



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SA-08(20)

Gestion sécurisée des métadonnées

Juill. 2026



Acquisition sécurisée des systèmes/services

System and Services

SA-08(20) – Gestion sécurisée des métadonnées (PbMM)

Énoncés :

Mettre en place le principe de conception sécurisée de la gestion sécurisée des métadonnées dans les [\[Affectation : systèmes ou composants de systèmes désignés par l'organisation\]](#).

Responsable : Aucun

Discussion :

Le principe de gestion sécurisée des métadonnées repose sur le fait que les métadonnées sont des objets de première classe en ce qui concerne la stratégie de sécurité lorsque la stratégie exige une protection complète de l'information ou que le sous-système de sécurité doit se protéger lui-même. Le principe de gestion sécurisée des métadonnées est axé sur la reconnaissance qu'un système, un sous-système ou un composant ne peut se protéger lui-même que s'il protège les données dont il dépend pour s'exécuter correctement. Les données ne sont généralement pas interprétées par le système sur lequel elles sont stockées. Ce dernier peut avoir une valeur sémantique (il contient l'information) pour les utilisatrices, les utilisateurs et les programmes qui traitent les données. À l'inverse, les métadonnées sont de l'information sur les données, comme un nom de fichier ou la date à laquelle le fichier a été créé. Les métadonnées sont liées aux données cibles qu'elles décrivent d'une manière que le système peut interpréter, mais elles n'ont pas à être stockées avec les données cibles ou à proximité de celles-ci. Certaines métadonnées peuvent avoir pour cible d'autres métadonnées (par exemple, le niveau de classification ou d'incidence sur un nom de fichier), ce qui est notamment le cas pour les métadonnées autoréférentes. La seconde nature apparente des métadonnées peut entraîner la négligence de son besoin de protection légitime, ce qui va à l'encontre de la stratégie de sécurité qui comprend l'exfiltration de l'information. Une préoccupation particulière associée à la protection insuffisante des métadonnées touche les systèmes à sécurité multiniveau (MLS pour Multilevel Secure). Les systèmes MLS gèrent l'accès d'une personne à un objet en fonction des niveaux de sensibilité relative. Par conséquent, les étiquettes du niveau de sensibilité sont apposées directement ou affectées indirectement aux personnes et aux objets qui relèvent du contrôle du système MLS. La conséquence des métadonnées étiquetées pour les systèmes MLS veut qu'une étiquette soit ajoutée aux objets contenant des métadonnées. Comme pour les évaluations des besoins de protection des données, il convient de s'assurer que les mesures de protection de la confidentialité et de l'intégrité soient évaluées, précisées et affectées aux métadonnées, comme ça serait le cas pour les données de la mission, de l'organisation ou des systèmes.