

# CH0 : Sensibilisation et initiation à la cybersécurité

## 1. Les enjeux de la sécurité des S.I

- SI : ensemble des ressources destinées à collecter, classer, gérer des infos au sein d'une organisation.

### D. I. C. P

- Le niveau de sécurité ( Si un bien est bien sécurisé ou non ) est défini par 3 critères :  
D. I. C
  - Disponibilité : accès au moment voulu.
  - Intégrité: exactitude et complétude des infos.
  - Confidentialité: être accessible qu'aux personnes autorisées.
- + 1 critère compl : Preuve; capacité à reconstituer un événement avec confiance. → Elle repose notamment sur la traçabilité des actions, l'authentification des utilisateurs et l'imputabilité des responsables des actions effectuées.

### Diff entre Sûreté et Sécurité :

Sûreté	<ul style="list-style-type: none"><li>- Protection contre les pannes et accidents involontaires (ex : panne disque, saturation).</li><li>- Mécanismes garantissant le bon fonctionnement et la continuité du système dans des conditions normales (disponibilité, fiabilité, maintenabilité...).</li><li>→ Risques quantifiables statistiquement.</li><li>→ Parades : sauvegarde, redondance, dimensionnement.</li></ul>
Sécurité	<ul style="list-style-type: none"><li>- Protection contre les actions malveillantes volontaires (ex : vol ou modification d'informations).</li><li>- Mécanismes protégeant contre les accès ou actions non autorisés (confidentialité, intégrité...).</li><li>→ Risques difficiles à quantifier, mais évaluables.</li><li>→ Parades : contrôle d'accès, filtrage, surveillance, configuration renforcée.</li></ul>

## 2. Vulnérabilité, menace, attaque

**Vulnérabilité** : Faiblesse au niv d'un bien.

**Menace** : Cause potentielle d'un incident.

**Attaque** : Action malveillante visant à porter atteinte à la sécurité d'un bien.--> Action malveillante visant à porter atteinte à la sécurité d'un bien.

⇒ Le travail des experts sécurité consiste à s'assurer que le S.I ne possède aucune vulnérabilité.

Cybercriminalité	Ensemble des actes illégaux utilisant les réseaux ou systèmes d'information pour commettre un délit/crime ou les visant directement.
------------------	--

Investigation numérique (forensics)	Procédures techniques permettant de rechercher, analyser et préserver des preuves numériques en respectant une méthodologie rigoureuse.
-------------------------------------	---

### Rôle de la CNIL

- La loi (1978) encadre la protection des données personnelles.
- Elle s'applique aux traitements automatisés et non automatisés de données personnelles (hors usage strictement personnel).

### Donnée personnelle :

Toute information concernant une personne physique identifiée ou identifiable, directement ou indirectement.

CyberSécurité	- Regroupe l'ensemble des probs (Notions de malveillance + Protection des données numériques)
CyberDefense	- Il ya une notion d'organisation : comment d'organiser contre un attaque ( RSSI : resp de sec des SI)

### Trois étapes face à une nouvelle attaque

1. C'est inutile
2. C'est dangereux
3. C'est évident

nap(network access point ) ? siem ? ids ? Firewall ?

# CH1 : Sécurité informatique

**La sécurité informatique** : Protéger les ordinateurs, les serveurs ...contre les attaques malveillantes.

## Objectifs de la sécurité (CAID)

- Confidentialité : pas de divulgation non autorisée des données.
- Authentification : preuve de l'identité de l'utilisateur.
- Disponibilité : données accessibles aux utilisateurs autorisés.
- Intégrité : pas de modification non autorisée des données.

## Autres objectifs

- Traçabilité : enregistrement des accès et tentatives d'accès.
- Non-répudiation : impossibilité de nier une action réalisée.

## Comment garantir les CAID ?

Confidentialité	S'assurer que les sauvegardes ne sont pas accessibles à tous (accès restreint).
Authentification	- Utiliser un mot de passe robuste. - Mettre en place un 2FA (carte à puce, biométrie, SMS...).
Intégrité	Ne pas modifier les sauvegardes inutilement.
Disponibilité	- Effectuer des sauvegardes régulières. - Conserver des anciennes sauvegardes (rotation maîtrisée).

## Règles de bon sens en sécurité

1. Ne pas contourner les dispositifs et politiques de sécurité de l'entreprise.
2. Respecter les règles internes (confidentialité des mots de passe, classification des documents...).
3. Appliquer les règles de gestion des documents (classement, conservation, destruction).
4. Signaler les comportements à risque (poste non verrouillé, mot de passe visible, visiteur non accompagné...).

## Choisir un mot de passe sécurisé

Au moins 10 caractères

Mélanger majuscules, minuscules, chiffres et caractères spéciaux

Éviter les mots du dictionnaire

Aucun lien avec vous ou le service utilisé

Ne pas réutiliser le même mot de passe

## Comment pirater un mot de passe ?

Brute force, Attaque par dictionnaire, Phishing (ingénierie sociale), Keylogger / virus, Espionnage, Vol de hash / rainbow table, Sniffing (Man in the Middle)

## Les normes de sécurité

<b>Les normes ISO 27000</b>	<p><b>ISO 27000</b> : famille de normes pour la gestion de la sécurité de l'information.</p> <p><b>ISO 27001</b> : définit les exigences pour mettre en place un SMSI (Système de Management de la Sécurité de l'Information) → norme certifiante. → Suit 4 phases : Établir – Implémenter – Maintenir – Améliorer (cycle PDCA).</p> <p><b>ISO 27002</b> : guide de bonnes pratiques (114 mesures de sécurité, 35 objectifs de contrôle).</p> <p><b>ISO 27005</b> : gestion des risques dans un SMSI, basée sur l'amélioration continue (PDCA). (seulement une démarche)</p>
<b>PCI DSS</b>	<p>- <b>Payment Card Industry Data Security Standard</b></p> <p>Standard de sécurité pour les acteurs manipulant des cartes de paiement. Objectif : protéger les données bancaires et réduire la fraude.</p> <p>→ 6 grands objectifs (sécuriser le système, protéger les données, gérer les vulnérabilités, contrôler les accès, surveiller/tester, maintenir une politique de sécurité).</p>
<b>RGPD (GDPR)</b>	<p>Règlement européen sur la protection des données personnelles. Objectif : encadrer les traitements de données et harmoniser les règles en Europe.</p>

### Biométrie :

Méthode d'authentification basée sur les caractéristiques physiques ou comportementales uniques d'une personne.

Exemples :

Empreinte digitale

Reconnaissance faciale

Iris

Voix

Signature dynamique

## CH2 : SOC et CyberSOC

Security Operations Center (SOC)	<ul style="list-style-type: none"> <li>- Le <b>SOC</b> surveille en continu les réseaux et systèmes.</li> <li>- Il <b>détecte, analyse et répond</b> aux incidents de sécurité.</li> <li>- Il met en place des <b>mesures de prévention</b>.</li> </ul>
CyberSOC	<ul style="list-style-type: none"> <li>- Équipe spécialisée contre les <b>cyberattaques avancées</b>.</li> <li>- Gère les <b>crises de cybersécurité</b>.</li> </ul>

**Qu'est-ce qu'un SIEM ?** SIEM (Security Information and Event Management) → Concept défini par Gartner (2005). **SIEM = SEM + SIM**

SEM (Security Event Management)	SIM (Security Information Management)	Un SIEM est une infrastructure technique complète permettant
<ul style="list-style-type: none"> <li>- Gestion en temps réel</li> <li>- Analyse et corrélation des événements</li> <li>- Détection d'incident</li> </ul>	<ul style="list-style-type: none"> <li>- Gestion des logs</li> <li>- Collecte et indexation</li> <li>- Stockage et recherche</li> </ul>	<ul style="list-style-type: none"> <li>- La surveillance de la sécurité</li> <li>- La détection d'incidents</li> <li>- La gestion et conservation des preuves (logs)</li> <li>- Voir le réseau</li> </ul>

**Log (journal) :** Trace numérique générée par un système (serveur, poste, pare-feu...) qui enregistre les activités et événements. → Ces logs constituent la donnée d'entrée d'un SIEM.

**Besoin de visibilité** Surveiller un système d'information nécessite la centralisation des logs provenant de multiples sources. → Cela permet l'analyse, la corrélation et la détection d'incidents. ⚠ Sans logs, le système de défense est aveugle.

### Cycle de vie de la donnée (SIEM) : 3 Phases

Centralisation	<ul style="list-style-type: none"> <li>- Collecte des événements (endpoints, serveurs, pare-feu...).</li> <li>- Envoi vers le SIEM pour une vue globale.</li> </ul>
Stockage & Indexation	<ul style="list-style-type: none"> <li>- Permet la recherche rapide des logs.</li> <li>- Essentiel pour la gestion de la preuve.</li> </ul>
Archivage	<ul style="list-style-type: none"> <li>- Conservation des données brutes à long terme (stockage froid).</li> <li>- Répond aux exigences légales et réglementaires.</li> </ul>

### Traitement de la donnée (SIEM)

Agrégation (réduire le volume)	<ul style="list-style-type: none"> <li>- Regrouper des événements identiques sur une période donnée.</li> <li>Exemple : 200 logs d'erreur → 1 événement unique.</li> <li>→ Objectif : simplifier l'analyse et réduire le bruit.</li> </ul>
Normalisation (uniformiser le langage)	<ul style="list-style-type: none"> <li>- Transformer des formats différents (Apache, IIS, Nginx, custom...)</li> <li>En un modèle standard commun (ex : IP + Timestamp + Action).</li> <li>→ Objectif : faciliter la corrélation et l'analyse automatique.</li> </ul>

## La Corrélation (SIEM)

Définition : Capacité de relier des événements provenant de sources différentes (firewall, serveurs, endpoints...) pour détecter un incident complexe en temps réel.

Fonctionnement : Événement A (ex : firewall) / Événement B (ex : serveur)

- Analyse via des règles de corrélation
- Génération d'une alerte qualifiée
- Incident de sécurité identifié

Objectif : Transformer un flux massif de logs bruts en une alerte, exploitable par le SOC.

## SOC vs CSIRT

CSIRT (Computer Security Incident Response Team)	Équipe d'intervention Gestion des incidents majeurs Réponse et remédiation en cas de crise
--	--

⇒ Le SOC surveille et détecte, le CSIRT intervient et gère la crise.

Le SOC est organisé en 3 niveaux, avec un principe d'escalade des incidents selon leur complexité.

Niveau 1 – Opérateur (Triage & Filtre)	<ul style="list-style-type: none"><li>- Surveillance des alertes</li><li>- Pré-qualification des incidents</li><li>- Filtrage des faux positifs</li></ul>
Niveau 2 – Ingénieur (Analyse & Maintenance)	<ul style="list-style-type: none"><li>- Analyse approfondie des incidents</li><li>- Traitement des incidents complexes</li><li>- Maintien en Condition Opérationnelle (MCO)</li></ul>
Niveau 3 – Expert (Investigation & Expertise) → cas critiques et stratégiques	<ul style="list-style-type: none"><li>- Threat Hunting</li><li>- Analyse forensique (investigation numérique)</li><li>- Gestion de crise</li></ul>

## SIEM vs IDS : différences et complémentarité

IDS (Intrusion Detection System)	SIEM (Security Information and Event Management)
<ul style="list-style-type: none"><li>- Détecter les intrusions ou activités suspectes.</li><li>- Surveiller le trafic réseau ou les hôtes.</li><li>- Recherche de signature d'attaque</li></ul>	<ul style="list-style-type: none"><li>- Centraliser les logs de multiples sources.</li><li>- Corréler les événements.</li><li>- Produire des alertes qualifiées.</li></ul>

L'IDS détecte, le SIEM analyse et orchestre.

Un IDS sans SIEM manque de contexte.

Un SIEM sans capteurs (IDS, firewall...) est aveugle.

## Qu'est-ce qu'un IDS ?

Définition : Un IDS (Intrusion Detection System) est un logiciel ou dispositif qui surveille un réseau ou un système afin de détecter : des activités malveillantes, des tentatives d'intrusion et des violations de politique de sécurité

### Méthodes de détection

**Signature-based** : Recherche de motifs connus (malwares, attaques répertoriées).

**Anomaly-based** : Détection de comportements inhabituels (souvent via apprentissage automatique).

**Reputation-based** : Analyse fondée sur la réputation d'adresses IP, domaines ou sources.

### Types d'IDS

**NIDS (Network IDS)** : Surveille le trafic réseau à des points stratégiques (switch, firewall, passerelle).

**HIDS (Host IDS)** : Surveille les fichiers, processus et activités d'un hôte spécifique (serveur, poste).

Objectif: Détecter rapidement une intrusion et générer une alerte pour permettre une réaction. → L'IDS détecte, mais ne bloque pas automatiquement (contrairement à un IPS).

---

**L'IDS** détecte et génère des alertes en temps réel.

**Le SIEM** centralise ces alertes, les analyse et les corrèle.

**L'équipe sécurité (SOC)** intervient à partir des données consolidées.

**IPS** → Blocage automatique

un IDS se distingue par son architecture, son mode d'analyse et sa méthode de détection.

Architecture	Mode de fonctionnement	Type de signature
Centralisé Hiérarchique P2P	Batch : analyse périodique des logs	Par motif (signature connue)
	Temps réel : analyse continue	Par détection d'anomalie

## CH3 : Détection d'intrusion

**Le cycle PPR** PPR = Planification → Protection → Réaction

- C'est un cycle de gestion de la sécurité permettant d'anticiper, de se protéger et de réagir efficacement face aux incidents.

Planification	Protection	Réaction
Analyse des risques et des menaces → Mise en place de règles, politiques et réglementations.	Mise en œuvre des mesures de sécurité → réduire la surface d'attaque et prévenir les incidents	Gestion des incidents, retour d'exp → Amélioration continue du dispositif de sécurité

<b>Vulnérabilité</b>	Faiblesse d'un bien ou d'un système pouvant exister à la conception, à la réalisation, à l'installation, à la configuration et à l'utilisation → Une vulnérabilité peut être exploitée par une attaque.
<b>Menace</b>	Cause potentielle d'un incident pouvant provoquer des dommages si elle se concrétise.
<b>Attaque</b>	Action visant à compromettre la sécurité d'un système. → Elle exploite généralement une vulnérabilité.
<b>Intrusion</b>	Prise de contrôle partielle ou totale d'un système à distance. → Résultat possible d'une attaque réussie.
<b>Usurpation (Spoofing)</b>	Prise d'identité d'un utilisateur ou d'un système afin d'obtenir un accès illégitime.

<b>Attaques non ciblées</b>	Attaques lancées à grande échelle sans viser une organisation précise. → Victimes choisies de manière aléatoire
<b>Attaques ciblées</b>	Attaques dirigées contre une organisation, une entreprise ou une personne identifiée. → Cible précise et étudiée → Préparation et reconnaissance préalable

	NIDS (IDS orienté réseau)	HIDS (IDS orienté hôte)
<b>Définition</b>	Surveille et analyse le trafic réseau.	Surveille une machine spécifique.
<b>Fonctionnement</b>	<ul style="list-style-type: none"> <li>- Placé sur le réseau (souvent relié à un switch).</li> <li>- Détecte via signatures ou anomalies.</li> <li>- Envoie des alertes.</li> </ul>	<ul style="list-style-type: none"> <li>- Analyse les logs système</li> <li>- Surveille ports et ressources (mémoire, disque, etc.)</li> </ul>
<b>Avantages</b>	<ul style="list-style-type: none"> <li>- Supervision de tout le réseau</li> <li>- Détection en temps réel</li> <li>- Indépendant des systèmes d'exploitation</li> </ul>	<ul style="list-style-type: none"> <li>Fonctionne avec trafic chiffré</li> <li>- Vérification précise sur la machine</li> </ul>

<b>Inconvénients</b>	<ul style="list-style-type: none"> <li>- Moins efficace si trafic très élevé</li> <li>- Difficulté avec les flux chiffrés</li> <li>- Problèmes possibles avec les fragments IP</li> </ul>	<ul style="list-style-type: none"> <li>- Dépend du système d'exploitation</li> <li>- Consomme des ressources</li> <li>- Souvent basé sur analyse de logs (pas toujours temps réel)</li> </ul>
----------------------	---	---

### Limites générales des IDS

- Manque de partage d'informations sur les attaques → base de détection incomplète
- Peuvent être inefficaces dans certains cas
- Limites valables pour :
  - Détection par signature
  - Détection par anomalie

### Vulnérabilités techniques (TCP)

Les IDS peuvent être contournés via :

- Manipulation des flags TCP (ex : faux SYN)
- Spoofing (FIN/RST, data)
- Mauvais numéros de séquence
- Mauvaise somme de contrôle
- Désynchronisation de la connexion
- TTL court pour tromper l'analyse

→ Un IDS peut être contourné ou trompé par des techniques réseau avancées → il ne garantit pas une protection totale.

### Limites des IPS

- Tolérance zéro à l'erreur
- Risque de blocage du réseau
- Mise en place complexe
- Administration lourde

→ Un IPS protège activement, mais une mauvaise configuration peut perturber ou bloquer le système.

### Snort (outil IDS)

- IDS open source
- Type : NIDS
- Détection en temps réel
- Fonctionne sur IP, TCP, UDP, ICMP
- Utilise des règles simples et paramétrables

### Exemple simple de règle :

```

alert tcp any any -> 192.168.1.0/24 any
(flags:SF; msg:"Scan SYN FIN");
alert tcp any any -> 192.168.1.0/24 21 (content:
"USER root"; msg: "Tentative d'accès au FTP
pour l'utilisateur root");

```

## CH4 : DevSecOps

### Définition :

- Intégrer la sécurité dès le début du cycle de développement (SDLC).
- Automatiser la sécurité tout au long du cycle de vie.
- Collaboration entre Dev + Sec + Ops.

### Pourquoi c'est essentiel ?

- Réagir rapidement aux vulnérabilités
- Réduire les coûts de correction
- Mettre en place une sécurité proactive
- Automatiser détection et correction

### Principe du "Shift Left"

Déplacer les tests de sécurité le plus tôt possible dans le cycle.

Avantages	Etapas
Détection précoce Moins cher à corriger Meilleure qualité logicielle	1. Planifier 2. Coder 3. Construire 4. Tester 5. Déployer

### Piliers DevSecOps

- Automatisation (tests sécurité, déploiements continus)
- Collaboration entre équipes
- CI/CD avec contrôles de sécurité intégrés
- Monitoring en temps réel

### Outils clés

- CI/CD : Jenkins, GitLab CI
- Sécurité : SAST, DAST, OWASP ZAP, Snyk
- IaC : Terraform, Ansible
- Monitoring : Prometheus, ELK

### Bonne pratique type (SCA)

- Scanner les dépendances
- Alerter en cas de vulnérabilité
- Corriger rapidement (PR automatique)