VARS

7 SIGNES QUI MONTRENT QUE VOUS AVEZ BESOIN D'UNE NOUVELLE SOLUTION DE DÉTECTION ET DE RÉPONSE AUX INCIDENTS

Propulsée par Cynet

Introduction

Nous avons tendance à nous contenter du *statu quo* dans de nombreux aspects de la vie. Même lorsqu'il existe de meilleures options, c'est contre la nature humaine de changer. Ce qui nous est familier est confortable. L'inconnu, eh bien… c'est inconnu.

Le monde de la détection et de la réponse aux menaces connaît des innovations constantes; les technologies peuvent effectivement devenir obsolescentes du jour au lendemain. Il est toutefois difficile pour les professionnels de se tenir au courant des nouvelles avancées. Étant souvent trop accaparés pour rester au fait d'un marché en constante évolution et bombardés d'annonces de fournisseurs, de nombreux praticiens de la sécurité font profil bas et se contentent de ce qu'ils ont en place.

Pour aider ceux d'entre vous qui sont trop occupés pour être à l'affût des nouveautés en matière de technologies de sécurité et qui s'efforcent de s'en sortir avec des outils plus anciens, voici les signes que l'heure est peut-être venue d'effectuer un changement.

> *« Un bateau dans un port est en sécurité, mais ce n'est pas pour cela qu'il a été construit. »*
>
> John A. Shedd

1. Si vous tenez uniquement compte des alertes de risque les plus sérieuses, vous avez peut-être besoin d'une nouvelle solution de détection, d'intervention et de réponse…

Si vous ajoutez à une équipe de sécurité trop petite des systèmes de détection qui génèrent une quantité massive d'alertes, vous risquez de manquer de temps pour mener des recherches sur les alertes et faire les suivis appropriés. Dans ces circonstances, vous ne porterez probablement attention qu'aux alertes de menace les plus sérieuses.

En dépit des inévitables fausses alertes (« faux positifs »), nous passons à côté de nombreuses menaces réelles parce qu'elles se trouvent sous le seuil de risque acceptable pour déclencher une intervention. Dans les faits, toute alerte devrait faire l'objet d'une enquête, et ce, même si on l'écarte rapidement parce qu'elle est banale ou fausse. Avant de semer le chaos, certaines attaques graves apparaissent d'abord comme de petites anomalies sans conséquence, comme un processus de démarrage anormal ou un dossier qui a l'air légèrement suspicieux.

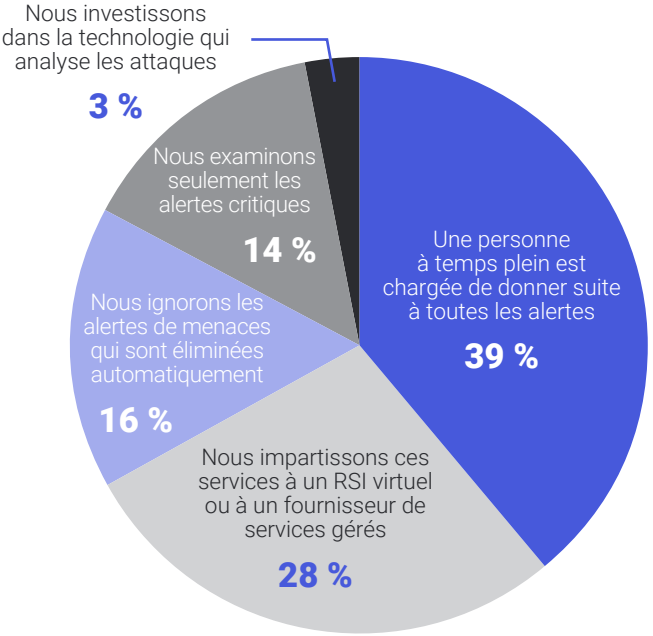
Que cela veut-il dire pour vos outils de détection et d'intervention? Si votre équipe fait fi de la majorité des alertes qu'elle reçoit, vos outils de détection ne sont que partiellement efficaces.

La solution? Trouvez une plateforme XDR (détection et réponse étendues) qui collecte et analyse automatiquement les alertes de multiples flux de télémétrie, afin que les signaux d'apparence bénigne soient évalués adéquatement et selon le contexte. Les alertes deviendront alors beaucoup plus précises.

2. Si vous avez besoin de cinq outils différents pour enquêter sur un seul incident, vous avez peut-être besoin d'une nouvelle solution de détection, d'intervention et de réponse…

Si le fait d'enquêter sur les alertes était simple et facile, nous n'aurions pas besoin de nous demander si elles sont pertinentes. Malheureusement, pour enquêter manuellement sur une alerte, les analystes doivent accéder à plusieurs systèmes afin d'en déterminer la source. Cela mène au dilemme des « équations à plusieurs inconnues » auxquelles répondent uniquement les plus grandes entreprises disposant d'outils unifiés assurant à la fois la gestion de l'information et des événements de sécurité, l'orchestration de la sécurité et l'automatisation de l'intervention ou de la réponse. Chaque enquête prend plusieurs minutes, voire plusieurs heures, lesquelles s'accumulent au fil des nombreuses alertes reçues par les entreprises d'aujourd'hui.

Un sondage récent mené auprès de 200 responsables de la sécurité informatique disposant de petites équipes (cinq personnes ou moins) a révélé que 39 % de ces entreprises avaient un analyste à temps plein chargé de donner suite aux alertes. Ce qui est alarmant, c'est que 14 % des entreprises se contentent d'examiner les alertes critiques, ce qui veut dire que toute alerte qui a été incorrectement classée est ignorée. De plus, 16 % font abstraction des alertes de menaces qui ont été éliminées automatiquement, même si cette menace risque de faire partie d'une attaque plus vaste et continue.

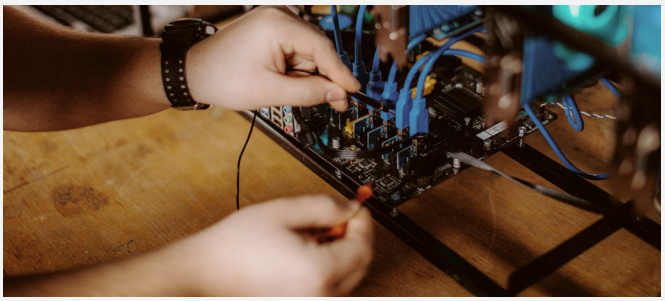


Une autre solution consiste à consolider les enquêtes dans une seule plateforme unifiée et automatisée. Ainsi, au lieu d'avoir à jongler manuellement avec plusieurs outils, on peut utiliser une solution XDR qui combine les signaux de menace en mode natif et lancer automatiquement une enquête pour déterminer la cause et la portée d'une menace détectée. Ce genre de solution vous permet surtout d'intervenir plus rapidement et de façon plus efficace pour éliminer une menace avant qu'elle ne devienne un problème.

3. Si votre solution EDR exige plusieurs logiciels complémentaires pour bien fonctionner, vous avez peut-être besoin d'une nouvelle solution de détection, d'intervention et de réponse…

Souvent, les plateformes offertes par les fournisseurs de services EDR (détection et intervention sur les postes de travail et serveurs) comptent plusieurs niveaux. Leurs coûts augmenteront avec les fonctionnalités et les capacités sélectionnées. D'autres fournisseurs offrent une solution EDR de base, mais exigent l'ajout de logiciels complémentaires pour des fonctions particulières, comme la recherche des sources d'une attaque, la recherche des vulnérabilités, la correction automatisée et plus encore. Lorsque vous avez enfin configuré tout ce dont vous avez besoin, les coûts ont explosé et l'implémentation et la gestion des activités se sont grandement compliquées.

En réalité, ajouter des services ne fait qu'aggraver le problème et augmenter les coûts : frais de services professionnels pour l'intégration et la configuration, services gérés de détection et d'intervention, services de recherche de vulnérabilités et de menaces, analyse de la posture, analyse d'écart, formation et ainsi de suite. Plusieurs fournisseurs EDR sont plus concentrés à trouver de nouvelles sources de revenus qu'à détecter des cybermenaces.

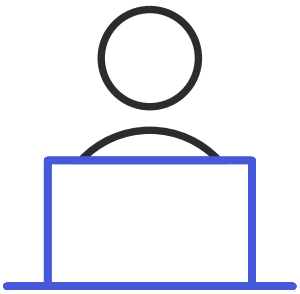


Vous pouvez trouver à la place un fournisseur qui vous offre toutes les fonctionnalités et tous les services pour un seul prix, fixe et transparent. Ainsi, vous évitez d'avoir à choisir entre des services de recherche des cybermenaces et des capacités de correction automatisée, et ce, même si votre budget est limité. Cynet vous offre, pour un seul prix fixe, l'ensemble de ces capacités, fonctionnalités et services : la prévention et la détection XDR, des capacités d'intervention automatisées et étendues, ainsi que des services gérés complets de détection et de réponse disponibles 24 heures sur 24, sept jours sur sept.

4. Si un seul membre de votre équipe sait comment gérer votre solution EDR, vous avez peut-être besoin d'une nouvelle solution de détection, d'intervention et de réponse…

La courbe d'apprentissage abrupte est un autre effet indésirable des solutions de sécurité multiples et complexes. La plupart des solutions EDR et des autres logiciels de détection sont très complexes; les mettre en place, les calibrer, les adapter à une organisation et les entretenir exigent un investissement important en temps et en formation.

Selon une étude de Cynet, il faut plus de quatre mois pour une entreprise pour déployer et maîtriser les meilleurs outils de sécurité, dans près de 80 % des cas. Les organisations qui disposent de vastes budgets et de grandes équipes chargées de la sécurité peuvent affecter quelques employés à la gestion de ces activités, mais les équipes plus petites ne peuvent pas s'offrir ce luxe et se fient à une seule personne qui est chargée d'orchestrer la stratégie de sécurité. Lorsqu'on se fie à un seul employé pour gérer les logiciels de sécurité, il en résulte un système généralement moins sécuritaire puisque toute absence ou non-disponibilité donne lieu à une potentielle brèche de sécurité importante.



Cela signifie également que toute réponse à un incident majeur sera ralentie, car une seule personne ne peut pas forcément gérer toutes les facettes d'une crise. Même dans les moments les plus paisibles, il n'est pas assuré qu'une seule personne soit capable de réparer un système complexe. Le problème est d'autant plus grave que, selon une étude de Cynet, 47 % des entreprises estiment que leur plus grand défi est le manque de compétences et d'expérience.

La solution consiste à simplifier et à réduire les obstacles à l'accessibilité. Au lieu de recourir à des systèmes complexes qui nécessitent un diplôme supérieur et des mois de formation, les entreprises devraient rechercher des outils qui réduisent ces obstacles et permettent à un plus grand nombre d'employés de devenir des experts en un minimum de temps. La plateforme Cynet, par exemple, a été spécialement conçue avec une interface utilisateur intuitive qui peut être maîtrisée facilement en quelques jours. Ainsi, vous n'avez pas besoin de consacrer des ressources massives à l'apprentissage d'un nouveau système, vos équipes ne sont pas surchargées et la sécurité peut être plus efficace.

5. Si votre solution EDR se targue soudainement d'être une solution XDR mais que rien n'a changé, vous avez peut-être besoin d'une nouvelle solution de détection, d'intervention et de réponse…

La XDR est la dernière tendance dans le domaine de la protection contre les menaces, si bien que tous les fournisseurs de sécurité veulent leur part du gâteau – qu'ils offrent vraiment une solution XDR ou non. Lorsqu'une nouvelle technologie apparaît sur le marché, la confusion règne et de nombreux fournisseurs pensent qu'ils peuvent la définir comme ils le souhaitent. Un fournisseur disposant à la fois d'une solution EDR et d'une solution de sécurité infonuagique prétendra que, ensemble, elles forment une solution XDR. Or, il arrive souvent que les deux solutions ne soient pas vraiment intégrées et qu'elles aient peu de capacités d'automatisation. Certains fournisseurs de solutions « XDR libre d'accès » n'offrent guère plus qu'une plateforme de services gérés améliorée qui nécessite une intégration, une configuration et une maintenance poussées; c'est tout le contraire de ce que la XDR devrait offrir, et c'est pourtant ainsi qu'ils la désignent.

Il est effectivement difficile de distinguer une vraie solution XDR d'une fausse. Il n'est pas simple, non plus, d'évaluer le niveau d'intégration des différents contrôles offerts par un fournisseur et leur capacité globale à analyser les signaux pour améliorer la précision de la détection. Recherchez plutôt des solutions dotées de capacités natives qui ont été construites à partir de zéro. Ne vous contentez pas de solutions intégrées après coup ou de solutions XDR « hybrides » qui offrent la plupart des capacités clés en main, lesquelles peuvent également intégrer des signaux et des données provenant de solutions et de composants de système d'autres fournisseurs.

Vous pouvez trouver un fournisseur qui offre toutes les fonctionnalités et tous les services à un prix unique et transparent. Ainsi, vous n'avez pas à décider si vous consacrerez votre budget limité aux services de recherche des menaces ou aux capacités de réponse automatisée. Cynet, par exemple, offre toutes les fonctionnalités et tous les services – prévention et détection XDR complètes, capacités étendues d'intervention et de réponse automatisée ainsi que services gérés complets de détection et d'intervention – en tout temps et moyennant un prix unique.

6. Si vous payez plus cher vos services MDR que vous outils EDR, vous avez peut-être besoin d'une nouvelle solution de détection, d'intervention et de réponse…

Dans une enquête menée en 2019 par Tripwire, 80 % des professionnels de la sécurité ont affirmé qu'il était difficile de trouver des personnes possédant de bonnes compétences en matière de sécurité. Parmi ceux-ci, 69 % ont affirmé que la pénurie de main-d'œuvre possédant ces compétences avait un impact direct sur leurs opérations de sécurité.

Le manque de personnel adéquat ainsi que des outils EDR qui sont difficiles et longs à utiliser sont deux facteurs qui peuvent entraîner une situation inconfortable pour de nombreuses entreprises. Les services MDR (services gérés de détection et d'intervention) sont devenus une nécessité pour de nombreuses organisations, surtout avec le volume d'alertes et de postes de travail et serveurs que la plupart des équipes de sécurité doivent gérer. Si vous devez consacrer un budget supplémentaire à des services gérés pour vous aider avec votre solution EDR, posez-vous la question suivante : que fait réellement cette solution pour vous? Lorsque les personnes qui vous aident à gérer votre solution vous coûtent plus cher que la solution elle-même, il est temps de procéder à une mise à niveau.

Vous devriez plutôt rechercher un outil de détection, d'intervention et de réponse qui fournit par défaut des services gérés dans le cadre de son offre. Cynet offre des services gérés qui sont disponibles en permanence et inclus dans le coût de la solution. Ainsi, vous avez un accès complet à des experts qui peuvent vous prêter main-forte en fournissant des ressources clés, lesquelles vous libéreront pour d'autres tâches critiques.

7. Si vous rêvez d'une technologie de leurre mais que vous n'en avez pas les moyens, vous avez peut-être besoin d'une nouvelle solution de détection, d'intervention et de réponse…

L'un des outils les plus précieux apparus ces dernières années est la technologie de leurre. La capacité des organisations de tendre des pièges et d'attraper les assaillants, qui ont réussi à contourner les autres couches de défense, avant qu'ils ne puissent causer des dommages est essentielle. Cependant, on ne peut pas tous s'offrir des outils de leurre en plus des systèmes de sécurité existants qui sont déjà très coûteux.

Le déploiement de la technologie de leurre pose deux problèmes majeurs. Le premier est le coût : ils sont dispendieux et rarement inclus dans les offres EDR. Les équipes qui cherchent à conserver des couches de sécurité légères seront donc réticentes à ajouter des outils de leurre. Pour de nombreuses équipes de sécurité, la technologie de leurre est donc un luxe plutôt qu'une nécessité.

Le deuxième obstacle à l'adoption de la technologie de leurre est de nature technique. Les outils de leurre sont des logiciels complexes qui nécessitent de la finesse et un savoir-faire particulier pour être correctement déployés. Lorsqu'ils fonctionnent, ces outils constituent un excellent moyen de dissuasion. Dans le cas contraire, ils ne représentent rien de plus que des gadgets coûteux.

Il existe toutefois des plateformes qui incluent des outils de leurre par défaut. Dans le cas des services gérés, l'intégration d'une suite d'outils de leurre permet une configuration, un calibrage et un déploiement rapide de ces outils. La suite intégrée d'outils de leurre de Cynet ne prend que quelques minutes à maîtriser, à déployer et à surveiller. Au lieu d'augmenter votre facture mensuelle de sécurité, vous pouvez profiter de la couche de protection supplémentaire de la plateforme Cynet.

En conclusion

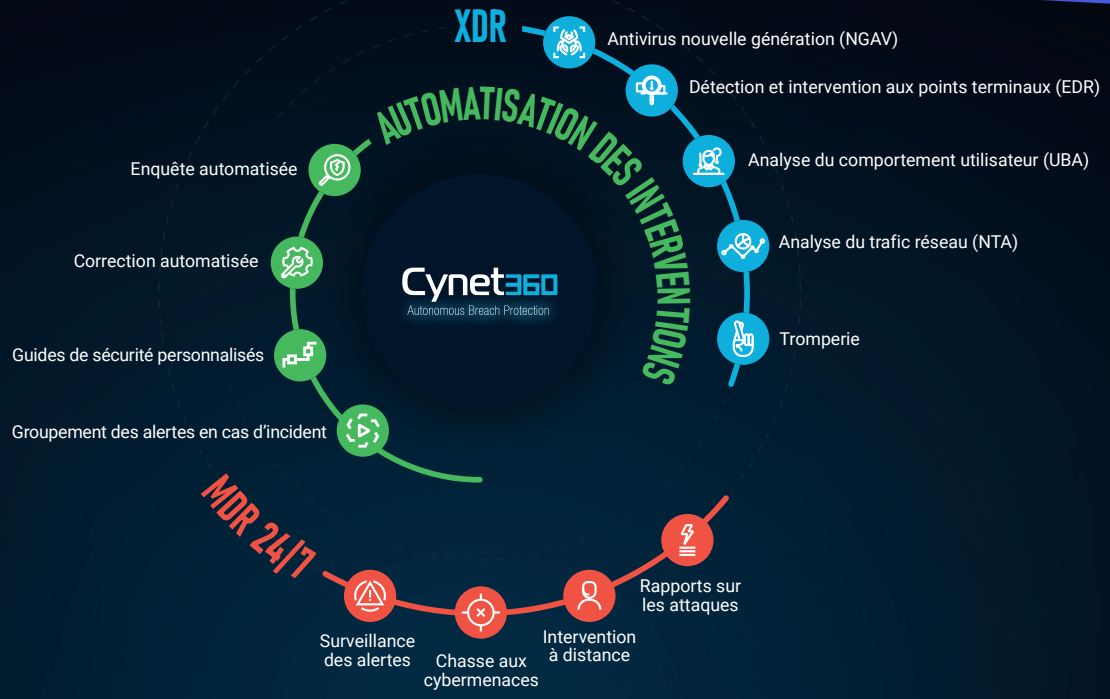
Il est temps que vos outils de détection, d'intervention et de réponse travaillent pour vous.

Si les considérations qui précèdent vous interpellent, il est sans doute temps que vous recherchiez un meilleur outil de détection et d'intervention. Les outils EDR offrent des avantages considérables et, dans certains cas, ils peuvent être une excellente première ligne de défense. Dans les organisations lourdement connectées d'aujourd'hui, ils sont toutefois rarement suffisants. Au lieu d'ajouter toujours plus d'outils, vous devriez opter pour la pertinence et l'efficacité de ceux-ci.

Les solutions XDR sont une excellente amélioration aux outils EDR, car elles protègent l'intégralité de votre environnement, et pas seulement vos postes de travail. En outre, elles réduisent le nombre d'outils dont vous avez besoin pour vous protéger. Au lieu d'un ensemble disparate d'outils, de tableaux de bord et de méthodes de résolution, vous pouvez vous fier à une seule interface et obtenir toutes les réponses, la visibilité et la protection dont vous avez besoin.

Qui plus est, la bonne solution XDR peut également inclure des outils essentiels qui accroissent encore davantage vos défenses, par exemple un outil MDR et une technologie de leurre. Ainsi, au lieu de devoir assembler des couches complexes de sécurité, vous pouvez en obtenir une complète et prête à utiliser. Arrêtez d'ajouter des éléments à une solution qui ne répond pas à vos attentes et trouvez une plateforme de sécurité qui répond à vos besoins.

À propos de Cynet et de VARS



Cynet

Cynet permet aux organisations de mettre leur cybersécurité en mode autopilote en simplifiant et en automatisant toutes leurs opérations de sécurité, et ce, tout en fournissant une meilleure visibilité et une meilleure protection, quelles que soient la taille, les compétences ou les ressources de l'équipe, sans nécessiter des couches de sécurité de plusieurs produits. Pour ce faire, Cynet consolide de façon native toutes les technologies de sécurité dont les organisations ont besoin pour se protéger contre les menaces et les réunit en une seule plateforme XDR facile à utiliser. Le processus manuel d'investigation et de correction est automatisé dans l'ensemble de l'environnement. Un service MDR gratuit et proactif qui comprend la surveillance, l'investigation, l'analyse sur demande, la réponse aux incidents et la détection des menaces est de plus disponible en tout temps.

VARS

À l'avant-garde de l'industrie de la sécurité de l'information, VARS sélectionne et offre des solutions novatrices et primées aux petites, moyennes et grandes entreprises à travers l'Amérique du Nord.

VARS répond aux besoins immédiats de cybersécurité du monde moderne, en offrant un soutien et des conseils continus.