7 LA SECURITE DES EQUIPEMENT ACTIFS

7

Equipements Actifs

- Le Hardening.
- Les antivirus.
- Le patch Management.
- La virtualisation.
- Les vulnérabilités des équipements actifs.
- Les Attaques sur les équipements.
- Les Malwares.

7 Principes du hardening : la sécurité « en profondeur »

- Le **Renforcement des systèmes** par la mise en œuvre de mesures de sécurité afin de réduire au minimum les possibilités d'exploitation des points vulnérables d'un système informatique.
- Choix et installation du système lui-même
- Choix des **services** activés par défaut et des **applications** installées sur le système (**un système minimal**)
- Restriction des accès locaux ou distants
- Optimiser le paramétrage des applications et processus utilisant les protocoles TCP/IP
- Définir une **stratégie des mots de passe**
- Bien contrôler les **droits des utilisateurs** et les accès aux ressources (fichiers, applications ..)
- Contrôler les **accès aux ressources matériels** (ports USB, accès aux BIOS ...)
- Optimiser son système de fichiers (type, partitionnement, **chiffrement** ...)
- Utiliser des « Anti » (Antivirus, antimalware, antispy, etc.) et des **contrôleurs d'intégrité**
- Activer le **firewall logiciel**
- Mises à jour régulières des systèmes (hors réseaux hostiles) : le **patch management**
- Avoir une stratégie de **sauvegardes**
- Utiliser des **V.D.S.** (scanner de vulnérabilités)
- **Tout documenter !**

7 Exemple de hardening : Windows »

A. Microsoft Security Baselines :

- Tout d'abord, il faut savoir que Microsoft propose un ensemble de documents baptisés **"Microsoft Security baseline"** et correspondants à chaque version de Windows, Windows Server, et certaines applications comme le navigateur Microsoft Edge.

- À chaque fois, Microsoft propose une documentation pour lister chaque paramètre à configurer et de quelle façon. Celle-ci est accompagnée par des modèles de GPO, ainsi que des modèles d'administration pour ces mêmes GPO (ADMX), et des scripts PowerShell.

B. Les guides du CIS Benchmark

Le CIS (*Center for Internet Security*) propose un ensemble de guides de bonnes pratiques pour de nombreux produits et services : Windows, Windows Server, Debian, Cisco, Apache, Fortinet, Google Chrome, Google Workspace, Kubernetes, SQL Server, VMware, Azure, etc... Ces guides, maintenus à jour au fil des versions, ont une excellente réputation. Ils sont très souvent utilisés comme référence lorsque l'on souhaite durcir la configuration d'un système ou d'une application.

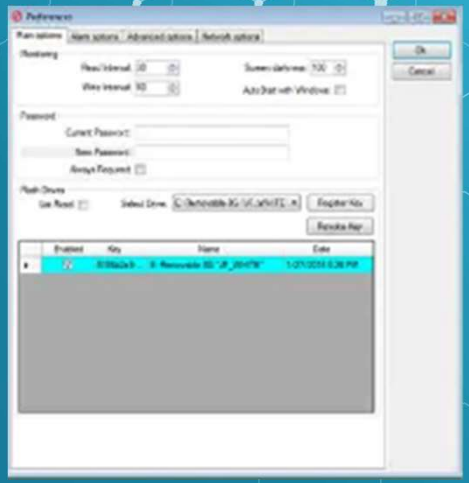
C. Les autres ressources :

Au-delà des ressources proposées par Microsoft et les guides du CIS, nous pouvons compter sur ceux d'autres organisations et entités : l'ANSSI en France, la BSI en Allemagne (l'équivalent de l'ANSSI), la CISA aux Etats-Unis, etc..

- **Quelques outils :**
  - Script PowerShell
  - HardeningKitty

7 Exemple de hardening : Périphérique USB »

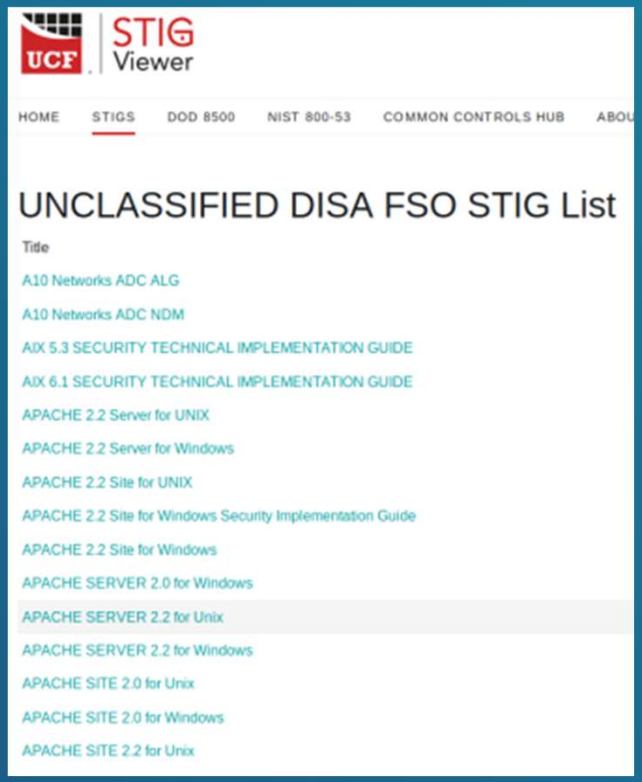
- Le Pour éviter le pod slurping (copie des données sur un appareil nomade comme un disque dur) ou toute autre attaque par USB, il est possible :
  - soit de contrôler les appareils que l'on branche en USB ou en FireWire,
  - soit d'en interdire l'utilisation.
- **Un exemple de hardening : contrôle des périphériques USB**



- **Quelques outils :**
  - USB Disk Manager
  - USB PC Lock Pro
  - Fonction de certains antivirus
  - Manuellement dans la base de registre ou dans les fichiers de montage des périphériques (Linux)
- **Solutions physiques :**
  - Bouchons de verrouillage
  - Déconnexion électrique du port

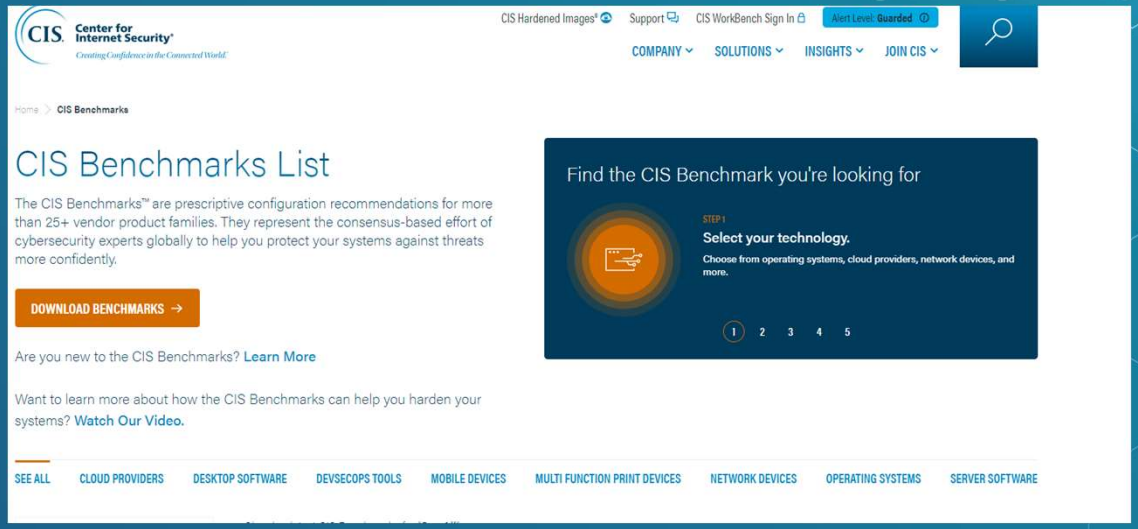
7 Les STIG - Security Technical Implementation Guide

- **Guides** de mesures de sécurité pour différents systèmes et applicatifs.
- **Scripts** payants ou gratuits permettant de vérifier les mesures de sécurité



7 CIS Benchmarks - Center for Internet Security

- **100 guides** pour 25 constructeurs de mesures de sécurité pour différents systèmes et applicatifs.



Srv : https://www.cisecurity.org/cis-benchmarks

7 Protection des terminaux - Solutions

Logiciel qui protège un équipement (PC, Serveur, téléphone etc…) contre les programmes et fichiers malveillants.

- Ils peuvent scanner :
  - Le contenu d'un disque dur
  - La mémoire de l'ordinateur
  - Les échanges de fichiers avec l'extérieur à la demande (**On-Demand Scanners**) ou actif à l'arrière-plan (**On-Access Scanners**).

- **2 méthodes de détection :**
  - Reconnaissance de motifs
  - Analyse comportementale

7 Le vocabulaire

Antivirus vs Anti-malware :

- Protègent des mêmes types de malveillants
- Anti-malware : pas conçus pour restaurer des fichiers qui ont été modifiés ou remplacés par un malveillant de type « virus ».

HIPS – Host Intrusion Protection System

- Basée sur :
  - la reconnaissance de motifs dans les logs
  - la reconnaissance de motifs dans les trames réseau
  - un contrôle d'intégrité sur des fichiers systèmes
  - un monitoring sur les terminaux (lignes de commande, scripts)

EPP – Endpoint Protection Plateform

- En plus de la protection temps réel « anti-virale », ils intègrent les fonctionnalités suivantes :
- **Gestion centralisée :** MaJ du parc, déploiement des règles, remontée d'alertes
- **HIPS**
- Pare-feu logiciel
- Protection de la flotte mobile

EDR – Endpoint Detection Response

- Solution qui a des capacités de détection, d'investigation et enfin de remédiation par de l'**IA** et du **Machine Learning** (détection par l'apprentissage)
- Solution proposant parfois les fonctionnalités de l'EPP

XDR – eXtended Detection Response

- EDR intégrant des fonctionnalités de protection des **hyperviseurs** et des services du **cloud**
- Rôle de SIEM en intégrant différentes sources de données

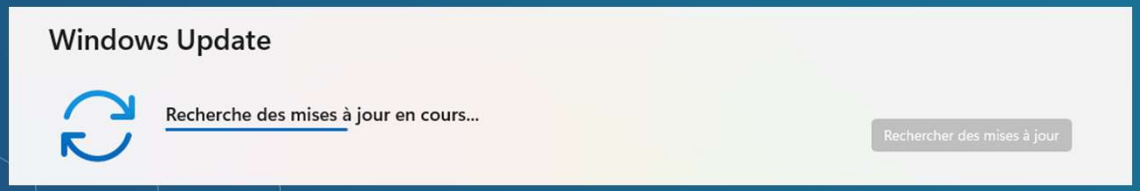
7 Guides essentiels et bonnes pratiques de cybersécurité de l'ANSSI,

Ils s'adressent aux dirigeants, gestionnaires de risques et de crises (FSSI, RSSI, CISO...), directeurs du numérique, chefs de projets, experts en cybersécurité, qui souhaitent prendre connaissance des recommandations et bonnes pratiques proposées par l'ANSSI.

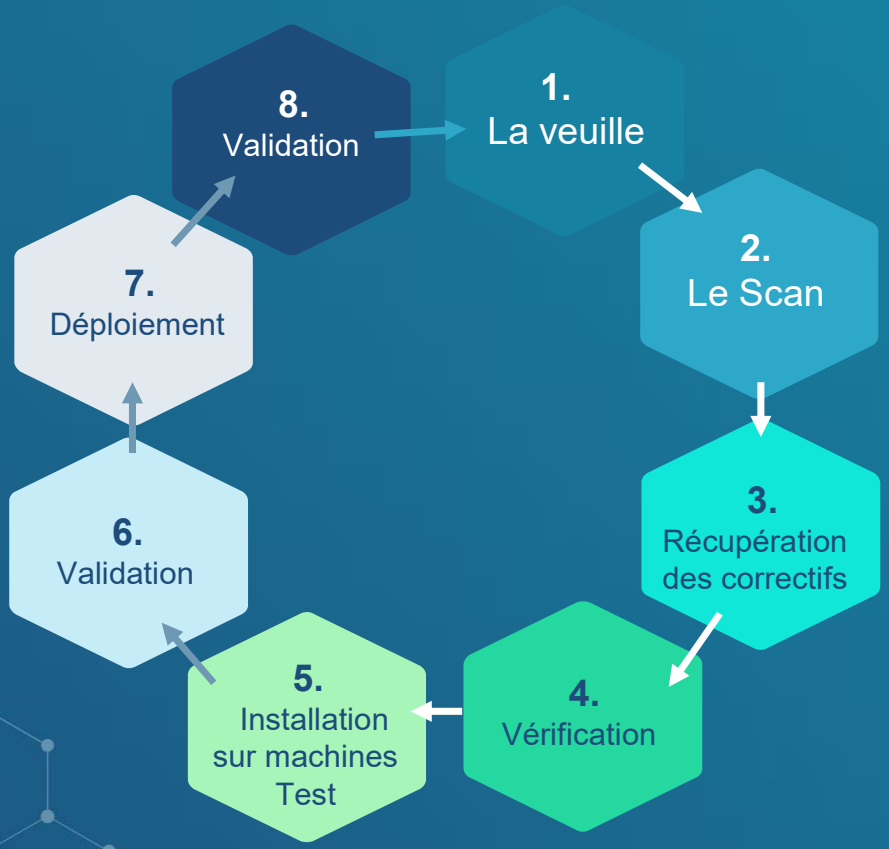
7 Patchs, Hotfixes et patch management

Un **hotfixe** est une mise à jour corrigeant un problème utilisateur spécifique.

- Un **patch** est un correctif résolvant des problèmes de sécurité, performance, stabilité, ergonomie, etc.
- Des hotfixes sont parfois packagés sous forme de « **combined hotfixes** » ou « **service pack** ».
- La période pendant laquelle un OS, un firmware ou une application n'est pas «patché» correspond à **une fenêtre de vulnérabilité**.
- Le « **patch management** » est le process utilisé pour assurer que les différents correctifs sont bien déployés sur les systèmes.

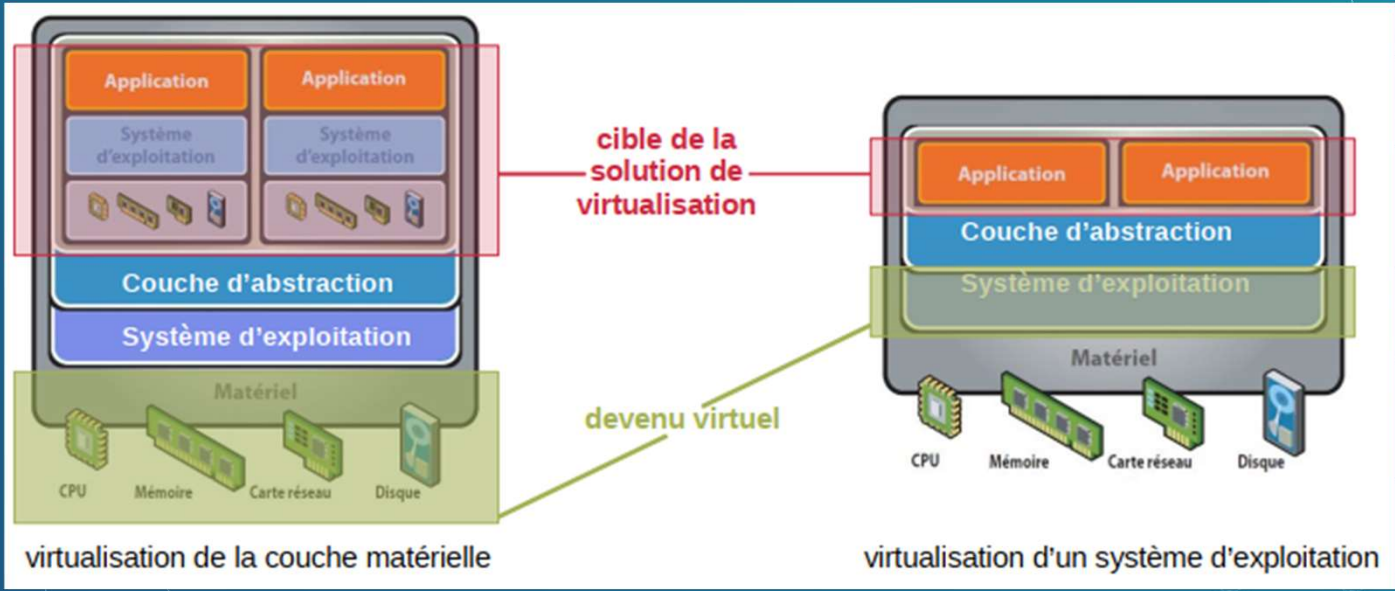


7 Gestion des correctifs en 8 Etapes

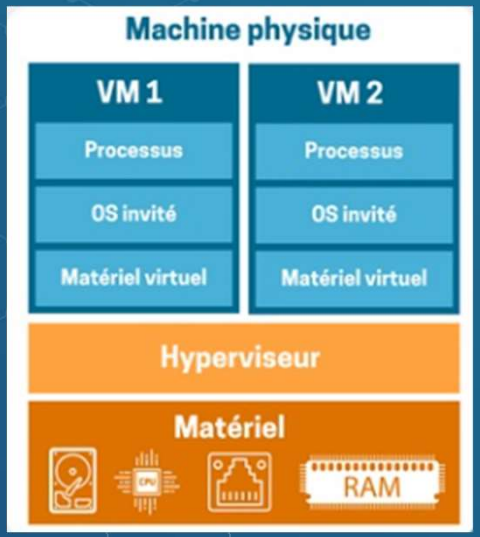


7 Définition - La virtualisation

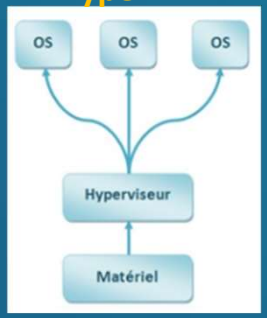
Ensemble des techniques matérielles et/ou logicielles qui permettent de faire fonctionner un programme, un système d'exploitation ou un matériel indépendamment de la structure physique et logique sous-jacente



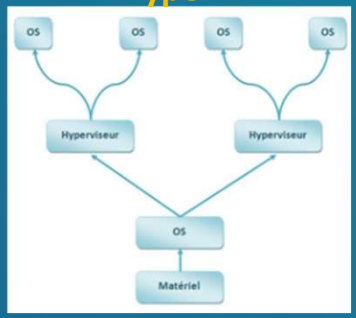
7 Les différents types de virtualisation



Hyperviseur Type 1

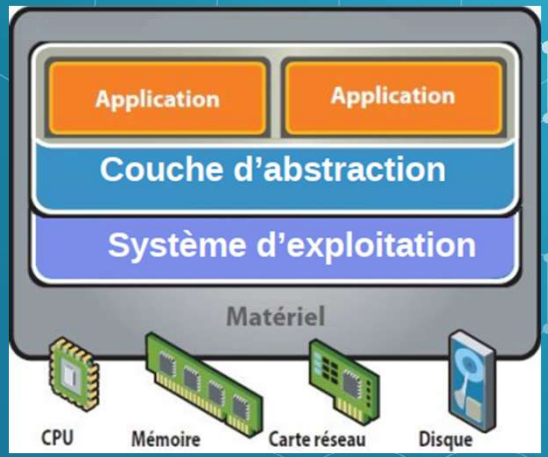


Hyperviseur Type 2



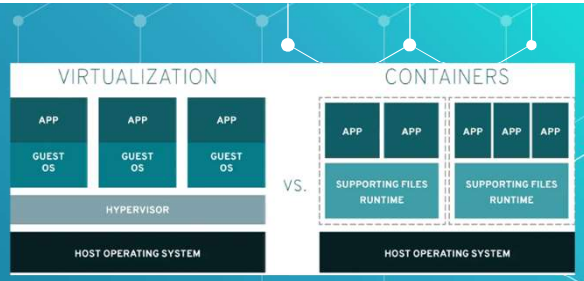
Virtualisation de la couche matérielle :

- Paravirtualisation ou **Type 1** : Xen, VMware ESXi, Vsphere, ProxMox, Hyper-V, KVM...
- Virtualisation totale ou **Type 2** : Vmware Workstation, VirtualBox, QEMU, Parallels Desktop ...
- Virtualisation assistée par le matériel



Virtualisation d'un système d'exploitation :

- **Par émulation :** Citrix, Java Virtual Machine, .Net framework, App-V ...
- **Par cloisonnement :** LXC, Docker, OpenVZ ...



7 Virtualisation VS Conteneurisation

Les deux technologies, la virtualisation et la conteneurisation, permettent d'isoler des applications ou des services pour les exécuter de manière indépendante. Cependant, elles fonctionnent de manière différente et offrent des avantages distincts.

Virtualisation :

- Virtualise l'infrastructure physique sous-jacente (machine virtuelle)
  Crée une copie complète d'un système d'exploitation (OS) pour chaque instance virtuelle.
- Chaque machine virtuelle (VM) fonctionne comme une machine physique distincte avec son propre OS, applications, bibliothèques et binaires
  Isolation totale entre les VMs.
- Consomme plus de ressources système (mémoire, processeur, etc.)

Avantages :

- Isolation totale entre les VMs
- Facile à gérer et à déployer
- Supporte des systèmes d'exploitation hétérogènes

Conteneurisation :

- Virtualise le système d'exploitation (OS) pour isoler les applications
- Partage le même noyau d'OS que l'hôte (machine physique ou VM)
- Chaque conteneur utilise les mêmes bibliothèques et binaires que l'hôte, ce qui réduit les ressources système nécessaires
- Isolation au niveau du processus (processus isolé) plutôt qu'au niveau du système (machine virtuelle)
- Léger et portable, permettant l'exécution sur n'importe quelle machine capable d'exécuter le moteur de conteneurisation
- Exemple : Docker, Kubernetes, AWS

Avantages :

- Léger et portable
- Plus efficace en termes de ressources système
- Facile à déployer et à gérer en masse

En résumé, la virtualisation est plus appropriée pour les scénarios où il est nécessaire d'exécuter des systèmes d'exploitation distincts ou des applications avec des exigences spécifiques en termes d'infrastructure. La conteneurisation est plus adaptée aux applications légères et portables qui peuvent partager le même noyau d'OS que l'hôte, offrant ainsi une isolation au niveau du processus et une meilleure efficacité en termes de ressources système