

Analyse du niveau de sécurité des infrastructures

11.1. Introduction à l'analyse de sécurité

L'administrateur AIS joue un rôle essentiel dans l'**évaluation continue de la sécurité des infrastructures**, qu'elles soient physiques, virtuelles ou cloud. L'objectif est d'**identifier les vulnérabilités**, d'**évaluer les risques**, et de **proposer des mesures correctives** en lien avec la **PSSI** (Politique de Sécurité des Systèmes d'Information) de l'organisation.

Objectifs :

- Évaluer les risques techniques et organisationnels
 - Mettre en conformité avec les référentiels (RGPD, ANSSI, ISO 27001...)
 - Prévenir les incidents et intrusions
 - Renforcer la résilience globale du système d'information
-

11.2. Les grands principes de sécurité informatique

Principe	Définition
Confidentialité	Empêcher l'accès non autorisé à l'information
Intégrité	Garantir que les données ne sont pas altérées
Disponibilité	Assurer l'accès aux données et services
Traçabilité	Conserver les preuves des accès et actions
Preuve	S'assurer de l'authenticité et de la non-répudiation

11.3. Cadres de référence et exigences réglementaires

Référentiels français et européens :

- **RGPD** (données personnelles)
- **Référentiel ANSSI** (guides techniques, Hygiène informatique, PDIS, SecNumCloud...)
- **ISO/IEC 27001** (SMSI)
- **RGS v2** (Référentiel Général de Sécurité)
- **Politique de sécurité locale (PSSI)**

Obligations pour l'entreprise :

- Journalisation et conservation des logs
- Gestion des habilitations
- Protection des données sensibles (santé, finance, RH...)

- Déclaration des violations à la CNIL (sous 72h)
-

11.4. Identification des actifs et des risques

Méthodologie :

1. **Cartographie des actifs** (matériel, logiciel, données, flux)
2. **Évaluation des menaces** (malveillance, erreur, défaillance)
3. **Analyse de vulnérabilités** (tests, scan, audit)
4. **Calcul du risque** = Gravité x Probabilité
5. **Plan d'action de sécurité**

Outils :

- GLPI + CMDB
 - OCS Inventory
 - Asset management dans Azure, AWS
-

11.5. Scans de vulnérabilités et tests de sécurité

Outils de scan :

- **OpenVAS / Greenbone**
- **Nessus**
- **Qualys**
- **Nmap + scripts NSE**
- **Lynis** (Linux)
- **Nikto** (Web)

Bonnes pratiques :

- Cadrer les scans (hors prod sans validation !)
 - Tenir compte des fausses alertes
 - Documenter les résultats
 - Prioriser les corrections
 - Intégrer au cycle DevSecOps (CI/CD + scan automatique)
-

11.6. Analyse des configurations et de la surface d'exposition

L'administrateur vérifie :

- Les ports ouverts inutiles
- Les services en écoute non utilisés
- La version des logiciels (supportée, à jour ?)
- Les règles de pare-feu (sortantes et entrantes)
- Les droits d'accès excessifs
- L'exposition à Internet (Shodan, censys...)

Outils :

- **Audit CIS Benchmarks** (par OS)
 - **Audit scripts PowerShell / Bash**
 - **Audit de GPO / ACL / NTFS**
-

11.7. Journalisation, logs et alertes

Éléments à surveiller :

- Connexions anormales
- Tentatives d'accès interdit
- Changements de permissions
- Accès hors plages horaires
- Utilisation excessive de ressources

Outils :

- Wazuh, OSSEC, ELK Stack
 - Sysmon (Windows), auditd (Linux)
 - SIEM (Security Information and Event Management)
-

11.8. Analyse des accès et gestion des droits

Audits périodiques :

- Liste des comptes inactifs ou orphelins
- Utilisateurs administrateurs non justifiés
- Mots de passe trop simples ou inchangés
- Partages réseau trop ouverts
- Groupes AD mal structurés

Mesures à prendre :

- Mise en œuvre de MFA
 - Principe du moindre privilège (PoLP)
 - Revue semestrielle des habilitations
 - Activation de l'audit d'authentification
-

11.9. Recommandations ANSSI et plan d'action**Bonnes pratiques ANSSI :**

- Appliquer les 42 règles du guide d'hygiène informatique
- Utiliser des OS à jour et supportés
- Séparer les comptes d'administration
- Chiffrer les flux sensibles (VPN, TLS, IPsec)
- Documenter toute modification
- Former les utilisateurs (cybersécurité, phishing...)

Plan d'action :

- Actions préventives (durcissement, patch management)
 - Actions correctives (réduction de surface, segmentation)
 - Plan de reprise après attaque
 - Indicateurs de suivi sécurité (KPI)
-

11.10. Activités pratiques et évaluation**Études de cas :**

- Audit d'un serveur exposé à Internet
- Analyse d'une configuration Active Directory
- Scan de vulnérabilités + rapport avec priorisation
- Correction d'une faille critique avec justification

Évaluations :

- QCM sur les référentiels (ANSSI, RGPD, ISO)
- Projet : diagnostic + proposition d'amélioration
- Oral : restitution d'un audit et plan d'action