MIRA SOC

Un service clé en main pour ***prévenir***, ***détecter***, ***investiguer*** et ***remédier,*** adapté à toutes les tailles d'entreprise.

Le SOC (Security Operations Center) est, de nos jours, un dispositif indispensable de protection et de sécurisation du système d'information d'une entreprise. Il lui permet de réduire le risque face aux cyberattaques et d'avoir une réponse instantanée lors d'incidents de sécurité.

Pourquoi un SOC est indispensable ?

- Multiplication des attaques et professionnalisme des attaquants.
- Solutions de sécurité chronophages nécessitant une écoute 24/7.
- Détection, investigation, réponse et remédiation nécessitant une expertise, un savoir-faire.

Le périmètre couvert

- Postes de travail, serveurs et mobiles.
- Messagerie, environnement collaboratif, Microsoft et Google.
- Réseaux, Firewall, IDS / IPS.
- Filtrage web, cloud, proxy.

MIRA SOC

- Nos offres SOC sont faites sur-mesure pour bénéficier d'un service qui correspond à vos besoins, à votre taille d'entreprise et à votre budget.
- Le SOC Aramys, c'est aussi l'expertise de nos équipes pluridisciplinaires, dédiées et mobilisées quotidiennement pour un service clé en main et une gestion de la sécurité de votre SI.
- Cette offre de service granulaire et évolutif s'adapte à vos besoins dans la durée.

Une architecture ciblée

- Découverte automatisée des **Zéro Day** et des attaques ciblées
- Recherche des IOC dans tout l'environnement
- Gestion des faux positifs et classification des menaces
- Suivi des attaques entre plusieurs machines
- Automatisation de votre travail grâce à nos puissantes API (Automatiser les Réponses aux Incidents)
- Visualisation de la situation globale de votre entreprise en matière de sécurité

DÉTECTION - INVESTIGATION - RÉPONSE

L'offre SOC d'Aramys

- Une surveillance 24/7 des évènements par le pôle cybersécurité Aramys.
- Une investigation sur les incidents avec rédaction de rapports incluant l'analyse et les recommandations. (qualification des alertes, question des faux positifs, classification de la menace et notifications sur alertes avérées).
- Des actifs logiciels et matériels centralisés pour permettre la mise en œuvre d'une approche plus holistique (globale) de la sécurité.
- Une réponse aux menaces avec intervention s'appuyant sur une posture Zéro Trust et mapping MITRE ATT&CK (isolement de la menace, actions de réponse, remédiation, plan d'action).
- Réunion trimestrielle avec un expert en cybersécurité chez vous, pour commenter le rapport de sécurité et les axes d'améliorations de votre système d'information.

Équipes

Analyste SOC/CSIRT : Détection, réaction et reporting
des incidents de sécurité.
Ethical Hackers : Identification des menaces potentielles au sein d'un SI.
Analyste Forensics : Enquête après incident de sécurité.
Auditeur ISO : Conformité, gouvernance et management d'un SMSI.
IR Team : Équipe de réponse à incident mobilisable 24/7

Certifications

EXPERT CYBER – Label Sécurité Numérique – Cybermalveillance.gouv.fr – République Française

CYBER MALVEILLANCE .GOUV.FR

Prestataire de terrain :

ISO 27001 – Information Security Management – Certified

FRANCE RELANCE

ARAMYS

ARAMYS SAS
5 rue Voltaire - 62300 LENS
+33 3 21 15 68 91 - **contact@aramys.fr** - www.aramys.fr