



Gigamon®

2018 CYBERMENACES RAPPORT DE DÉFENSE

Le cinquième rapport annuel de défense contre les cybermenaces du Groupe CyberEdge révèle la façon dont les professionnels de la sécurité des TI perçoivent les dispositifs de sécurité de leurs organisations, les défis qu'ils rencontrent lors de l'élaboration des défenses efficaces contre les cybermenaces et leurs plans afin de surmonter ces difficultés. Poursuivez votre lecture à propos de certaines trouvailles essentielles exposées dans ce rapport annuel.

LES FUITES SONT INÉVITABLES

Les organisations deviennent victimes des cyberattaques réussies à un rythme alarmant et prévoient que la situation s'aggravera avec le temps.



AU MOINS UNE ATTAQUE EN 2017



77,2 %



SIX FOIS PLUS D'ATTAQUES EN 2017



27,4 %



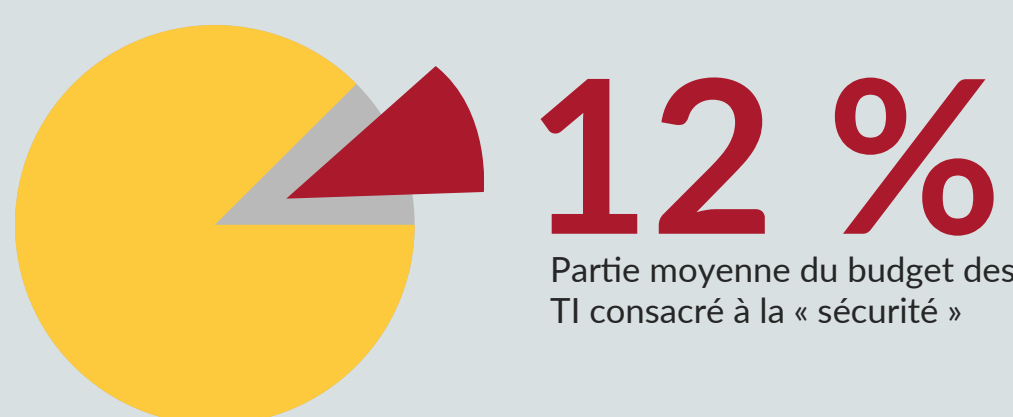
PRÉVISION DES ATTAQUES EN 2018



62,3 %

AUGMENTATION DES BUDGETS CONSACRÉS À LA SÉCURITÉ

En guise de réaction, pour 2018, les entreprises prévoient, en moyenne, d'accroître de 4,7 % leurs dépenses de sécurité quant aux produits et aux services et prévoient d'augmenter la quantité de spécialistes à leur service.



12 %

Partie moyenne du budget des TI consacré à la « sécurité »

CEPENDANT, UN CERTAIN NOMBRE DE DÉFIS DOIVENT ENCORE ÊTRE RELEVÉS

DÉFI N°1 : TROP À FAIRE

À l'époque où l'empreinte technologique s'élargit pour les entreprises d'aujourd'hui, la même chose se produit pour la superficie d'attaque à défendre.

L'INFRASTRUCTURE AYANT OBTENU L'ÉVALUATION DU DISPOSITIF DE SÉCURITÉ LE PLUS FAIBLE



Réceptacles



Appareils mobiles



Infrastructure infonuagique

PROCÉDÉS/FONCTIONS QUI COMPORTENT LE PLUS DE LACUNES



Élaboration d'application et d'essai (cycle de développement logiciel)



Réduction de superficie d'attaque



Détection des attaques internes indésirables

UN OBSTACLE IMPORTANT À L'EFFICACITÉ



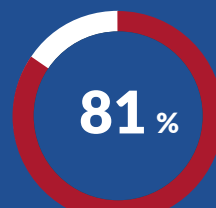
Trop de données à analyser

DÉFI N°2 : MANQUE DE PERSONNEL COMPÉTENT

Avoir de l'argent supplémentaire pour des dépenses dédiées à la sécurité est une mince consolation lorsqu'il y a une pénurie mondiale de spécialistes en cybersécurité.



Le manque de personnel compétent a été évalué comme étant le plus grand obstacle à la défense efficace contre les cybermenaces



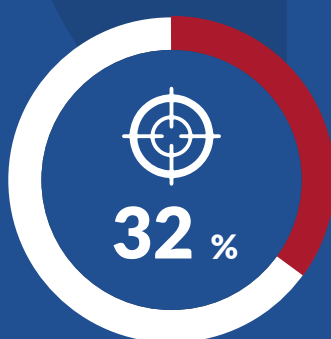
Les organisations connaissant un manque de personnel compétent en sécurité des TI

Formation	87 %
Technologie	85 %
Industries de transformation	82 %
Finance	81 %

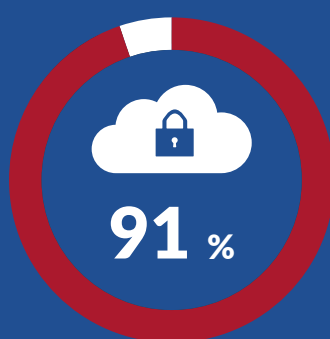
L'atteinte de l'industrie verticale par la pénurie de qualifications en matière de sécurité des TI

DÉFI N°3 : TOUJOURS À LA RECHERCHE DES BONNES SOLUTIONS

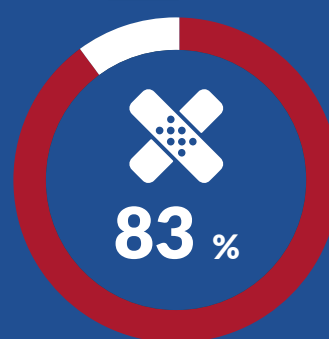
Investir suffisamment en matière de technologies et aux bons endroits ET optimiser leur rendement est un casse-tête que peu d'organisations arrivent à résoudre.



Plus d'un tiers des organisations ont investi efficacement quant à la chasse aux cybermenaces



Plus de neuf organisations sur dix éprouvent d'importantes difficultés associées à la sécurité infonuagique



Plus de quatre organisations sur cinq luttent afin de corriger les vulnérabilités de façon ponctuelle

TRACER UNE VOIE VERS L'AVENIR

Surmonter les difficultés liées à la sécurité des TI affligeant les entreprises nécessite des moyens de défense efficaces contre les cybermenaces, par exemple :



Donne une visibilité omniprésente



Désencombre et simplifie l'infrastructure de sécurité



Accélère le lancement et l'intégration des nouveaux outils de sécurité



Permet l'orchestration et l'automatisation