Cybersecurity Accelerator Program (CSAP)

Accélérer votre transformation numérique sécurisée avec Inetum-Realdolmen

inetum realdolmen
Positive digital flow

Les organisations commencent à récolter les fruits de la transformation numérique qu'elles ont entamée ces dernières années. Certaines ont mené cette transition plus facilement et plus rapidement que d'autres. Mais s'est-elle toujours déroulée en toute sécurité ?

Selon la dernière enquête annuelle de Beltug, la plus grande association de CIO et de décideurs informatiques de Belgique, les organisations placent la sécurité en tête de leurs priorités. Elles manifestent un niveau élevé de **sensibilité** – voire d'inquiétude ? – quant à son importance et son impact.

Une autre enquête utilisateur de Beltug révèle que les organisations ont continué à investir dans les **produits de sécurité** ces dernières années. Les solutions antivirus (81 %), de sauvegarde des données (66 %) et de pare-feu (64 %) ont été les achats les plus populaires, laissant le top 3 inchangé par rapport à 2020. Deux tiers (64 %) des entreprises interrogées par Beltug ont l'intention de poursuivre ces investissements en 2023. Une entreprise sur quatre s'attend même à ce qu'ils augmentent, et la majorité d'entre elles (60 %) préconisent l'achat de solutions de sécurité supplémentaires.

Mais la sécurité **ne se limite pas à l'achat de produits**. Et malheureusement, c'est là que le bât blesse encore…

> « Les dirigeants d'entreprise définissent de nouvelles priorités, comme des stratégies de sécurité informatique, de gestion des données et de sensibilisation des utilisateurs. »
>
> Danielle Jacobs, Beltug

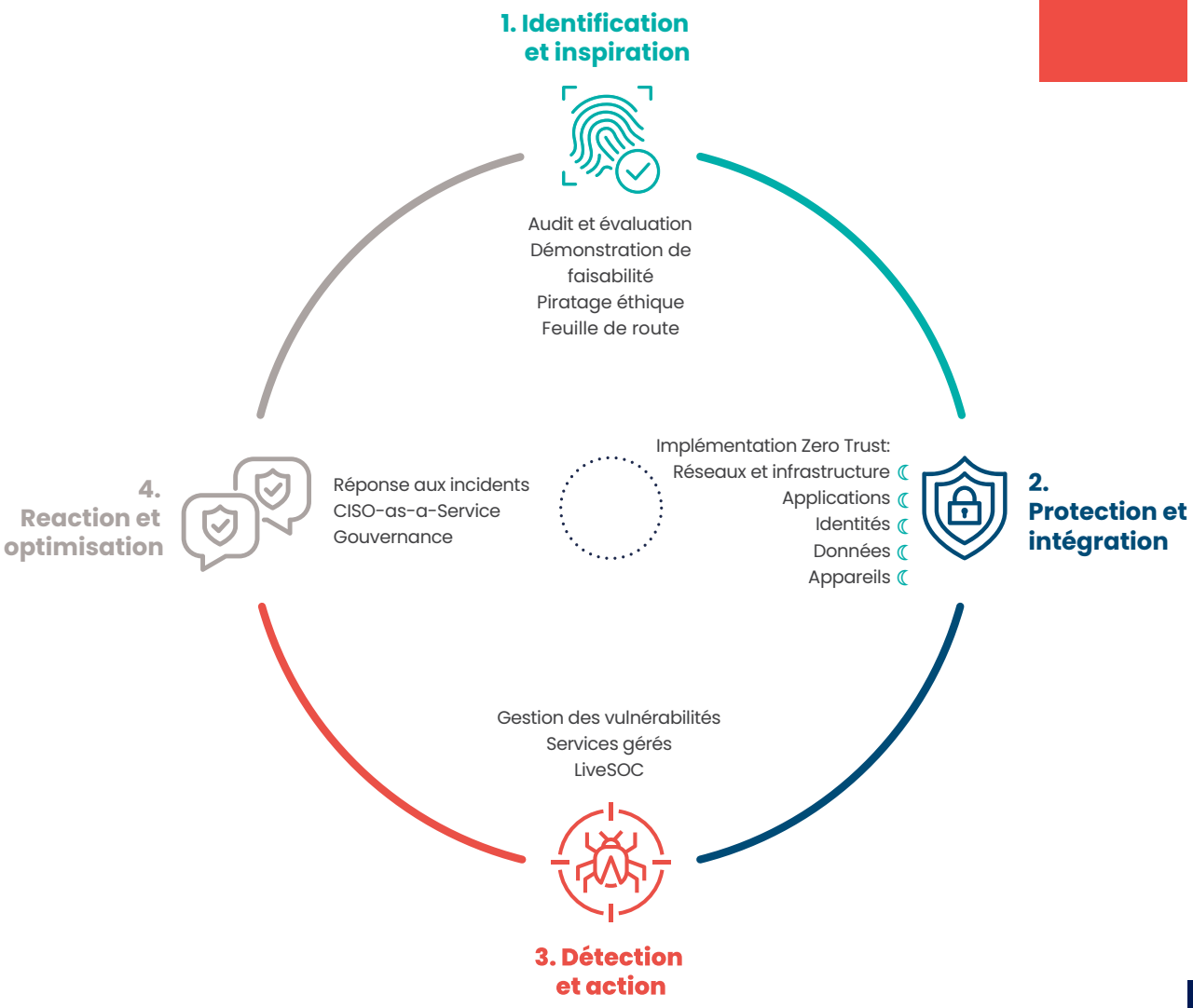
CSAP :
votre garantie d'une accélération numérique sécurisée

Ce n'est pas pour rien que, selon l'enquête annuelle de Beltug, la première priorité des CIO belges consiste à définir et faire appliquer une **vision** claire en matière de cybersécurité dans l'entreprise (46 %). Les problématiques relatives à **l'architecture de sécurité** (39 %) et à **l'engagement des employés** dans les questions de sécurité (38 %) figurent aussi en tête de leurs préoccupations.

Ces aspects clés de la sécurité informatique, qui ne sont pas en lien direct avec les produits, ni parfois même avec la technologie, méritent au moins autant d'attention. Pour qu'aucun d'entre eux ne vous échappe, nous avons développé notre **Cybersecurity Accelerator Program (CSAP)** : un programme complet en quatre étapes fondé sur une offre intégrale de services et de solutions de sécurité, développés selon une approche holistique. Inetum-Realdolmen vous aide ainsi à réaliser la transformation numérique de votre entreprise rapidement et en toute sécurité.

VOUS SOUHAITEZ EN SAVOIR PLUS SUR LES QUATRE ÉTAPES DE NOTRE CYBERSECURITY ACCELERATOR PROGRAM ?

Lisez vite la suite !



1. Identification et inspiration : une bonne préparation est la clé du succès

Avant de pouvoir faire passer votre sécurité au niveau supérieur, vous devez bien sûr savoir où vous en êtes dans votre trajet d'amélioration. C'est pourquoi tout commence par des prises de mesure, des analyses… et des expériences inspirantes !

Pour vous éviter de naviguer à vue, nous commençons par cartographier les points faibles et les **vulnérabilités** de votre organisation. Nous effectuons un **audit de sécurité** pour déterminer son degré de **maturité** en la matière. Pour ce faire, nous utilisons notre propre Cybersecurity Assessment Tool, mais aussi divers audits sur mesure conçus pour évaluer une technologie donnée (comme les réseaux) ou un fournisseur spécifique (comme Microsoft).

Si nécessaire, nous faisons appel à des **pirates éthiques** pour détecter et identifier vos vulnérabilités. Leurs techniques s'étendent de **tests de pénétration** internes et externes à la simulation **d'une attaque par rançongiciel**, en passant par l'**ingénierie sociale** – c'est-à-dire l'exploitation de faiblesses humaines, comme la curiosité ou l'égoïsme – et **l'évaluation de votre code**.

Après avoir identifié les risques potentiels, nous vous aidons à définir les priorités et les actions à entreprendre pour mieux vous protéger contre les cyberattaques. Cet exercice d'analyse stratégique se traduit par une **feuille de route** de cybersécurité, un plan par étapes avec des recommandations concrètes, une liste de projets et les budgets à prévoir, qui pourra vous servir de guide pratique pour les années à venir.

Vous vous demandez si une solution donnée conviendrait à votre organisation ? Nous élaborons volontiers une **démonstration de faisabilité** pour en explorer les possibilités et la valeur ajoutée. Pour vous inspirer, nous organisons aussi des **ateliers** sur les dernières innovations dans le domaine de la cybersécurité.

« La cybersécurité n'est pas une obligation de conformité, mais un aspect vital de la protection de votre entreprise. »

Pieter Byttebier, CCB

VOTRE ORGANISATION EST-ELLE PRÊTE POUR NIS2 ?

En plus du marché, **la législation aussi impose de plus en plus d'exigences en matière de cybersécurité** aux entreprises. Un exemple frappant est la directive NIS2, **une nouvelle directive européenne qui entrera en vigueur en 2024** et est déjà considérée comme le RGPD de la cybersécurité. Son objectif ultime est d'améliorer la protection des organisations et la gestion des risques et de prévenir les incidents, ou d'en limiter les conséquences.
La directive NIS2 concerne **11 secteurs** de plus que NIS1. Selon une première estimation du Centre pour la Cybersécurité Belgique (CCB), **2 400 entreprises belges** relèveraient du champ d'application de la nouvelle directive.

Vous faites partie des entreprises concernées par NIS2 ? Dans ce cas, nous vous recommandons de réaliser dès à présent une analyse de maturité et une feuille de route de cybersécurité. Vous aurez ainsi le temps de prendre les mesures nécessaires pour poursuivre vos activités en toute sécurité, conformément à la nouvelle directive NIS2. Cela vous permettra aussi d'étaler vos frais.

2. Protection et intégration : une approche proactive avec la sécurité Zero Trust

Passée l'étape de préparation, il est important de développer une infrastructure de sécurité solide et adaptée à vos besoins. Vous devez en outre veiller à ce qu'elle s'intègre parfaitement à votre environnement informatique existant. Mais plus important encore, cette infrastructure doit reposer sur une architecture de sécurité innovante et tournée vers l'avenir : l'architecture Zero Trust.

Cette nouvelle **approche proactive** de la sécurité est basée sur un **processus de vérification continue**, selon un principe fondamental : « Ne jamais faire confiance, toujours vérifier ! »

Le concept de sécurité Zero Trust vous permet de réagir plus rapidement et plus efficacement aux menaces. Il vous met en mesure de combattre efficacement les attaques, voire de les prévenir. Pour ce faire, cette approche combine un large éventail d'**outils de contrôle et de mécanismes adaptatifs**.

Pour mettre en œuvre le modèle Zero Trust, il ne suffit donc pas d'acquérir un produit, un service, une solution ou une technologie et de l'implémenter une fois pour toutes. Il s'agit d'une dynamique de **gestion constante**, d'effort à long terme et de **vigilance permanente** face à l'émergence de nouveaux risques.

« Pour l'achat de produits de sécurité, la plupart des entreprises préfèrent un partenaire informatique local. »

Beltug. – B2B Market Survey, ICT Trends 2022: Security

UNE ARCHITECTURE ZERO TRUST REPOSE SUR 5 PILIERS ESSENTIELS :

1. **Identités :** vérifiez les identités et authentifiez toujours les utilisateurs avant de leur donner accès à votre environnement de travail, via l'authentification multifactorielle, l'authentification unique, la gestion des identités et des accès, la gestion des accès à privilèges et l'authentification basée sur les risques
2. **Appareils :** interdisez l'accès votre environnement de travail aux appareils non sécurisés via la gestion des appareils mobiles, la conformité des appareils et la protection des terminaux
3. **Réseaux et infrastructure :** sécurisez vos réseaux et votre infrastructure grâce à la segmentation, la protection contre les menaces et le chiffrement
4. **Applications et API :** contrôlez vos applications et API via les autorisations d'accès, l'accessibilité, le contrôle et la gestion des correctifs
5. **Données :** protégez vos données à tout moment en les classifiant, les étiquetant et les chiffrant, par la prévention de la perte des accès et des données et en prévoyant des solutions de sauvegarde et de récupération

Pour sécuriser chacun de ces piliers, vous avez non seulement besoin des **solutions technologiques** adéquates, mais aussi de l'**expertise nécessaire** pour les implémenter et les intégrer. Avec notre offre de **services et de solutions de bout en bout**, vous avez déjà tout ce qu'il vous faut. Nous pouvons vous garantir une **base solide** pour chacun des piliers ci-dessus, grâce à des solutions de visibilité et d'analyse, d'automatisation et d'orchestration et enfin, de gouvernance.

VOUS SOUHAITEZ DÉCOUVRIR LES TECHNOLOGIES ET LES SOLUTIONS DE SÉCURITÉ CONCRÈTES QUE NOUS PROPOSONS POUR LA MISE EN ŒUVRE DE L'APPROCHE DE SÉCURITÉ ZERO TRUST ?

Pour en savoir plus, consultez notre brochure : « Zero Trust : la nouvelle norme du paysage de la cybersécurité ».

3. Détection et action : une vigilance de chaque instant

Votre architecture et votre infrastructure de sécurité sont parfaitement au point ? Là encore, la vigilance reste de mise !

En effet, la majorité des cyberattaques réussies trouvent leur origine dans une vulnérabilité connue qui n'a pas été découverte et corrigée à temps. Pire, il arrive qu'elles exploitent une vulnérabilité dont l'organisation ignorait l'existence et qu'elle n'a repérée que des semaines, voire plusieurs mois après les faits. Lors d'une étude menée par le centre de recherche américain Ponemon Institute, six personnes interrogées sur dix (62 %) ont déclaré qu'elles n'avaient pas connaissance des vulnérabilités dans leur organisation avant d'être victimes d'une cyberattaque.

Cela montre l'importance d'une gestion continue et systématique des points faibles. Cette gestion passe par la définition, l'identification, la classification et la **hiérarchisation des vulnérabilités** dans votre infrastructure et vos applications. Pour vous aider à traiter l'énorme quantité de vulnérabilités potentielles, nous menons une **analyse approfondie des risques**, qui vous donne une vision claire des priorités et vous permet d'intervenir rapidement et efficacement.

Dans une proposition de résolution contre la fraude sur Internet, la Chambre des représentants de Belgique a dénombré 37 982 incidents liés à la cybercriminalité pour l'année 2021. Cela représente **plus de 100 cyberattaques par jour**, soit une augmentation de 37 % par rapport à 2019.

VOTRE SÉCURITÉ NOUS TIENT PLUS QUE JAMAIS À CŒUR

Si la mise en place d'une infrastructure de sécurité est une chose, sa **gestion** et son **optimisation** en est une autre. C'est peut-être un défi encore plus important, car vous devez exercer une **surveillance permanente** pour détecter les menaces et les vulnérabilités potentielles.

Aussi automatisé soit-il, un tel suivi **24 h/24 et 7 j/7** requiert beaucoup de main-d'œuvre et d'expertise. Vous n'avez pas les capacités nécessaires ? Pas de problème : nous pouvons gérer, optimiser et contrôler toutes les solutions que nous mettons en œuvre dans votre organisation, à la fois sur site et à distance.

Rien qu'en Belgique, vous pouvez compter sur près d'une centaine de spécialistes en sécurité. En collaboration avec les plus de 85 experts nearshore de **LiveSOC**, notre **Security Operations Center (SOC)** en Espagne, ils vous proposent une large gamme de **managed security services**, de la prévention à la récupération en cas de sinistre, pour que vous puissiez mener vos activités l'esprit tranquille.

Avec la technologie **SIEM (Security Information & Event Management) et SOC-as-a-Service**, nous vous proposons un service géré 24/7, qui analyse et corrèle les données de sécurité et soumet des rapports au regard critique de nos experts. Vous préférez démarrer à plus petite échelle ? Vous pouvez compter sur notre service MicroSOC, qui surveille votre environnement et vous informe en cas d'urgence, sans que vous ayez besoin d'une solution SIEM/SOC complète.

4. Réaction et optimisation : une question d'amélioration continue

En cas de problème, avez-vous un plan ? En réagissant rapidement et de manière appropriée à un incident de sécurité, vous pouvez non seulement limiter les dégâts, mais aussi empêcher d'autres incidents et accélérer votre reprise.

Pourtant, selon la dernière enquête utilisateur de Beltug, à peine la moitié des entreprises en Belgique disposent d'un plan de sécurité. Les grandes entreprises (74 %) et les moyennes (61 %) s'en sortent un peu mieux en la matière.

Or, **les petites entreprises** sont de plus en plus souvent prises pour cible par les cybercriminels. En 2020, pas moins de quatre PME sur dix (42 %) en Belgique et aux Pays-Bas ont été confrontées à des attaques, lesquelles ont entraîné une interruption des activités dans quatre entreprises touchées sur dix (38 %).

Que faire si vous êtes victime d'une cyberattaque ? Bien entendu, nous sommes à vos côtés. En amont, nous formulons des recommandations ciblées et vous aidons à établir un plan de récupération. En aval, vous pouvez compter sur nous pour **traiter les incidents** éventuels – c'est le volet « Incident Response ». Grâce à **nos équipes d'intervention spécialisées**, nous mettons tout en œuvre pour que votre entreprise soit à nouveau opérationnelle dans les plus brefs délais.

> « 48 % des organisations ne savent pas quoi faire ou comment réagir de manière appropriée en cas de cyberattaque. »
>
> Agoria, « La sécurité industrielle dans l'industrie manufacturière », 2021

Un **Chief Information Security Officer (CISO)** peut apporter une valeur ajoutée à votre entreprise pour plusieurs raisons, sans compter que vous pouvez être légalement tenu d'en désigner un. Vous n'avez pas besoin d'un CISO à temps plein ? Dans ce cas, nous vous présentons volontiers notre CISO-as-a-Service : un expert en sécurité qui remplit la fonction de CISO chez vous à temps partiel.

AVANT D'OUBLIER… NE PERDEZ PAS DE VUE LA GOUVERNANCE

La cybersécurité **n'est pas qu'une question technologique**. La gouvernance est un aspect au moins aussi important. Concrètement, il s'agit de votre **politique** et de vos **procédures** en la matière, ainsi que de la **culture** de sécurité que vous instaurez. Par exemple, il est essentiel que vos employés soient informés des risques et connaissent le rôle qu'ils ont à jouer pour protéger l'organisation.

Il est important de savoir que la cybersécurité n'est pas un aspect statique de votre gestion d'entreprise, mais un **processus cyclique** et un chantier permanent. En tant que responsable de la sécurité, vous n'avez jamais vraiment terminé. Une politique de gouvernance efficace vise donc l'amélioration continue des attitudes relatives à la cybersécurité, notamment par des **formations régulières**, des campagnes de **sensibilisation** et un plan de réponse aux incidents.

En alignant vos **objectifs de cybersécurité** sur vos objectifs d'entreprise généraux et vos stratégies de gestion des risques, vous intégrez les meilleures pratiques à votre culture et vos processus d'entreprise. Plutôt qu'un poste de frais, la cybersécurité devient ainsi un **investissement stratégique rentable**.

LA SÉCURITÉ ? UN TRAVAIL D'ÉQUIPE !

Dans quelle mesure votre environnement est-il sécurisé ? Avez-vous déjà pris un instantané de la cybersécurité dans votre organisation ? Comment faire pour implémenter une architecture Zero Trust et la tenir à jour ? Vous avez peut-être déjà suivi une partie de ce Cybersecurity Accelerator Program, mais vous souhaitez approfondir certains aspects. Où que vous en soyez dans votre parcours de sécurité, nous sommes à vos côtés. Pour tous les services et piliers technologiques abordés dans ce document, nous disposons de l'expertise nécessaire. Car la sécurité de votre environnement est un travail d'équipe !

CONTACTEZ-NOUS

Powered by our Cybersecurity Partners

Microsoft · paloalto NETWORKS · FORTINET · CHECK POINT · vmware · TREND MICRO
HPE aruba networking · HOXHUNT · citrix · CROWDSTRIKE · AvePoint · CISCO
tenable · kaspersky · VEEAM · COMMVAULT · Secutec · THALES
splunk> · zscaler · netskope · MICRO FOCUS · Forcepoint

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

inetum realdolmen
Positive digital flow