

☰ SOC MANAGÉ ALTER SOLUTIONS

Avec le **SOC Managé Alter Solutions**, nous vous proposons un service complet de détection et réponse aux incidents de sécurité. Nous nous appuyons sur les dernières avancées technologiques (UEBA, Machine Learning) ainsi que sur notre expertise pour améliorer vos capacités de détection, accélérer vos réponses à incident et réduire vos coûts.

☰ PRÉVENIR



Veille

Nos experts s'informent en continu sur les nouvelles menaces.



Amélioration continue des règles de détection

Nous mettons constamment à jour nos règles de détection en fonction de l'évolution de la menace et des environnements de nos clients.



Blocage automatique des menaces

Nous mettons en place des réponses automatiques sur des cas d'usage à haute-fidélité (sans faux positifs).



Conseil technologique

Nous faisons bénéficier nos clients de notre expertise en cybersécurité pour les guider dans leurs choix technologiques.

☰ DÉTECTER



Détection 24x7x365

Nous supervisons en continu pour une réponse rapide et efficace.



La bonne donnée, au bon moment

Nous conseillons sur la stratégie de collecte à adopter et accompagnement dans sa mise en



Techniques de détection avancées

Nous nous appuyons sur les technologies de pointe comme l'Intelligence Artificielle, le Machine Learning, l'UEBA, la détection de signaux faibles et le Threat Intelligence.

☰ INVESTIGUER



Contextualisation

Les alertes sont enrichies automatiquement avec des données contextuelles afin de les traiter plus efficacement.



Investigation approfondie

Une investigation manuelle est réalisée par nos experts pour mener une analyse approfondie lorsque cela est nécessaire.



Qualification

Tri des vrais et faux positifs et détermination de la criticité de l'alerte.

☰ RÉPONDRE



Réponse rapide et accélérée par l'automatisation

Réponse effectuée par nos experts et appuyée par notre plateforme SOAR.



Suivi des réponses à incident

Processus de notification et de suivi des incidents éprouvé permettant aux clients de suivre l'ensemble des étapes de la réponse.

Vos solutions de sécurité orchestrées sur une seule plateforme

L'ensemble des solutions de prévention, détection et réponse à incident pilotées depuis une seule et même plateforme : SIEM / SOAR / EDR / NDR / UEBA.

Liberté de choix des éditeurs

Avec le SOC Managé Alter Solutions, vous avez le choix d'apporter vos propres solutions de prévention, détection et réponse à incident que nous intégrons à notre plateforme, ou de profiter de nos solutions partenaires.

☰ L'OFFRE ADAPTÉE A VOS BESOINS

SOC Co-Managed

Alter Solutions assure le déploiement et le maintien en condition opérationnelle de vos solutions de sécurité. Ainsi, vos équipes se chargent de l'analyse des événements de sécurité sans avoir à se préoccuper de la maintenance de la plateforme. De plus, elles profitent du panel de règles de détection mis à disposition par Alter Solutions et régulièrement actualisé.

SOC Managé Avancé

Un service de détection complet opéré en 24x7. De plus, vous profitez d'un service de réponse à incident à distance permettant à nos équipes d'effectuer les actions primordiales de réponse lors d'un incident de sécurité. L'offre la plus adaptée à toute organisation souhaitant améliorer significativement leur capacité de détection et de réponse à incident.

SOC Managé Essentiel

L'essentiel d'un service de détection incluant le maintien en condition opérationnelle de vos solutions de sécurité, mais également un service de supervision en heures ouvrées (5x8) opéré par nos équipes SOC. Idéal pour les organisations souhaitant mettre en œuvre un service de détection efficace pour un coût réduit.

Soc Managé Elite

L'offre de détection et de réponse à incident la plus avancée, incluant un service de détection 24x7 par nos équipes SOC ainsi qu'un service de réponse à incident à distance. Profitez d'un suivi rapproché des activités de détection, mais également de l'inclusion de marqueurs de compromission avancés et dédiés à votre environnement (CTI) permettant de détecter les menaces les plus avancées. Une offre adaptée à toute organisation ayant une activité continue en 24x7 souhaitant profiter des capacités de détection et de réponse à incident les plus approfondies et réactives.

☰ Comparez nos offres

Composants et fonctionnalités	SOC Co-Managed	SOC Managé Essentiel	SOC Managé Avancé	SOC Managé Elite
Intégration d'outils de sécurité (EDR,NDR, XDR, etc)	✓	✓	✓	✓
Maintien en condition opérationnelle	✓	✓	✓	✓
Maintien en condition de détection	✓	✓	✓	✓
Service de détection		Heures ouvrées	24/7/365	24/7/365
Reporting		Mensuel	Bimensuel	Hebdomadaire
Réunion de point de contact		Trimensuel	Mensuel	Bimensuel
Exécution des réponses à incidents à distance		Option	✓	✓
Réponse à incident sur site	Sur demande	Sur demande	Sur demande	Sur demande