a Sopra Steria company

SEDUCS
Unifyer

SEDUCS UNIFYER

POSTE BI-DOMAINE

Face à la **multiplication des cyberattaques,** les entreprises doivent pouvoir **garantir la sécurité de leurs données, de leurs échanges, protéger leur patrimoine informationnel** et tout contenu reconnu comme sensible. Cela tout en **assurant une conformité réglementaire** et en tentant de réduire au maximum les risques et les vulnérabilités.

Les entreprises font face à un contexte où les **portes d'entrée se sont multipliées** (télétravail, BYOD...) induisant un changement de paradigme dans la manière d'aborder la protection des Systèmes d'Information.

Il devient nécessaire de **cloisonner les domaines** ainsi que les acteurs afin de **protéger les fonctions vitales de l'entreprise.**

La solution à la dualité des postes

Si la sécurisation des postes de travail et de leurs connexions aux SI de l'entreprise, la protection des données (chiffrement des supports, authentification multi facteurs...) ont parfois entraîné la mise en œuvre de processus complexes et lourds, il devient primordial de fluidifier les modes de travail tout en assurant la confidentialité, intégrité et sécurité.

Avantages Clés

Minimisation de la surface d'attaque par selection fine des composants et dépendances strictement nécessaires et suffisants

Un poste très sécurisé avec des applicatifs constamment à jour

Une sécurité assurée nominalement

OS Durci Souverain

Plusieurs domaines dans un même poste (Sensible /SIA/ DR)

Réduction des coûts par la mutualisation des postes

Le poste bi-domaines / bi-niveaux Seducs-Unifyer est un poste de travail permettant à un utilisateur de **travailler en toute mobilité, sur deux environnements isolés** dont les besoins en sécurité sont différents.
Les environnements de travail sur le poste sont **des machines virtuelles généralement fournies par nos clients**. Le poste, basé sur une solution SEDUCS conçue à cet effet, agit comme un **hyperviseur multiniveaux sécurisés aux fonctions cloisonnées.**
Le poste utilise des mécanismes de configuration et de restriction pour **garantir la sécurité et l'isolation des environnements virtualisés.**
Ce produit a été conçu pour **répondre aux besoins de disposer d'un poste matériel unique** exploitant différents environnements cloisonnées.

Avantages en termes de sécurité

Un système d'exploitation à faible surface d'attaque

Résilience renforcée «aux attaques»

La mise en place de scellé de confiance dès le démarrage (boot)

Une séparation forte des environnements et des identités

Cloisonnement fort des environnements, IHM d'administration, IHM différenciée par environnement

Chiffrement intégral des disques par l'usage de composants physiques (TPM)

Augmentation forte par carte à puce possible

Une sécurisation native des flux réseaux

VPN primaire pour l'accès sécurisé de l'hyperviseur au domaine général

VPN secondaire dans le VPN primaire pour l'accès au SI sensible

VPN secondaire dans le VPN primaire pour l'accès au SI non sensible

Une politique de cybersécurité adaptative selon l'environnement

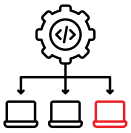
Maîtrise et utilisation périphériques (micro, caméra, port USB) selon le domaine de travail (sensible, non sensible)

Maîtrise et utilisation des périphériques selon l'origine de la connexion réseau (entreprise, public)

Maîtrise et utilisation des flux autorisés selon le domaine et/ou le type de connexion

Avantages en termes d'usage

Prise en main facilitée



Ergonomie optimisée pour passer d'un environnement à l'autre

Diminution des erreurs humaines et des mauvaises pratiques (clés USB d'un PC à un autre par ex)

Optimisation du poids lors des déplacements et interventions

Avantages en termes financiers et budgétaires

Un seul poste multi-usage, au lieu de plusieurs postes à usage unique

Reprise et intégration des environnements de travail existants

Réduction des coûts de maintenance du parc de PC

MCO / MCS

a Sopra Steria company

CS GROUP
22, Avenue Galilée - 92350 Le Plessis Robinson, France
tél : +33 (0)1 41 28 40 00 - contact.cyber@csgroup.eu
www.csgroup.eu