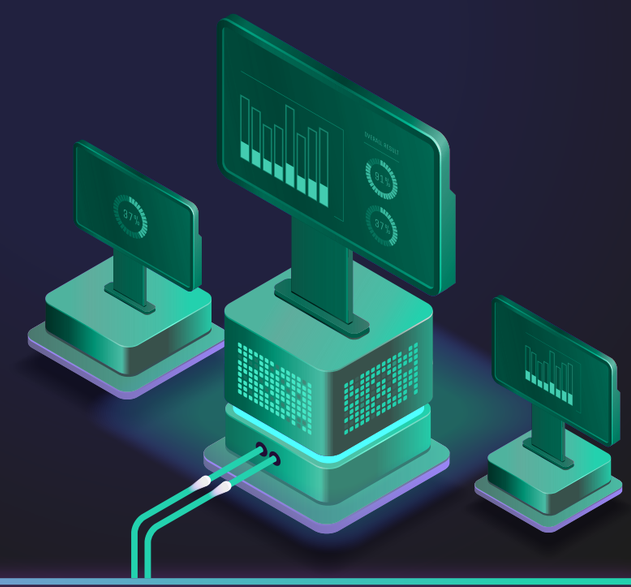
Info ou intox ? Top 5 des mythes concernant le SOC

Avec un marché potentiel global des centres opérationnels de sécurité (SOC) estimé à 30 milliards de dollars, le potentiel de valorisation de votre investissement dans un SOC est plus fort que jamais. Examinons ensemble à la loupe l'effet de mode (justifié) qui entoure les SOC, en questionnant certains des mythes les plus courants qui entourent cette solution incroyable offrant davantage de résilience, d'efficacité et de protection face aux menaces modernes.



Mythe n °1 :

C'est tout ou rien

Le mythe :

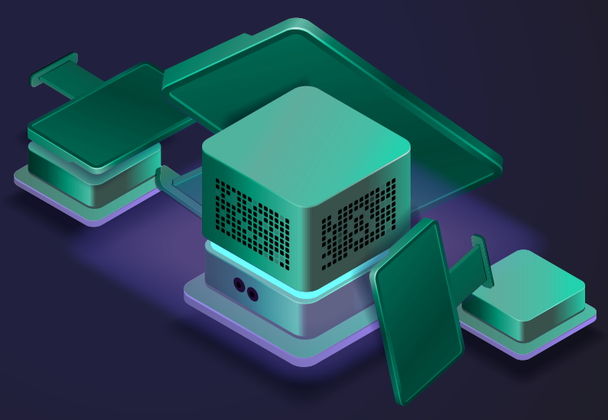
Le SOC est une fonction centralisée permettant de surveiller et d'analyser les menaces en continu. Alors, pourquoi ne pas en créer un en interne ? Malheureusement, ce n'est pas si simple.

La réalité :

En raison des nombreuses contraintes et du panorama des menaces, une autonomie complète pourrait bien n'être ni atteignable, ni même souhaitable. La bonne nouvelle, c'est que vous pouvez relâcher la pression. Au lieu de vous lancer bille en tête dans un SOC indépendant en circuit fermé, vous pouvez opter plutôt pour un modèle hybride en employant vos ressources internes pour maximiser l'expertise spécifique à votre entreprise tout en faisant appel à un partenaire externe pour les tâches expertes plus courantes.

Mythe n °2 :

Le SOC n'obéit qu'à lui-même



Le mythe :

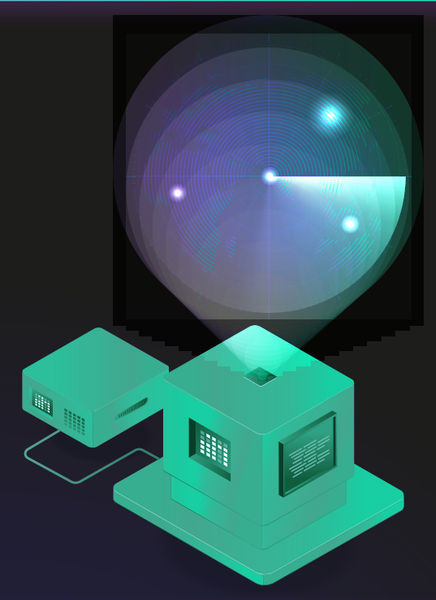
Vos collaborateurs SOC font sans aucun doute partie des experts les plus qualifiés de votre entreprise dans ces technologies de pointe. Ce sont eux qui sont chargés de gérer et de surveiller un système particulièrement complexe qui en laisserait perplexe plus d'un.

La réalité :

Votre SOC ne sera pas efficace s'il copie la compartimentation et les guerres de territoire inter-départements à l'origine du chaos et de la désunion qui laissent tant d'entreprises vulnérables face au cybercrime. La bonne entente entre les départements informatique, sécurité informatique et commercial doit être votre priorité absolue.

Mythe n °3 :

Le but ultime du SOC est de surveiller



Le mythe :

Bien que la surveillance 24 h/24 soit la valeur fondamentale du SOC, la prévention complète des menaces exige bien plus qu'un bouclier de cyberinformations sans faille.

La réalité :

Considérer le SOC comme un système de tickets de cyberincidents est un écueil majeur que les entreprises doivent prendre soin d'éviter. Un SOC inclut plusieurs autres tâches et fonctions de sécurité vitales, en particulier la Threat Intelligence, l'évaluation de la sécurité et, dans bien des cas, la réponse aux incidents, qui doivent être efficacement intégrées au système informatique pour permettre d'apporter les modifications nécessaires à l'infrastructure technique et à la configuration.

Mythe n °4 :

Plus d'alertes, plus d'informations, plus de sécurité ?

Le mythe :

L'information étant un aspect indispensable à la sécurité, il semble logique de penser que plus vous avez d'informations, plus votre sécurité sera robuste.

La réalité :

Votre SOC interne ne résoudra pas la question de la lassitude face aux alertes. À moins que vous ne soyez capable d'éliminer automatiquement les faux positifs et de hiérarchiser le reste, même une équipe interne parfaitement équipée ne sera pas capable de gérer efficacement le volume d'alertes entrantes et les performances de surveillance de votre SOC pourraient bientôt devenir un encombrant fardeau.

Mythe n° 5 :

Le SOC optimise automatiquement l'efficacité de l'équipe

Le mythe :

On croyait auparavant qu'un SOC interne apporterait une solution technologique à la pénurie mondiale de talents en cybersécurité. Mais cette vision est trop simpliste.

La réalité :

La mission fondamentale d'un SOC est de défendre l'entreprise contre le panorama des menaces internes et externes, tout en tenant compte de sa tolérance au risque. Votre SOC n'est pas une entité que vous pouvez laisser s'autogérer après sa mise en service. C'est un organisme vivant où travaillent des êtres humains qui devront faire l'objet d'une attention particulière pour maximiser votre retour sur investissement.

Comment Kaspersky peut vous aider

Nous comprenons les difficultés que représentent la mise en place et l'exploitation d'un SOC interne, et nous sommes fiers des grands progrès réalisés par les grandes entreprises internationales dans leur lutte contre les APT et autres menaces similaires en décidant de mener ce combat en interne.

Forts de plus de 20 années de recherche permanente de menaces, de technologies de protection leaders du marché, d'une expertise reconnue et d'une expérience éprouvée dans les projets de cybersécurité complexes, nous sommes à même de vous aider à libérer le potentiel de votre SOC pour gagner en efficacité à tous les niveaux afin de vous protéger contre des cybermenaces de plus en plus sophistiquées.

Contactez-nous

go.kaspersky.com/fr_expert

kaspersky