

## Formation Bonnes pratiques de l'Analyste SOC : sensibilisation, veille et CERT, analyse de risques et traitement d'alertes

<b>Durée :</b>	5 jours
<b>Public :</b>	Analystes SOC, Administrateurs Systèmes et Réseaux, Chefs de projets Infrastructures
<b>Pré-requis :</b>	Fondamentaux de la Cybersécurité
<b>Objectifs :</b>	Découvrir les fondamentaux de l'Analyse SOC
<b>Sanction :</b>	Attestation de fin de stage mentionnant le résultat des acquis
<b>Taux de retour à l'emploi:</b>	Aucune donnée disponible
<b>Référence:</b>	RéS101765-F
<b>Note de satisfaction des participants:</b>	Pas de données disponibles

### 1) SOC et sensibilisation à la sécurité

Définitions  
Sensibilisation à la sécurité

### 2- Veille informatique

Veille :  
- ANSSI, CERT, Cybermalveillance, CNIL  
- Signal SPAM, BlocTel, ZATAZ  
Certification (Mooc ANSSI, et atelier CNIL)  
Vérification fuite DATA

### 3- Analyse du risque

Définitions  
Calcul du risque  
Analyse (Audit/ Monitoring) du risque

### 4- Traitement d'alertes

PRA/PCA – RTO/RPO  
DPIA  
Mise en place de moyens palliatif ou correctif du risque

### 5- Gestion de crise

Mise en situation  
Étude de Cas

## **6- Cadre juridique**

Norme ISO  
Loi et Article  
Responsabilité

## **7- Organisation / planification de l'analyse SOC**

Help SOC  
Mise en place d'un SOC  
Rapport SOC