Enterprise Strategy Group | Getting to the bigger truth.™

Combler les lacunes des opérations de sécurité avec des services gérés de détection et d'intervention

Puisque le risque croissant de cyberattaques nuisibles détourne l'esprit et le budget des objectifs commerciaux principaux, les organisations doivent réagir en renforçant leurs programmes de cybersécurité. Les opérations de sécurité (SecOps) sont au cœur de tous les programmes de cybersécurité et sont responsables de la surveillance et de la protection de tous les aspects de la surface d'attaque numérique.

Malgré les investissements, les opérations de sécurité sont plus difficiles

PLUS DE LA MOITIÉ
des répondants pensent que les opérations de sécurité sont **plus difficiles** aujourd'hui qu'il y a deux ans.

» **Les cinq principales raisons qui expliquent pourquoi les opérations de sécurité sont plus difficiles.**

1. **41%** L'environnement des menaces évolue rapidement
2. **39%** La surface d'attaque est en constante évolution
3. **37%** Le volume et la complexité des alertes de sécurité ont augmenté
4. **34%** Mon organisation utilise de plus en plus les services infonuagiques publics
5. **33%** Nous avons du mal à répondre aux besoins opérationnels associés aux technologies d'opérations de sécurité

Repenser les stratégies du programme

Les surfaces d'attaque et l'environnement des menaces ont augmenté en taille et en complexité, de même que l'utilisation des contrôles de sécurité, qui génèrent des milliers d'alertes et de grandes quantités de données de sécurité. Les équipes de sécurité repensent l'ensemble des opérations de programmes afin d'incorporer davantage les données sur les actifs et les risques provenant des TI et des équipes du secteur d'activités afin de se concentrer sur les menaces qui posent le plus grand risque pour les objectifs organisationnels.

98% des organisations font déjà appel à un fournisseur de services gérés de détection et d'intervention ou prévoient le faire dans les 12 prochains mois.

88% de ces organisations prévoient augmenter leur utilisation de services gérés de détection et d'intervention dans les 12 prochains mois.

» **Principaux générateurs de valeur de l'utilisation des services gérés de détection et d'intervention.**

AMÉLIORATION ET EFFICACITÉ OPÉRATIONNELLES.
Les services gérés de détection et d'intervention peuvent aider les organisations à réduire le coût total des opérations de sécurité de plusieurs manières, comme l'infrastructure, le personnel et la gestion. Ils peuvent également résoudre le problème de « lassitude d'alertes » et permettre une importante réduction des faux positifs.

AMÉLIORATION DE L'EFFICACITÉ DE LA CYBERSÉCURITÉ ET RÉDUCTION DES RISQUES.
Les services gérés de détection et d'intervention peuvent aider les organisations à stopper les menaces déjà en cours, à améliorer la détection des menaces et des attaques persistantes avancées, à lancer la chasse proactive aux menaces et à renforcer les contrôles pour déceler et prévenir les attaques futures.

» **Principales raisons pour lesquelles votre organisation utilise ou prévoit utiliser les services gérés.**

55%
Objectif: Mon organisation souhaite que son personnel de sécurité cible des initiatives de sécurité plus stratégiques plutôt que de consacrer du temps aux tâches associées aux opérations de sécurité.

52%
Services: Mon organisation croit que les fournisseurs de services peuvent mieux gérer les opérations de sécurité que nous.

49%
Enrichissement: Mon organisation croit qu'un fournisseur de services peut enrichir notre équipe responsable des opérations de sécurité.

42%
Compétences: Mon organisation ne dispose pas des compétences nécessaires pour les opérations de sécurité.

> **Plusieurs solutions de services gérés de détection et d'intervention de première génération étaient conçues et mises en œuvre pour une ère différente :** moins de données, moins de menaces et des détections plus simples."
>
> *- Dave Gruber, analyste principal d'ESG*

Nouvelles exigences pour les services gérés de détection et d'intervention

Plusieurs solutions de services gérés de détection et d'intervention de première génération étaient conçues et mises en œuvre pour une ère différente : moins de données, moins de menaces et des détections plus simples. La prochaine génération de solutions de services gérés de détection et d'intervention doit être en mesure de protéger une surface d'attaque plus diversifiée, de détecter des menaces plus complexes et de tirer le meilleur parti d'une approche axée sur les risques pour la hiérarchisation et l'atténuation.

- Surveillance des événements et des journaux en tout temps.
- Des renseignements rapides et à visibilité élevée sur les activités suspectes et les alertes par volume, par emplacement et par type.
- Surveillance continue et évolutive du réseau et analyse des menaces.
- Recommandations basées sur l'IA pour les options de réaction aux menaces.
- Rapports de conformité légale.
- Conseillers en sécurité en communication directe avec les équipes internes.
- Analyse détaillée et en temps réel basée sur la détection, le triage, l'enquête et l'aspect juridique des menaces.
- Évaluations de vulnérabilité, hiérarchisation et conseils d'atténuation.

Lorsque les organisations examinent le grand nombre de fournisseurs de services potentiels qui peuvent offrir certaines, la plupart ou même toutes les fonctionnalités de services gérés de détection et d'intervention en sous-traitance, **elles doivent rechercher des partenaires qui peuvent fournir les services suivants:**

- Renseignements sur la surveillance des menaces.
- Antécédents éprouvés en matière de zone de couverture géographique, de marché vertical et de profil réglementaire de l'organisation.
- Capacités démontrées de chasse aux menaces.
- Un engagement à long terme envers les services gérés de détection et d'intervention infonuagiques.
- Des capacités étendues dans les environnements à nuages multiples et à nuage hybride, le modèle Zero Trust et le modèle de responsabilité partagée de la sécurité infonuagique.
- Capacité éprouvée à développer leurs services au fil du temps grâce à une technologie novatrice, à des processus éprouvés et à une expertise démontrée par ses employés.

La grande vérité

Puisque le risque croissant de cyberattaques nuisibles détourne l'esprit et le budget des objectifs commerciaux principaux, les organisations doivent renforcer leurs programmes de cybersécurité. Bien que les cas d'utilisation varient, la plupart des organisations font appel à des fournisseurs de services gérés de détection et d'intervention pour développer et adapter leurs programmes.

L'approche de Dell Technologies en matière de détection et d'intervention gérées combine des technologies flexibles, intelligentes et évolutives et des professionnels expérimentés en cybersécurité afin d'aider des organisations de toutes les tailles et de tous les profils de ressources à accélérer et à renforcer leurs programmes de sécurité.

EN SAVOIR PLUS

DELL Technologies

Source : résultats du sondage complet d'ESG intitulé, *SOC Modernization and the Role of XDR*, août 2022.