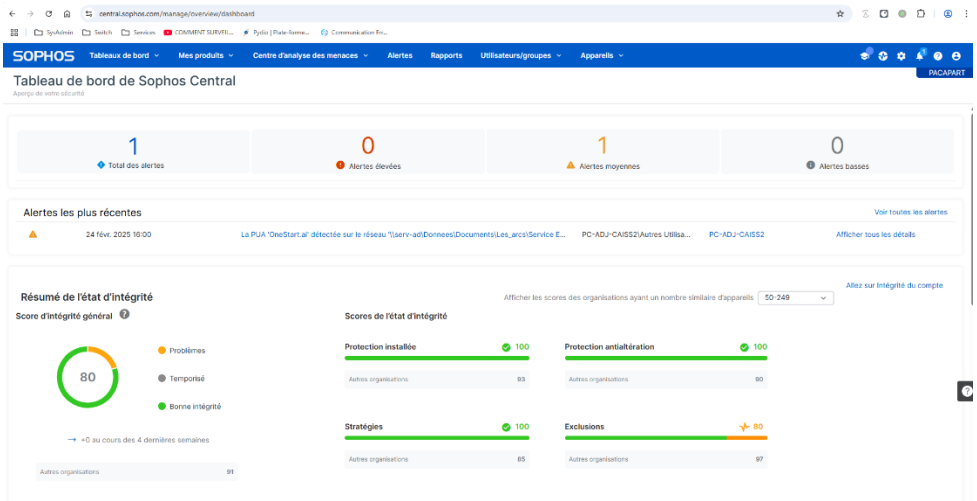
Présentation de la solution EDR Sophos Central & procédure de filtrage web

Contexte et usage de Sophos Central dans l'entreprise

Solution EDR déployée :

Sophos Central Endpoint Protection, plateforme cloud de cybersécurité utilisée pour :

- Protéger les postes de travail (Windows) contre les menaces : virus, ransomwares, PUA, etc.
- Gérer les politiques de sécurité (pare-feu, protection des données, contrôle d'accès web…)
- Superviser les alertes en temps réel via un **tableau de bord centralisé**.



Modules activés par utilisateur/poste :

Chaque utilisateur ou machine peut se voir appliquer des **stratégies spécifiques** :

- Contrôle d'applications
- Prévention des pertes de données (DLP)
- Pare-feu Windows
- Contrôle des périphériques
- **Contrôle de la navigation Web**
- Gestion des mises à jour

Exemple de procédure : blocage ou déblocage d'une catégorie de sites

Objectif :

Interdire ou autoriser l'accès à des **catégories de sites web spécifiques**, comme les sites liés à l'alcool, via la stratégie de **Web Control**.

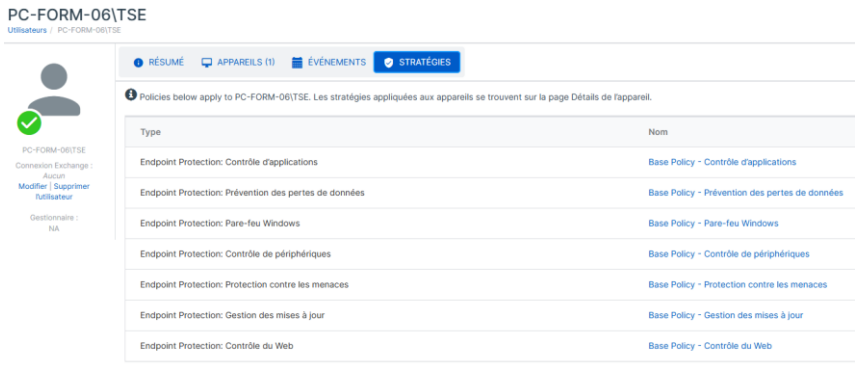
Étapes de mise en œuvre

1. Connexion à Sophos Central

- URL : https://central.sophos.com
- Compte administrateur : pacaparticipations.informatique@...

2. Accéder à la stratégie Web Control

- Menu de gauche : **Stratégies**
- Choisir la stratégie à modifier (ex. : Stratégie Open – Web Control)
- Cliquer sur **"Paramètres"** > **"Contrôle du Web"**



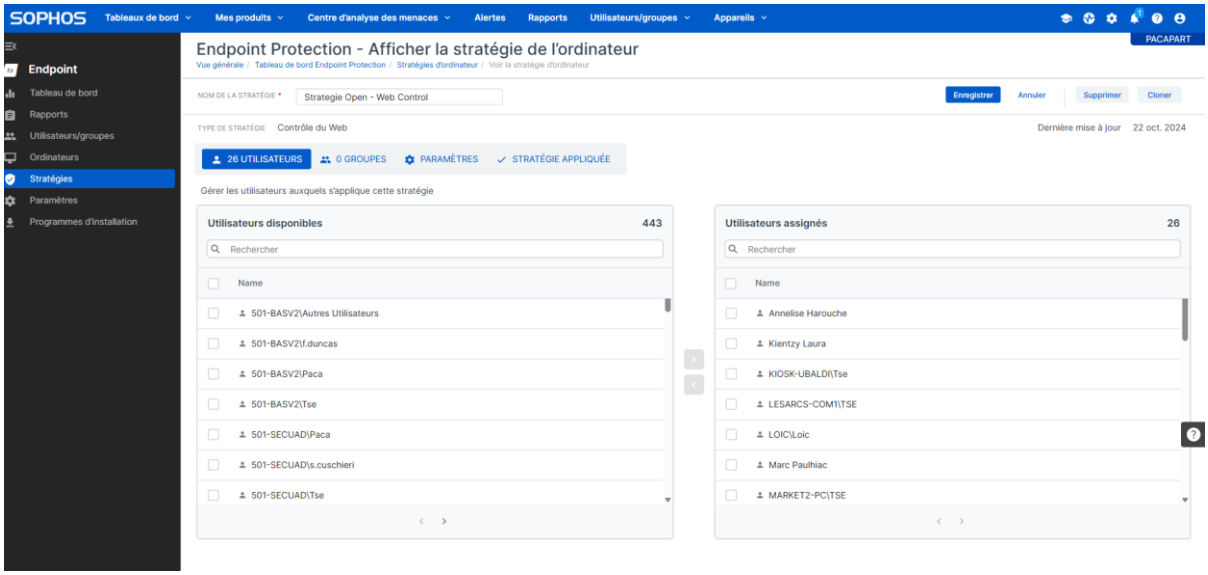
3. Modifier les paramètres de filtrage

Dans la section **"Catégories de sites web"** :

- Rechercher ou localiser la catégorie.
- Choisir l'action souhaitée :
  - **Autoriser** pour débloquer l'accès
  - **Bloquer** pour interdire l'accès
  - **Alerter** pour autoriser tout en générant une alerte dans le tableau de bord

4. Affectation ou vérification des utilisateurs concernés

- Toujours dans la stratégie, onglet **"Utilisateurs"**
- Ajouter ou retirer des comptes si nécessaire :
  - Exemple : bloquer les sites d'alcool pour les machines TSE
  - Autoriser l'accès pour les comptes informatiques ou administratifs



5. Suivi et alertes

- Toute tentative d’accès bloqué peut générer une alerte visible dans le **tableau de bord** Sophos.
- Exemple d’alerte : tentative d’accès à un site classé **PUA ou contenu restreint**.

Conclusion

La solution **Sophos Central** permet une gestion centralisée, granulaire et réactive de la sécurité des postes utilisateurs. Le module **Web Control** offre un **filtrage fin par catégorie de sites**, permettant d’assurer le respect des politiques de navigation (blocage de sites inappropriés ou non productifs).