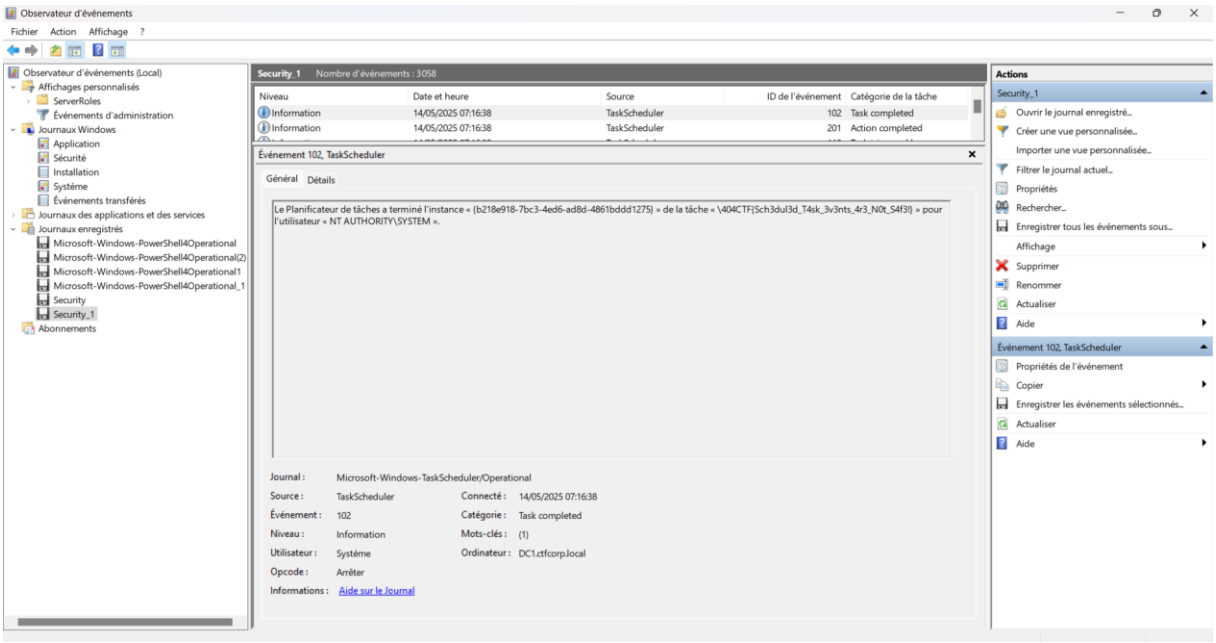
Résolution de l’Analyse Forensique Forensic et Mat [1/2] (mode bis)

Une première méthode de résolution ayant été déjà exposée, ci-dessous une deuxième méthode de résolution suit.

En ouvrant le journal d’événement Security.evtx dans l'observateur d'évènement Windows, parmi la liste répertoriée des événements de sécurité, nous découvrons d’un log de Security, le flag en direct, depuis une séquence des tâches.



Le Planificateur de tâches a terminé l’instance « {b218e918-7bc3-4ed6-ad8d-4861bddd1275} » associé à un ordonnanceur de tâche via l’événement 102 de la tâche complétée d’utilisateur : Système du 14/05/25. « **\404CTF{Sch3dul3d_T4sk_3v3nts_4r3_N0t_S4f3!}** » pour l’utilisateur « NT AUTHORITY\SYSTEM ».