SOC en mode MSSP: Cybersécurité augmentée

« La résilience n’est plus une option, c’est la nouvelle architecture du progrès. »

kaspersky

Samy TADJINE
Enterprise Account Manager North, West & Central Africa

L’urgence numérique : un monde sous pression

Explosion des cybermenaces

Hybridation du travail

Durcissement réglementaire

Le risque n’est plus une éventualité : il structure désormais les stratégies IT.

Les nouveaux défis du DSI moderne

- Complexité technologique croissante
- Pénurie de talents cyber
- Multiplication des surfaces d’attaque
- Exigence de réactivité accrue

Maintenir le cap de votre Mission:

Renforcer la sécurité de votre système d‘information afin de contrer toutes les attaques d‘ou qu‘elles viennent

La fin du modèle défensif traditionnel

Les approches réactives appartiennent au passé.

La cybersécurité moderne repose sur la détection continue, la réponse proactive et l'anticipation des menaces.

XDR

Threat Intelligence

SIEM

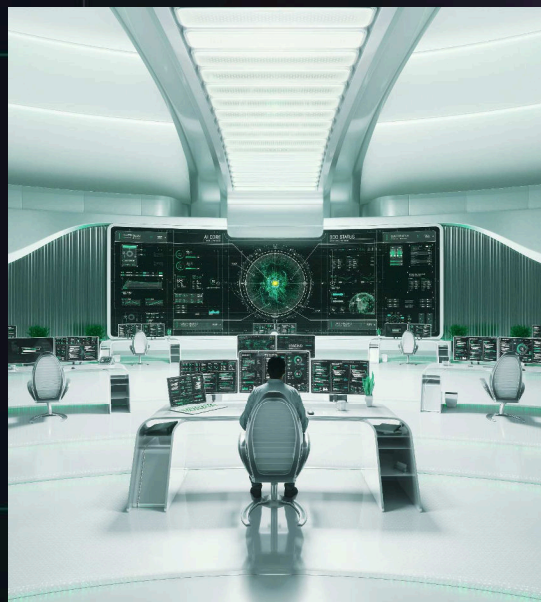
Le modèle MSSP : une réponse agile et durable

- Externaliser la surveillance, la détection et la réponse aux incidents.
- S’appuyer sur un partenaire de confiance permet d’assurer une protection 24/7 et de renforcer la résilience globale.

Un Managed Security Service Provider (MSSP) gère et surveille les appareils et les systèmes et permet à ses clients de se protéger des acteurs malveillants. Toute organisation ne disposant pas de l'expertise ou des ressources nécessaires en interne pour se défendre peut se tourner vers un MSSP, qu'il s'agisse d'une agence de création de 20 personnes, d'une grande entité gouvernementale ou de toute autre entité intermédiaire.

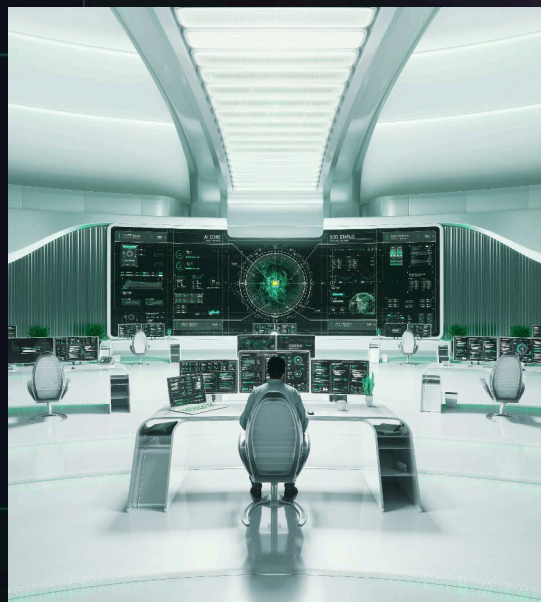
Aujourd'hui, les MSSP devraient être en mesure de fournir :

- Détection proactive des menaces (attaques, anomalies, comportements suspects...).
- Réponse rapide aux incidents (investigation, remédiation).
- Renseignements sur les menaces (Threat Intelligence).
- Surveillance continue des systèmes d'information, réseaux, endpoints, etc....
- Technologies avancées (Machine learning, IA, etc....).
- Réduction des risques de sécurité (audits).
- Evolutivité (Capacité à gérer des environnements complexes ou multi-sites).
- Conformité réglementaire (ex : RGPD, ISO 27001...).



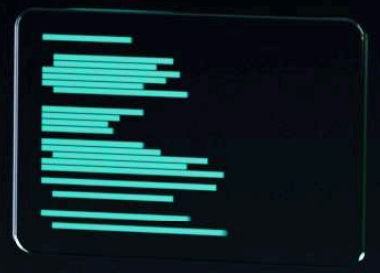
DSI : Comment Choisir votre MSSP?

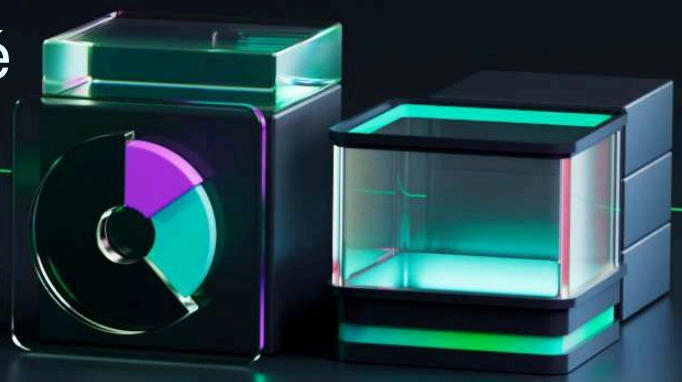
- Evaluation des besoins
- Réputation et références clients
- Certifications et conformité
- Services Offerts
- Support et communication:
  - SLA
  - Réactivité et Accessibilité
- Expérience sectorielle
- Technologies utilisées



Cybersécurité augmentée : IA, ML et automatisation

- Les nouvelles technologies renforcent la détection, l'analyse et la réponse aux menaces.
- L'intelligence artificielle rend la cybersécurité plus prédictive, rapide et efficace.



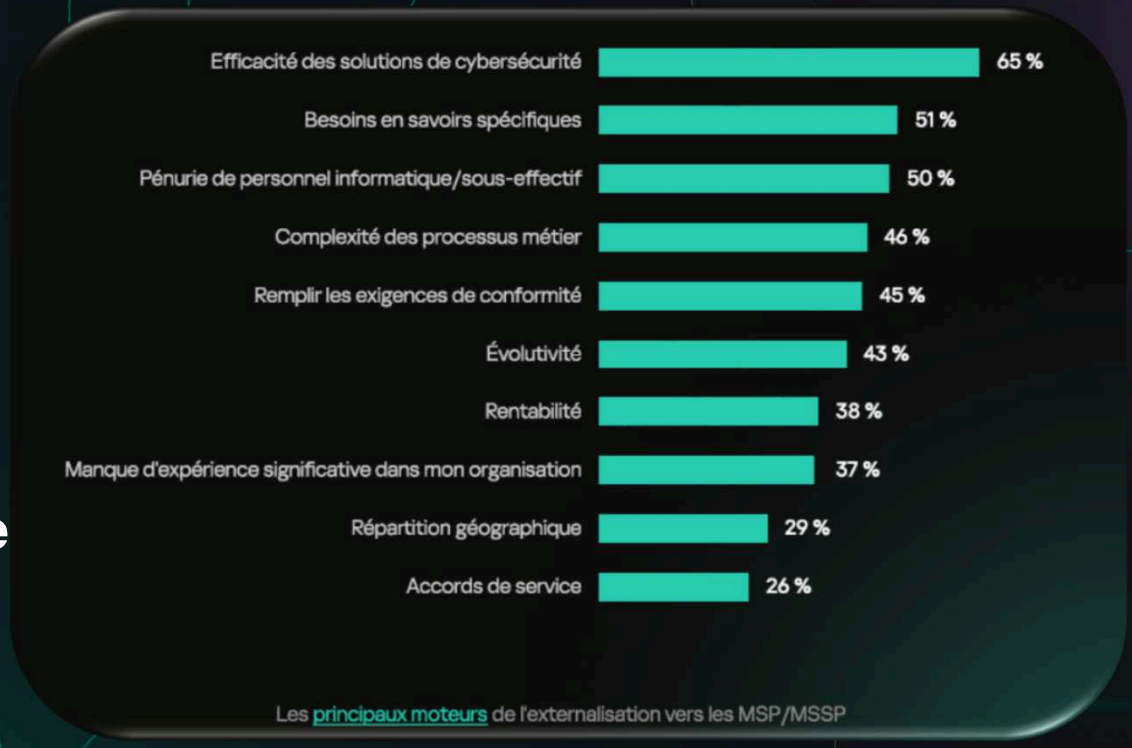


L'importance du choix: Pourquoi les DSI basculent vers ce modèle

Mais pour réussir, il convient de vous associer à **un partenaire stable et digne de confiance**, capable de protéger votre investissement. Si choisir une entreprise naissante peut s'avérer rentable à court terme, vous risquez de voir votre investissement englouti par la suite.

- Coût moyen d'une violation de données 4,45 Millions $
- Axe majeur: la sécurité

Le MSSP devient un levier stratégique d'agilité et de performance



Les principaux moteurs de l'externalisation vers les MSP/MSSP

Report 2023 by IBM and the Ponemon Institute - IT Security Economics 2022 reseach

La valeur stratégique du MSSP pour l'entreprise

- Libérer les ressources internes pour l'innovation
- Réduire le risque et renforcer la conformité
- Accélérer la transformation numérique
- Construire la confiance digitale sur la durée

Le DSI, chef d'orchestre de la confiance numérique

Le DSI ne se contente plus de gérer l'IT : il pilote la confiance, la sécurité et la continuité d'activité.

Son rôle devient central dans la gouvernance de la résilience numérique.

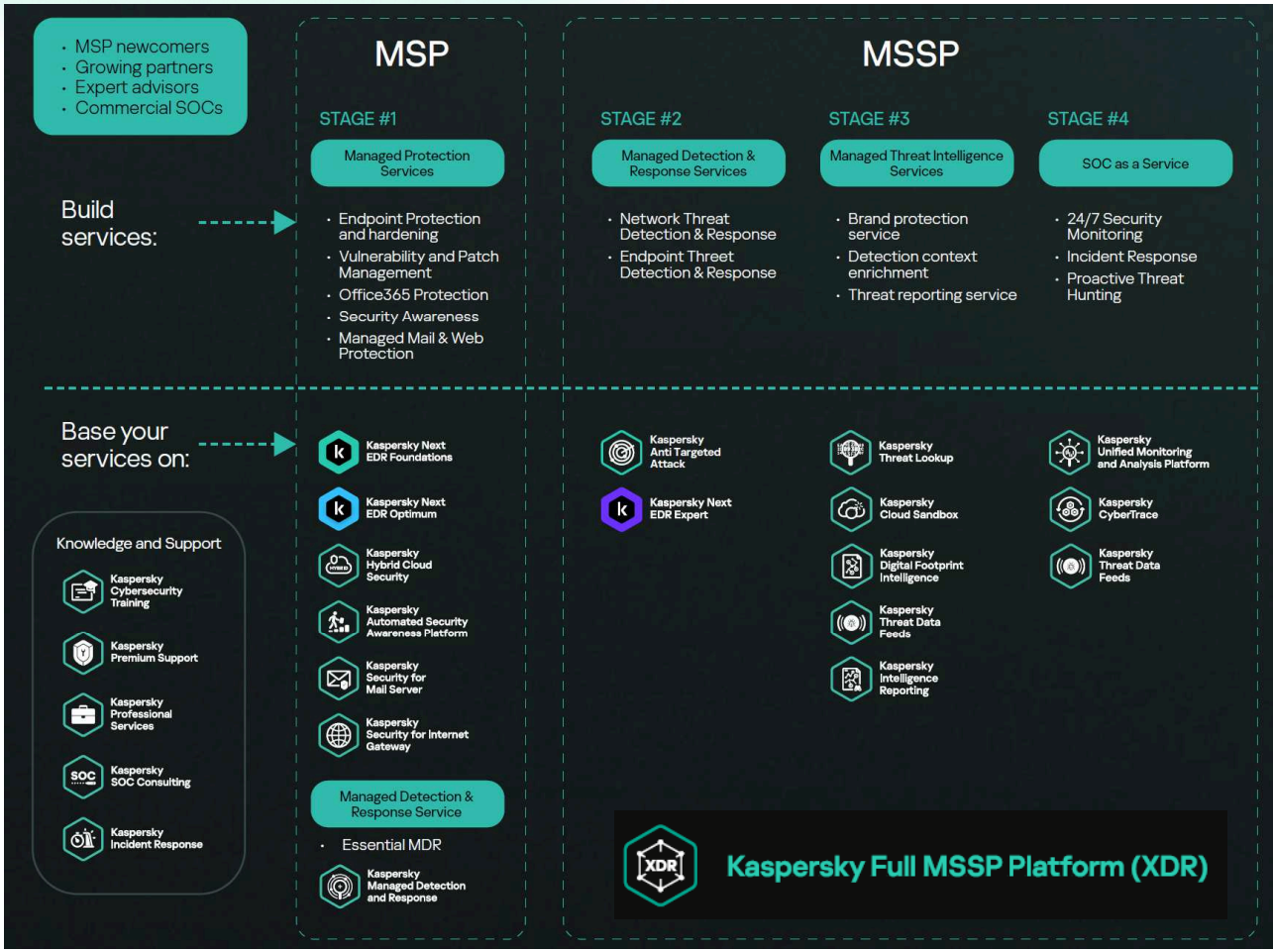
Vision: La sécurité n'est plus un coût, c'est un catalyseur de compétitivité, un accélérateur de performance

Tendances à venir!!!!

- IA générative : double tranchant entre innovation et menace
- Automatisation : vers des SOC autonomes et intelligents
- Souveraineté numérique : maîtrise des données et confiance locale

Comment Kaspersky accompagne le MSP/MSSP? Vue par étapes

- Des fonctionnalités de sécurité de qualité
- Technologies Multi-tenantes
- Réponse aux incidents et support continu
- Formation et Documentation
- Offre complète



Adopter le modèle MSSP, c’est investir dans la sérénité, la vitesse et la vision.

La cybersécurité de demain se construit aujourd’hui.

MERCI

kaspersky

Samy TADJINE
Enterprise Account Manager North, West & Central Africa

Les pilliers du modèle MSSP

Surveillance 24/7
Équipe dédiée active en continu

Expertise spécialisée
Accès à des analystes SOC, ingénieurs sécurité

Réduction des coûts
Pas besoin d'infrastructure interne coûteuse

Évolutivité
Capacité à gérer des environnements complexes ou multi-sites

Réduction des risques
Meilleure détection et réponse face aux menaces