Managed Exposure Defence : un programme pour couvrir toute la Response Loop

Enjeux business

En avril 2026, le projet Glasswing d'Anthropic a permis de mettre au point un modèle d'IA avancé capable de détecter des vulnérabilités critiques à grande échelle. Résultat : des milliers de failles, jusqu'ici inconnues, ont été révélées dans les principaux systèmes d'exploitation et navigateurs, certaines étant restées invisibles depuis des années. Les éditeurs doivent désormais réagir très vite pour corriger ces failles, ce qui entraîne une vague de mises à jour coordonnée sans précédent.

Pour la plupart des organisations, le vrai enjeu n'est plus d'avoir l'info, mais de pouvoir agir. L'IA accélère fortement la création et l'exploitation des failles, réduisant les délais de réaction de plusieurs jours à quelques heures. Or, les équipes sécurité sont déjà sous pression : pas d'équipe dédiée aux correctifs, pas de capacité supplémentaire mobilisable rapidement. Le régulateur souhaite valider qu'il existe des réponses à des événements concrets, les directions s'interrogent, et la menace ne laisse aucune place à des cycles d'achat longs ou à une multiplication de prestataires.

Notre solution

Insight Managed Exposure Defence est un service managé intégré, conçu pour répondre à cette nouvelle réalité. Il réunit cinq briques complémentaires au sein d'un programme unifié, permettant aux organisations de passer rapidement d'une situation d'exposition à un environnement sécurisé, au rythme imposé par la menace. Plutôt que de multiplier les outils isolés et les prestataires, les entreprises bénéficient d'une prise en charge complète de l'ensemble de la chaîne de gestion des vulnérabilités, avec un pilotage et une responsabilité unifiée.

Le programme peut être défini et chiffré en moins de 24 heures après le premier échange. Il s'adapte aussi bien à des environnements d'une centaine d'actifs qu'à des organisations de grande envergure, sans développement spécifique, et apporte un soulagement opérationnel immédiat, quelle que soit la taille de l'entreprise.

Fonctionnalités et avantages

Un seul contrat. Une seule équipe. Une réponse claire.

Insight couvre l'ensemble des cinq étapes de la boucle de réponse avec une équipe unique.

Pas de zones grises entre prestataires. Pas de complexité de coordination.

Cadré et chiffré en 24 heures

Du premier échange à un environnement sécurisé, sans passer par des cycles d'achat inutilement longs.

De 100 actifs à des environnements de grande taille

Une solution prête à l'emploi, quel que soit le périmètre, sans développement spécifique ni complexité d'engagement.

Conçu pour la conformité dès le départ

Aligné avec les principaux cadres réglementaires (NIS2, DORA, RGPD…), avec une traçabilité intégrée dès le premier jour.

Résultats

Avec Insight Managed Exposure Defence, on passe de « Comment allons-nous réagir ? » à « C'est déjà pris en charge. » Les organisations bénéficient d'un soulagement opérationnel immédiat face à une menace qui dépasse les ressources disponibles, d'un dispositif clair et documenté pour répondre aux attentes des autorités et des dirigeants, et de la tranquillité d'esprit qu'apporte un partenaire unique responsable de l'ensemble de la réponse.

Cinq étapes. Un seul partenaire.

C'est l'approche globale qui fait la différence.

Insight intervient à chaque étape de la boucle de réponse : détection des expositions, visibilité sur les logiciels de supply chain, remédiation côté opérations, remédiation côté code, ainsi que détection et confinement des exploits.

Le tout dans le cadre d'un contrat unique, avec une seule équipe de delivery.

Managed CTEM

Une surveillance continue des endpoints, du Cloud, des identités et des applications, offrant une vision en temps réel des expositions, priorisée selon le niveau de risque. Le socle sur lequel repose toute la réponse.

Logiciels de supply chain & risques OSS

Génération de SBOM, suivi des dépendances open source et analyse de la posture des éditeurs et fournisseurs.

Une visibilité claire sur ce qui compose réellement vos applications.

Managed Patch

Gestion des correctifs à grande échelle sur les environnements Windows®, Linux®, hyperviseurs et bases de données.

Déploiements maîtrisés, avec phases de test, possibilité de retour arrière et traçabilité complète des actions.

Managed XDR

Détection, qualification et réponse 24/7, assurées par un SOC mondial (États Unis, Royaume Uni, Inde, Manille).

Un filet de sécurité essentiel lorsque les correctifs ne peuvent pas être déployés immédiatement.

Externalisation du développement logiciel

Mobilisation rapide de ressources d'ingénierie pour la mise à jour des dépendances, la refonte de bibliothèques et la correction des applications spécifiques.

Les risques sont traités directement au niveau du code, sans bloquer la feuille de route produit.

Vous souhaitez aller plus loin ?

Évaluation GRC

Évaluez votre niveau de gouvernance, de gestion des risques et de conformité au regard des principaux référentiels du marché, afin d'identifier les écarts et de structurer clairement la préparation aux audits.

Tests d'intrusion ponctuels et réguliers

Validez de manière proactive votre niveau de sécurité grâce à des scénarios d'attaque simulés, afin de vous assurer que les correctifs et les mesures de protection fonctionnent réellement.

Pilotage et gouvernance de l'IA

Permet aux organisations de déployer l'IA de manière responsable grâce à une visibilité continue, des repères clairs de gouvernance et des recommandations concrètes, couvrant les usages, les agents, les identités et les coûts.

Pourquoi Insight ?

Insight est un intégrateur de solutions technologiques qui accompagne les organisations dans la résolution de leurs enjeux IT en combinant matériel, logiciels et services adaptés à leurs besoins.

Entreprise technologique du Fortune 500, avec plus de 35 ans d'expertise et un écosystème de plus de 6 000 partenaires, Insight conçoit et déploie des solutions IT sécurisées, de bout en bout, pour des organisations partout dans le monde.