SECURESEAT

L'offre sécurité managée par © TD SYNNEX 365

Pourquoi SECURESEAT 365 offre la meilleure protection à vos clients PME ?

TD SYNNEX | aDvens
Security for the greater good

Microsoft

Et si vous deveniez acteur d'une solution qui ne vous demande pas d'investissement ?

Dans un contexte où les menaces informatiques qui pèsent sur les entreprises prennent de multiples formes, **il est de plus en plus difficile pour les PME de se protéger correctement.**

En effet, elles n'ont pas la possibilité d'engager tous les spécialistes dont elles auraient besoin, **alors même que les attaques informatiques sont de plus en plus virulentes.**

Souhaitant se mettre à l'abri des dommages considérables que peuvent produire ces cyberattaques, **les PME ont donc besoin de solutions simples à mettre en place pour externaliser facilement leur sécurité tout en bénéficiant de la protection la plus avancée.**

De votre côté, vous êtes en recherche **d'offres clés en main,** qui ne nécessitent pas d'investissement (ressources, matériel, logiciels…), qui valorisent votre expertise pour accompagner vos clients.

SECURESEAT 365 by TD SYNNEX est une offre de services de sécurité avancés, développée grâce à la collaboration avec Advens et Microsoft. Elle assure un service de détection et de réponses (MDR : Managed Detection & Response).

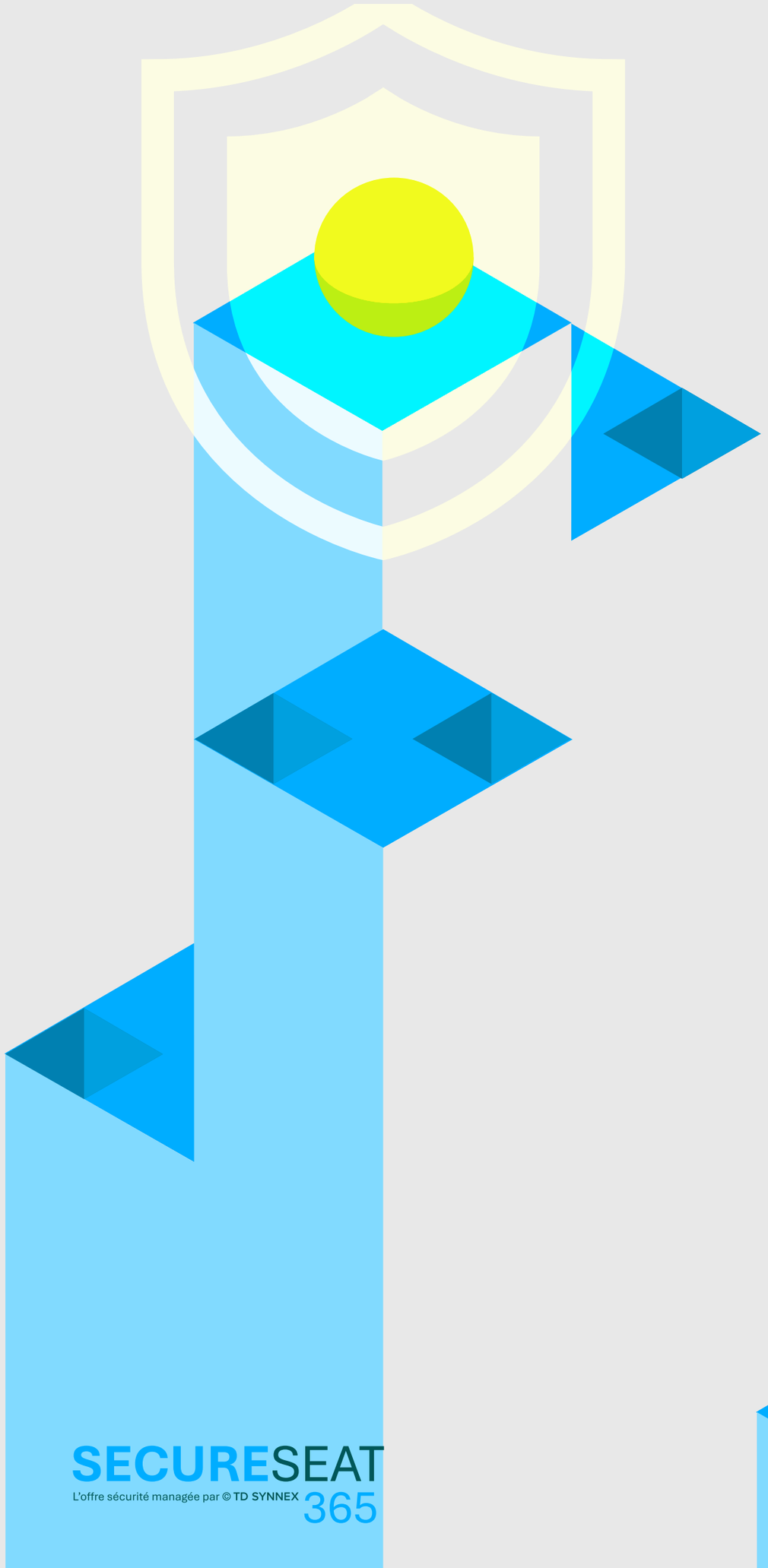
Pour vous, c'est l'opportunité de proposer **une offre facile à mettre en place,** qui ne vous demande pas d'investissement, et qui vous permet de mettre en avant votre rôle de conseil tout en vous reposant sur notre expertise.

Pour vos clients, **c'est la première offre de cybersécurité qui s'appuie sur les fonctionnalités disponibles dans la suite Microsoft pour sécuriser les environnements Microsoft.** Grâce à vous, il peut être épaulé par une équipe complète de professionnels pour faire face aux attaques multiples et complexes.

En 2025, **50%** des organisations utiliseront l'offre de service MDR.

Source Gartner 2020

SECURESEAT
L'offre sécurité managée par © TD SYNNEX 365



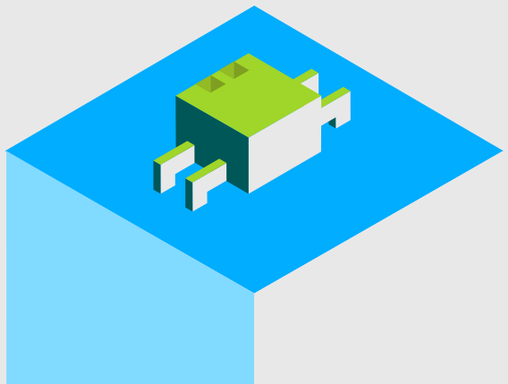
L'offre Managed Detection & Response de TD SYNNEX

Profitez de vos licences Microsoft pour renforcer votre sécurité

SECURESEAT 365 est particulièrement adaptée pour les PME, car elles ne disposent généralement pas des outils et des compétences nécessaires pour sécuriser leur environnement informatique.

Cette solution MDR assure **la surveillance des infrastructures tout en détectant et en résolvant activement les menaces** actuelles et émergentes grâce à une combinaison de technologies de sécurité avancées, d'outils et d'expertises. **C'est un accès facilité à une protection de pointe.**

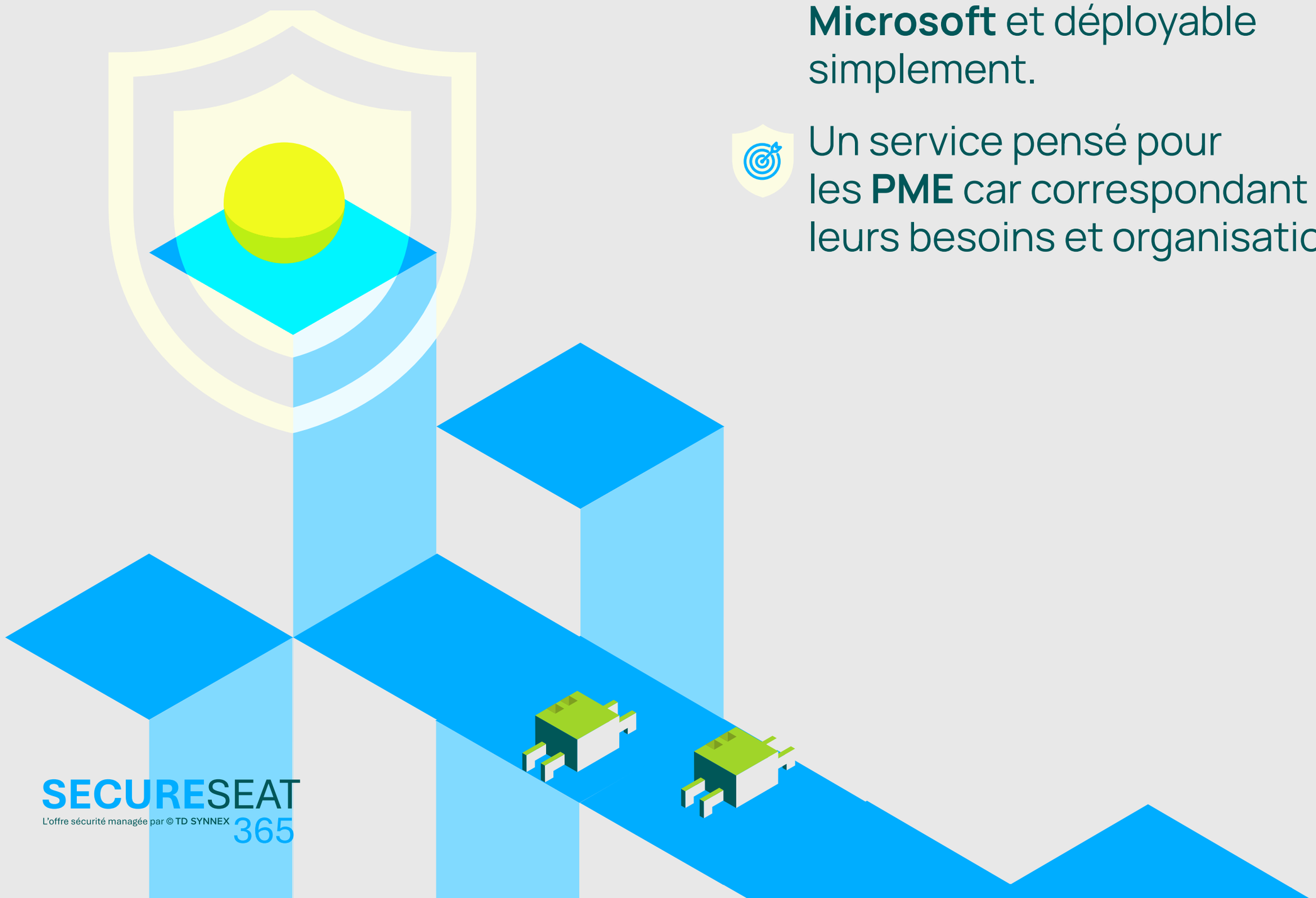
Basée sur un SOC, elle utilise les outils Microsoft (XDR, SIEM/SOAR, Microsoft 365 Defender et Sentinel).



Comment ça marche ?

Une équipe de sécurité surveille de manière constante le réseau de la PME, ainsi que ses points d'accès, et analyse les données provenant de tous les autres systèmes, offrant ainsi une vision globale de son paysage sécuritaire.

Cette approche permet aux organisations **d'acquérir une compréhension approfondie de leurs environnements de sécurité** tout en renforçant leurs capacités de détection et de réponse aux menaces.



- Un service **24/7** offrant une protection cyber proactive et préventive entièrement gérée.
- Une capacité à **bloquer les cyberattaques** en temps réel grâce aux analyses et aux actions des analystes cyber.
- Un service totalement **intégré aux outils technologiques Microsoft** et déployable simplement.
- Un service pensé pour les **PME** car correspondant à leurs besoins et organisation.

Une réglementation européenne attentive aux PME

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a pour mission de développer une politique permettant de défendre les infrastructures numériques publiques et privées les plus critiques.
Face à l'augmentation de la menace, elle a publié la directive NIS 2 au Journal Officiel de l'Union Européenne en décembre 2022.

En effet, les acteurs malveillants, toujours plus performants et mieux outillés, touchent de plus en plus d'entités trop souvent mal protégées.

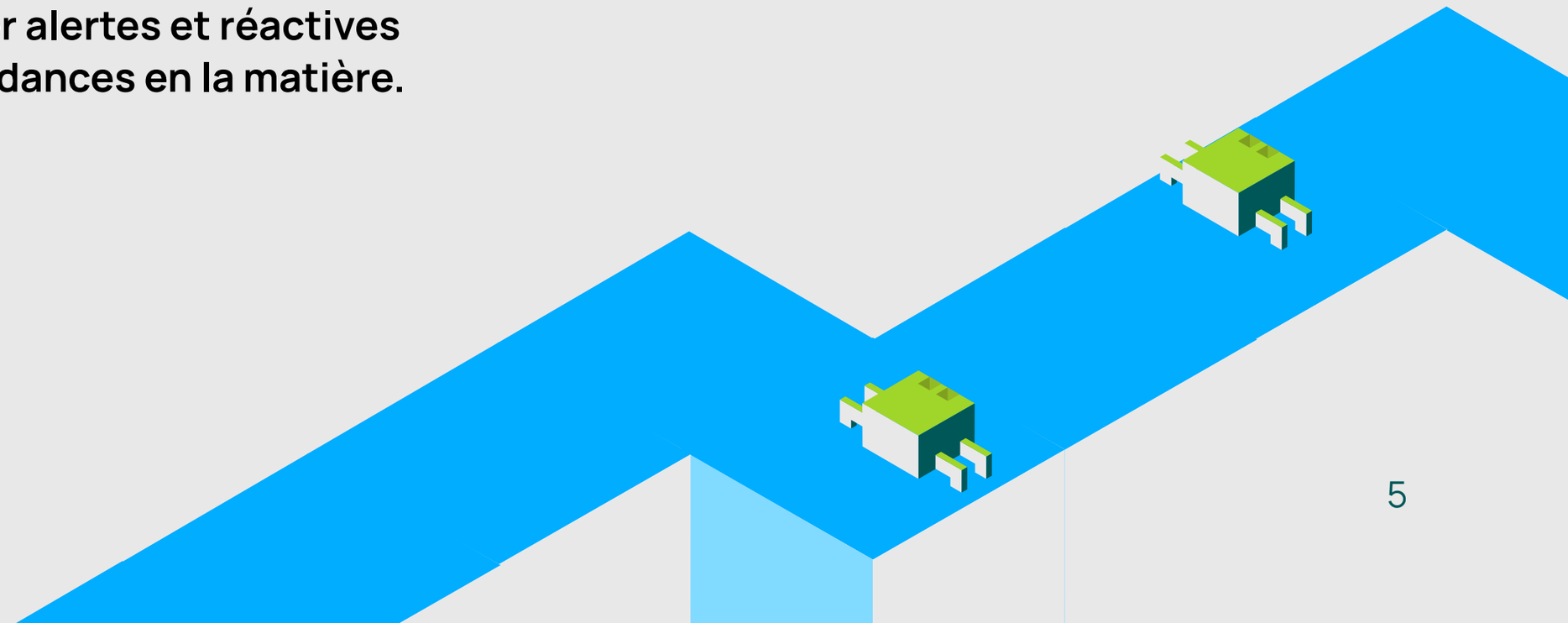
60 % des attaques qui sont remontées à l'ANSSI concernent des petites structures (PME/TPE/ETI et collectivités territoriales).

Cela s'explique car il est difficile pour ces organisations de rester alertes et réactives face aux dernières tendances en la matière.

La directive NIS 2 élargit donc ses objectifs et son périmètre d'application pour leur apporter davantage de protection. En faisant la promotion de la sécurité numérique auprès d'entités ne disposant pas d'expertise en la matière, **elle souhaite les inciter à mettre en place les mesures de protection de base face à la cybercriminalité.**

Vigilante, l'ANSSI observe également une évolution des attaques qui ciblent désormais les chaînes de sous-traitance pour se rapprocher de leurs clients finaux.

Les cybercriminels ciblent souvent des fournisseurs ou partenaires d'une entreprise pour compromettre indirectement la sécurité de la cible principale, exploitant les relations inter-entreprises pour propager les attaques.



Accélération des menaces

Les tendances en matière de cyberattaques sont nombreuses et mouvantes.
En voici quelques-unes :

Ransomware en tant que service (RaaS)

Certains criminels proposent des services de ransomware sur le dark web. Ce système rend la piraterie informatique accessible à des individus malveillants moins experts, moyennant le paiement d'une commission.

Double extorsion

Les attaquants adoptent de plus en plus la tactique de la double extorsion. En plus de chiffrer les fichiers, ils menacent de divulguer des données sensibles préalablement volées, incitant ainsi les victimes à payer la rançon pour éviter une fuite d'informations compromettantes.

Attaques contre les objets connectés (IoT)

Les objets connectés, souvent moins sécurisés, sont devenus une cible privilégiée pour les attaquants qui exploitent leur vulnérabilité afin d'accéder aux réseaux d'entreprises.

Utilisation accrue de l'IA et de l'apprentissage automatique

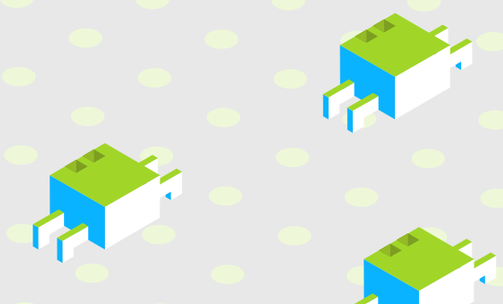
Les attaquants exploitent des technologies comme l'intelligence artificielle et l'apprentissage automatique pour améliorer l'efficacité de leurs attaques, en adaptant leurs méthodes en fonction des défenses de sécurité mises en place.

Attaques par hameçonnage sophistiquées

Les attaquants utilisent des techniques d'hameçonnage de plus en plus sophistiquées, telles que l'hameçonnage par ingénierie sociale ciblée, pour tromper les employés et les inciter à divulguer des informations sensibles.

Attaques contre les identifiants privilégiés

Les attaquants ciblent les comptes avec des privilèges élevés, tels que les administrateurs système, pour accéder à des informations sensibles et prendre le contrôle des systèmes critiques.



Top 3 des menaces les plus courantes

Ransomware

Aussi appelé “rançongiciel”, il s’agit d’un **type de logiciel malveillant (malware) conçu pour chiffrer les fichiers et les rendre inaccessibles à l’utilisateur.** Les cybercriminels exigent ensuite le paiement d’une rançon en échange de la clé de déchiffrement permettant de restaurer l’accès aux fichiers. Les attaques par ransomware peuvent avoir des conséquences dévastatrices, notamment pour les PME. Elles engendrent des perturbations opérationnelles, des coûts financiers considérables et potentiellement la perte de données importantes.

Cheval de Troie

Également appelé “trojan”, le cheval de Troie est **un type de logiciel malveillant qui se présente comme un programme légitime mais qui cache en réalité des fonctionnalités nuisibles.**

Les utilisateurs sont souvent trompés pour installer involontairement ces programmes malveillants, pensant qu’ils exécutent une tâche légitime. Une fois installé, le cheval de Troie permet à des attaquants d’accéder et de prendre le contrôle du système infecté, d’espionner l’utilisateur, de voler des informations sensibles, ou encore de compromettre la sécurité du système.

Vol de données

La collecte non autorisée d’informations sensibles, stratégiques ou confidentielles peut cibler des secrets commerciaux, des informations de recherche et développement, des données client, des plans financiers, etc. **Ces données volées peuvent ensuite être exploitées à des fins lucratives, politiques ou compétitives,** mettant en péril la sécurité et la compétitivité de l’entreprise visée.

Les bénéfices de l'offre SECURESEAT 365

Réduction des risques

Grâce à la détection et à la réponse proactive des menaces, votre organisation est mieux protégée et les cyber-risques sont considérablement réduits :

- **Assurance de la résilience** de votre entreprise contre tout risque d'interruption d'activité (ex : ransomware),
- **Renforcement de la confidentialité** de vos données clients (exfiltration, spyware),
- **Aide pour minimiser les primes de cyber assurance,** et pour vous mettre en conformité avec les réglementations françaises et européennes,
- **Surveillance de vos actifs** les plus exposés (laptops, messagerie, identités).

Service de protection en continu et pro-actif

L'offre SECURESEAT 365 fournit **un service managé avancé,** délivré par une équipe d'analystes SOC hautement qualifiés et expérimentés grâce à :

- **Un SOC moderne et innovant disponible 24 heures sur 24, 7 jours sur 7** pour opérer une détection précoce des menaces et des incidents, minimisant ainsi le temps de réaction face à une attaque.
- **Une surveillance continue** pour tirer le meilleur parti des innovations techniques. En cas d'incident, les équipes MDR réagissent rapidement pour contenir la menace, minimiser les dommages et faciliter la récupération, ce qui est particulièrement crucial pour les PME souhaitant limiter les perturbations opérationnelles.
- **Des technologies de sécurité cloud de pointe** afin de fournir un service managé avancé, délivré par une équipe d'analystes SOC hautement qualifiés et expérimentés. Les technologies telles que l'analyse comportementale, l'intelligence artificielle et l'apprentissage automatique, permettent de détecter les menaces sophistiquées qui pourraient échapper aux solutions de sécurité traditionnelles.

Notre équipe protège votre organisation en permanence et intervient en temps réel pour contenir les attaques pouvant impacter votre activité. Ainsi, nous réduisons la probabilité et l'impact potentiel d'attaques réussies, afin de garder une longueur d'avance sur l'évolution des menaces.

Protection proactive et préventive, alignée sur l'évolution de la menace et des groupes d'attaquants

Nos services de sécurité managés ont tiré parti des dernières technologies Microsoft. Ils intègrent une protection préventive et proactive grâce à une mise à jour en temps réel des menaces et des renseignements sur les cybermenaces. Cela permet d'anticiper et de bloquer les menaces émergentes et inconnues avant qu'elles ne surviennent.

La proactivité et la prévention sont des approches complémentaires de la protection contre les menaces informatiques.
En combinant les deux, SECURESEAT 365 crée une défense multicouche :

- **Les mesures préventives créent une barrière initiale** contre un large éventail de menaces connues, réduisant ainsi la surface d'attaque globale.
- **Les solutions proactives** permettent de détecter les menaces émergentes et les attaques sophistiquées qui pourraient contourner les mesures préventives.

Gestion technique de l'architecture technologique de détection

Vous bénéficiez d'une architecture technique et technologique de pointe, basée sur Microsoft 365 Defender et Microsoft Sentinel intégrée dans vos outils collaboratifs (M365).

Elle est conçue selon les meilleures pratiques pour offrir plusieurs avantages :

- En utilisant des **fonctionnalités avancées telles que l'intelligence artificielle et l'analyse comportementale,** Microsoft 365 Defender et Sentinel permettent une détection précoce des menaces et des activités malveillantes sur les points d'extrémité, dans la messagerie, et au niveau de l'identité.
- Cette architecture inclut aussi des **fonctionnalités d'automatisation** visant à simplifier et à accélérer certaines tâches courantes de sécurité. Ces fonctionnalités automatisées permettent aux équipes de sécurité de gagner du temps et d'améliorer leur efficacité opérationnelle. Par exemple, Microsoft 365 Defender peut automatiser la réponse aux incidents de sécurité en prenant des mesures correctives préconfigurées en réponse à certaines alertes.
- **Sentinel et Microsoft 365** intègrent des fonctionnalités visant à réduire les fausses alertes telles que le filtrage intelligent des alertes.

Nos analystes adaptent en permanence la configuration des sources de détection à votre contexte et mettent à jour l'ensemble de la chaîne logiciel sans exigence de votre part.

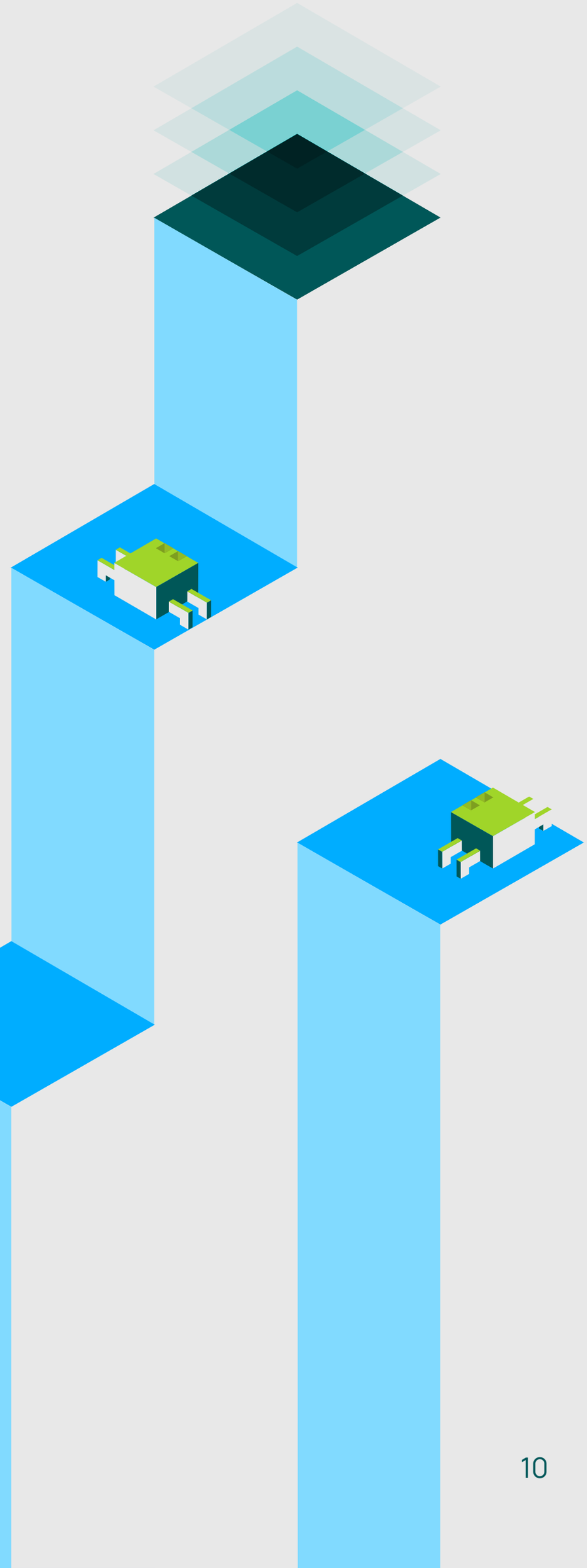
Plus de 20 ans d'expertise en cybersécurité

Avec une longue expérience dans la prestation de services de cybersécurité managés et près d'un million de postes surveillés, **Advens dispose d'un modèle de prestation de services avancés pour compléter nos compétences techniques.**

Ce modèle continue de s'affiner avec les organisations privées et publiques les plus matures en Europe.

Nos services sont certifiés par **les visas de sécurité de l'ANSSI, et nos experts par la certification Sécurité de Microsoft.** Les démarches accessibles sont adaptées à vos besoins et orientées résultats.

Grâce à l'amélioration continue des services, à la gouvernance des services et à la production de rapports, nous assurons une prestation de services optimale.



Un partenariat tripartite

TD SYNNEX x Advens Cybersecurity x Microsoft

Construite autour des solutions Microsoft 365 Defender et Microsoft Sentinel, SECURESEAT 365 est une nouvelle offre qui combine la vaste expertise, la maturité et la portée de TD SYNNEX en matière de cybersécurité avec l'expérience et les références cyber d'Advens.

Le service MDR est fourni au nom du partenaire par Advens, tandis que les experts en sécurité de TD SYNNEX soutiennent les revendeurs en matière d'engagement, d'activité de mise sur le marché et de ventes initiales.

« Nous avons été très impressionnés par les capacités de cybersécurité avancées qu'Advens propose avec son offre MDR. Cela a demandé beaucoup d'efforts et d'investissements pendant de nombreuses années - et ce n'est pas quelque chose qui peut être facilement reproduit ».

Cédric Sroussi, directeur des services pour TD SYNNEX France

Advens est un leader français, indépendant et souverain en matière de Cybersécurité. Présent partout en France (Paris, Lille, Lyon, Marseille, Toulouse, Bordeaux, Nantes et Rennes), ainsi qu'au Québec, à Tahiti et en Espagne, Advens est également un partenaire cybersécurité de premier plan de Microsoft.

« Grâce à ce partenariat stratégique, Advens poursuit sa mission de démocratisation de la cybersécurité sur l'ensemble des organisations françaises. Nous sommes fiers de pouvoir accompagner les partenaires de TD SYNNEX pour faciliter et sécuriser la transformation digitale de leurs clients ».

David Buhan, directeur général d'Advens

TD SYNNEX | Advens
Security for the greater good

Microsoft