FICHE DE RÉVISION

Module : Fondamentaux de la Sécurité des SI et des Réseaux

Formation : Pilotage et Animation de la Cybersécurité

🖥️ 1. Introduction à la Sécurité des SI

Objectif : Identifier les grandes familles de SI et leurs vulnérabilités

▸ Les grandes familles de Systèmes d'Information

Famille de SI	Description	Exemples
SI de Gestion	Traitement des données métier et administratives	ERP, CRM, SIRH
SI Industriel (SCI/SCADA)	Contrôle des processus industriels et infrastructures critiques	Automates PLC, DCS, SCADA
SI de Communication	Messagerie, téléphonie, collaboration	Serveurs mail, VoIP, Teams
SI Cloud	Infrastructure hébergée externalisée	AWS, Azure, Google Cloud
SI embarqué / IoT	Objets connectés et systèmes temps réel	Capteurs, caméras, montres

▸ Vulnérabilités courantes par famille

- SI de Gestion : droits d'accès trop larges, mots de passe faibles, interfaces web mal protégées
- SI Industriel : protocoles anciens (Modbus, DNP3) sans chiffrement, isolation réseau insuffisante
- SI de Communication : interception des échanges, phishing, spoofing
- Cloud : mauvaise configuration des buckets, APIs exposées, gestion des identités défaillante
- IoT : firmware non mis à jour, identifiants par défaut, absence d'authentification

▸ Les 3 piliers fondamentaux de la sécurité (Triptyque CIA)

🔒 Confidentialité	✅ Intégrité	🟢 Disponibilité
Seules les personnes autorisées accèdent aux données	Les données ne sont pas altérées de manière non autorisée	Les ressources sont accessibles quand nécessaire

⚠️ 2. Les Principales Menaces et Failles

Objectif : Comprendre les typologies d'attaques et les vulnérabilités courantes

▸ Typologies d'attaques

Catégorie	Exemples d'attaques	Impact principal
Ingénierie sociale	Phishing, spear phishing, vishing, pretexting	Vol de credentials, accès frauduleux
Malware	Virus, ransomware, spyware, rootkit, cheval de Troie	Perte de données, chiffrement, espionnage

Attaques réseau	DoS/DDoS, Man-in-the-Middle, ARP spoofing, sniffing	Interruption de service, interception
Exploitation applicative	Injection SQL, XSS, CSRF, buffer overflow	Exfiltration données, prise de contrôle
Attaques sur identités	Brute force, credential stuffing, pass-the-hash	Compromission de comptes privilégiés
Supply chain	Compromission de fournisseurs, librairies malveillantes	Propagation à l'ensemble du SI

▸ Référentiel des vulnérabilités : TOP 10 OWASP (extrait)

- A01 – Broken Access Control : mauvaise gestion des autorisations
- A02 – Cryptographic Failures : chiffrement faible ou absent
- A03 – Injection : SQL, LDAP, OS command injection
- A04 – Insecure Design : défauts de conception architecturale
- A07 – Identification & Authentication Failures : auth faible, sessions non expirées

▸ Notion de CVE et scoring CVSS

CVE (Common Vulnerabilities and Exposures) : identifiant unique pour chaque vulnérabilité publiée.
CVSS (Common Vulnerability Scoring System) : score de 0 à 10 évaluant la criticité.

Score CVSS	Criticité	Action recommandée
0.0 – 3.9	Faible	Surveillance et patch planifié
4.0 – 6.9	Modérée	Patch dans les 30 jours
7.0 – 8.9	Haute	Patch en urgence (< 7 jours)
9.0 – 10.0	Critique	Isolation et patch immédiat

🔧 3. Architecture et équipements de sécurité

Objectif : Découvrir le rôle et les interactions des firewalls, antivirus, IDS/IPS, VPN, etc.

▸ Les équipements clés et leurs rôles

Équipement	Rôle principal	Points clés
Firewall (pare-feu)	Filtrer le trafic entrant/sortant selon des règles	Stateful, Next-Gen (NGFW), règles ACL
Antivirus / EDR	Détecter et bloquer les malwares sur les postes	Signatures + analyse comportementale (EDR)
IDS / IPS	Détecter (IDS) ou bloquer (IPS) les intrusions	Analyse de signatures et anomalies réseau
VPN	Créer un tunnel chiffré sur réseau public	IPSec, SSL/TLS, accès distant sécurisé
SIEM	Centraliser et corréler les logs de sécurité	Détection d'incidents, tableaux de bord SOC
WAF	Protéger les applications web des attaques OWASP	Proxy inverse, filtrage HTTP/HTTPS

Bastion / PAM	Sécuriser l'accès aux comptes privilégiés	Journalisation, rebond SSH/RDP, rotation mdp
Proxy / Reverse proxy	Filtrer et contrôler les accès web	Filtrage URL, cache, TLS termination

▸ Architecture de défense en profondeur

- Zone Démilitarisée (DMZ) : zone tampon entre Internet et le réseau interne
- Segmentation réseau : cloisonnement des zones (LAN, DMZ, VLAN) par le firewall
- Principes : défense en profondeur (plusieurs couches), moindre privilège, zéro confiance (Zero Trust)

▸ Schéma conceptuel des zones réseau

4. Sécurisation des Systèmes et Réseaux

Objectif : Mettre en oeuvre des mesures de protection : droits, mise à jour, segmentation, chiffrement

▸ Gestion des droits et des accès

Principe	Mise en oeuvre
Moindre privilège	N'attribuer que les droits strictement nécessaires à chaque utilisateur
Séparation des tâches	Éviter qu'une seule personne contrôle tout un processus critique
MFA (Authentification multifacteur)	Combiner mot de passe + OTP / biométrie / clé physique (FIDO2)
Gestion des comptes privilégiés (PAM)	Bastion, rotation automatique des mots de passe admin
Revue périodique des droits	Audit trimestriel des comptes actifs et des droits attribués

▸ Gestion des mises à jour et des correctifs (Patch Management)

- Inventaire continu des actifs (logiciels, OS, firmwares)
- Veille CVE : surveiller les bulletins CERT-FR, éditeurs, NVD
- Processus de qualification : tester en préprod avant déploiement en prod
- Délais cibles : critique < 24-72h, haute < 7 jours, modérée < 30 jours
- Gestion des EOL (End of Life) : planifier la migration des systèmes obsolètes

▸ Segmentation et cloisonnement réseau

Technique	Objectif et mise en oeuvre
VLAN	Isoler logiquement les flux réseau (ex : VLAN users / serveurs / IoT)
Micro-segmentation	Contrôle des flux est-ouest, utilisé en environnements virtualisés/cloud
Firewall inter-zones	Filtrer tout trafic entre les segments, whitelist des flux autorisés

Zero Trust Network Access	Vérification systématique de l'identité et du contexte à chaque accès

▸ Chiffrement des données et des communications

- Données en transit : TLS 1.2/1.3 (HTTPS, SMTPS, SFTP), VPN IPSec ou SSL
- Données au repos : chiffrement de disque (BitLocker, LUKS), chiffrement de BDD (TDE)
- Gestion des clés : HSM (Hardware Security Module), rotation régulière des clés
- Algorithmes recommandés (ANSSI) : AES-256, RSA-4096, EC-DSA, SHA-256 minimum

🔐 5. Sécurité des Échanges et des Données

Objectif : Appliquer les principes de confidentialité, intégrité, disponibilité et non-répudiation

▸ Les 4 propriétés fondamentales de la sécurité de l'information

Propriété	Signification	Mécanismes techniques associés
🔒 Confidentialité	Accès réservé aux personnes autorisées	Chiffrement (AES, TLS), contrôle d'accès, VPN
✅ Intégrité	Données non altérées sans autorisation	Hachage (SHA-256), signature numérique, HMAC
🟢 Disponibilité	Accès garanti quand nécessaire	PRA/PCA, redondance, sauvegardes, DDoS protection
✍️ Non-répudiation	Impossibilité de nier avoir effectué une action	Signature électronique, journaux horodatés, PKI

▸ Cryptographie appliquée

Type	Principe	Usage
Chiffrement symétrique	Clé unique pour chiffrer et déchiffrer (AES)	Chiffrement de volumes, données au repos
Chiffrement asymétrique	Paire clé publique / clé privée (RSA, ECC)	Échange de clés, signature numérique, TLS
Hachage	Empreinte unique et irréversible (SHA-256)	Vérification d'intégrité, stockage de mots de passe
PKI / Certificats	Infrastructure de confiance (CA, certificat X.509)	HTTPS, signature de code, email sécurisé (S/MIME)

▸ Sécurisation des échanges de messagerie

- SPF (Sender Policy Framework) : valider les serveurs autorisés à envoyer des emails pour un domaine
- DKIM (DomainKeys Identified Mail) : signer cryptographiquement les emails sortants
- DMARC : politique de traitement des emails échouant les vérifications SPF/DKIM
- Chiffrement de bout en bout : S/MIME ou PGP pour le contenu des emails

▸ Protection des données personnelles (RGPD)

- Minimisation des données : ne collecter que le strict nécessaire
- Pseudonymisation / anonymisation : réduire les risques en cas de fuite
- Notification de violation : 72h pour informer la CNIL, sans délai pour les personnes concernées si risque élevé
- DPO (Délégué à la Protection des Données) : interlocuteur désigné pour la conformité

📡 6. Veille Technologique et Réglementaire

Objectif : Identifier les sources fiables : ANSSI, CNIL, CERT-FR

▸ Sources de référence en cybersécurité

Organisme	Rôle	Ressources clés
ANSSI	Agence nationale de la sécurité des SI – certification et régulation	Guides de bonnes pratiques, SecNumCloud, visas, référentiels (RGS, PGSSI-S)
CERT-FR	Centre gouvernemental de veille, alerte et réponse aux cyberattaques	Bulletins de sécurité, avis, alertes, indicateurs de compromission (IoC)
CNIL	Autorité de contrôle RGPD – protection des données personnelles	Recommandations sécurité, AIPD, notifications de violations
MITRE ATT&CK	Base de connaissances des TTPs des attaquants	Framework des tactiques et techniques d'attaque, cartographie menaces
ENISA	Agence européenne de cybersécurité	Rapports sur l'état des menaces, guidelines NIS2
CVE / NVD	Base de données des vulnérabilités publiques	Fiches CVE, scores CVSS, patches associés

▸ Principales réglementations et référentiels

Réglementation	Périmètre	Exigences principales
RGPD	UE – données personnelles	Consentement, droits des personnes, notification violations, DPO
Directive NIS2	UE – entités essentielles et importantes	Mesures de sécurité, signalement incidents, gouvernance cyber
LPM (Loi Programmation Militaire)	France – OIV	Obligation de détection, qualification ANSSI, signalement incidents
RGS (Référentiel Général de Sécurité)	France – SI de l'État	Homologation, authentification, signature, chiffrement
ISO 27001	International – SMSI	Système de management de la sécurité, certification, amélioration continue

▸ Mettre en place une veille efficace

- Abonnement aux flux CERT-FR et bulletins ANSSI (flux RSS, alertes email)
- Suivi des CVEs critiques via NVD et newsletters sécurité (The Hacker News, Bleeping Computer)

- Participation aux groupes de partage d'information : FSIRT, ISACs sectoriels
- Tableaux de bord de veille : agrégation via des outils comme MISP, OpenCTI
- Revues réglementaires périodiques : RGPD, NIS2, LPM, ISO 27001 – au moins 2 fois par an

📌 Mémo Récapitulatif — À Retenir

Concepts Fondamentaux	Outils et Organismes Clés
• Triptyque CIA : Confidentialité, Intégrité, Disponibilité • Non-répudiation = signature électronique + horodatage • Défense en profondeur : DMZ + segmentation + Zero Trust • Moindre privilège + MFA = socle IAM indispensable • CVSS 9-10 = patch immédiat, isolation si nécessaire • Chiffrement : AES-256 (repos), TLS 1.3 (transit)	• ANSSI : référentiels, guides, homologation • CERT-FR : alertes, bulletins, IoC • CNIL : RGPD, AIPD, notification en 72h • MITRE ATT&CK : cartographie des menaces • ISO 27001 : SMSI, amélioration continue • NIS2 + LPM : obligations OIV et entités essentielles