Gigamon

2019 RAPPORT SUR LES DÉFENSES CONTRE LES CYBERMENACES

Le sixième rapport annuel sur la défense contre les cybermenaces du Groupe CyberEdge révèle la façon dont les professionnels de la sécurité informatique élaborent des défenses efficaces contre les cybermenaces et leurs plans pour surmonter ces difficultés. Poursuivez votre lecture à propos de certaines conclusions essentielles figurant dans ce rapport annuel.

ENCORE EN ÉTAT DE SIÈGE

Les organisations deviennent victimes de cyberattaques réussies à un rythme alarmant et prévoient que la situation s'aggravera à l'avenir.

AU MOINS UNE ATTAQUE EN 2018 — 78,0 %

SIX ATTAQUES OU PLUS EN 2018 — 31,5 %

ONT ÉTÉ VICTIMES DE RANSOMWARE EN 2018 — 56,1 %

PRÉVOIENT DES ATTAQUES EN 2019 — 65,2 %

PRINCIPAUX DÉFIS

Malgré des budgets solides pour la sécurité informatique ces dernières années, la plupart des entreprises se débattent contre certains problèmes majeurs qui les empêchent de mettre en place des défenses efficaces contre les cybermenaces.

1er OBSTACLE À L'EFFICACITÉ

Trop de données à analyser

2e OBSTACLE À L'EFFICACITÉ

Les organisations connaissent une pénurie de personnel compétent en sécurité informatique

PRINCIPAL OBSTACLE À LA CHASSE AUX MENACES

Difficulté à mettre en œuvre ou à intégrer des outils de chasse aux menaces

UN AUTRE OBSTACLE IMPORTANT

Près des trois quarts des personnes interrogées mentionnent qu'exposer efficacement le trafic SSL / TLS à des inspections est problématique

EN PASSE D'AIDER

Même si quelques nouvelles technologies sont prometteuses pour aider les équipes de sécurité à éliminer les distractions causées par la surcharge de données de sécurité ...

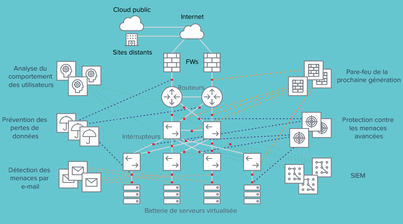
L'analyse de la sécurité est en tête de liste des technologies dont l'acquisition est prévue en 2019 (citée par 46,9 % des répondants)

81 % des personnes interrogées s'accordent à dire que les technologies d'apprentissage automatique et d'intelligence artificielle aident à venir à bout des cybermenaces sophistiquées

...elles ne s'attaquent malheureusement pas à la cause première.

UN PROBLÈME SOUS-JACENT

L'ajout de nombreuses couches parallèles d'outils de sécurité au fil des ans a mené à une architecture de sécurité ad-hoc. Outre leur contribution au déluge de données de sécurité, de telles conceptions posent les problèmes suivants :



- Accès non fiable au trafic réseau
- Incapacité d'inspecter efficacement le trafic chiffré
- Augmentation de la complexité et des coûts de la pile de dispositifs de sécurité
- Faux positifs et alertes récurrents
- Support médiocre pour tester de nouveaux outils de sécurité

UNE SOLUTION QUI MARCHE

Relever ces défis nécessite une solution offrant une visibilité omniprésente tout en minimisant la distribution et le traitement redondant des données source et les événements de sécurité en résultant.
Le but est donc de faire parvenir le renseignement et les perspectives pertinents à vos outils et à vos équipes, sans les submerger :

1

En fournissant un trafic optimisé aux outils (d'environnements physiques, virtuels et cloud)

2

En les déchargeant des processus exigeant des ressources considérables (par exemple, le déchiffrement)

3

En accélérant le déploiement et l'intégration de nouveaux outils de sécurité

4

En permettant l'orchestration et l'automatisation (pour améliorer l'efficacité opérationnelle)

TÉLÉCHARGEZ LE RAPPORT COMPLET À L'ADRESSE :
www.gigamon.com/cdr2019

CYBEREDGE GROUP