Sectotem MSSP

securing your success

Qui sommes-nous, que signifie exactement MSSP ?

Table of content

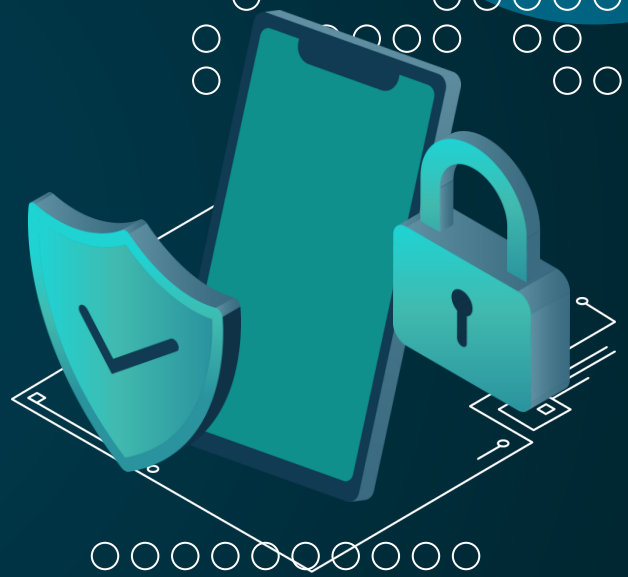
01. MSSP ?!

Introduction à ce que signifie MSSP et à nos services

Extension de la défense cybernétique de votre équipe informatique!

- Nous sommes un fournisseur de services de sécurité gérés (MSSP) — votre partenaire externalisé en cybersécurité. Nous agissons comme une extension de votre équipe informatique existante — ou comme votre équipe de sécurité complète si vous n'en avez pas.

- Nos services incluent la surveillance des menaces 24h/24 et 7j/7, la réponse aux incidents, la gestion des vulnérabilités et le support en matière de conformité — le tout via un modèle d'abonnement évolutif, adapté à la taille de votre organisation et à son profil de risque.



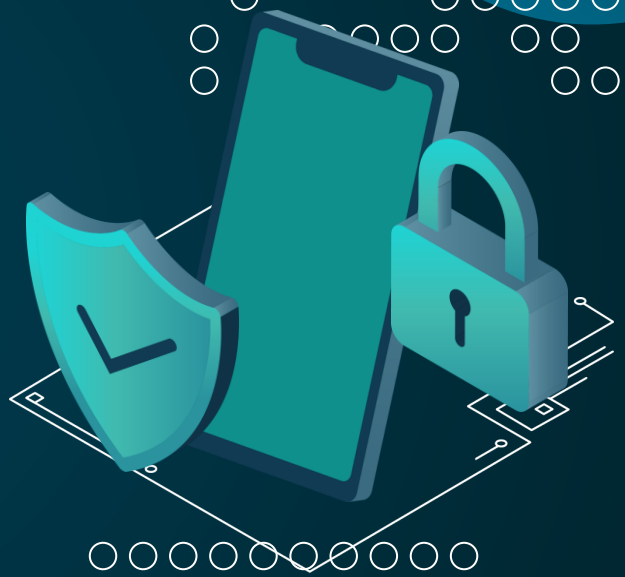
02

Pourquoi vous en avez besoin

Pourquoi les entreprises modernes s'appuient sur les MSSP pour gérer les menaces et assurer la conformité

Pourquoi vous avez besoin de nos services!

- **Évolution des menaces cybernétiques :** Les cyberattaques deviennent de plus en plus fréquentes et sophistiquées, exerçant une pression constante sur les ressources informatiques internes.
- **Conformité et gestion des risques** : Respecter les réglementations en matière de sécurité et les normes sectorielles est complexe et chronophage sans l'expertise appropriée.
- **Expertise et surveillance 24h/24 et 7j/7 :** Les MSSP offrent une protection continue, la détection des menaces et la réponse aux incidents par des professionnels de la sécurité qualifiés.
- **Défense proactive :** Les MSSP contribuent à prévenir les incidents avant qu'ils ne surviennent, réduisant les temps d'arrêt et assurant la continuité des activités.

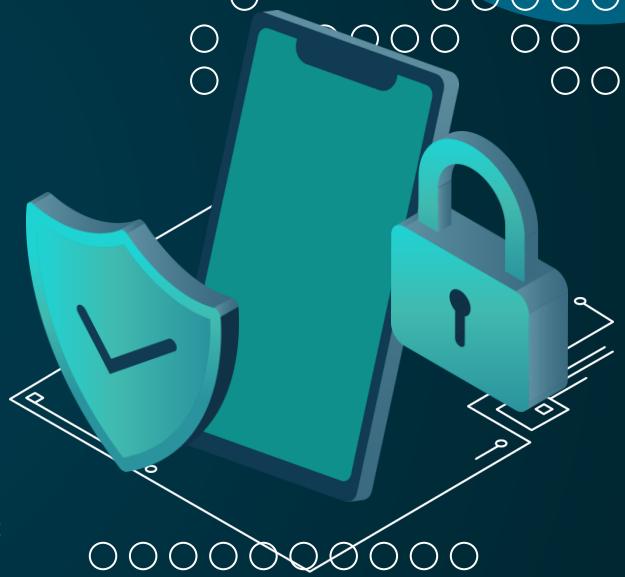


03

Nos services et offres

Aperçu de nos principaux services de sécurité

Tout ce dont vous avez besoin dans un seul package:



- Choisissez parmi des services individuels, des forfaits personnalisés ou un abonnement complet — et laissez-nous gérer votre sécurité afin que vous puissiez vous concentrer sur l'essentiel : votre entreprise..

Nos expertises principales :

01 Incident response

02 Security operation center (soc)

03 Threat intelligence

04 Penetration testing & redteam

05 Cybersecurity awareness training

Security Operations Center (SOC)

- Équipe centralisée d'experts en sécurité surveillant les réseaux, systèmes et terminaux.
- Fonctionne 24h/24 pour identifier les activités suspectes ou les violations.
- Sert de première ligne de défense contre les menaces cybernétiques.

Fonction principale :

Surveillance des menaces : Surveillance continue du trafic réseau, des terminaux et des environnements cloud.

Détection des incidents : Corrélation des alertes provenant de plusieurs outils de sécurité (SIEM, pare-feux, IDS/IPS).

Réponse aux incidents : Contenir, éradiquer et rétablir les systèmes après des incidents cybernétiques.

Rapports et conformité : Assurer l'alignement avec les réglementations et les politiques internes.

workflow : *Monitoring → Detection → Analysis → Response → Recovery*

Incident Response

Confinement immédiat des menaces : Identification et isolation rapides des incidents de sécurité pour éviter tout dommage ou perte de données supplémentaire.
Analyse des causes profondes : Enquête détaillée pour comprendre comment la violation s'est produite et quelles vulnérabilités ont été exploitées.
Réponse coordonnée : Les équipes d'experts collaborent avec votre organisation pour gérer efficacement la communication, la récupération et les mesures correctives.
Temps d'arrêt minimisé : Une intervention rapide garantit la continuité des activités et réduit l'impact opérationnel.
Rapports post-incident : Des rapports complets et les enseignements tirés permettent de renforcer les défenses et de prévenir les incidents futurs.

Threat Intelligence

Aperçu :

L'intelligence sur les menaces consiste en la collecte et l'analyse continues de données sur les menaces cybernétiques actuelles et émergentes. Elle transforme des informations brutes en **informations exploitables** qui aident les organisations à anticiper et à se préparer à d'éventuelles attaques.

Fonctionnement :

Collecte de données à partir de multiples sources internes et externes.

Analyse des schémas de menaces, des indicateurs de compromission (IOC) et du comportement des attaquants.

Transmission des informations directement au **Centre des opérations de sécurité (SOC)** et aux équipes de **réponse aux incidents (IR)** pour permettre une défense proactive.

Penetration Testing & Red Teaming

Aperçu :

Les **tests d'intrusion (Penetration Testing)** et le **Red Teaming** sont des évaluations de sécurité proactives conçues pour identifier les vulnérabilités et évaluer la préparation aux attaques réelles. Les deux approches simulent des tactiques adverses afin de renforcer les défenses de votre organisation avant que de véritables menaces n'apparaissent.

Fonctionnement :

Tests d'intrusion : Tests ciblés et contrôlés pour détecter les faiblesses techniques dans les applications, réseaux ou systèmes.

Red Teaming : Simulation plus large du comportement réel des attaquants, testant à la fois la technologie et la réaction humaine.

Fournit des rapports exploitables et des recommandations de correction pour améliorer la résilience.

Principaux avantages :

Identifier les points faibles : Découvrir les vulnérabilités cachées avant que les attaquants ne le fassent.

Tester la réponse : Évaluer l'efficacité de la détection et de la gestion des incidents.

Renforcer la préparation : Construire une posture de sécurité plus solide et adaptable.

NEXT STEP:

Contactez-nous

Contactez-nous!

Si vous avez des questions ou si vous avez besoin de professionnels de confiance pour la résilience de votre cybersécurité, contactez-nous:

info@sectotem.com
+216 20 171 019
sectotem.com