# SOC MANAGÉ

Le plus haut niveau de protection pour votre SI

RESILIENZ

***« Nous croyons fermement qu'il est essentiel de garantir la souveraineté numérique des organisations dans un contexte d'intensification des risques ».***

Vous êtes soumis à des défis de sécurité croissants avec des menaces qui évoluent rapidement et profitent d'une surface d'attaque en expansion constante. Pour autant, vous ne disposez pas en interne des ressources et du temps nécessaires pour garantir votre résilience.

**Notre objectif :** vous doter d'un SOC * pour surveiller et protéger votre SI de manière continue

** SOC : Security Operation Center (Centre opérationnel de sécurité)*

Le SOC Resilienz détecte "à bas bruit" les signaux et menaces en temps réel, 24/7 et propose un plan de remédiation pour protéger vos :

**UTILISATEURS**

**RÉSEAUX**

**APPLICATIONS CLOUD**

## Les fonctionnalités de notre SOC managé

Notre SOC est paramétré sur mesure pour les besoins de votre organisation et inclut :

- La recherche de menaces en temps réel 24/7
  (postes & serveurs Windows, MacOS & Linux, réseau, M365, Azure AD…)
- La surveillance de connexions avec des réseaux cyber terroristes
- Une visibilité accrue des menaces emails on premise et cloud
  (compromission, redirection non autorisée, privilèges excessifs)
- La surveillance Active Directory
  (connexions malveillantes, comportements et activités suspects, contrôle des autorisations et des accès)
- La surveillance des journaux des pare-feux
- La centralisation et surveillance des journaux d'événements
- La détection des outils et programmes suspects
- La surveillance des flux réseaux
  (exfiltration de données)
- L'investigation et la surveillance de la réputation des menaces
  (threat intelligence)
- La surveillance continue du Dark Web à la recherche d'identifiants compromis
- La surveillance du filtrage DNS

Mettre en place un SOC est une étape indispensable à la conformité légale (NIS2, HIPAA, RGPD, DORA…).

## NOTRE **OFFRE**

Nos équipes SOC sont réparties en 2 groupes :

> 1 équipe "**Détection et alerte 24/7**" de 30 personnes
> 1 équipe "**Filtrage et remédiation**" de 5 interlocuteurs

Vous choisissez parmi ces 3 options :

### DÉTECTION & ALERTE

Nous surveillons et alertons, vous remédiez

### HYBRIDE

Nous surveillons et alertons, nous remédions ensemble selon le périmètre concerné

### DÉTECTION & REMÉDIATION

Nous surveillons, détectons et remédions pour vous

## NOTRE MISSION : VOTRE RÉSILIENCE

Notre plateforme SOC s'intègre dans une **démarche globale de sécurisation des systèmes d'information.** Nous sommes en mesure de proposer par exemple des tests d'intrusion automatisés, des scans de vulnérabilité et le patching de sécurité.

Au-delà de l'aspect opérationnel, nos équipes vous accompagnent également sur vos **problématiques de gouvernance, de gestion des risques cyber** (Guide d'hygiène ANSSI, ISO 27001) **et de conformité** (NIS2).

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Si après la **démo de notre SOC** vous avez l'impression d'être équipé pour partir en guerre...

**C'est parce que c'est le cas !**