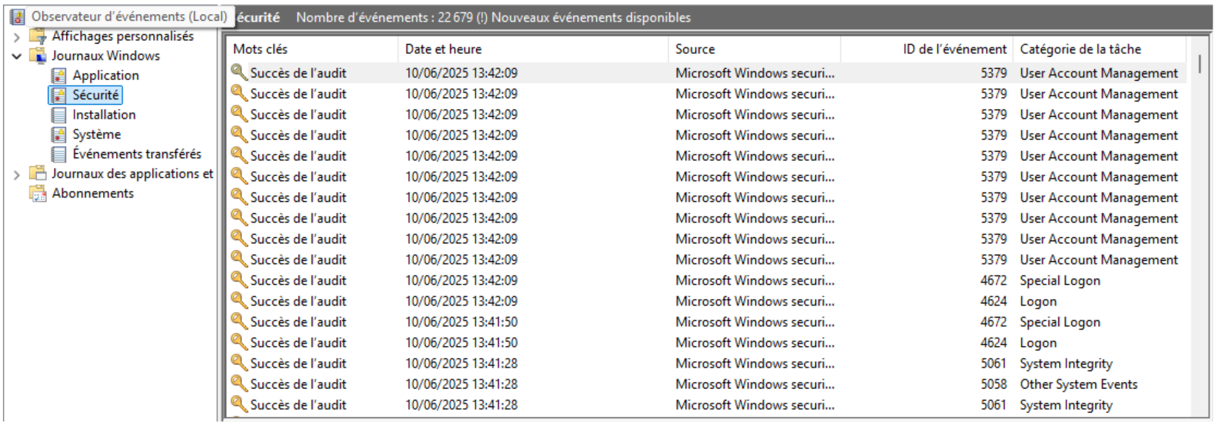
Réponse à un incident de sécurité

Ransomware

1. Stratégie de détection

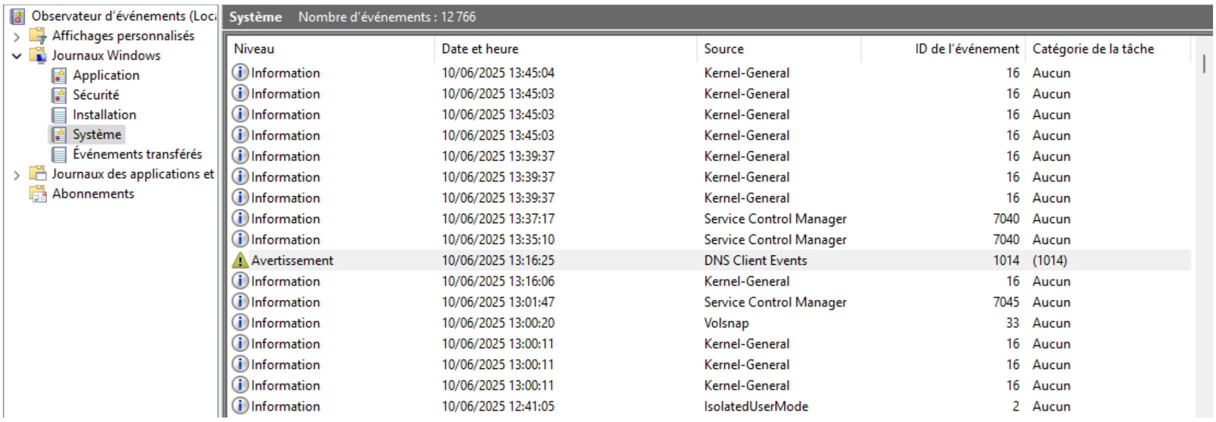
En cas d'une attaque par Ransomware, voici les fichiers à analyser :

Journal de Sécurité :



Mots clés	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	5379	User Account Management
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	4672	Special Logon
Succès de l'audit	10/06/2025 13:42:09	Microsoft Windows securi...	4624	Logon
Succès de l'audit	10/06/2025 13:41:50	Microsoft Windows securi...	4672	Special Logon
Succès de l'audit	10/06/2025 13:41:50	Microsoft Windows securi...	4624	Logon
Succès de l'audit	10/06/2025 13:41:28	Microsoft Windows securi...	5061	System Integrity
Succès de l'audit	10/06/2025 13:41:28	Microsoft Windows securi...	5058	Other System Events
Succès de l'audit	10/06/2025 13:41:28	Microsoft Windows securi...	5061	System Integrity

Journal Système :



Niveau	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Information	10/06/2025 13:45:04	Kernel-General	16	Aucun
Information	10/06/2025 13:45:03	Kernel-General	16	Aucun
Information	10/06/2025 13:45:03	Kernel-General	16	Aucun
Information	10/06/2025 13:45:03	Kernel-General	16	Aucun
Information	10/06/2025 13:39:37	Kernel-General	16	Aucun
Information	10/06/2025 13:39:37	Kernel-General	16	Aucun
Information	10/06/2025 13:39:37	Kernel-General	16	Aucun
Information	10/06/2025 13:37:17	Service Control Manager	7040	Aucun
Information	10/06/2025 13:35:10	Service Control Manager	7040	Aucun
Avertissement	10/06/2025 13:16:25	DNS Client Events	1014	(1014)
Information	10/06/2025 13:16:06	Kernel-General	16	Aucun
Information	10/06/2025 13:01:47	Service Control Manager	7045	Aucun
Information	10/06/2025 13:00:20	Volsnap	33	Aucun
Information	10/06/2025 13:00:11	Kernel-General	16	Aucun
Information	10/06/2025 13:00:11	Kernel-General	16	Aucun
Information	10/06/2025 13:00:11	Kernel-General	16	Aucun
Information	10/06/2025 12:41:05	IsolatedUserMode	2	Aucun

2. Stratégie de réponse

Pour répondre à cet incident, selon moi voici l'ordre de priorité :

a) Identifier le problème
b) Isolement du poste
c) Lancer une vérification anti-virus
d) Documenter le problème

e) Eradiquer si possible
f) Récupération des données à partir d’une sauvegarde

Ou

a. Déconnecter immédiatement l'ordinateur du réseau pour éviter la propagation.
b. Identifier l'origine de l'infection (fichier téléchargé, email suspect, etc.).
c. Ne pas payer la rançon : cela ne garantit pas la récupération des fichiers et encourage les cybercriminels.
d. Vérifier les sauvegardes pour restaurer les données sans compromettre le système.
e. Analyser le système avec un antivirus et des outils spécialisés pour éliminer la menace.
f. Consulter les logs dans l'Observateur d'événements pour comprendre l'attaque et renforcer la sécurité.
g. Informer les autorités compétentes, surtout si l'attaque concerne une entreprise.
h. Renforcer la protection pour éviter toute récidive : mises à jour, sécurité renforcée, et formation des utilisateurs.