RSSI : un déficit de compétences freine la prévention–détection

Près de 7 responsables de la sécurité IT sur 10 en France s'inquiètent d'un déficit de compétences à l'ère de la prévention–détection–réponse aux incidents, selon une enquête internationale commandée par Bitdefender à Censuswide.

L'enquête a été réalisée en février et mars 2018 auprès de 1 050 responsables des achats et de la sécurité IT. Leurs organisations gèrent plus de 1000 postes de travail et serveurs. États-Unis, France, Allemagne, Royaume-Uni, Italie, Danemark et Suède sont couverts.

Premier enseignement : plus d'un répondant sur deux (et 68% des 150 RSSI interrogés en France) s'inquiètent de la pénurie de compétences en sécurité informatique. Par ailleurs, 69% (72% en France) estiment que les équipes sont trop réduites.

Or, le risque élevé de cyberattaques et l'urgence d'une mise en conformité avec le Règlement général sur la protection des données (RGPD) impactent à la hausse la charge de travail.

Prévention–détection–réponse

En France, 58% des organisations reconnaissent avoir été la cible de programmes malveillants (malwares) ou d'attaques informatiques avancées.

Dans ce contexte, les alertes de sécurité (dont 45% jugées fausses) se multiplient et submergent des équipes dont la productivité baisse, selon 72% des répondants.

La prévention par des moyens classiques (pare-feux, plateformes de protection des terminaux (EPP), systèmes de prévention des intrusions…) ne suffit pas face au cyber risque élevé. Les entreprises réorientent donc leurs investissements.

Les organisations passent ainsi progressivement d'une démarche préventive à une approche axée sur l'amélioration des capacités de détection et de réponse sur les terminaux et serveurs (EDR – Endpoint Detection and Response). La tendance a été soulignée par le cabinet Gartner dès 2017. Elle devrait s'amplifier d'ici 2020. Et Bitdefender s'en félicite…

Selon l'éditeur de solutions de sécurité, une approche EDR permet de limiter les interventions humaines tout en préservant la qualité des investigations en cas d'incident. Notamment pour les entreprises ne disposant pas d'un centre opérationnel de sécurité (SOC). Et ce grâce à une méthode *« en entonnoir »* de type prévention–détection–réponse.

« À l'entrée, les contrôles préventifs utilisent l'apprentissage automatique et l'analyse comportementale pour détecter un pourcentage élevé de menaces connues. La brique EDR, elle, se focalise sur le bas de l'entonnoir pour traiter les menaces potentielles ou inconnues », a expliqué Harish Agastya, vice-président Enterprise Solutions chez Bitdefender. *« Les administrateurs peuvent ainsi se concentrer sur une meilleure protection des actifs critiques »*.

Pour illustrer les résultats du sondage, Bitdefender propose l'infographie ci-dessous :

Lire également :

Cybersécurité : les RSSI parient sur l'automatisation et l'IA

Le RGPD arrive : les responsables de la sécurité IT sous pression

(crédit photo de une © Shutterstock)