

# Réduire les faux positifs DLP avec des exclusions de correspondance de données

## Table des matières

---

---

### Introduction

Ce document décrit comment utiliser les exclusions de correspondance des données pour réduire les faux positifs dans les classifications de données DLP (Data Loss Prevention).

### Aperçu

Les exclusions de correspondance des données vous permettent d'exclure des données correspondantes spécifiques, ce qui vous aide à affiner les classifications de données DLP et à réduire considérablement les faux positifs. Cette fonctionnalité offre une protection des données plus précise en vous permettant d'exclure des analyses DLP les données connues, non sensibles ou les correspondances non pertinentes.

### Comment les exclusions de correspondance de données réduisent les faux positifs

Les identificateurs intégrés et personnalisés peuvent générer des faux positifs lorsque des mots clés ou des modèles correspondent à des données non sensibles. Exemple :

- Identificateurs basés sur le nombre :  
Les identificateurs tels que le numéro de sécurité sociale américain (SSN) peuvent correspondre à d'autres numéros à 9 chiffres, tels que les ID de compte internes. L'exclusion des ID de compte connus réduit ces faux positifs.
- Identificateurs textuels :  
Les clients du secteur de la santé utilisant la classification de données conforme à la HIPAA peuvent détecter le terme « cancer » dans des contextes non patients, tels que « l'organisation de don de cancer ». Vous pouvez exclure des termes spécifiques pour empêcher de telles fausses alertes.

Avec les exclusions de correspondance de données, vous pouvez spécifier des termes ou des modèles d'expressions rationnelles, en vous assurant que les correspondances sur ces derniers ne déclenchent pas d'événements de violation de données. Cela permet un contrôle précis des alertes DLP.

### Comment utiliser les exclusions de correspondance de données

1. Dans le tableau de bord Umbrella, accédez à la page Classification des données.
2. Dans la section Exclure les identificateurs de données, sélectionnez un identificateur personnalisé ou un identificateur intégré à exclure.
3. Entrez les termes ou modèles d'expression régulière spécifiques que vous souhaitez exclure.
  - Les exclusions s'appliquent uniquement au contenu correspondant spécifique, et non à l'intégralité du document.
  - Par exemple, si vous excluez « Cancer Donation Organization », seul ce terme est exclu des violations, tandis que le reste du document est encore numérisé.

The screenshot shows a web form titled "Add New Data Classification". It has two input fields at the top: "Data Classification Name" containing "New Data Classification" and "Description (Optional)" which is empty. Below these are two main sections: "Include Data Identifiers" and "Exclude Data Identifiers". Each section has a "Select Boolean Operator" with radio buttons for "OR" (selected) and "AND". Under each section, there are two expandable lists: "Built-in Data Identifiers" and "Custom Identifiers". At the bottom right, there are "CANCEL" and "SAVE" buttons.

4. Si le même identificateur de données est inclus et exclu dans la même classification, l'exclusion est prioritaire.

## Ressources connexes

Reportez-vous à la documentation Umbrella pour obtenir des instructions détaillées : [Créer une classification de données.](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.