Microsoft Defender XDR géré par Inetum

La cybersécurité en action

inetum

Dans le domaine de la sécurité, ce ne sont pas les acronymes qui manquent. C'est ainsi que nous sommes passés de AV à EPP et ensuite EDR pour à présent utiliser XDR. Ces technologies en continuelle évolution sont nécessaires afin de garder constamment une longueur d'avance sur les menaces. Il n'est pas toujours évident de se tenir informé et de prendre à temps les mesures appropriées pour éviter un incident. Avec la nouvelle solution Microsoft Defender XDR gérée par nos soins, nous offrons non seulement une visibilité sur les dangers qui menacent votre environnement informatique, mais aussi une surveillance et une réponse aux incidents 24 h/24 et 7 j/7.

Le nombre de cyberattaques ne cesse d'augmenter. La question n'est pas de savoir si vous y serez confronté, mais plutôt quand. Heureusement, la plupart des entreprises sont désormais conscientes de cette **cybermenace grandissante** et s'efforcent de se protéger au mieux contre les risques liés à la cybercriminalité. Et si elles ne le font pas de leur propre initiative, la pression croissante exercée par les régulateurs externes les encourage dans cette voie.

La NIS2 change la donne

Les pouvoirs publics, sous l'impulsion de l'UE, imposent de plus en plus d'exigences aux entreprises en termes de cybersécurité. La directive européenne NIS2 élargie en est un bon exemple. Celle-ci servira de levier et d'accélérateur pour toutes sortes d'investissements nécessaires en matière de cybersécurité dans les années à venir. Ceux-ci doivent également permettre aux entreprises d'atteindre un niveau minimum commun ou seuil de sécurité dans ce domaine.

Dans un premier temps, la NIS2 entrera en vigueur pour 180 000 entreprises de 18 secteurs au sein de l'Union européenne. Il y a de fortes chances que votre entreprise en fasse partie, ou fasse partie de la chaîne d'approvisionnement de ces organisations. Si c'est le cas, vous devrez vous aussi prendre un certain nombre de mesures pour maîtriser suffisamment les risques en matière de cybersécurité, prévenir autant que possible les incidents ou en **limiter au maximum les conséquences**.

Bien démarrer

Concrètement, il s'agit d'intervenir dans dix domaines. L'un de ces domaines est le **traitement des incidents : la prévention et la détection des cyberincidents et la réaction à adopter s'ils ont lieu**.

La bonne nouvelle, c'est qu'il existe aujourd'hui de nombreuses solutions sur le marché qui peuvent vous aider à traiter ces incidents. L'une des plus connues a été développée par Microsoft. Microsoft Defender XDR vous permet avant tout de mieux comprendre les nombreux dangers qui menacent votre environnement informatique.

Mais il y a aussi de moins bonnes nouvelles. Les entreprises ne disposent pas toujours en interne du personnel et de l'expertise nécessaires pour implémenter et gérer facilement une telle solution. Investir dans ce **savoir-faire** et ces **profils spécialisés** est non seulement coûteux, mais ces ressources sont également très difficiles à trouver sur le marché du travail.

Microsoft Defender XDR :
une meilleure visibilité sur les menaces

XDR (eXtended Detection and Response) étend les capacités de base de l'EDR (Endpoint Detection and Response) pour assurer une protection **au-delà des seuls terminaux**. Ainsi, Microsoft Defender XDR vous permet également de sécuriser **vos identités hybrides, vos e-mails, vos outils de collaboration, vos applications et votre environnement cloud**, sur **plusieurs plateformes**. En d'autres termes, la solution ne se limite pas à la plateforme Microsoft seule, elle s'étend à l'ensemble de votre infrastructure.

En rationalisant la collecte, l'analyse et les flux de données de sécurité, Microsoft Defender XDR améliore la visibilité sur les menaces cachées et avancées. Les **informations supplémentaires et de meilleure qualité** que vous obtenez vous aident à réagir à temps et de manière appropriée à ces menaces, de manière automatique ou non.

Prendre des mesures

En tant que **partenaire informatique de confiance**, nous pouvons faire la différence grâce à nos **experts Microsoft certifiés en sécurité**. Car il ne suffit pas de mettre en œuvre une solution telle que Microsoft Defender XDR, ni d'obtenir des informations via cette solution.

Les rapports et les « alertes » ou avertissements automatiques eux-mêmes ne suffisent pas. Il faut également pouvoir prendre **les mesures appropriées à temps** pour prévenir un incident ou y réagir de manière efficace et éviter ainsi des dommages plus graves. Et ceci **à toute heure**, y compris la nuit et le week-end.

XDR en tant que managed service

Vous n'avez peut-être pas non plus les ressources et les moyens en interne pour le faire. Pas d'inquiétude : c'est précisément pour cela que nous vous proposons désormais de prendre en charge ce traitement des incidents indispensable et, qui sait, même obligatoire à terme, sous la forme d'un **managed service**.

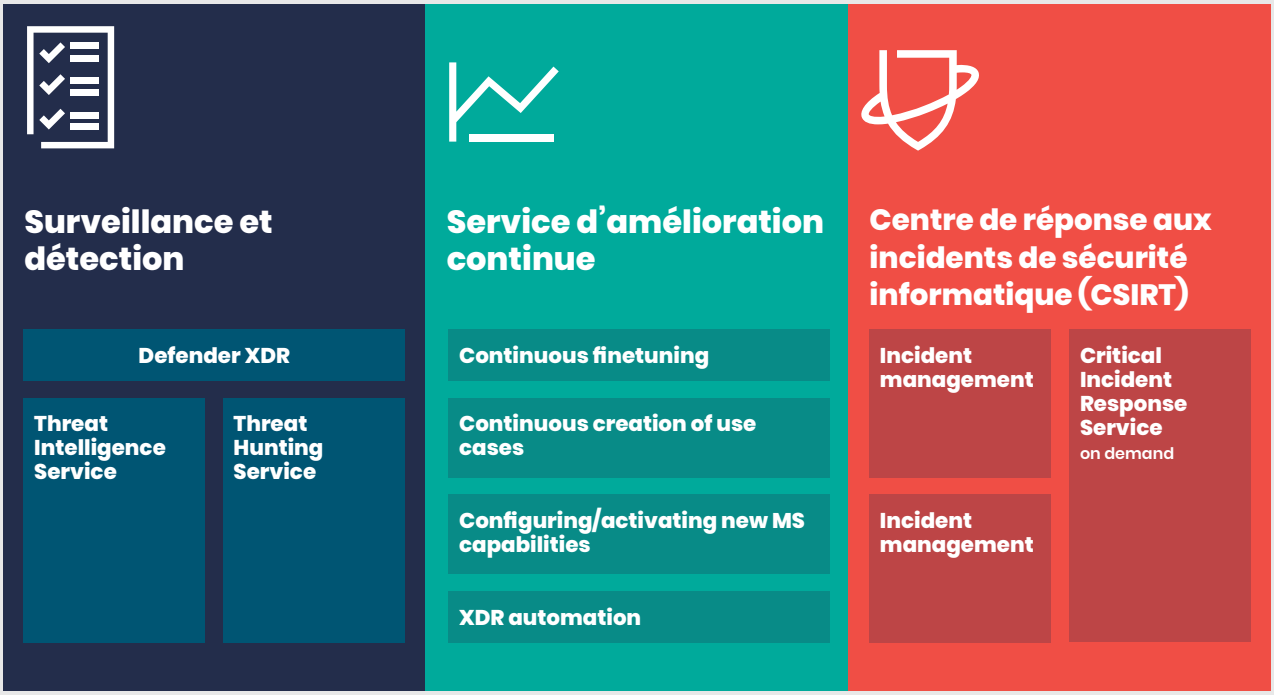
Ce nouveau managed service s'appuie sur la solution existante de Microsoft XDR (pour eXtended Detection and Response), y compris le volet critique « Réponse aux incidents ». Notre propre **Security Operations Center (SOC)** international assure **la surveillance et la réponse aux incidents, 24 heures sur 24**.

En même temps, vous bénéficiez des avantages d'un **partenaire informatique local et proche** pour le déploiement proprement dit de la solution XDR. Un partenaire qui prend en compte l'ensemble de votre environnement informatique. Ainsi, vous pouvez également utiliser ce nouveau managed service si votre environnement n'est pas principalement basé sur la technologie Microsoft.

Le service MDR Inetum LiveSOC

Nous disposons d'un **réseau de SOC hautement certifiés répartis sur trois emplacements**. Grâce au fonctionnement coordonné et aux procédures de haute disponibilité de nos SOC, nous pouvons vous garantir le bon déploiement de tous nos services.

Notre service de **Managed Detection and Response (MDR)** comprend plusieurs prestations qui se complètent et s'alimentent mutuellement :



Vous voulez en savoir plus ?

Les managed services sont aussi des **solutions sur mesure**. Votre environnement informatique existant, les licences dont vous disposez déjà, votre maturité en matière de cybersécurité : tous ces éléments contribuent à déterminer le type de services que nous pouvons vous offrir, en nous adaptant toujours à votre environnement et à votre organisation.

Vous aimeriez savoir ce que nous pouvons vous apporter ? Nos experts examinent les solutions avec vous. Grâce à notre feuille de route cybersécurité, nous déterminons la maturité de votre cybersécurité et donnons des recommandations pour minimiser vos risques, en conformité avec la réglementation NIS2. Nos experts se feront également un plaisir de vous informer sur les autres services que nous pouvons vous offrir.

Microsoft

Inetum
A. Vaucampslaan 42
1654 Huizingen, België
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum