Fiche mémo · Leçon 31 · 37 min

Actions irréversibles et coûts qui dérapent, les garde-fous

Un agent devient dangereux quand il dispose de trop de fonctions, de trop de droits ou de trop d'autonomie : c'est l'agentivité excessive décrite par l'OWASP. Vous apprenez à repérer les actions qui ne se rattrapent pas, à les garder sous votre accord, puis à borner chaque tâche et à régler plafonds et alertes pour que la facture reste prévisible.

Objectifs

- Classer les actions d'une tâche selon qu'elles se rattrapent ou non, avant de la confier
- Retirer à un agent les fonctions, les droits et l'autonomie dont sa mission n'a pas besoin
- Borner une tâche et régler plafonds et alertes pour que son coût reste prévisible

À retenir

- L'agentivité excessive naît de trois excès : trop de fonctions, trop de droits, trop d'autonomie. Retirez chacun avant de lancer la tâche.
- Classez chaque action avant de la confier : ce qui sort de l'entreprise, se paie ou se supprime définitivement reste toujours à une personne.
- Un droit retiré protège mieux qu'une interdiction écrite dans la fiche.
- Le coût d'une tâche vient de ce qu'elle lit, de ses tentatives et de sa durée : bornez-les en chiffres dans la fiche.
- Mesurez trois exécutions, puis posez plafond et alerte, et relevez chaque coût au registre.

La demande à recopier

Demande à recopier Une fiche qui propose sans rien toucher

```
MISSION : un tableau Excel des doublons probables du dossier Drive « Clients 2023 », une ligne par paire de fichiers, à ranger dans « Clients 2023 / _Revue ». Une seule mission.
APPUIS : le dossier « Clients 2023 » et lui seul. Un doublon probable : même nom à la date près, ou même taille et même type dans le même sous-dossier.
NIVEAU D'ACCÈS : Google Drive en lecture sur ce dossier ; création d'un seul fichier dans « _Revue ». Aucun autre connecteur pour cette tâche.
DÉROULÉ : 1. Parcourir les sous-dossiers. 2. Relever les paires selon la règle. 3. Pour chaque paire, indiquer le fichier le plus récent et le plus complet. 4. En cas de doute, classer la paire en « à voir » plutôt que de trancher.
ARRÊTS : aucun déplacement, aucune mise à la corbeille, aucune suppression, aucun partage. Si la règle donne plus de 300 paires, s'arrêter et me le signaler avant de continuer.
TERMINÉ QUAND : le tableau existe avec les colonnes chemin A, chemin B, raison, fichier à garder, certitude (sûr ou à voir) ; le compte rendu liste le nombre de paires, les cas « à voir », la durée de la tâche et confirme qu'aucun fichier n'a bougé.
```

Note : La suppression se fera ensuite par lots, sur votre validation, dans une seconde fiche au niveau 3.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Passer une tâche qui lit la messagerie en mode sans contrôle « pour ne pas être dérangé ». Ce mode supprime l'examen des actions. Une boîte aux lettres reçoit des courriels de n'importe qui, donc des consignes possibles : rien ne s'interpose entre un courriel piégé et un envoi, un transfert ou une suppression.	Mode Manuel tant que la tâche n'a pas fait dix exécutions propres au registre, puis Auto au plus. Le mode sans contrôle seulement sur des fichiers et des outils dont vous maîtrisez chaque élément, jamais sur une boîte ouverte à l'extérieur.
Écrire « ne supprime rien » dans la fiche et laisser le connecteur avec tous ses droits. Une consigne se lit, s'interprète, et peut être contredite par un texte que l'agent rencontre en chemin. L'OWASP recommande de faire respecter les autorisations par l'outil, pas par le jugement du modèle.	Retirez le droit quand le réglage existe : connecteur en lecture seule, action bloquée ou soumise à approbation par l'administrateur. Gardez la phrase dans les ARRÊTS, en plus du réglage, jamais à sa place.
Programmer une tâche quotidienne sans avoir mesuré son coût, et découvrir la consommation en fin de mois. Le coût d'une tâche dépend de ce qu'elle lit, de ses tentatives et de sa durée. Une fiche qui dit « la bibliothèque » ou « réessaie jusqu'à réussir » peut multiplier la facture par trois sans que le livrable change.	Trois exécutions accompagnées avec relevé du coût, des bornes chiffrées dans la fiche (sources, éléments, tentatives, minutes), puis un plafond et une alerte posés à partir de la mesure, et chaque coût noté au registre.
Approuver d'un clic un lot de 200 actions proposées par l'agent, sans rien lire. L'accord groupé n'a de valeur que si vous savez ce que vous validez. Un lot non lu transforme un niveau 3 en niveau 4 déguisé, avec votre accord en prime dans le journal.	Demandez des lots de taille fixée dans la fiche (50 par exemple), lisez un échantillon de dix lignes et toutes les lignes marquées « à voir », et refusez le lot entier au premier écart.

Ce qui se rattrape, ou non

Sans conséquence hors de l'agent

- Lire, chercher, résumer
- Rédiger un brouillon
- Préparer un tableau à relire

Réversible si le journal est tenu

- Créer ou déplacer un événement
- Mettre à jour une fiche CRM
- Déplacer un fichier, mettre à la corbeille

Irréversible ou engageant

- Envoyer à l'extérieur
- Payer, commander, valider un panier
- Supprimer définitivement, partager hors de l'entreprise

Classez chaque action de la tâche avant de la confier, pas après.