Cyberdefense

Micro-SOC Shield

Protéger votre sécurité périmétrique des cyberattaques

La bordure Internet, terrain d'opportunités aux attaques

Votre organisation n'a jamais été aussi connectée à l'Internet qu'aujourd'hui, et elle le sera encore plus demain.

L'augmentation des flux en transit et du remote access renforcent votre exposition en externe, ce qui participe à l'essor de vulnérabilités nouvelles et ouvre plusieurs portes d'entrée aux attaques malveillantes.

De plus, les difficultés de détection, de filtrage et de réaction avec les solutions actuelles, font de la bordure Internet une cible parfaite pour les cyberattaquants.

Il est donc nécessaire de réinventer votre modèle de sécurité périmétrique pour vous protéger des menaces potentielles provenant de l'extérieur.

+ de 42 000
Adresses IP en France présentent une vulnérabilité critique et facilement exploitable
Source : Orange Cyberdefense

94%
Des entreprises scannées en 2022 avaient au moins un service non chiffré exposé à l'Internet
Source : Le Monde Informatique

Près de 70%
Des organisations indiquent que le risque de cyberattaques a augmenté avec l'essor du télétravail
Source : Ponemon Institute

Les risques et les enjeux pour votre entreprise

Phishing

Téléchargement de malwares

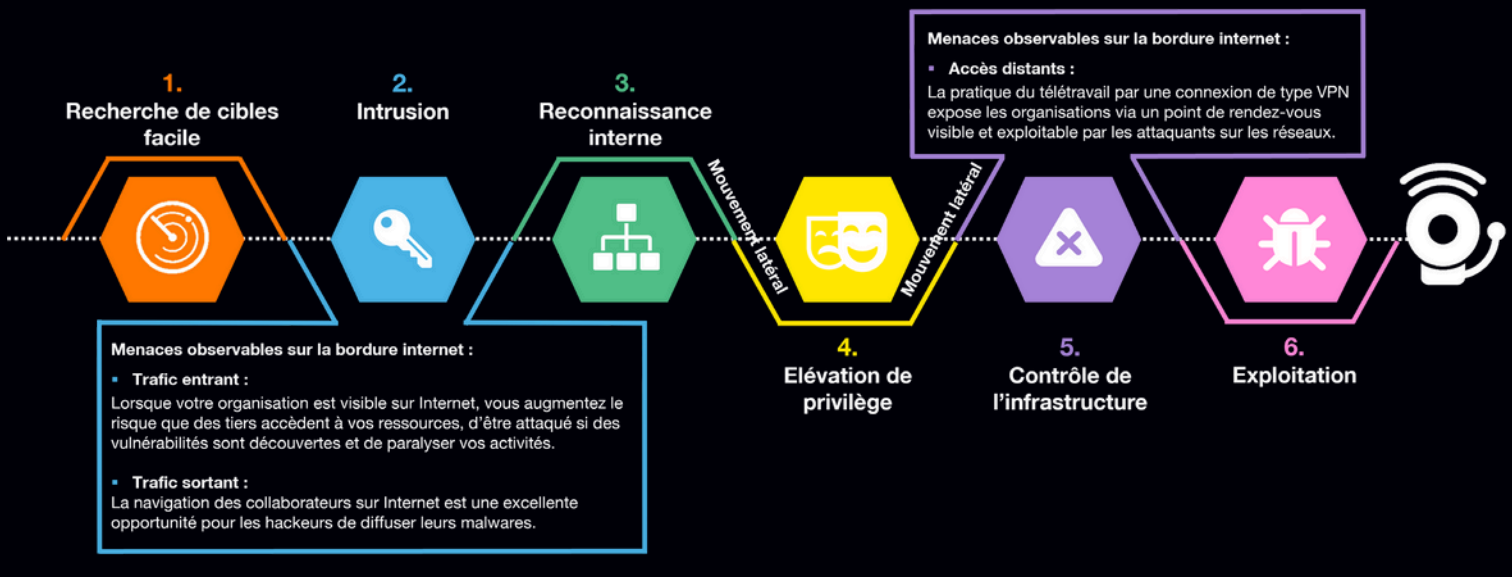
Exploitation de Vulnérabilités

Utilisation de leak user / Mote de passe

Ces incidents peuvent avoir de lourdes conséquences sur votre activité et votre image de marque. Ils peuvent les perturber voire les interrompre et engendrer des dommages et des pertes (chiffrement du SI, extorsion de fonds, fuite de données) en cas d'attaque réussie.

Pour maintenir en condition de sécurité la bordure Internet, il est nécessaire de réinventer votre modèle de sécurité périmétrique pour aller plus loin dans la surveillance et dans la réaction, adaptée à l'évolution de la menace globale.

Les phases d'une cyberattaque, de la reconnaissance à l'exfiltration : Kill Chain



Notre réponse : Micro-SOC Shield

3 piliers de détection et réaction à la menace globale

Flux Internet entrants : les services exposés sur Internet

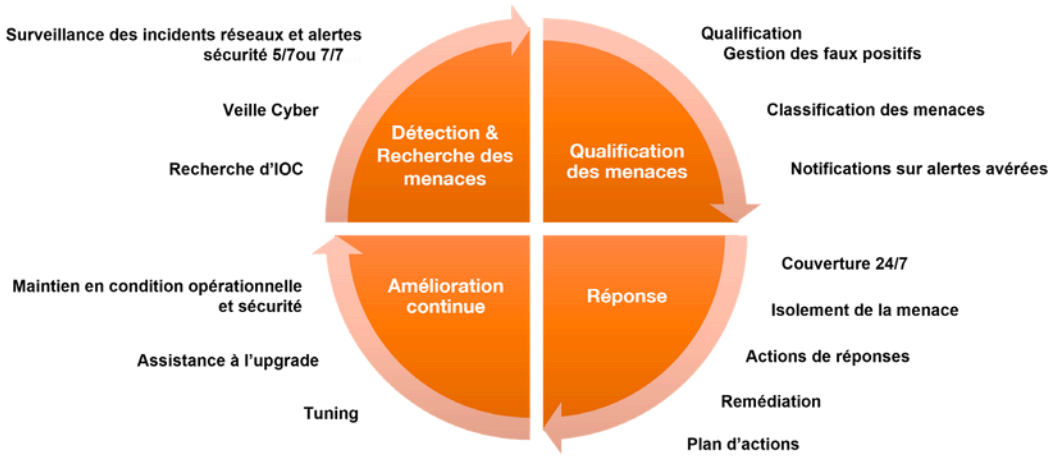
L'identification et la surveillance en continu du trafic entrant permettent de détecter les requêtes suspectes, les actions malveillantes et de filtrer les flux illégitimes selon l'évolution de la menace globale. Nos analystes veillent sur vos portes d'accès, analysent les comportements suspicieux et réagissent pour vous protéger contre ces malveillances.

Flux Internet sortants : le surf des utilisateurs

Le filtrage et la détection en temps-réel des menaces potentielles sur le trafic sortant garantit que chaque clic, téléchargement ou toute autre action de vos collaborateurs restent sécurisées, tout en préservant la productivité et la connectivité. En collaboration avec nos experts, vous définissez une politique de sécurité pour autoriser le trafic approprié tout en vous protégeant des attaques à haut niveau de

Les accès des utilisateurs distants

La mise en place d'un nouveau point de connexion invisible pour les cyberattaquants, au travers d'un agent propre installé sur vos appareils, fait disparaître le point de rendez-vous. Ainsi, un tunnel sécurisé est établi pour permettre à vos travailleurs à distance d'accéder à leurs applications et ressources hébergées en interne et dans le Cloud sans passer par votre organisation.



Vos bénéfices

Sécurisation des flux en transit

Maintenez en condition de sécurité votre exposition sur Internet et réduisez les risques liés au surf de vos collaborateurs.

Un bouclier cyber adapté à vous

Une solution co-managée accessible, performante et intégrée en toute simplicité à votre politique de sécurité.

Protection du télétravailleur

Renforcez la détection et la réaction sur les accès distants et sécurisez la connectivité de vos utilisateurs et ressources.

Amélioration continue par nos experts

Les équipes Micro-SOC gèrent et mettent à jour le Shield face à l'évolution de la menace globale. Vous restez concentré sur vos activités.

Pourquoi Orange Cyberdefense ?

Tout ce que nous faisons est nourri par notre connaissance de la menace.

+ de 1300 clients font confiance au service Micro-SOC.

+ de 280 experts répartis dans 13 CyberSOC pour vous protéger des menaces les plus avancées.