Cyberdefense

Micro-SOC Poste de travail

Protéger mes postes de travail et serveurs des cyberattaques

Le poste de travail et les serveurs, cibles privilégiées des attaquants

Les entreprises sont confrontées à une recrudescence des cyberattaques, avec des menaces de plus en plus sophistiquées. Les postes de travail et les serveurs constituent des points d'entrée stratégiques pour accéder à l'ensemble du système d'information de l'entreprise.

Il devient donc nécessaire de mettre en place des solutions pour anticiper les attaques, sécuriser vos actifs numériques et protéger vos données au travers d'une surveillance continue de vos postes de travail et de vos serveurs.

330 000 PME et TPE attaquées en France en 2022. Ce sont les entreprises les plus touchées.
Source : Cabinet Asterès, 2023

55% des actifs impactés par un incident sont des postes de travail et des serveurs.
Source : Security Navigator 2024

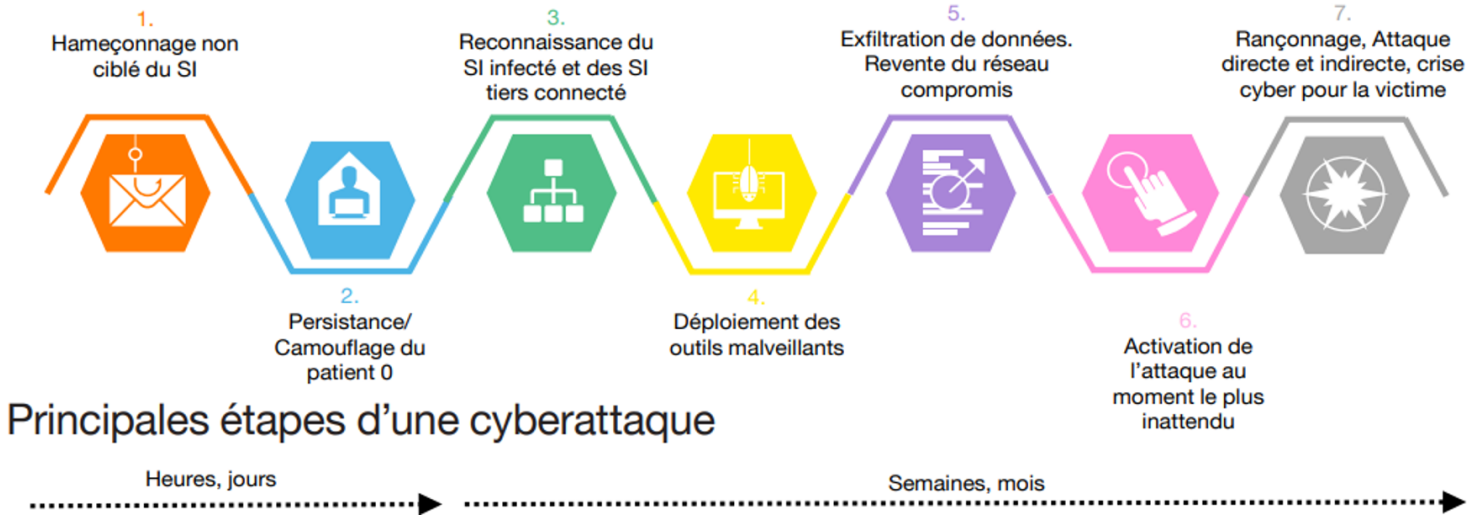
30 % du CA
Correspond au coût moyen d'une cyberattaque pour une entreprise, en plus d'une perte de confiance de ses clients et des partenaires.
Source : Cabinet Asterès, 2023

70 jours
Correspond au temps moyen pour mettre en œuvre une stratégie de remédiation et relancer l'activité de l'entreprise après une cyberattaque.
Source : ANSSI, 2023

Pourquoi anticiper mes cyberattaques ?

Ces attaques peuvent avoir de lourdes conséquences sur votre activité et votre image de marque. Elles peuvent les perturber voire les interrompre et engendrer des dommages matériels et des pertes financières.

En détectant les anomalies au plus tôt, il est possible de les contrer avant qu'elles ne se déploient plus largement.



Principales étapes d'une cyberattaque

Notre réponse : Micro-SOC Postes de Travail

Détection proactive des menaces

Protection et surveillance préventive de vos serveurs et postes de travail. Analyse des incidents et corrélation des informations basées sur l'état de la menace et les dernières techniques cybercriminelles.

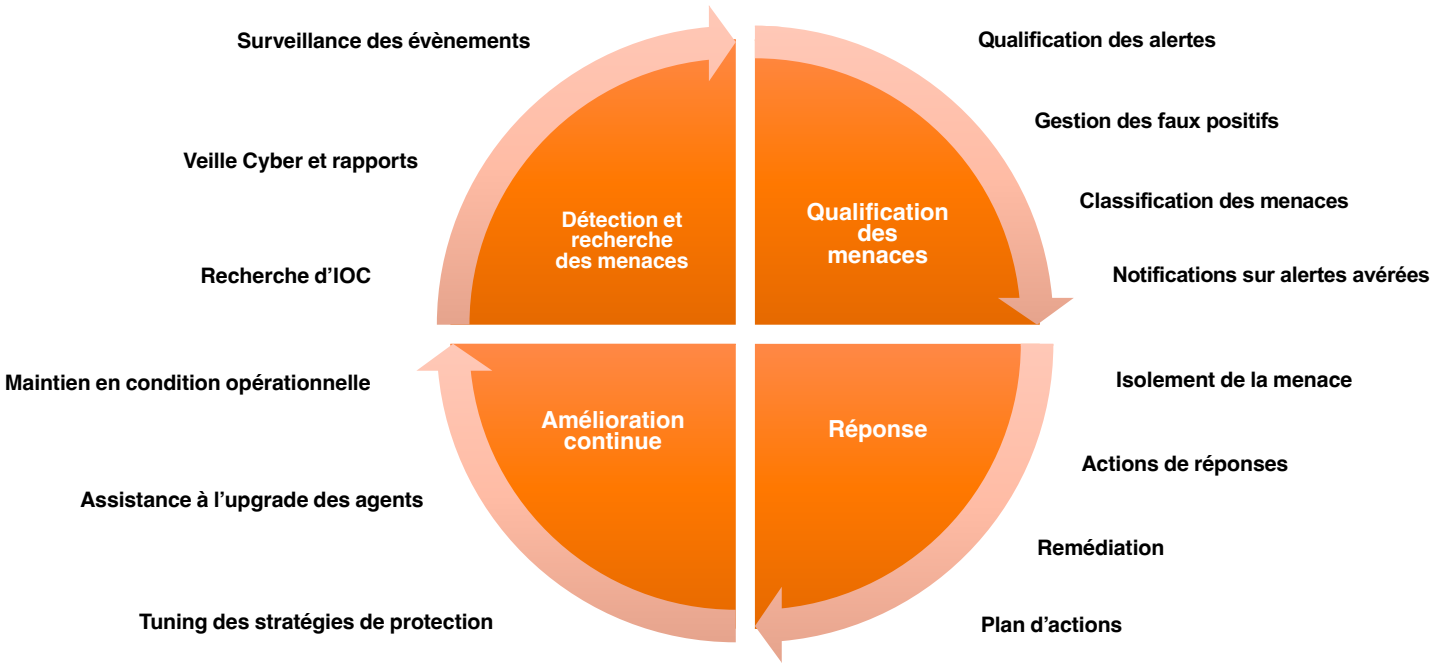
Renfort de la posture de sécurité

Investigations poussées pour une résolution en profondeur de l'incident. Evaluation en continu de votre niveau de vulnérabilité et identification de vos risques cyber.

Réponse ciblée

Neutralisation automatique des compromissions les plus courantes et application de mesures de confinement ciblées des systèmes impactés par l'attaque, adaptées à vos enjeux business.

Les services inclus dans notre offre



Vos bénéfices

- Surveillance 8h/5jours de votre parc. Possibilité de passer en 24h/7jours en option.
- Portail dédié permettant de visualiser votre situation et les actions correctrices à mener, en complément de nos recommandations.
- La tarification à la licence pour adapter la solution à vos évolutions.

Pourquoi Orange Cyberdefense ?

- Tout ce que nous faisons est nourri par notre connaissance de la menace.
- + de 280 experts répartis dans 13 CyberSOC pour vous protéger des menaces les plus avancées.
- + de 1500 clients font confiance au service Micro-SOC.