



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

AU-06(08)

Analyse plein texte des commandes privilégiées

Juill. 2026



Journaux d'audit, traçabilité des actions

Audit and Accountability

AU-06(08) – Analyse plein texte des commandes privilégiées (PcE-)

Énoncés :

Mener une analyse plein texte des commandes privilégiées enregistrées dans un composant de système ou un sous-système physiquement distinct du système ou dans un autre système conçu pour mener cette analyse.

Responsable : Aucun

Discussion :

Une analyse plein texte de commandes privilégiées exige l'utilisation d'un environnement distinct pour analyser l'information enregistrée de vérification concernant les utilisateurs qui détiennent des droits d'accès privilégiés afin de ne pas compromettre l'information dans le système dans lequel les utilisatrices et utilisateurs ont des privilèges élevés, dont la capacité d'exécuter des commandes privilégiées. On entend par analyse plein texte l'analyse qui prend en compte le texte intégral associé aux commandes privilégiées (c'est-à-dire, les commandes et les paramètres) contrairement aux analyses qui ne tiennent compte que du nom de la commande. L'analyse plein texte comprend le recours au filtrage et à l'heuristique.