Module 1 – Fondamentaux techniques et règlementaires

Fondamentaux de la sécurité des SI et réseaux

Séquence 4 : Sécurisation des systèmes et réseaux

OIDANEOS

Présentation de la séquence
Objectifs et notions abordées

XXX

- Le contrôle d’accès
- Les protocoles d’authentification

Le contrôle d'accès

Le contrôle d’accès

Principe et définition du contrôle d’accès

Détermine qui est autorisé à accéder à quoi et dans quelles conditions (données, applications, ressources)

- DAC : Contrôle d’accès discrétionnaire
- MAC : Contrôle d’accès obligatoire
- RBAC : Contrôle d’accès basé sur les rôles
- RSBAC : Contrôle d’accès basé sur les règles
- ABAC : Contrôle d’accès basé sur les attributs

Le contrôle d'accès
Modèle DAC

Le modèle DAC (Discretionary Access Control ou contrôle d'accès discrétionnaire) est l'un des modèles de gestion des accès permettant de limiter l'accès aux ressources en fonction de l'identité des utilisateurs

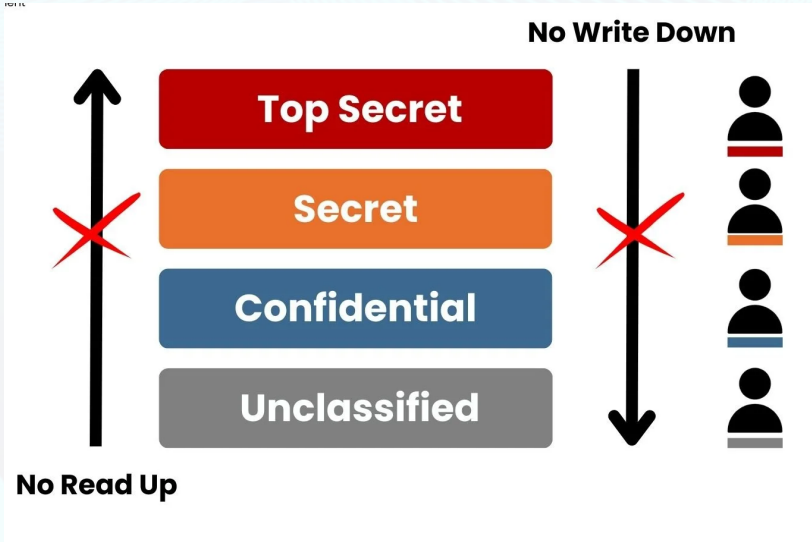
- **Définition et principe de base**
  - Le modèle DAC limite l'accès aux objets (données, ressources) en se basant sur l'**identité des sujets** (utilisateurs, applications) ou des groupes auxquels ils appartiennent.
  - Son nom "discrétionnaire" vient du fait que **chaque objet possède un propriétaire**.

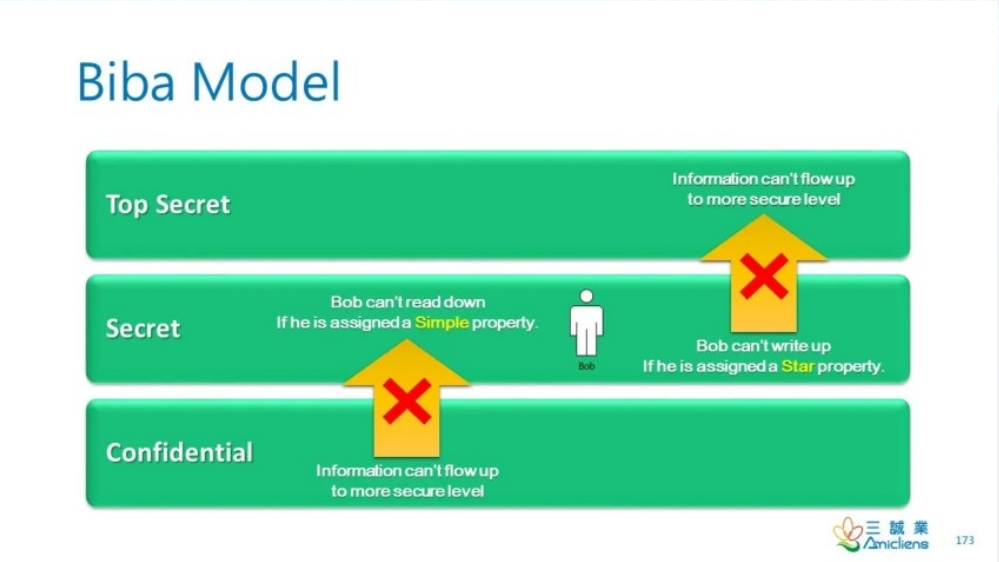
- **Mise en œuvre : matrice de Lampson (1971)**
  - Pour représenter ces droits, le modèle DAC utilise souvent une **matrice de contrôle d'accès**, concept introduit par Butler Lampson en 1971.
    - Le modèle fonctionne comme une machine à états définie par un triplet **(S, O, M)**, où **S** est l'ensemble des sujets, **O** l'ensemble des objets, et **M** la matrice.
    - Chaque cellule de la matrice contient les droits spécifiques (comme **Read**/Lecture, **Write**/Écriture, **Execute**/Exécution) qu'un sujet possède sur un objet donné.

	File 1	File 2	File 3	Program 1
Ann	own read write	read write		execute
Bob	read		read write	
Carl		read		execute read

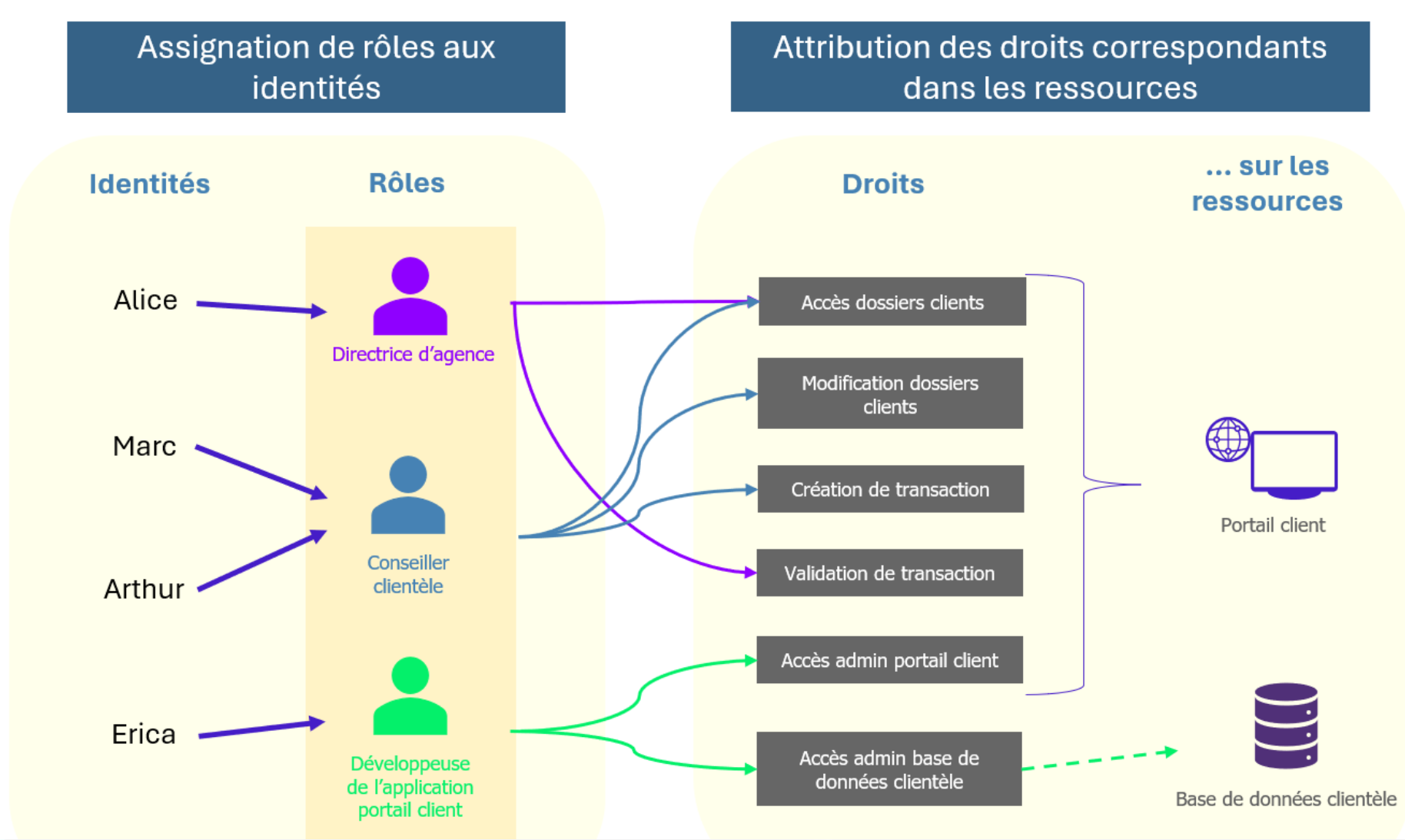
Le contrôle d'accès
Modèle MAC

Le modèle MAC (Mandatory Access Control ou contrôle d'accès obligatoire) est un système où les décisions de protection ne sont pas prises par le propriétaire de l'objet, mais sont imposées par le système lui-même.





Le contrôle d'accès
Modèle RBAC



Le contrôle d’accès
Modèle RSBAC

Le modèle RSBAC (RSBAC pour Rule-Set-Based Access Control) désigne le contrôle d'accès basé sur les règles.

- Dans ce système, c'est l'administrateur système qui définit explicitement les règles régissant l'accès aux objets et aux ressources.

- Contrairement aux modèles basés uniquement sur l'identité, les décisions d'accès reposent sur des conditions contextuelles spécifiques, telles que :
  - L'heure (ex: accès autorisé uniquement pendant les heures de bureau).
  - Le lieu géographique.
  - L'adresse IP de l'appelant.
  - Le numéro de port ou le protocole utilisé.

- Ce modèle est fréquemment combiné avec le modèle RBAC (basé sur les rôles) afin d'appliquer des politiques et des procédures d'accès plus précises et spécifiques. Par exemple, un utilisateur peut avoir le rôle "Comptable" (RBAC), mais ne peut accéder aux serveurs de comptabilité que s'il est physiquement dans les locaux de l'entreprise (RSBA).

Le contrôle d’accès
Modèle ABAC

Dans le modèle ABAC, l'accès n'est pas simplement basé sur l'identité ou un rôle, mais sur une combinaison d'attributs associés à différents éléments du système.

- Le système évalue des informations provenant de quatre catégories distinctes :
  - Attributs du sujet (l'utilisateur)
  - Attributs de l'objet (la ressource)
  - Attributs d'environnement
  - Attributs d'action

- Scénario d'accès autorisé : Amina demande l'accès à des données de vente depuis son bureau à Alger. Les attributs du sujet (Département Marketing), de l'objet (Données Algérie) et de l'environnement (Localisation Alger) correspondent à la politique → l'accès est accordé.

- Scénario d'accès refusé : Si Amina se déplace à Dakar pour un voyage d'affaires, son département et la ressource ne changent pas, mais l'attribut de localisation (Sénégal) ne correspond plus à la politique "depuis l'Algérie". L'accès lui est alors automatiquement refusé.

Les protocoles d’authentification

Les protocoles d'authentification

Les différents types de protocoles d'authentification

TACACS, XTACACS, TACACS+

RADIUS

Kerberos

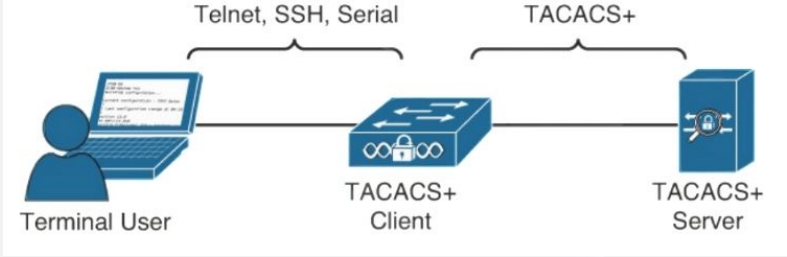
Les protocoles d’authentification
TACACS, XTACACS et TACACS+

La famille TACACS (Terminal Access Controller Access Control System) regroupe des protocoles d'authentification à distance conçus pour communiquer avec un serveur central afin de gérer l'accès au réseau.

- TACACS est le protocole d’authentification d’origine, créé en 1984. Son rôle principal est de déterminer si un utilisateur a le droit d’accéder à un réseau en communiquant avec un serveur d'authentification.

- XTACACS (Extended TACACS) est une extension du protocole d'origine. Il a été développé par Cisco en 1990 pour offrir des fonctionnalités plus étendues que la version initiale.

- TACACS+ est Développé par Cisco en 1993, le TACACS+ est la version la plus moderne et a remplacé les versions précédentes. C’est un protocole propriétaire de Cisco qui fonctionne principalement avec ses périphériques réseau.
    - *Contrairement à d'autres protocoles (comme RADIUS), le TACACS+ sépare distinctement les fonctions d'Authentification, d'Autorisation et de Traçabilité (Accounting).*
    - *Il utilise le protocole TCP (port 49) et chiffre l'intégralité des paquets échangés, ce qui le rend plus sûr que RADIUS (qui ne chiffre que le mot de passe).*
    - *Il permet aux administrateurs de contrôler précisément les commandes qu'un utilisateur peut exécuter sur un équipement réseau et d'en garder une trace complète pour les audits ou le dépannage.*
    - *Il prend en charge plusieurs niveaux de privilège et supporte plusieurs protocoles en dehors de l'IP.*
    - *Il est essentiellement utilisé pour l'administration des périphériques réseau via des serveurs de contrôle d'accès.*

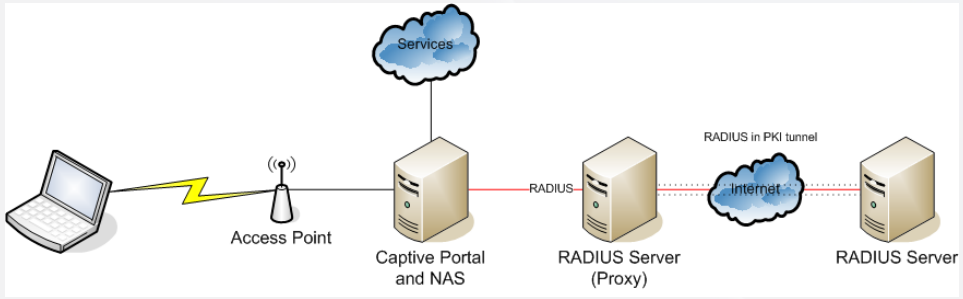


Les protocoles d'authentification
RADIUS

- Le protocole RADIUS (Remote Authentication Dial-In User Service) est un standard ouvert de communication utilisé pour gérer la sécurité des accès réseau. Créé en 1991 et adopté comme norme par l'IETF (RFC 2865), il est conçu pour centraliser la gestion des utilisateurs se connectant à distance.

- RADIUS est un protocole qui assure les fonctions AAA : Authentification, Autorisation et Traçabilité (Accounting). Il s'appuie sur une base de données centrale contenant les profils des utilisateurs.

- Son architecture repose sur un modèle client-serveur spécifique :
  - Le Client RADIUS : Contrairement aux modèles classiques, le client n'est pas l'utilisateur final, mais le NAS (Network Access Server). Il peut s'agir d'un point d'accès Wi-Fi, d'un serveur VPN, d'un commutateur (switch) géré ou d'un pool de modems.
  - Le Serveur RADIUS : C'est le serveur d'authentification central qui reçoit les requêtes du NAS et décide d'accorder ou non l'accès.



Les protocoles d'authentification
RADIUS

- Le protocole utilise UDP comme protocole de transport, ce qui le distingue de TACACS+ (qui utilise TCP).
  - *Les ports 1812 ou 1645 sont dédiés à l'authentification et l'autorisation, tandis que les ports 1813 ou 1646 gèrent la traçabilité.*
  - *Lorsqu'un utilisateur tente de se connecter, le NAS envoie une requête d'accès (Access Request) au serveur. Le serveur peut répondre de trois manières : Access Accept (accès autorisé), Access Reject (accès refusé) ou Access Challenge (demande d'informations complémentaires).*

- Le protocole supporte principalement deux approches pour vérifier l'identité :
  - *PAP (Password Authentication Protocol) : Le client transmet l'identifiant et le mot de passe au serveur pour vérification.*
  - *CHAP (Challenge Handshake Authentication Protocol) : Plus sécurisée, cette méthode utilise un défi (challenge) et un secret partagé chiffré. Elle permet également des ré-authentifications répétées durant la session.*

- Ce protocole présente quelques limites
  - *RADIUS ne chiffre que les mots de passe dans les paquets envoyés ; les autres informations (identifiants, attributs) circulent en clair.*
  - *Il regroupe l'authentification et l'autorisation. Il est donc impossible d'exécuter ces deux fonctions séparément, bien que la traçabilité puisse être gérée à part.*
  - *RADIUS ne prend en charge qu'un seul niveau de privilège.*
  - *En tant que standard ouvert, il est compatible avec la quasi-totalité des équipements réseau modernes, ce qui en fait la solution privilégiée pour les environnements hétérogènes (mélange de différentes marques de matériel).*
  - *Il utilise uniquement le protocole IP.*

Les protocoles d’authentification
Kerberos

Le protocole Kerberos est un mécanisme d'authentification conçu pour sécuriser les échanges entre des hôtes de confiance à travers un réseau non sûr. Créé au MIT en 1988 et standardisé par l'IETF en 2005 (RFC 4120), il repose principalement sur la cryptographie symétrique.

- Le fonctionnement de Kerberos s'articule autour de trois éléments clés :
  - Le Royaume (Realm) : C'est un domaine administratif définissant les limites de contrôle du serveur d'authentification. Il regroupe les utilisateurs, les hôtes et les services réseau enregistrés.
  - Le Centre de Distribution de Clés (KDC) : Il s'agit du serveur central composé de :
    - Une base de données contenant toutes les clés secrètes du domaine.
    - Serveur d'Authentification (AS) qui authentifie l'utilisateur et génère un ticket spécifique appelé TGT (*Ticket Granting Ticket*).
    - Serveur d'Attribution de Tickets (TGS) qui distribue les tickets de session nécessaires pour accéder aux services demandés.

- Pour accéder à un service (comme une imprimante), le processus suit plusieurs étapes :
  - 1. Demande initiale : Le client s'identifie auprès de l’AS.
  - 2. Réception du TGT : L'AS renvoie une clé de session et un TGT chiffré avec la clé secrète du TGS.
  - 3. Requête de service : Le client envoie ce TGT au TGS pour demander l'accès à un service spécifique.
  - 4. Obtention du ticket de session : Le TGS vérifie les droits et renvoie un ticket de session chiffré avec la clé du serveur d'application.
  - 5. Accès au service : Le client présente enfin ce ticket au serveur d'application pour obtenir l'accès

Les protocoles d'authentification
Kerberos

- Avantages et sécurité :
  - Kerberos permet au client et au serveur de vérifier mutuellement leur identité.
  - L'utilisation de l'horodatage (timestamps) avec une durée de validité limitée (souvent 600 minutes par défaut) permet d'atténuer les attaques par rejeu.

- Bien que performant, Kerberos présente certains inconvénients :
  - Le KDC est une cible critique. Si le KDC est compromis, toutes les clés du domaine le sont également. Si le serveur tombe en panne, plus personne ne peut s'authentifier.
  - Contrairement à RADIUS ou TACACS+, Kerberos ne gère nativement que l'authentification. Il ne permet pas de gérer l'autorisation ou la traçabilité.
  - Pour obtenir une solution complète (authentification et autorisation), il est fréquent de coupler Kerberos avec un protocole d'annuaire comme LDAP ou Active Directory.

Le durcissement des systèmes et réseaux

Le durcissement des systèmes et des réseaux
Principe

« Le principe du Hardening (ou durcissement système) est de manière générale de venir mettre en application des mesures de sécurité avancées sur les différentes couches qui composent un système »

Il s'agit donc de venir étudier la surface d'attaque de chacun de nos systèmes pour en définir les mesures de sécurité à mettre en application en cohérence avec le besoin de sécurité locale et les différentes politiques de sécurité applicables.

La mise en place de ce type de principe est que « tout ce qui n'est pas utile au bon fonctionnement du service délivré par la machine est inutile et doit donc être désactivé ou désinstallé » - ANSSI

Le durcissement des systèmes et des réseaux
Principe

Le fait de se débarrasser de tout ce qui n'est pas strictement nécessaire au bon fonctionnement de notre machine permettra d'éviter la présence de brèches potentielles.

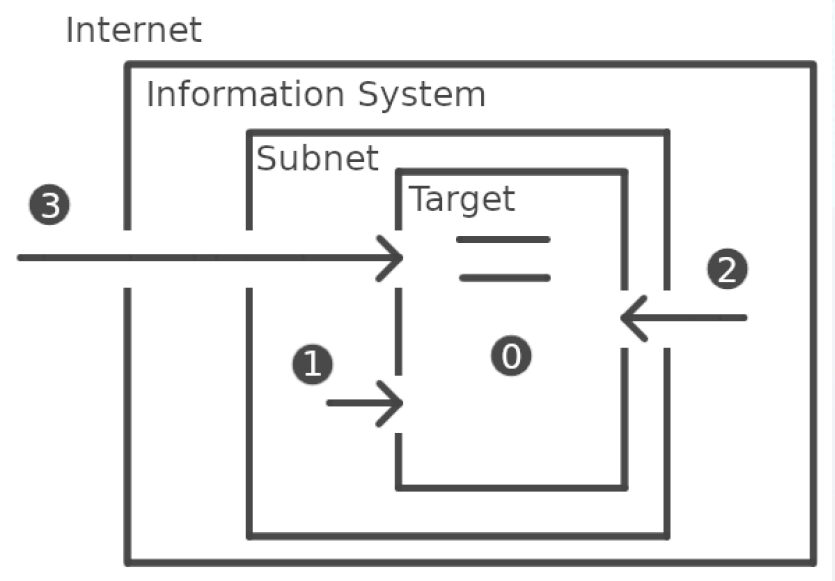
En effet, un outil inutilisé pour la production sur une machine est potentiellement unvecteur d'élévation de privilège ou de pivoting pour un attaquant.

On conservera alors les services, les outils et les accès strictement nécessaires et on désactivera tous les autres.

Une fois la machine assainie, il sera tout de même nécessaire d'ajouter l'ensemble des outils nécessaires à la sécurisation de la machine.

Le durcissement des systèmes et des réseaux
La notion de surface d'attaque

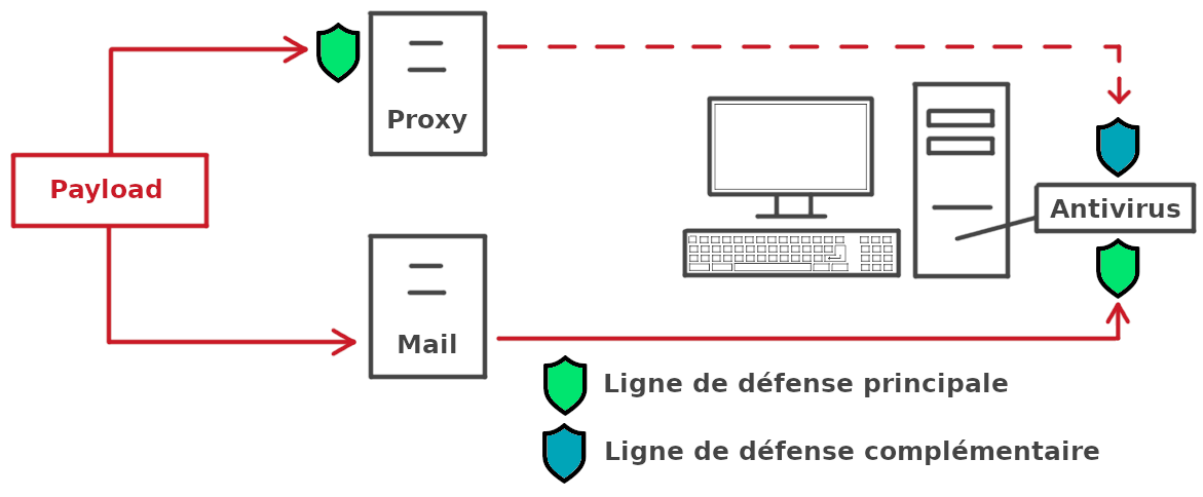
- *La surface d'attaque est définie comme étant le périmètre d'exploitation de la machine.*
- *Ce périmètre va de l'exposition maximale possible pour un système (internet) jusqu'à la surface d'exploitabilité du système en lui-même (noyau, …)*
- *L'objectif va être à la fois de réduire les points d'entrées et l'écart entre ces couches.*



Le durcissement des systèmes et des réseaux
La notion de surface d'attaque

- *Le durcissement pose les bases du concept de « défense en profondeur ». L'idée générale est de construire plusieurs barrières indépendantes que l'on qualifiera dans une logique de ligne de défense.*

- *Note : Les moyens de protections classiques (firewall, …) seront plus considérés comme étant des filtres que de réelles barrières de sécurité donc ne seront pas pris en considération pour la ligne de défense*



Le durcissement des systèmes et des réseaux
La notion de surface d'attaque

Le concept de ligne de défense reste une notion très arbitraire et va dépendre des différents éléments de travail de la chaîne de sécurité locale

- *Politique de sécurité du système d'information (PSSI)*
- *Politique normative*
- *Analyse de risque*

Le nombre de ligne de défense ainsi que le niveau de mise en application de celles-ci reste donc pleinement dépendant du niveau de la menace établie et s'inscrit donc dans une vision large d'analyse de risque.

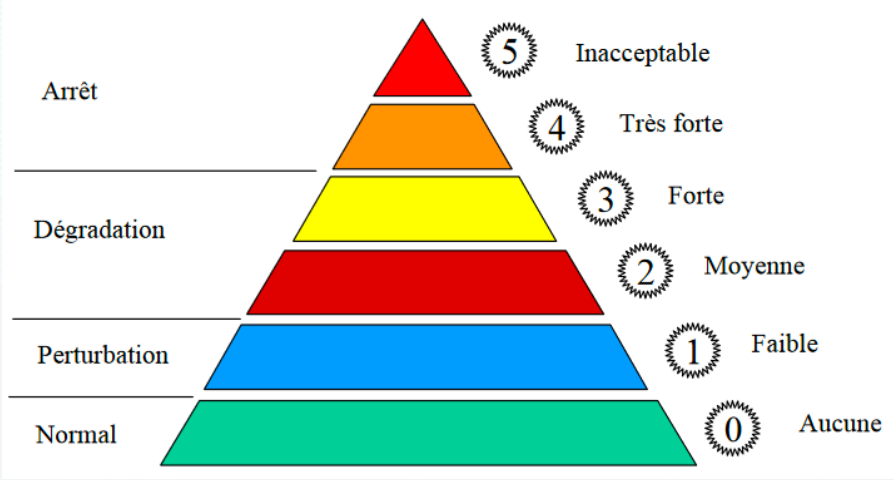
Une ligne est composée de une ou plusieurs barrières se basant sur l'échelle de gravité de chaque menace.

Le durcissement des systèmes et des réseaux
La notion de surface d'attaque

La démarche de définition se fera à la fois de manière déductive (par les ressources) et de manière inductive (par les menaces).

L'ANSSI recommande la mise en place d'au minimum 3 lignes de défense pour tout asset pouvant entrer dans une dynamique de dégradation (cf. échelle de gravité SSI).

C'est cette partie de l'élaboration de notre politique de défense qui sera définie lors de la mise en oeuvre de l'analyse de risque globale du système d'information



Le durcissement des systèmes et des réseaux
La notion de surface d'attaque

Le durcissement des machines s'inscrit donc dans une suite de principes de sécurité à mettre en oeuvre (ANSSI).

- *Minimisation : Seuls les composants nécessaires du service rendu par le système doivent être installés.*
- *Contrôle d'accès / Moindre privilège : Les services et exécutables disponibles doivent faire l'objet d'une analyse afin de connaître les privilèges qui leurs sont associés et doivent ensuite être configurés et intégrés en vue d'en utiliser le strict nécessaire.*
- *Défense en profondeur : Conception de plusieurs couches de sécurité indépendantes et complémentaires pour retarder la compromission d'un système.*

Le durcissement des systèmes et des réseaux
Les éléments à disposition

Baseline éditeur

CIS Benchmark

Outils automatisés

Le durcissement des systèmes et des réseaux
Les outils d'automatisation

scipag/
HardeningKitty

)SCIP(

HardeningKitty - Checks and hardens your Windows configuration

3 Contributors | 9 Issues | 2k Stars | 208 Forks

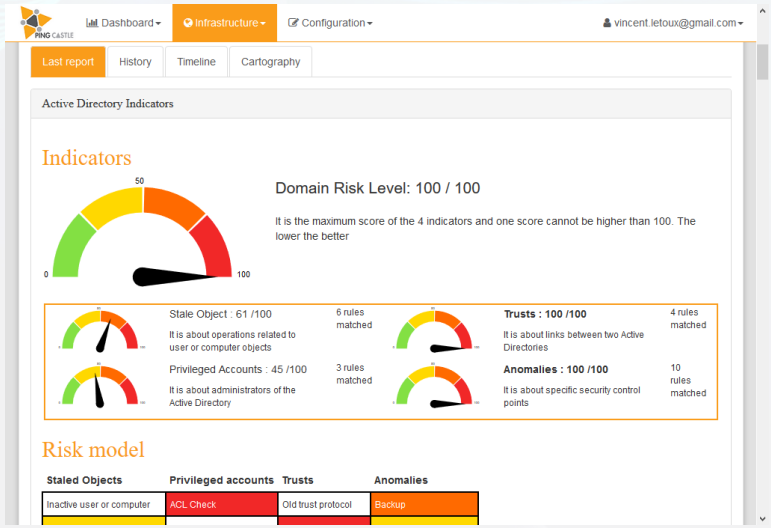
```
Lynis security scan details:

Hardening index : 66 [#############       ]
Tests performed : 268
Plugins enabled : 18

Components:
- Firewall               [V]
- Malware scanner        [X]

Lynis Modules:
- Compliance Status      [?]
- Security Audit         [V]
- Vulnerability Scan     [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat
```



Les mesures d'hygiène de l'ANSSI

Les mesures d'hygiène de l'ANSSI
La bonne connaissance de son SI

- Identification des informations et serveurs les plus sensibles et maintien d'un schéma du réseau
- Inventaire exhaustif et à jour des comptes privilégiés
- Organisation des procédures d'arrivée, de départ et de changement de fonction des utilisateurs
- Autorisation de la connexion au réseau de l'entité aux seuls équipements maîtrisés

Les mesures d'hygiène de l'ANSSI
La bonne connaissance de son SI

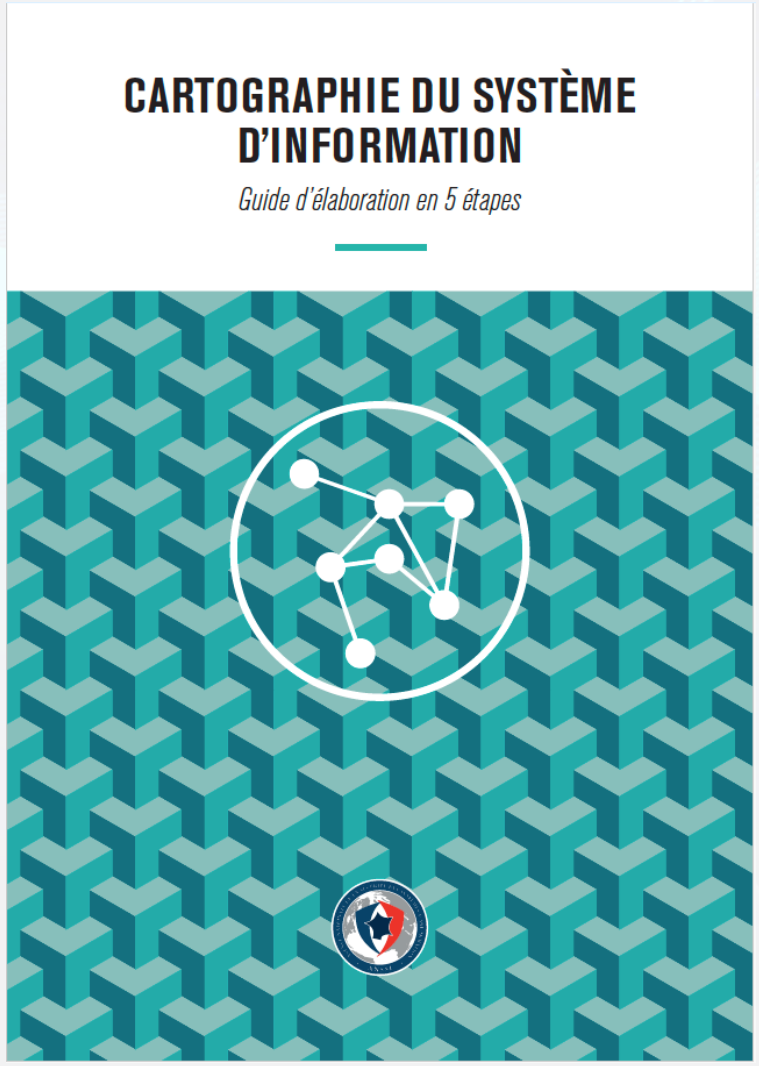


TABLE DES MATIÈRES

Les mesures d'hygiène de l'ANSSI
L'authentification et le contrôle d'accès

- Identification nominative de chaque personne accédant au système et distinction des rôles utilisateur/administrateur
- Attribution des bons droits sur les ressources sensibles du système d'information
- Définition et vérification des règles de choix et de dimensionnement des mots de passe
- Protection des mots de passe stockés sur les systèmes
- Changement des éléments d'authentification par défaut sur les équipements et services
- Mise en place de l'authentification forte

Les mesures d'hygiène de l'ANSSI
L'authentification et le contrôle d'accès

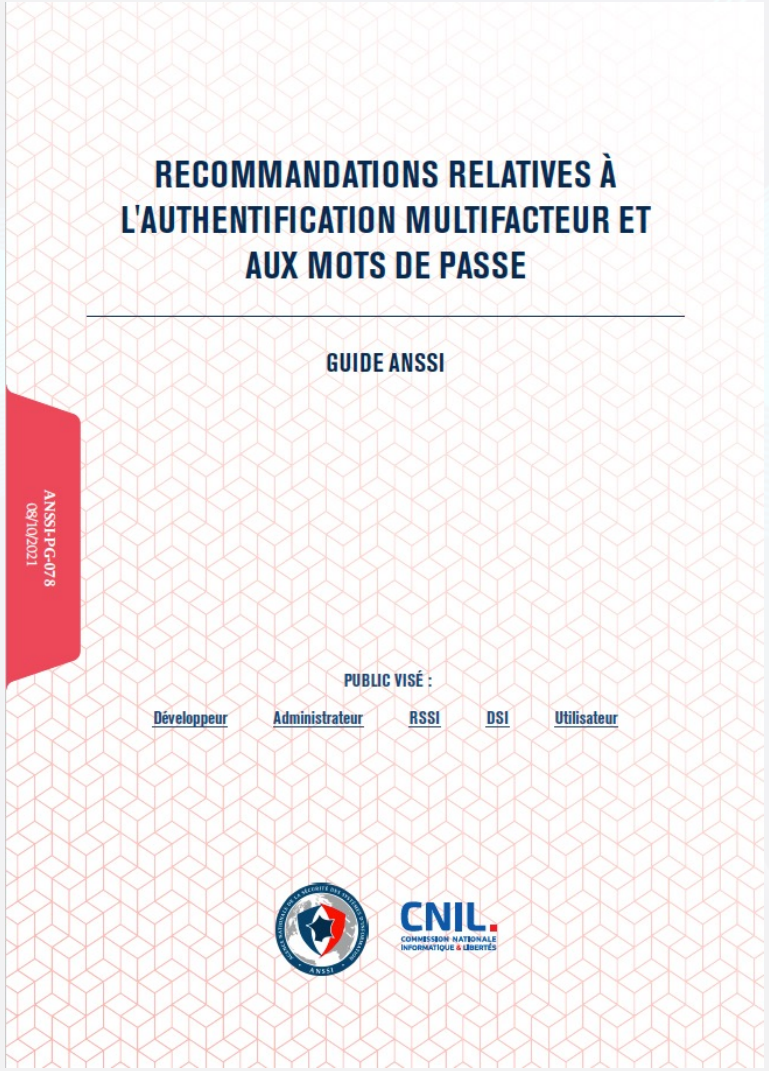


Table des matières

Les mesures d'hygiène de l'ANSSI
La sécurisation des postes de travail et réseaux

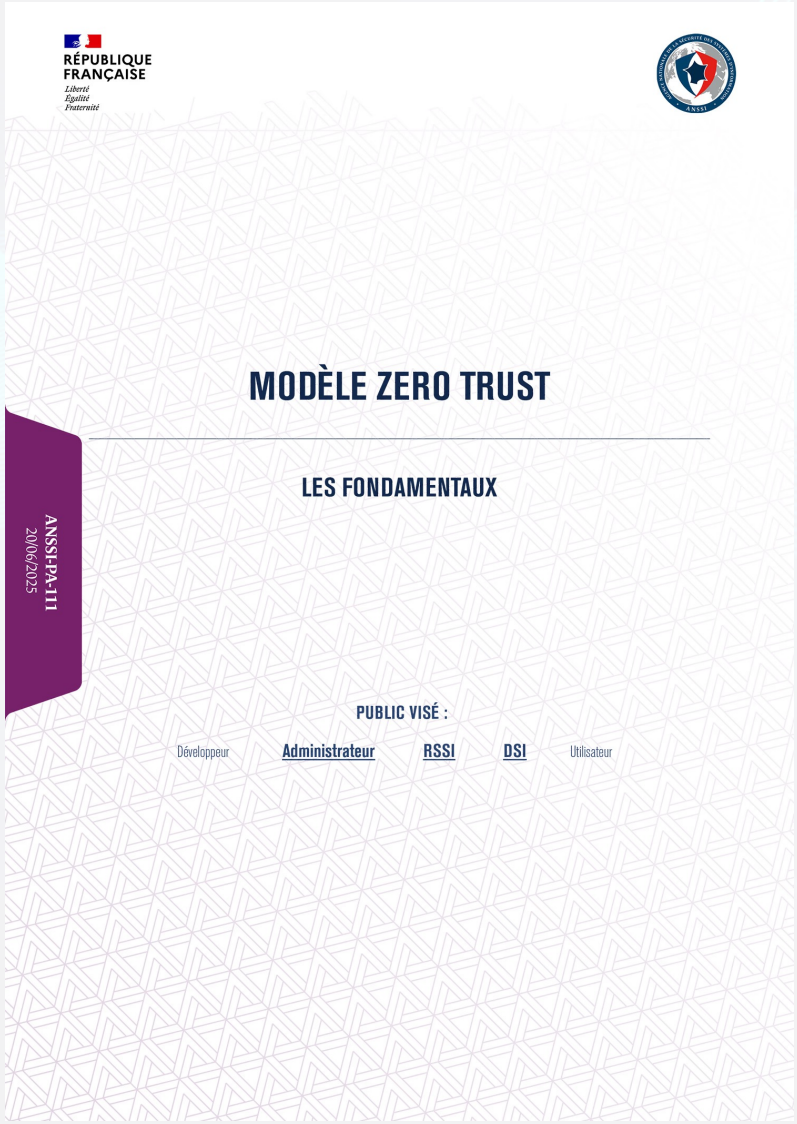
- La sécurisation des postes de travail
  - Mise en place d'un niveau de sécurité minimal sur l'ensemble du parc informatique
  - Protection contre les menaces relatives à l'utilisation de supports amovibles
  - Utilisation d'un outil de gestion centralisée pour homogénéiser les politiques de sécurité
  - Activation et configuration du pare-feu local des postes de travail
  - Chiffrement des données sensibles transmises par Internet

Les mesures d'hygiène de l'ANSSI
La sécurisation des postes de travail et réseaux

- La sécurisation du réseau
  - La segmentation du réseau et la mise en place d'un cloisonnement entre ces zones
  - La sécurité des réseaux d'accès Wi-Fi et la séparation des usages
  - L'utilisation des protocoles réseaux sécurisés dès qu'ils existent
  - La mise en place d'une passerelle d'accès sécurisé à Internet
  - Le cloisonnement des services visibles depuis Internet du reste du SI
  - La protection de la messagerie professionnelle
  - La sécurisation des interconnexions réseau dédiées avec les partenaires
  - Le contrôle et la protection de l'accès aux salles serveurs et aux locaux techniques

Les mesures d'hygiène de l'ANSSI

La sécurisation des postes de travail et réseaux



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI-PA-111
20/06/2025

MODÈLE ZERO TRUST

LES FONDAMENTAUX

PUBLIC VISÉ :

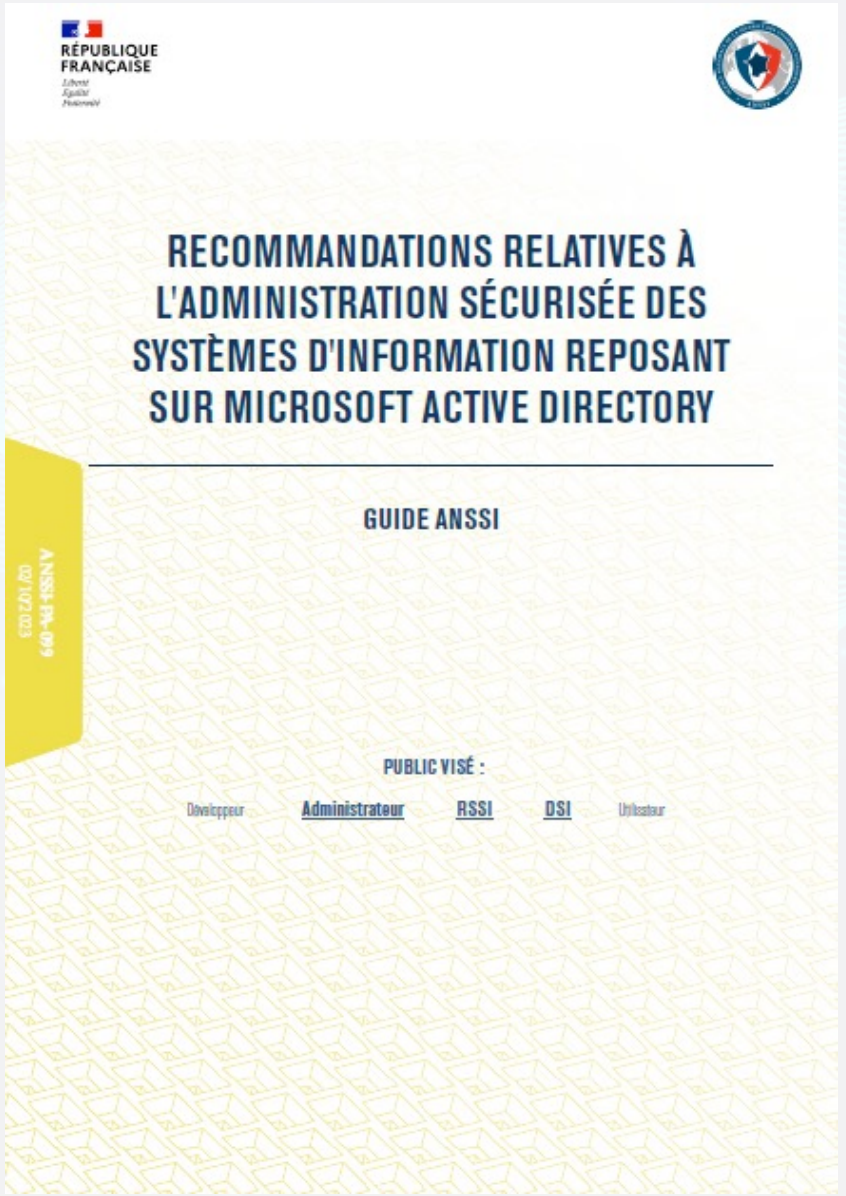
Développeur **Administrateur** **RSSI** **DSI** Utilisateur

Table des matières

Les mesures d'hygiène de l'ANSSI
La sécurisation de l'administration

- La sécurisation de l'administration
  - Interdiction de l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information
  - Utilisation d'un réseau dédié et cloisonné pour l'administration du système d'information
  - Limitation au strict besoin opérationnel des droits d'administration sur les postes de travail

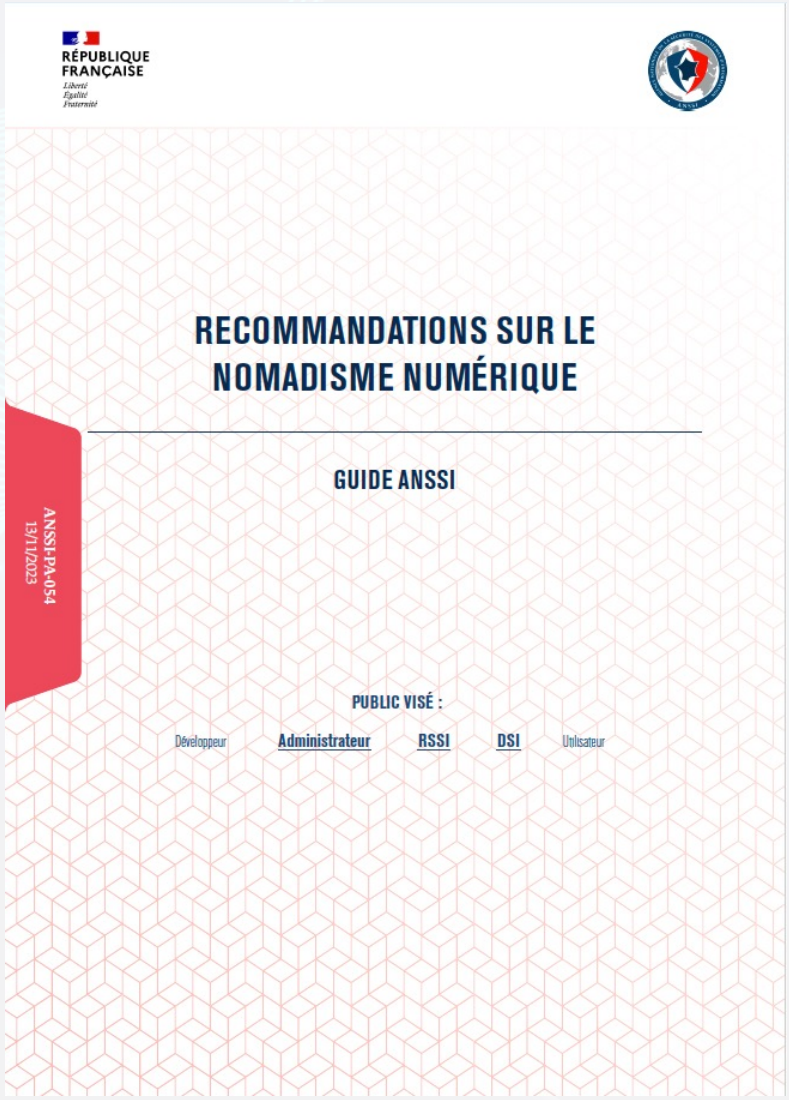
Les mesures d'hygiène de l'ANSSI
La sécurisation de l'administration



Les mesures d'hygiène de l'ANSSI
La gestion du nomadisme

- Déploiement de mesures de sécurisation physique des terminaux nomades
- Chiffrement des données sensibles en particulier sur le matériel potentiellement perdable
- Sécurisation de la connexion réseau des postes utilisés en situation de nomadisme
- Adoption de politiques de sécurité dédiées aux terminaux mobiles

Les mesures d'hygiène de l'ANSSI
La gestion du nomadisme



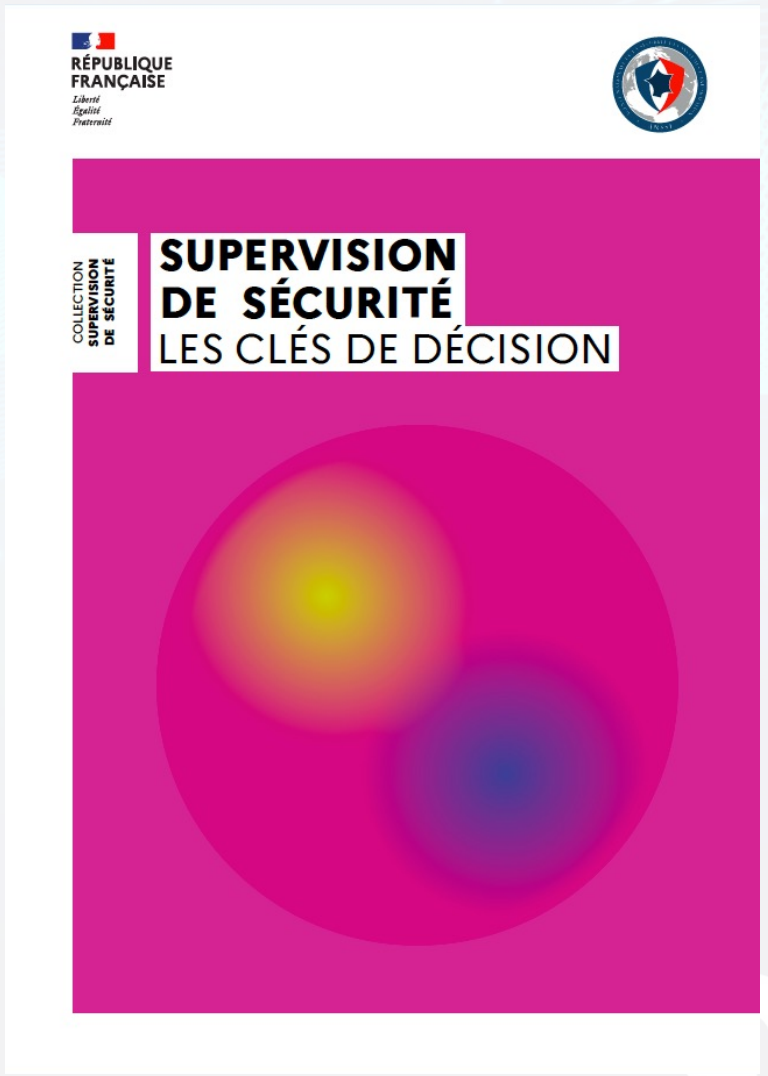
Les mesures d'hygiène de l'ANSSI
Le maintien à jour du SI

- Définition d'une politique de mise à jour des composants du système d'information
- Anticipation de la fin de la maintenance des logiciels et systèmes et limitation des adhérences logicielles

Les mesures d'hygiène de l'ANSSI
La supervision, l'audit et la réaction à incident

- Activation et configuration des journaux des composants les plus importants
- Définition et application d'une politique de sauvegarde des composants critiques
- Réalisation de contrôles et d'audits de sécurité réguliers et application des actions correctives associées
- Désignation d'un référent en sécurité des systèmes d'information
- Définition d'une procédure de gestion des incidents de sécurité

Les mesures d'hygiène de l'ANSSI
La sécurisation de l'administration



Les mesures d'hygiène de l'ANSSI
Visas ANSSI

CSPN **CC**

PASSI **PRIS** **PDIS** **PACS**