Sécurité des endpoints : plus de 20% des alertes sont ignorées

L'éditeur de solutions Cynet a diffusé un rapport sur l'état de la protection contre les menaces avancées de cybersécurité. Les entreprises qui consolident et automatisent leur approche sont encore minoritaires. Toutefois, elles sont prêtent à investir davantage.

C'est le point de vue défendu par le fournisseur de la plateforme Cynet 360, sondage à l'appui. L'enquête* a été menée auprès de 1536 professionnels de la cybersécurité.

Voici 4 des principaux points à retenir de ce rapport :

1. Faible niveau de consolidation >

11% seulement des répondants déclarent que les alertes de sécurité informatique (utilisateurs, réseaux et terminaux) sont normalisées et affichées sur une seule et même console. 28% indiquent que les alertes de sécurité sont visibles depuis un même tableau de bord, mais que la normalisation et l'évaluation de ces données ne sont pas automatisées.

En revanche, pour le plus grand nombre (61%) il n'y a pas d'agrégation centrale des alertes et l'investigation se fait depuis la console de gestion de chaque produit de sécurité.

2. Trop d'alertes de sécurité ignorées >

Résultat, en moyenne, entre 20% et 40% des alertes générées par les solutions de sécurité sont ignorées quotidiennement. Pour l'expliquer, près de 8 répondants sur 10 (78%) pointent des soucis de gestion et de maintenance des solutions de sécurité existantes au sein de leur organisation. Le niveau de compétences (67%) et la taille jugée trop limitée des effectifs de sécurité (53%) sont d'autres arguments souvent mentionnés.

Pour mieux faire, la plupart des répondants anticipent une progression des ressources.

3. Budgets de sécurité IT en hausse >

73% des organisations prévoient une hausse de leur budget consacré à la sécurité IT dans les 12 mois à venir. Il s'agit surtout pour les entreprises de soutenir la découverte et la correction de vulnérabilités dans leurs applications et systèmes existants (63%). Prévenir l'exploitation d'une faille « zero day » par un malware (54%) arrive ensuite.

4. EDR/EPP en devenir >

L'écrasante majorité des entreprises interrogées en décembre 2019 utilisent des firewalls (cités par 91% des répondants), des antivirus (89%), des outils de protection des emails (73%) et de gestion des vulnérabilités (71%).

Elle sont moins nombreuses à s'appuyer sur des solutions de gestion des informations et événements de sécurité (SIEM) (34%), des outils d'analyse du trafic réseau (31%), une protection

antimalware du poste client (EPP) ou de détection et réponse (EDR) (28%).

Suivent d'autres solutions, dont celles dédiées à l'analyse du comportement de l'utilisateur et de l'entité (UEBA) (utilisée par 12% du panel), ainsi que les courtiers en sécurité d'accès cloud (CASB) (11%) et les technologies de déception (les leurres destinés à tromper les cyberattaquants) (9%). Autant d'outils qui font partie de l'arsenal de fournisseurs de services de sécurité managés (MSSP) avec lesquels Cynet peut nouer des partenariats.

Un équilibre difficile à trouver

En matière de sécurité informatique, la prévalence d'une intégration sur site (on-premise) de solutions l'emporte. Ainsi, 61% des répondants disent avoir opté pour des déploiements à 80% sur site et à 20% dans le cloud (SaaS, PaaS, IaaS).

« Le thème sous-jacent de ce rapport est la consolidation des cyber-technologies », a déclaré Eyal Gruner, fondateur et CEO de Cynet. Pour l'entreprise basée à New York et Rishon (Israël), le manque de consolidation domine aujourd'hui. Mais la plupart des organisations le perçoivent « comme un problème clé à résoudre » pour assurer leur protection.

**(source : Cynet – « State of Breach Protection 2020 »).*