

GUIDE EBIOS RISK MANAGER

FICHE METHODE 6 – Atelier 3

DEFINIR LES MESURES DE SECURITE POUR L'ECOSYSTEME

Les fiches méthodes permettent aux responsables de la démarche d'analyse de risque d'identifier les points essentiels d'attention en fonction de la typologie du système d'information ou des concepts utilisés.

Elles n'ont pas vocation à remplacer les guides techniques de l'ANSSI ou les politiques de sécurité et les réglementations en vigueur qui doivent être appliquées.

Selon le niveau de menace d'une partie prenante vis-à-vis de l'objet de l'étude, des mesures de sécurité pourront être mises en place. Le jeu de règles suivant peut ainsi être adopté, le critère d'entrée étant le niveau de menace évalué pour la partie prenante.

NIVEAU DE MENACE	ACCEPTABILITÉ	RECOMMANDATIONS D'ACTIONS
TRÈS ÉLEVÉ – ZONE DE DANGER	Inacceptable	Aucune partie prenante dans cette zone : réduction du risque, ou refus d'établir l'interaction.
ÉLEVÉ – ZONE DE CONTRÔLE	Tolérable sous contrôle	Enrôlement de la partie prenante dans le processus de management du risque : - surveillance particulière, voire accrue, en termes de cybersécurité ; - audit de sécurité technique et organisationnel ; - réduction/transfert du risque dans le cadre d'un plan d'amélioration continue de la sécurité.
FAIBLE – ZONE DE VEILLE	Acceptable en l'état	Sans objet (menace résiduelle).

Vous pouvez définir une première orientation en proposant un critère sur lequel agir en priorité (par exemple : augmenter la confiance ou la maturité, diminuer la pénétration ou la dépendance). Ces orientations sont guidées notamment par les considérations suivantes :

- choix du critère le plus pénalisant dans la situation initiale ;
- choix du critère pour lequel une amélioration sera obtenue à moindre coût ; choix du critère le plus efficace a priori au vu des scénarios stratégiques identifiés.

Vous pouvez nuancer le jeu de règles ci-dessus pour les parties prenantes qui se trouvent dans la zone de danger, particulièrement s'il apparaît très difficile de les faire sortir de cette zone compte tenu de contraintes opérationnelles.

EXEMPLE : une partie prenante pourra être tolérée dans la zone de danger seulement si ses niveaux de maturité et de confiance sont au moins de 3