Tenacy

Atelier 5
Dérogation et écarts

tenacy.io

V1.0
11/10/2022

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

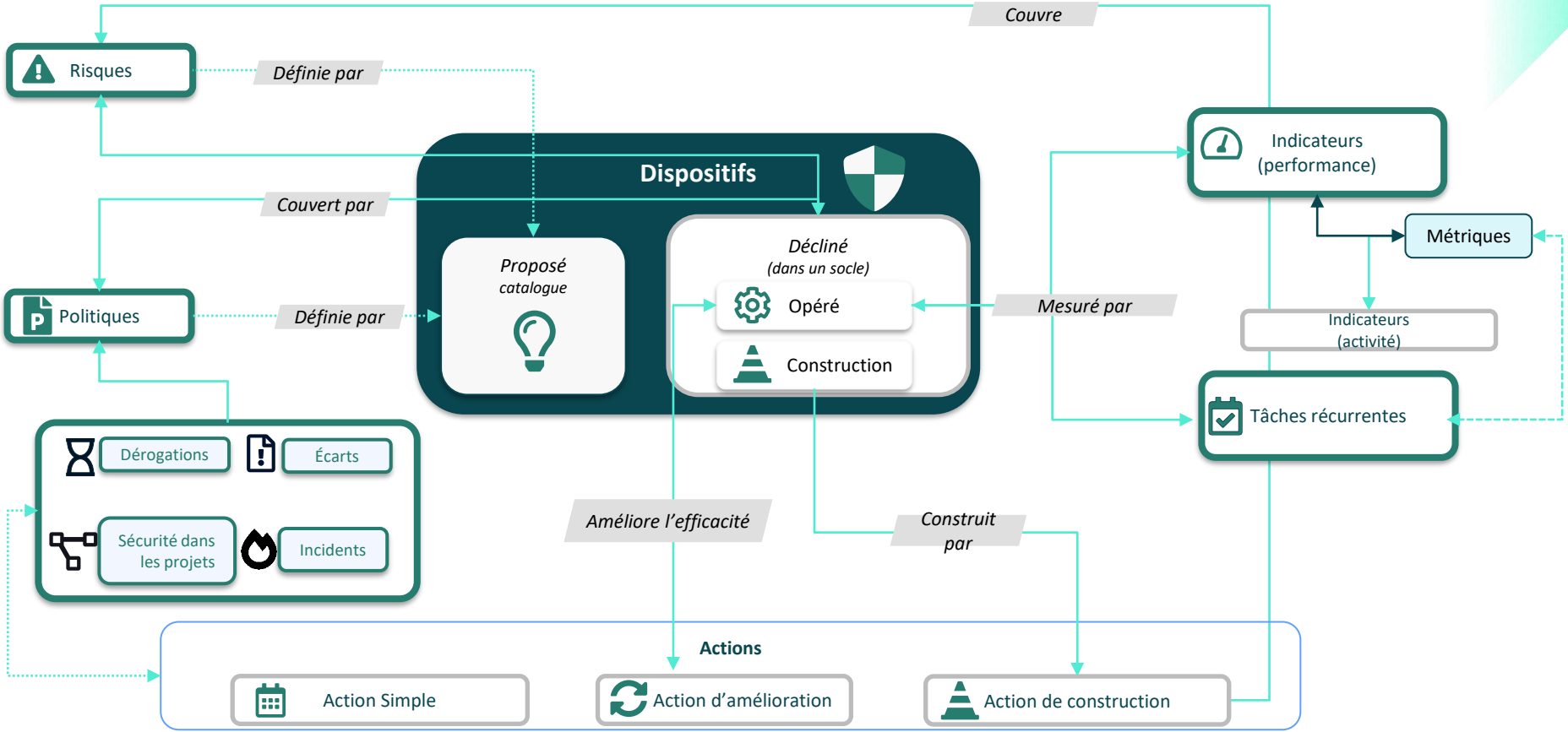
Les cas particuliers, les mises en œuvre seront à privilégiés sur les ateliers intégrateur / CSM

Qu’allons nous voir dans cet atelier ?

Sujets principaux

Sécurité dans les projets	Dérogations	Écarts
Incidents	Registres	Actions

Modèle fonctionnel



Modèle fonctionnel

applicable aux applications et fournisseurs

Sécurité dans les projets

La sécurité dans les projets permet de suivre la conformité aux politiques de sécurité applicables à un projet (non sécurité).

Un projet cible un unique élément (périmètre , application ou fournisseur)

L'échelle de criticité des éléments est personnalisable (*application.criticality_scale*)

Mode DICP / régular

En mode DICP chaque échelle est configurable (mais commune à l'ensemble des projets)

Le worflow implémenté est non configurable (ISO 27034)

À chaque étape du workflow des actions de suivi sécurité sont nécessaires: Création des actions – Mise à jours – mise en production etc.

L'ensemble des résultats, actions sont tracés dans le fil d'activité du projet

Sécurité dans les projets

Workflow Sécurité dans les projets

Initialisation

Analyse de l’application

Détermination des besoins de sécurité (politiques applicables)

Identification des besoins de tests

Besoins

Évaluations du projet versus les politiques

Output: liste des actions

Conception

Planification des actions

On attend en fin d'étape que toutes les actions soient planifiées.

Construction

Suivi de la réalisation des actions

On attend en fin d'étape que toutes les actions soient terminées.

Validation

Définition de l’avis sur la base de l'évaluation, de la correction des écarts et des scores de test

Production

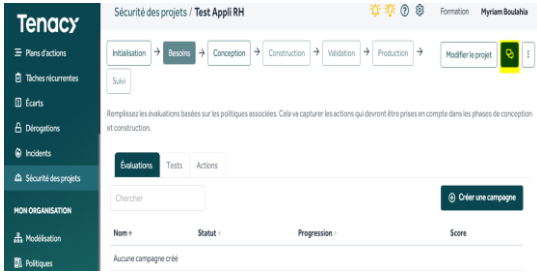
Dans cette étape on attend la **mise en production** du projet. L'activité sécurité peut consister en la **levée des réserves** liées à la fermeture des dernières actions.

Suivi

L'étape de suivi est **optionnelle. Elle peut être nécessaire quand des actions sont encore ouvertes malgré le passage en production**

En suivi il est encore possible de modifier l'avis sécurité, de créer ou mettre à jour des actions.

L’ensemble des changements de statut sont consignés dans le fil d’activité du projet.



Dérogations

Une dérogation est une non-conformité validée, tracée et suivie.
L'objectif est de pouvoir piloter des dérogations au travers la solution.

Une dérogation peut être demandé par un utilisateur Tenacy (contributeur)

Elle doit être approuvée par un administrateur

Elle peut être liée à une ou plusieurs mesures de politiques

Elle peut être liée à des actions (de mise en conformité)

Des indicateurs sont calculés sur le correct management de ces dérogations.

Une dérogations n'influe pas sur le score de conformité sur une politique

L'échelle de criticité des dérogations est configurable

exemption.criticality_scale

Écarts

Un écart est anomalie constatée par rapport à ce qui devrait être, généralement les exigences de sécurité énoncées dans les politiques.. Ce module permet de suivre et reporter le traitement.

Les état suivants sont possibles pour un écart:

- Ouvert – Par défaut - l'action de traitement n'a pas encore été déterminée
- Actif - l'écart a été accepté et en cours de traitement
- Ignoré – ne sera pas traité
- Rejeté - l'écart a été refusé – mauvais constat
- Fermé - le traitement est terminé

Cette icône viendra signaler un écart en erreur (date dépassé, pas d'action). Un indicateur interne est calculé sur la conformité des traitements

Les écarts sont utilisables (création) par les administrateurs	Les registres permettent de faire du reporting sur les écarts	Liens N x M entre écarts et actions	Liens possibles entre un écart une/plusieurs mesures (politiques)	Il est possible de définir une date macro pour un registre, et pour chaque écart
La progression est calculée suivant la couverture de chaque action sur l'écart	Import/Export En XL	Génération d'un rapport de traitement pour un registre (incluant le dernier commentaire sur l'action)	Indicateurs internes calculées par la solution	L'échelle de criticité des écarts est configurable gap.criticality_scale

Incidents

Le menu Incidents à pour objectifs de consigner les incidents et de suivre l'efficacité du traitement:

- Identification des incidents en cours
- Taux de traitement des incidents

Accessible uniquement aux admins

Échelle d'impact est **customisable**

incident.impact_scale

Le temps de traitement est la différence entre les dates de **détection et de fin déclarés**

Un seuil critique peut être défini pour séparer le reporting sur les 2 groupes: incident.critical_value

L'incident contient un fil d'activité (log) ainsi que le détail des évènements (historique)

Association avec des actions:

- Pilotage du traitement
- Amélioration (apprentissage)

Workflow de gestion des incidents

Pour aller plus loin

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