



## WINSOC

Notre métier : prévenir et gérer le risque

Conformité LPM 2015

Qualification PASSI

### Un SOC efficace est avant tout un SOC qui appuie votre métier...

SCASSI vous accompagne dans la conception de votre SOC-métier : depuis la **sélection des critères métiers critiques à surveiller** jusqu'à la mise en œuvre d'un **tableau de bord et d'alertes de sécurité**.

A travers son offre **WINSOC**, SCASSI assure à ses clients une **réactivité** optimale en cas d'atteinte aux processus métiers prioritaires.



Un SOC efficace pour le métier



Un coût maîtrisé



Une offre clé-en-main

## MÉTHODE

## LIVRABLES

## CAS D'ETUDE MÉTIER

1 Analyse de risques métiers

Définition d'indicateurs métiers primaires à surveiller en priorité



2 Analyse des moyens existants

Définition des indicateurs techniques et des sources



3 Expertise technique

Création des règles de corrélation à implémenter dans le système



4 Suivi et amélioration continue

Rapports d'activités, résolution de crise



Intégrité de la base de données des comptes clients d'un site de vente en ligne.

Logs d'accès à la base de données, logs des firewalls, logs des IPS, logs du serveur frontal, logs du serveur d'hébergement de la base.

Delta entre requête du serveur frontal et requête à la base, fréquence d'alertes sur l'IPS, taux de DROP sur le firewall, fréquence d'écriture sur le disque du serveur.

Nombre d'incidents sur la base par mois, adaptation des indicateurs à un projet de virtualisation des serveurs.

## VALEURS AJOUTÉES

- Formalisation méthodique et **pragmatique** du besoin **orienté risques (ISO 27005 - EBIOS)**
- Approche **métier et non produit** de la sécurité
- Une équipe de **40 personnes** spécialistes de la sécurité
- Certifiés **CISSP, ISO 27001, CEH**

## RÉFÉRENCES PRODUITS

Références	Nombre d'applications	Alertes métiers	Objets monitorés	Suivi continu	SOC IMS
SCA-INF-WSOC-1	2	5	20	OPTION	IMS-250EPS
SCA-INF-WSOC-2	5	12	50		IMS-500EPS
SCA-INF-WSOC-3	10	20	100		IMS-1000EPS