

Tenacy

Atelier 1

Introduction à TENACY

Les interactions

Usez et (abusez) des réactions émojis



Micro / Caméra possibles

Questions écrites dans le chat

Les interactions doivent se limiter aux incompréhensions ou aux précisions sur les notions à l'ordre du jour

Les cas particuliers, les mises en œuvre seront à privilégier sur les ateliers intégrateur / CSM



Qu'allons nous voir dans cet atelier ?

Sujets principaux

Prérequis
technique

Interfaces

Support et
documentation

Management des
utilisateurs

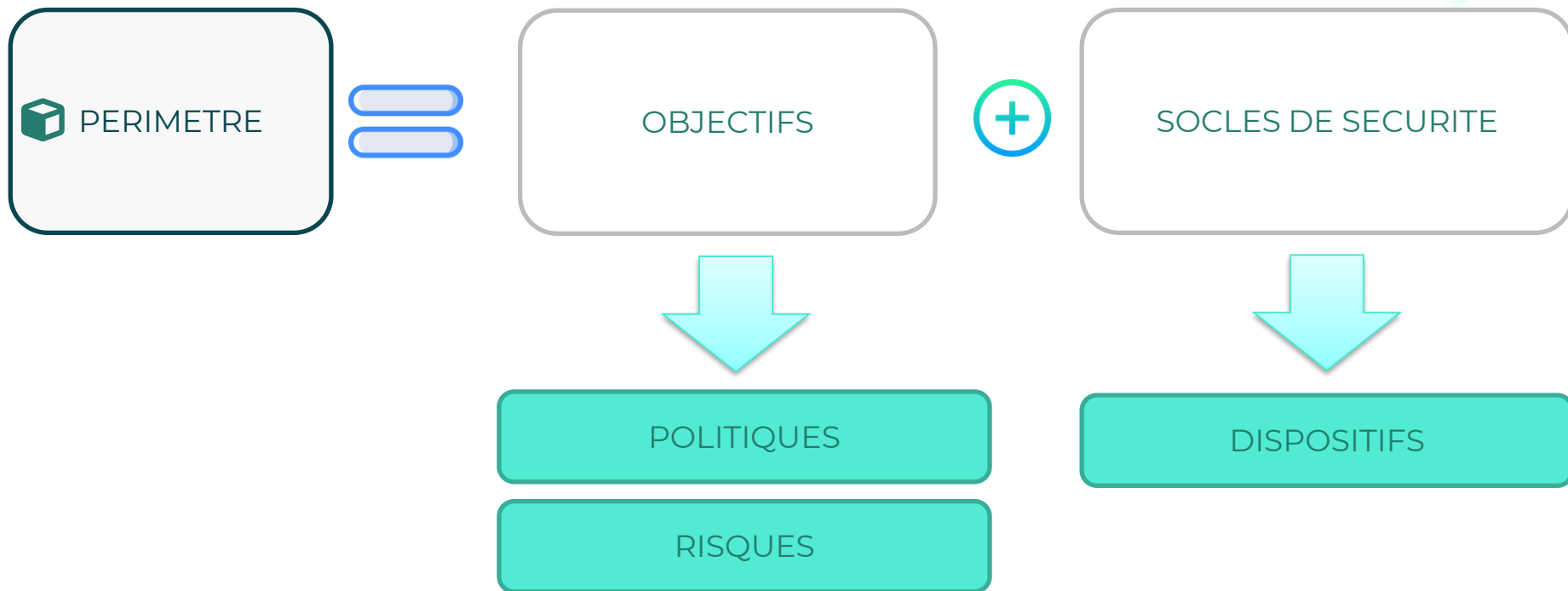
Modélisation de
votre organisation

- Périmètres
- Applications et fournisseurs

Schéma
fonctionnel

- Socles de sécurité
- Dispositifs de sécurité

Périmètres de sécurité



Périmètres de sécurité

 FOURNISSEUR



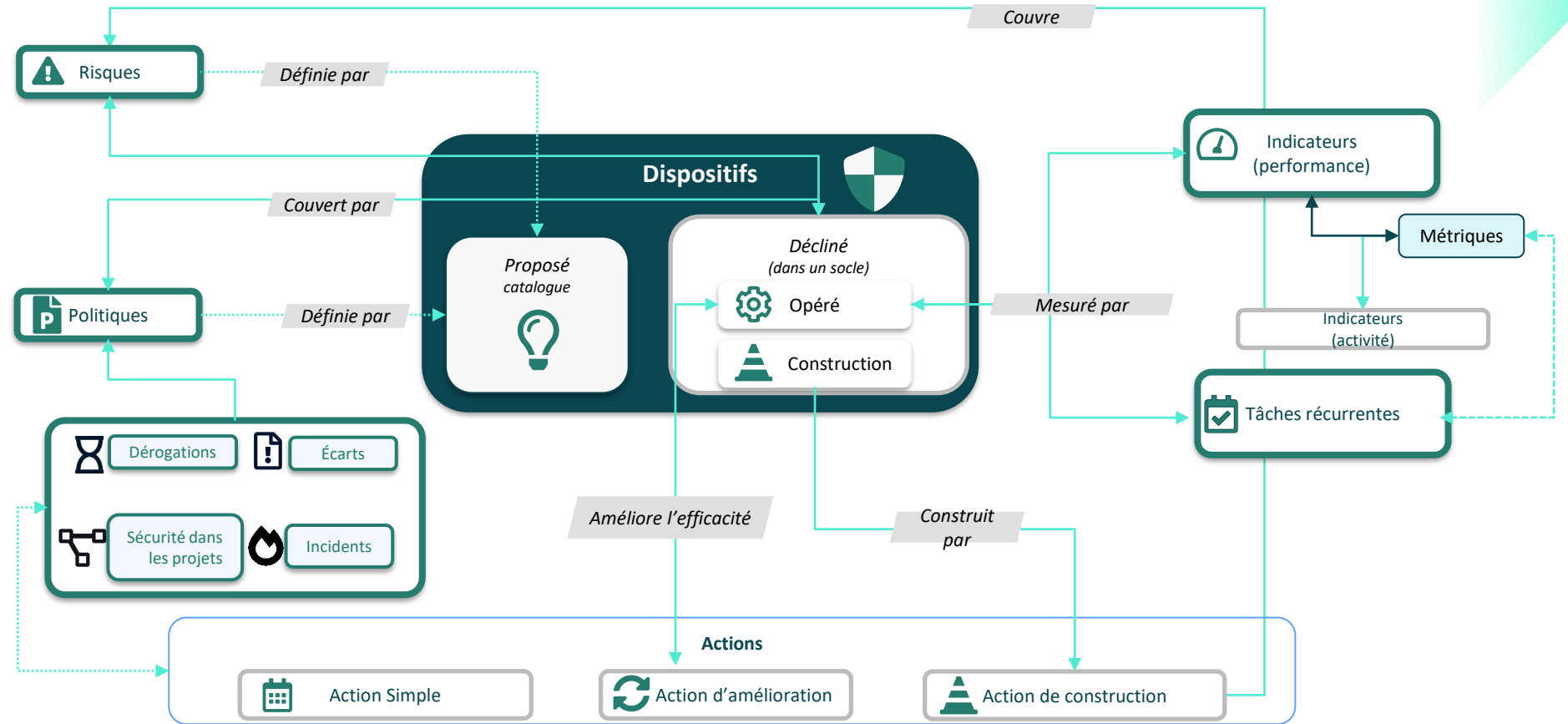
 APPLICATION

OBJECTIFS



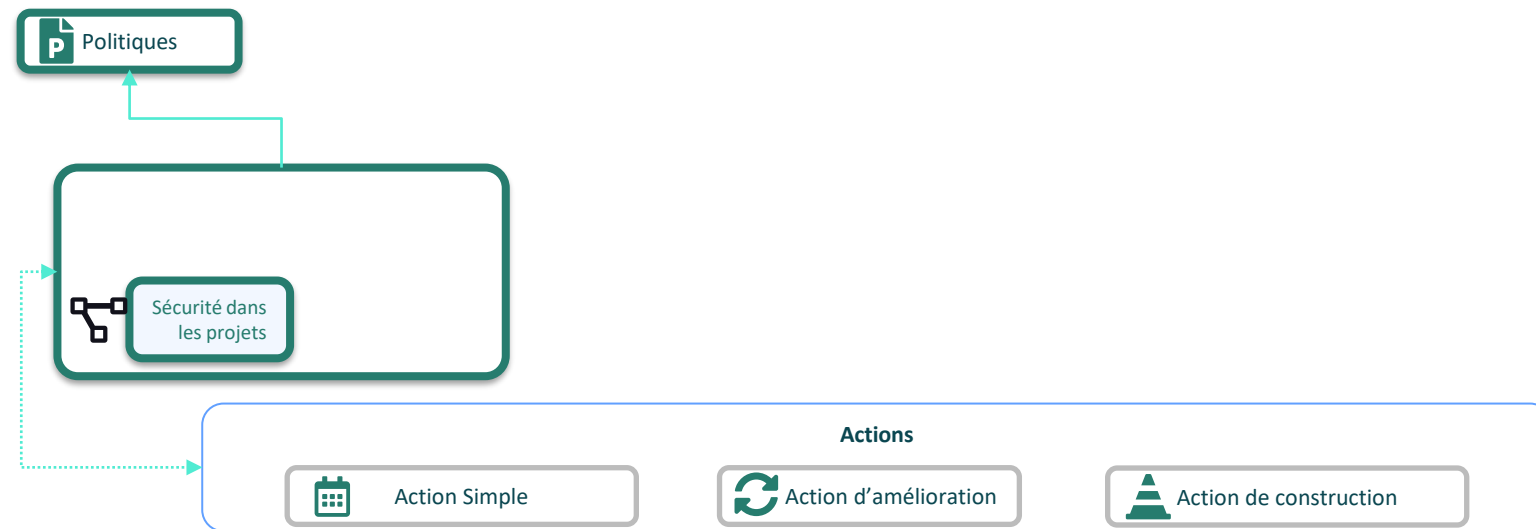
POLITIQUES

Modèle fonctionnel



Modèle fonctionnel

applicable aux applications et fournisseurs





Synthèse : Administration de la solution

Synthèse

Techniques, supports et documentations

Prérequis technique

Web interface

Navigateurs supportés: Edge, Firefox, Chrome et Safari (dernières versions)

Les mails sont envoyés par la solution par le domaine @tenacy.io

L'exécution de script (js) est obligatoire sur le domaine

Documentation

Documentation in app dans le menu en haut de la fenêtre

Documentation contextuelle adaptée à la page sur la quelle vous êtes.

Possibilité de chercher un mot clé, parcourir la documentation

La base de connaissances regroupe les trucs et astuces (accessibles via le chat)

Support

support@tenacy.io

Chat (en bas à gauche): le domaine « hubspot» doit être autorisé

Le suivi des tickets se fait via le chat (multi conversation)

Synthèse

Gestion des droits et accès

- À la création vous devez configurer:
 - Son mail (la clé) et son nom (pour générer les initiales)
 - La méthode de connexion (SAML ou mot de passe)
 - Son rôle et périmètres d'intervention: Les rôles ne peuvent pas être cumulatifs.
- Les groupes ne permettent **pas d'accorder** des rôles mais des **droits sur les objets** (actions, indicateurs etc.)
- Un utilisateur peut être **membre de plusieurs groupes**.
- Les **fonctions** sont à utiliser dans le cadre d'évaluation
- Un **résumé hebdomadaire** (lundi matin) peut être configure pour chaque utilisateur: il contient un rappel des actions affectés.
- Les **rappels** peuvent être aussi envoyé manuellement (pour un utilisateur ou pour une thème).

Synthèse

Échelle

Les scores Tenacy sont définis de 0 à 100

L'échelle définit comment ce score est présenté à l'utilisateur (niveau, couleurs, titre)

Métriques / indicateurs internes

Calculées automatiquement par la solution.

Ne peuvent pas être modifiées par un utilisateur

Peuvent être modifiées par le support (exceptionnellement)

Peuvent être insérés dans un dashboard

Configuration / préférences

Contient les valeurs par défaut (échelle, score etc.)

Définit la politique de mot de passe

Contient la configuration SAML

Peuvent être modifiés par un admin racine

Le support devrait être consulté avant toute modification

Licences

Utilisateurs admins

Périmètres internes

Politiques publiques

Les autres éléments ne sont pas limités dans les licences actuelles

Consulter le support pour toute question ou extension.

Catalogue

Les dispositifs proposés sont des templates présents dans le catalogue

Tous les objets du catalogue (politique, dispositifs, indicateurs, tâches récurrentes) sont liés entre eux.

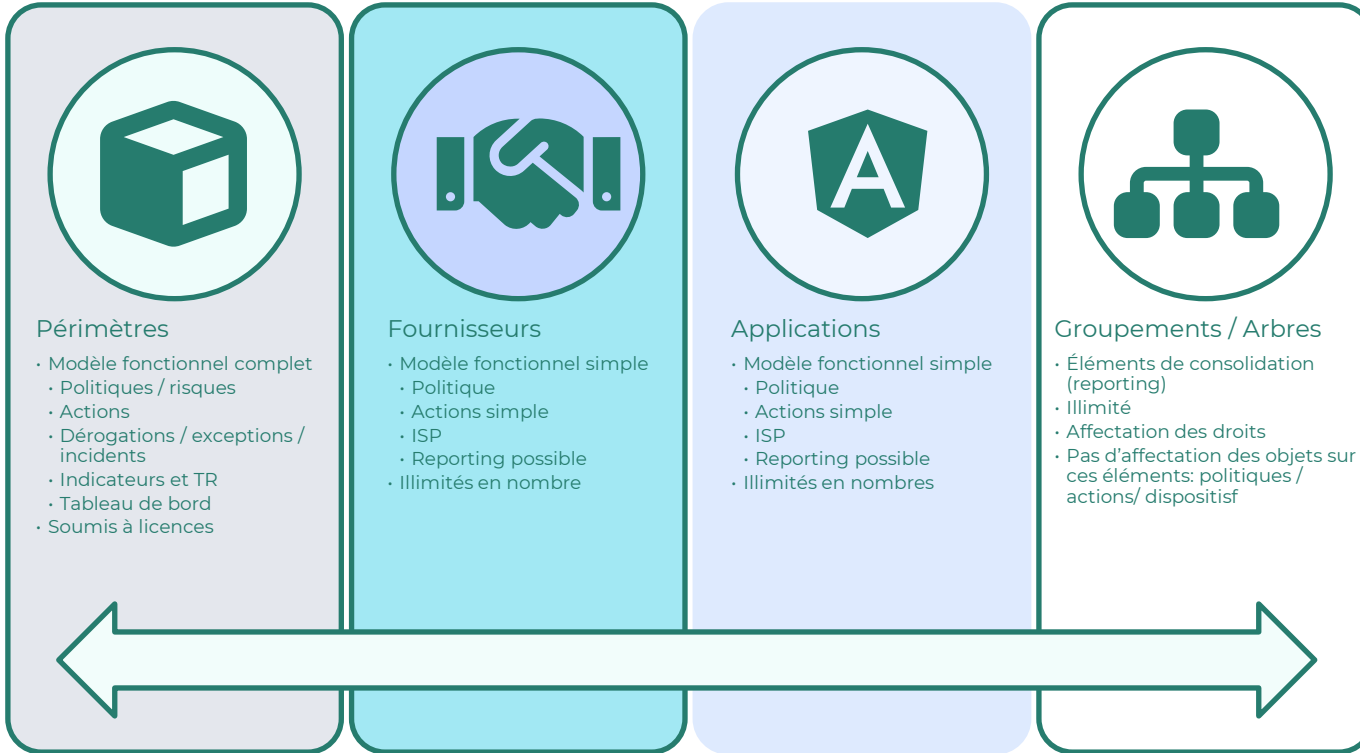
Peuvent être dérivés dans votre propre catalogue

Dériver ne veut pas dire instancier !



Synthèse : Model fonctionnel

Modélisation



Synthèse

Périmètres, dispositifs et socle de sécurité

Dispositifs de sécurité

Logiciels et/ou processus et/ou équipe permettant de sécuriser un périmètre

Peut être offert à différents périmètres

Élément pivot de Tenacy permettant de lier les objets entre eux

Manipulé sous différents états dans la solution

Peut être analysé pour repérer les anomalies

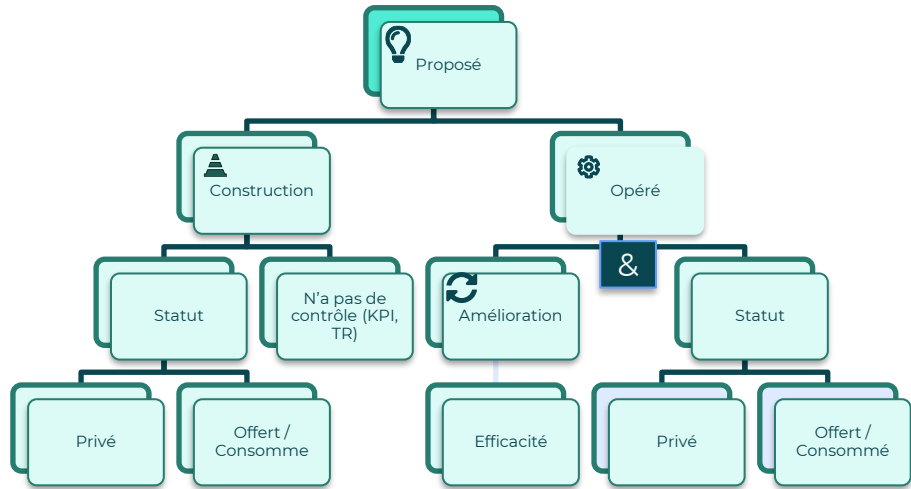
Socles de sécurité

Ensemble des dispositifs qui sécurisent un périmètre

Composé de dispositifs opérés, offerts et consommés

Comparé aux objectifs pour calculer un score

Synthèse – Le dispositif dans tous ses états



Template,
Crée par Tenacy OU par l'utilisateur

Est disponible dans le catalogue et doit
représenter le lien avec les autres objets
(objectifs et moyens de contrôles)

Décliné

Est présent dans les socles de sécurité

Un même dispositif ne devrait pas être deux
fois dans le même socle (même sous 2 états)

Modélisation d'un dispositif

Créer le dispositif Protection malware poste de travail

Dispositif privé Dispositif offert

Périmètres

Lyon Lille

Tâches récurrentes

MAL_R02 Contrôle des postes avec AV pas à jour
 MAL_R01 Contrôle des postes hors console AV

Indicateurs

MAL_I01 Postes dans la console AV
 MAL_I02 Postes avec AV à jour
 MAL_I24 Codes malveillants détectés sur les postes

Tâches récurrentes

Registre tâches récurrentes par défaut

Début

02/08/2021

Annuler Créer

Cas 1: Double dispositif

- Chaque périmètre aura son propre dispositif (issu du même dispositif proposé)
- Chaque périmètre aura ses propres TR
- Chaque périmètre collectera ses propres métriques

Modélisation d'un dispositif

Créer le dispositif Protection malware poste de travail

Dispositif privé (selected) / Dispositif offert

Périmètre opérateur: Lyon

Consommateurs: Lyon, Lille

Tâches récurrentes:

- MAL.002 Contrôle des postes avec AV pas à jour
- MAL.001 Contrôle des postes hors console AV

Indicateurs:

- MAL.001 Postes dans la console AV
- MAL.002 Postes avec AV à jour
- MAL.024 Codes malveillants détectés sur les postes

Tâches récurrentes: Régistre tâches récurrentes par défaut

Collecter les métriques pour chaque périmètre:

Début: 02/08/2021

Annuler / Créer

Cas 2: Dispositif offert

- Un seul dispositif est créé.
- Lyon est responsable du dispositif
- Une seule instance des RT sera créé (sous responsabilité de Lyon).
- Une seule métrique sera collectée: la valeur de l'indicateur sera la même pour Lyon et Lille

Modélisation d'un dispositif

Créer le dispositif Protection malware poste de travail

Dispositif privé Dispositif offert

Périmètre opérateur
Lyon

Consommateurs
Lyon Lille

Tâches récurrentes
 MAL_R02 Contrôle des postes avec AV pas à jour
 MAL_R01 Contrôle des postes hors console AV

Indicateurs
 MAL_I01 Postes dans la console AV
 MAL_I02 Postes avec AV à jour
 MAL_I04 Codes malveillants détectés sur les postes

Tâches récurrentes
Registre tâches récurrentes par défaut

Début
02/08/2021

Annuler Créer

Collecter les métriques pour chaque périmètre

Cas 3: Dispositif offert et mesuré en local








- Un seul dispositif est créé.
- Lyon est responsable du dispositif
- Une seule instance des RT sera créée (sous responsabilité de Lyon).
- Les métriques sont collectées pour chaque périmètre (Lyon peut quand même être en responsabilité de collecter pour Lille)



Un périmètre peut être consommateur du dispositif qu'il offre (mais pas nécessairement)

Création de nouveau élément dans le catalogue de dispositif :

Quand faut-il dériver un dispositif proposé ? Construire un nouveau dispositif proposé ?

Id. ↕	Name ↕	Build	Run	Category ↕	
EX001	Endpoint protection against malware			MAL	    
EX002	Web browsing protection			MAL	Fork measure blueprint in your catalog
EX003	Endpoint protection			MAL	

Créer un dispositif proposé dans votre catalogue ne veut pas dire l'instancier

Le dispositif n'existe pas dans notre catalogue

Vous n'utilisez pas le même vocable, vision du dispositif

Le dispositif est amené à être décliné plusieurs fois

Cas rencontré lors de dispositif spécifique (sûreté physique, organisation ITIL etc.)

Ne pas hésiter à nous remonter le cas pour intégration au catalogue public.

Protection malware = Endpoint Protection etc.

Changement du taux de couverture théorique

Il est préférable de l'instancier puis de modifier le dispositif opéré dans le socle

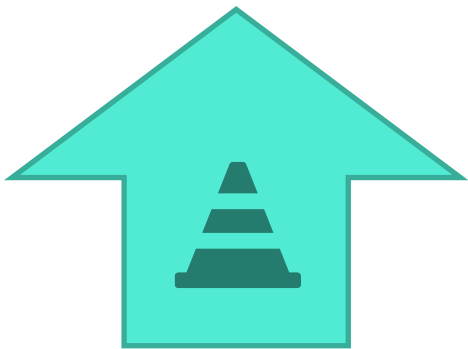
Redéfinir permet d'instancier à partir de ce nouveau modèle

Définir des dispositifs micro permet de gagner en finesse de pilotage mais nécessitera plus d'engagement: un dispositif = N Mesures à lier, des indicateurs et/ou RT.



Si vous dérivez un dispositif et le modifier, vous devrez appliquer les changements manuellement

Dans quel cas un dispositif est-il opéré (versus construction)?



Construction

- Build initial
- A une conséquence sur un risque: l'avancement permet de couvrir le risque
- N'impacte pas les scores de politiques (mais lien visible)
- Doit être une action identifiée / prévue
- → Socle cible



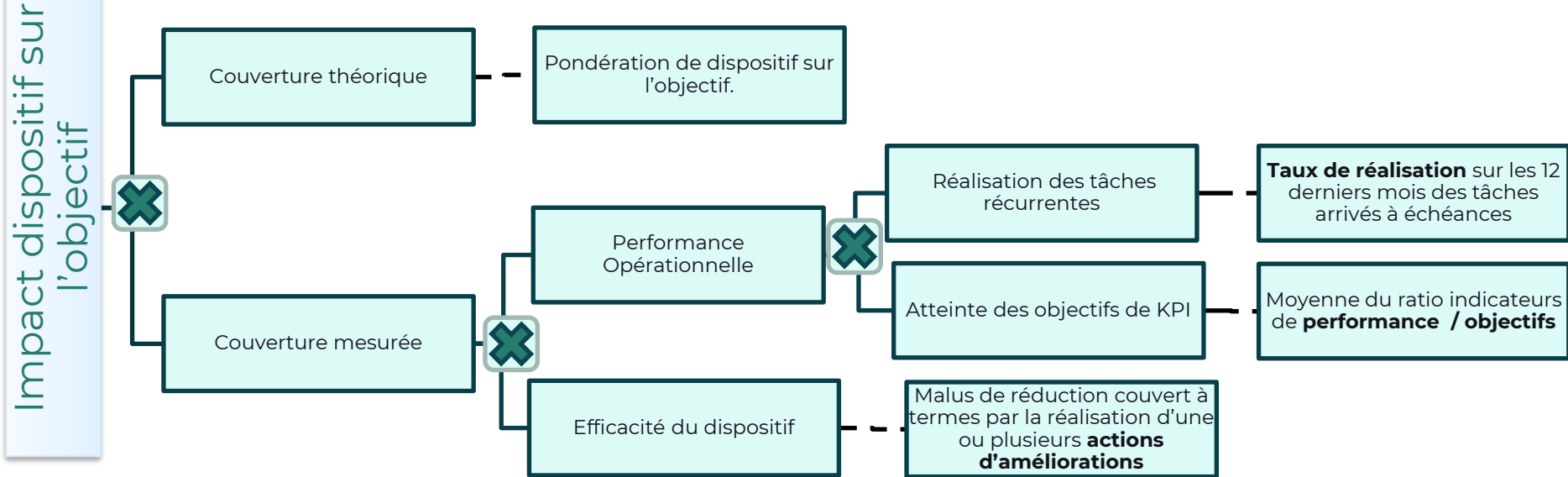
Opéré

- Peut être complété pour valider l'état par:
 - Améliorations
 - KPI/Tâches récurrentes
- Impacte un risque et une politique (mais minoré par la performance du dispositif)

Au sein d'un même socle le dispositif ne devrait pas être en construction ET opéré

Performance du dispositif

L'une des finalités de Tenacy est d'impacter la mesure d'atteinte de vos objectifs par la performance des dispositifs



Les dispositifs sans contrôle auront une valeur de « performance opérationnelle » appliquée pour le calcul des politiques. Valeur configurable pour les risques et politiques



Pour aller plus

Identifiez vos *objectifs* de sécurité et pilotez les

Politiques

- Définissez vos propres politiques et liez les à la base de connaissance Tenacy
Dérivez et personnalisez les politiques publiques
- Suivez votre niveau de conformité mesuré

Gestion des actions

- Pilotez l'ensemble de **vos actions**:
 - Construction
 - Amélioration
- Définissez vos niveaux de **reporting** !
- **Affectez** les actions et pilotez !

Pilotages Run

Définissez **vos moyens de contrôle**
KPI
Actions récurrentes
Définissez vos niveaux de **reporting** !
Affectez ces objets et pilotez !

Merci

Merci de votre feedback et évaluations !



<https://forms.office.com/r/d0a6s7YH0q>

Si vous avez des commentaires, ou des questions, contactez l'équipe support :
support@tenacy.io