Intégration de Sécurité dans les Projets

Introduction

VUE GLOBALE

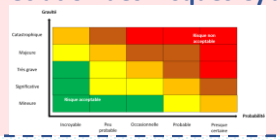
LOI REGLEMENT

NORMES

POLITIQUE RISQUES CONTROLES

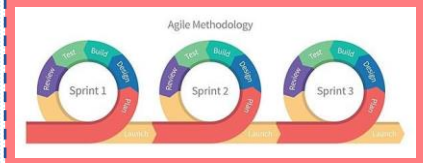
Politique & pilotage de la Cyber

Appréciation des Risques Cyber

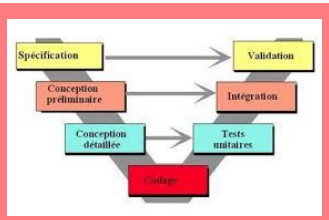


Contrôle & audit Cyber

SECURITE DANS LES PROJETS

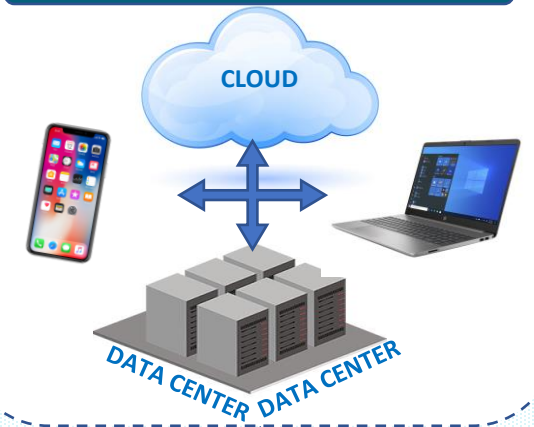


APPLICATIONS



INFRASTRUCTURES

SYSTÈME D'INFORMATIONS



MESURES DE SECURITE

Gestion des identités et des accès au SI

Protection des informations

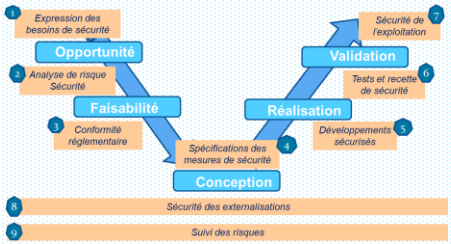
Cloisonnement et Robustesse du SI

Surveillance du SI

Gestion des vulnérabilités

MENACES

LES ACTIVITÉS ISP



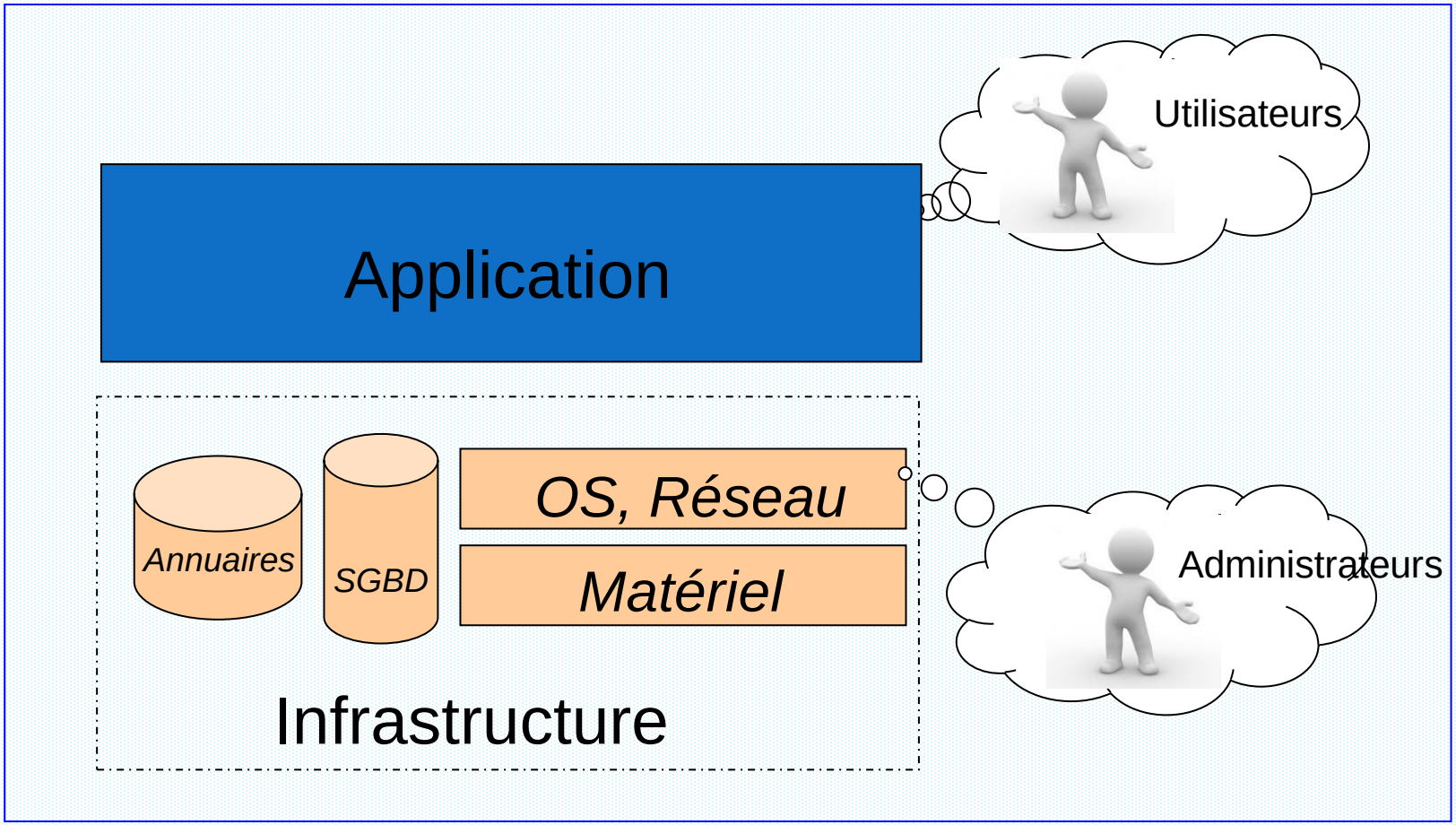
1. Besoin de sécurité
2. Analyse de risque
3. Les exigences réglementaires
4. **Les spécifications des mesures de sécurité**
5. La sécurisation des développements
6. Les tests et recettes de sécurité
7. La sécurisation de l'exploitation
8. La sécurisation de la sous-traitance
9. Le suivi des risques résiduels et induits

LES SPÉCIFICATIONS DE SÉCURITÉ

- Principes d'Architectures
  - Mesures de sécurité d'Infrastructure
  - Mesures de sécurité Applicatives
- Cas pratique

LES SPÉCIFICATIONS DE SÉCURITÉ

Les principes d'architectures



LES SPÉCIFICATIONS DE SÉCURITÉ

Les mesures de sécurité de l'infrastructure

Les principales fonctions de sécurité assurées par l'infrastructure technique

- ⇨ Chiffrement des flux
- ⇨ Filtrage réseau
- ⇨ Cloisonnement logique
- ⇨ Les « anti tout » : antimalware, antispam, anti déni, ..
- ⇨ …

LES SPÉCIFICATIONS DE SÉCURITÉ

Les mesures de sécurité de l'infrastructure

⇨ **La défense périmétrique (ou « muraille de Chine »)** :

- Attaque frontale pour percer
- Propagation une fois la muraille franchie

⇨ **La « défense en profondeur » (référence aux principes de Vauban)**

- Mise en place de plusieurs lignes de défense successives
- S'assurer qu'en cas de perte d'un élément de sécurité, d'autres prendront la suite
- Traiter aussi bien l'interne que l'externe
- Traiter des menaces différentes par des solutions complémentaires et ciblés
- Gérer des niveaux de sécurité différent)

LES SPÉCIFICATIONS DE SÉCURITÉ

Les mesures de sécurité de l'infrastructure

- **DMZ :** Isoler un sous-réseau des autres, au moyen d'équipement(s) de filtrage (firewalls – FW)

- **Bastion d'administration** : les tâches d'administration doivent être isolées
  - Utilisateurs privilégiés
  - Configuration des équipements administrés sur des interfaces dédiées
  - Traçabilité renforcée
  - Postes de travail durci
  - Isolation D'internet

LES SPÉCIFICATIONS DE SÉCURITÉ

Les mesures de sécurité de l'infrastructure

Installer et gérer des pare-feu pour protéger des zones du SI

Les pare-feu sont des dispositifs qui contrôlent le trafic autorisé entre le réseau d'une entreprise (interne) et les réseaux non approuvés (externes), ainsi que le trafic entrant et sortant dans des zones plus sensibles du réseau interne d'une société.

L'environnement des données sensibles est un exemple de zone plus sensible au sein du réseau approuvé d'une entreprise.

Tous les systèmes doivent être protégés contre les accès non autorisés depuis un réseau non approuvé, que ce soit en entrée via Internet ou via les réseaux sans fil

LES SPÉCIFICATIONS DE SÉCURITÉ

Les mesures de sécurité des applications

Les principales fonctions de sécurité fournies par l'application

- ⇨ La protection des données
- ⇨ L'identification et l'authentification des accédants
- ⇨ La gestion des droits d'accès aux fonctions / services de l'application

LES SPÉCIFICATIONS DE SÉCURITÉ

Les mesures de sécurité des applications

Protéger les données sensibles

Les méthodes de protection, telles que le chiffrement, le masquage et le hachage, sont des moyens très utilisés pour protéger les données sensibles d'une entreprise.

- Le chiffrement reste le moyen le plus répondu et le plus efficaces.

Si un intrus parvient à contourner les autres contrôles de sécurité et à accéder aux données préalablement cryptées, il ne pourra pas les lire ni les utiliser s'il n'a pas les clés cryptographiques appropriées.

De même, les informations sensibles doivent être chiffrées pendant leur transmission sur des réseaux non maitrisés (ex: réseaux publiques)

Pourquoi ?

LES SPÉCIFICATIONS DE SÉCURITÉ

Les mesures de sécurité des applications

Sécurité d'accès au SI

- La reconnaissance d'un accédant par le système informatique s'appui sur 2 éléments
  - L'identité numérique : « **dit** qui tu es ».
  - L'authentifiant : « **prouve** qui tu es »

- L'identité numérique doit être rattaché à l'identité d'une personne physique (ou un matériel connu)

- L'authentifiant est un élément secret connu uniquement par l'accédant et le système. Il prouve l'identité de l'accédant qui demande l'accès au SI

- Plusieurs moyens peuvent être utilisés comme authentifiant :
  - Ce que je sais : code, phrase, mot de passe
  - Ce que je possède : certificat, token, téléphone
  - Ce que je suis : biométrie
  - Ce que je sais faire : comportement

LES MESURES TECHNIQUES DE SECURITE

L'authentifiant le plus utilisé…

- La robustesse d'un mot de passe dépend plus particulièrement :
  - De sa complexité : type de caractères, **longueur,** procédé de construction
  - De sa fréquence de renouvellement
  - De la gestion de son historique
  - De la gestion des échecs

Longueur	Nature des caractères	Variabilité
Mot de passe « standard utilisateur »		
8 caractères	Alphabétiques, numériques et au moins un caractère spécial	Différents des 5 derniers avec 50 % des caractères différents du précédent
Mot de passe « renforcé utilisateur »		
12 caractères	Alphabétiques, numériques et au moins un caractère spécial	Différents des 9 derniers avec 50 % des caractères différents du précédent
Mot de passe « processus informatique»		
20 caractères	Alphabétiques, numériques et au moins un caractère spécial	Différents des 9 derniers avec 50 % des caractères différents du précédent

LES SPÉCIFICATIONS DE SÉCURITÉ

Cas pratique

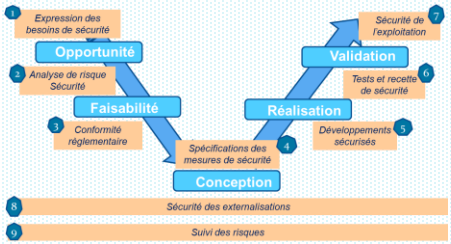
5 min

Le RSSI de l'hôpital a estimé que l'accès aux applications à partir du poste de travail des utilisateurs doit être particulièrement renforcé.

Travaux à réaliser

- **Décrivez les caractéristiques d'une fonction de gestion des Mots de Passe de manière à garantir son efficacité**

LES ACTIVITÉS ISP



1. Besoin de sécurité
2. Analyse de risque
3. Les exigences réglementaires
4. Les spécifications des mesures de sécurité
5. **La sécurisation des développements**
6. Les tests et recettes de sécurité
7. La sécurisation de l'exploitation
8. La sécurisation de la sous-traitance
9. Le suivi des risques résiduels et induits

LES MESURES DE DEVELOPPEMENT SECURISÉ

Sécuriser les applications

Développer (et gérer) des systèmes et des applications sécurisées

Des individus sans scrupule peuvent exploiter les points faibles de la sécurité pour obtenir un accès privilégié aux systèmes.

Bon nombre de ces vulnérabilités sont résolues par les correctifs de sécurité développés par les fournisseurs. Ceux-ci doivent être installés par les entités chargées de la gestion des systèmes.

Tous les systèmes stratégiques doivent être dotés des correctifs logiciels appropriés les plus récents afin d'empêcher l'exploitation et l'altération des données sensibles par des individus et des logiciels malveillants.

LES MESURES DE DEVELOPPEMENT SECURISÉ

Sécuriser les applications : comment- pourquoi

Respecter des normes et règles de développement concernant :

- les fonctions de sécurité
- les applications WEB
- Les progiciels

afin **de réduire les risques**:

- Utilisation de failles applicatives pour accéder à des données d'autres utilisateurs ou des fonctions permettant de réaliser des opérations frauduleuses
- Utilisation de failles applicatives pour acquérir des droits système et pour rebondir sur d'autres serveurs ou applications
- Stockage résiduel de données sensibles sur le poste client

LES MESURES DE DEVELOPPEMENT SECURISÉ

La sécurité vue par le développeur

Quelques statistiques :

75% des vulnérabilités se retrouvent dans la couche applicative (*Checkmarx 2015 - Gartner disait la même chose en 2002…)*

70% des applications avaient au moins une vulnérabilité classifiée dans le **top 10 OWASP (***Veracode 2015)*

15% des applications Web ont une vulnérabilité critique ou élevé (*Edgescan report 2015)*

85% des attaques ciblent la couche applicative (*Checkmarx 2015)*

Deux axes à traiter :

Sécuriser l'environnement de développement

Les méthodes de développement sécurisé

LES MESURES DE DEVELOPPEMENT SECURISÉ

Sécuriser l'environnement de développement

L'équipe projet

- L'équipe projet est indépendante de celle de l'exploitation de la production
- L'équipe projet n'a pas d'accès aux plateformes de production
- L'équipe projet a des accès restreints aux plates-formes de développement et de recette

Les plates-formes

- Les plates-formes de développement et de recette sont séparées de celles de productions

LES MESURES DE DEVELOPPEMENT SECURISÉ

Sécuriser l'environnement de développement

La documentation projets et contractuelles

- Les documents confidentiels du projet sont protégés
- Les documents contractuels sont restreints en accès

Les données, fichiers de l'application

- Les fichiers sources, les fichiers exécutables, Les paramètres sont protégés contre les défauts d'intégrité
- Les données de tests et recette sont sécurisées (désensibilisation, anonymisation, …)

LES MESURES DE DEVELOPPEMENT SECURISÉ

Les méthodes de développement sécurisé

Développer des applications en ce basant sur des méthodes de codage sécurisé.

Développer en prévenant les vulnérabilités/attaques connues

- Sources possibles: Top ten OWASP, Top 25 SANS , recommandations CERT, …
- Classification CVSS (prise en compte niv +=4)
- Injections (SQL, LDAP, …) , buffer overflow, attaques crypto (mauvais stockage des clés, man in the middle, …), XSS, CSRF, path/directory traversal, …

Contrôler les données en entrée des processus critiques

LES MESURES DE DEVELOPPEMENT SECURISÉ

OWASP

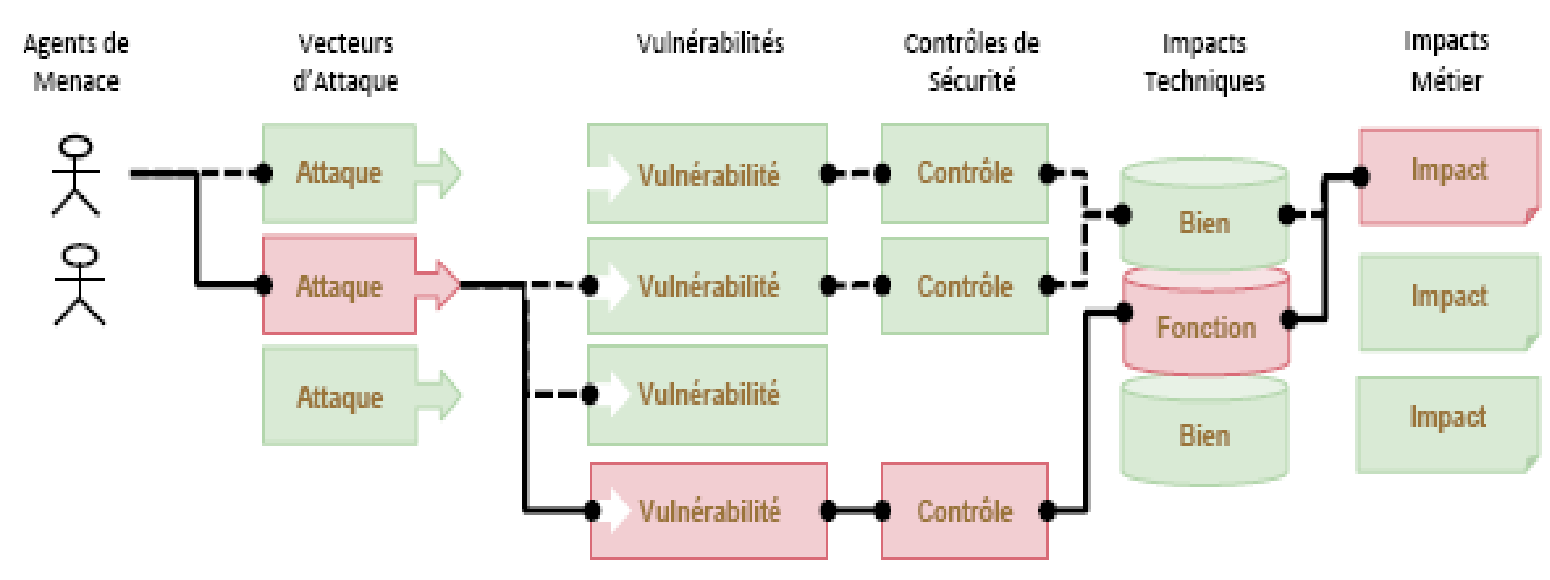
- **OWASP : Open Web App Security project**
  - OWASP est une communauté travaillant sur la sécurité des applications Web. Elle identifie les « failles » majeurs (et courantes) dans les applications Web :

www.owasp.org

LES MESURES DE DEVELOPPEMENT SECURISÉ

OWASP

- **Processus d'attaques selon l'OWASP**



LES MESURES DE DEVELOPPEMENT SECURISÉ

OWASP : Top 10 des attaques

A1	L'injection (SQL, shell, LDAP, etc…)	Exploitation du manque de contrôle dans un champs USR
A2	Broken Authentication and Session Management	Vols d'authentification, de la session
A3	Cross-Site Scripting:	Exploitation du manque de contrôle dans un champs USR
A4	Insecure Direct Object References	Exploitation d'un manque de contrôle d'accès aux données
A5	Security Misconfiguration	Outils mal configuré, non à jour, …
A6	Sensitive Data Exposure	Mauvais chiffrement de données sensibles, mdp en cache, …
A7	Missing Function Level Access Control	Exploitation d'un manque de contrôle d'accès aux fonctions
	…	

LES MESURES DE DEVELOPPEMENT SECURISÉ

OWASP : L'attaque par injection

A1 Injection

Agents de menace	Vecteurs d'attaque	Vulnérabilité		Impacts Technique	Impacts Métier
Spécifique Application	**Exploitabilité FACILE**	**Prévalence COMMUNE**	**Détection MOYENNE**	**Impact SEVERE**	**Spécifique Application/Métier**
Considérez que n'importe qui peut envoyer des données non fiables au système, y compris les utilisateurs externes, internes, et administrateurs.	L'attaquant utilise des scripts qui exploitent la syntaxe d'un interpréteur cible. Presque toute source de données peut être un vecteur d'injection, y compris des sources internes.	Les failles d'Injection surviennent quand une application envoie des données non fiable à un interpréteur. Les failles d'injection sont très fréquentes, surtout dans un code ancien. On les retrouve souvent en SQL, LDAP, XPath, ou NoSQL; commandes OS; parseurs XML; entêtes SMTP, arguments de programme, etc. Les failles d'Injection se détectent facilement via le code, difficilement via le test. Scanners et Fuzzers peuvent aider les attaquants à trouver les failles d'Injection.		L'Injection peut résulter en une perte ou une corruption de données, une perte de droits, ou un refus d'accès. L'Injection peut parfois mener à une prise de contrôle totale du serveur.	Considérez la valeur métier de la donnée impactée et la plateforme exécutant l'interpréteur. Toute donnée pourrait être volée, modifiée ou supprimée. Votre réputation pourrait-elle en pâtir?

Suis-je vulnérable?

Le meilleur moyen de savoir si une application est vulnérable à l'Injection est de vérifier que toute utilisation d'interpréteurs sépare explicitement les données non f… de la commande ou de la requête. Pour les appels SQL… signifie utiliser des variables liées dans toutes les instructions préparées et procédures stockées, et éviter les requêtes dynamiques.

Vérifier le code est un moyen rapide et adéquat pour s'assurer que l'application utilise sainement les interpréteurs. Les outils d'analyse de code peuvent aider à localiser l'usage des interpréteurs et tracer leur flux de données à travers l'application. Les Pentesters peuvent valider ces problèmes en concevant des exploits qui confirment la vulnérabilité.

Le scan dynamique peut donner un aperçu des failles d'Injection existantes. Les scanners ne savent pas toujours atteindre les interpréteurs, ni si une attaque a réussi. Une mauvaise gestion d'erreur aide à trouver les failles.

Comment s'en prémunir?

Empêcher une Injection… …leure option est d'utiliser une API saine évitant toute utilisation de l'interpréteur ou fournissant une interface paramétrable. Attention aux APIs telles que les procédures stockées qui, bien que paramétrables, peuvent envelopper une Injection.

2. En l'absence d'API paramétrable, vous devriez soigneusement échapper les caractères spéciaux en utilisant la syntaxe d'échappement spécifique à l'interpréteur. OWASP's ESAPI fournit des routines d'échappement.
3. La « whitelist » est recommand… données entrantes, mais n'est pas une def… plusieurs applications requérant des caractères spéciaux, le cas échéant, seules les approches 1. et 2. sécurisent. OWASP's ESAPI a une librairie extensible de routines de validation « whitelist » d'entrées.

Exemple de scénarios d'attaque

Scénario #1: Une application utilise des données non fiables dans la construction de l'appel SQL vulnérable suivant:

```
String query = "SELECT * FROM accounts …
custID='" + request.getParameter("id") +"'";
```

Scénario #2: Pareillement, la confiance aveugle d'une application aux frameworks peut déboucher sur des requêtes toujours vulnérables (p.ex. Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts
WHERE custID='" + request.getParameter("id") + "'");
```

Dans les deux cas, l'attaquant modifie le paramètre 'id' dans son navigateur et envoie: ' or '1'='1. Par exemple:

```
http://example.com/app/accountView?id=' or '1'='1
```

Le sens des deux requêtes est modifié pour retourner toutes les lignes de la table accounts. Les pires attaques peuvent altérer des données, voire invoquer des procédures stockées.

Références

OWASP

- OWASP SQL Injection Prevention Cheat Sheet
- …Injection Cheat Sheet
- …
- OWASP XML eXternal Entity (XXE) Reference Article
- ASVS: Output Encoding/Escaping Requirements (V6)
- OWASP Testing Guide: Chapter on SQL Injection Testing

Externes

- CWE Entry 77 on Command Injection
- CWE Entry 89 on SQL Injection
- CWE Entry 564 on Hibernate Injection

Description de l'attaque

Identifier son niveau de risque

Mesures à prendre

Exemples de scénarios

LES MESURES DE DEVELOPPEMENT SECURISÉ

OWASP : Guide de tests de sécurité

Description de contrôles de sécurité des applications WEB à travers une méthodologie pour la conduite de tests de sécurité.

⇨ Ensemble de pratiques organisationnelles (méthodes, processus, acteurs)

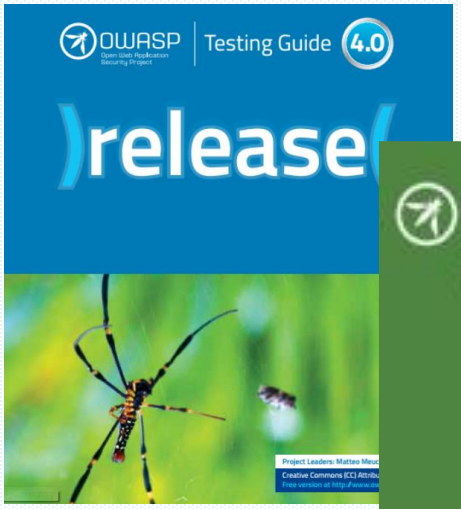
⇨ Pratiques techniques, formalisées sous la forme d'une centaine de tests
- Tests de configuration
- Identity Management tests
- Authentification tests
- Session Management test
- Input Validation Tests
- …

⇨ Liste de vulnérabilités exploitables

LES MESURES DE DEVELOPPEMENT SECURISE

OWASP : Guide de tests de sécurité

Plusieurs guides :



LES MESURES DE DEVELOPPEMENT SECURISÉ

Quizz

Une mauvaise programmation et des pratiques de codification inadéquates présentent un risque de :

- hameçonnage (phishing)
- débordement de mémoire tampon
- attaques par force brute

LES MESURES DE DEVELOPPEMENT SECURISÉ

QUIZZ

Lequel des moyens biométriques suivants présente la plus haute fiabilité et le plus bas taux de faux-positifs ?

- Scanner de la paume
- Reconnaissance faciale
- Scanner de rétine
- Géométrie de mains

LES MESURES DE DEVELOPPEMENT SECURISÉ

QUIZZ

Le partage des informations de connexion par les utilisateurs entraîne un manque de :

- Disponibilité.
- D'authentification.
- D'autorisation.

LES MESURES DE DEVELOPPEMENT SECURISÉ

QUIZZ

Lors de l'analyse des contrôles d'authentification, quel est le point le plus préoccupant :

- Les comptes des utilisateurs ne sont pas verrouillés après cinq tentatives ratées.
- Les mots de passe peuvent être réutilisés par les invités après une période déterminée.
- Les administrateurs du système utilisent des identifiants de connexion partagés.
- L'expiration des mots de passe n'est pas automatisée.

LES MESURES DE DEVELOPPEMENT SECURISÉ

QUIZZ

Parmi les choix suivants, lequel est le MEILLEUR moyen de garantir une authentification d'utilisateur à deux facteurs ?

- Une carte à puce requérant le numéro d'identification personnel de l'utilisateur (PIN)
- Un identifiant d'utilisateur et un mot de passe
- Un scanner oculaire plus un scanner d'empreinte
- Une carte magnétique requérant le PIN de l'utilisateur

LES MESURES DE DEVELOPPEMENT SECURISÉ

QUIZZ

Une mauvaise programmation et des pratiques de codification inadéquates présentent un risque de :

- hameçonnage (phishing)
- débordement de mémoire tampon
- attaques par force brute

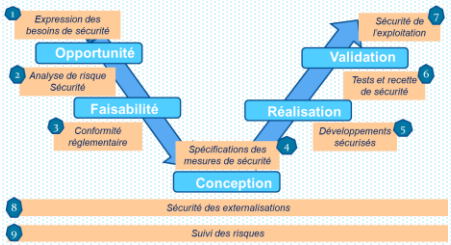
LES MESURES DE DEVELOPPEMENT SECURISÉ

QUIZZ

Durant la phase de test d'un projet de développement d'application, un auditeur doit examiner :

- Les spécifications du design et de la conception
- Le contrat vendeur
- Les rapports d'erreur
- Les demandes de modification de programme

Les activités ISP



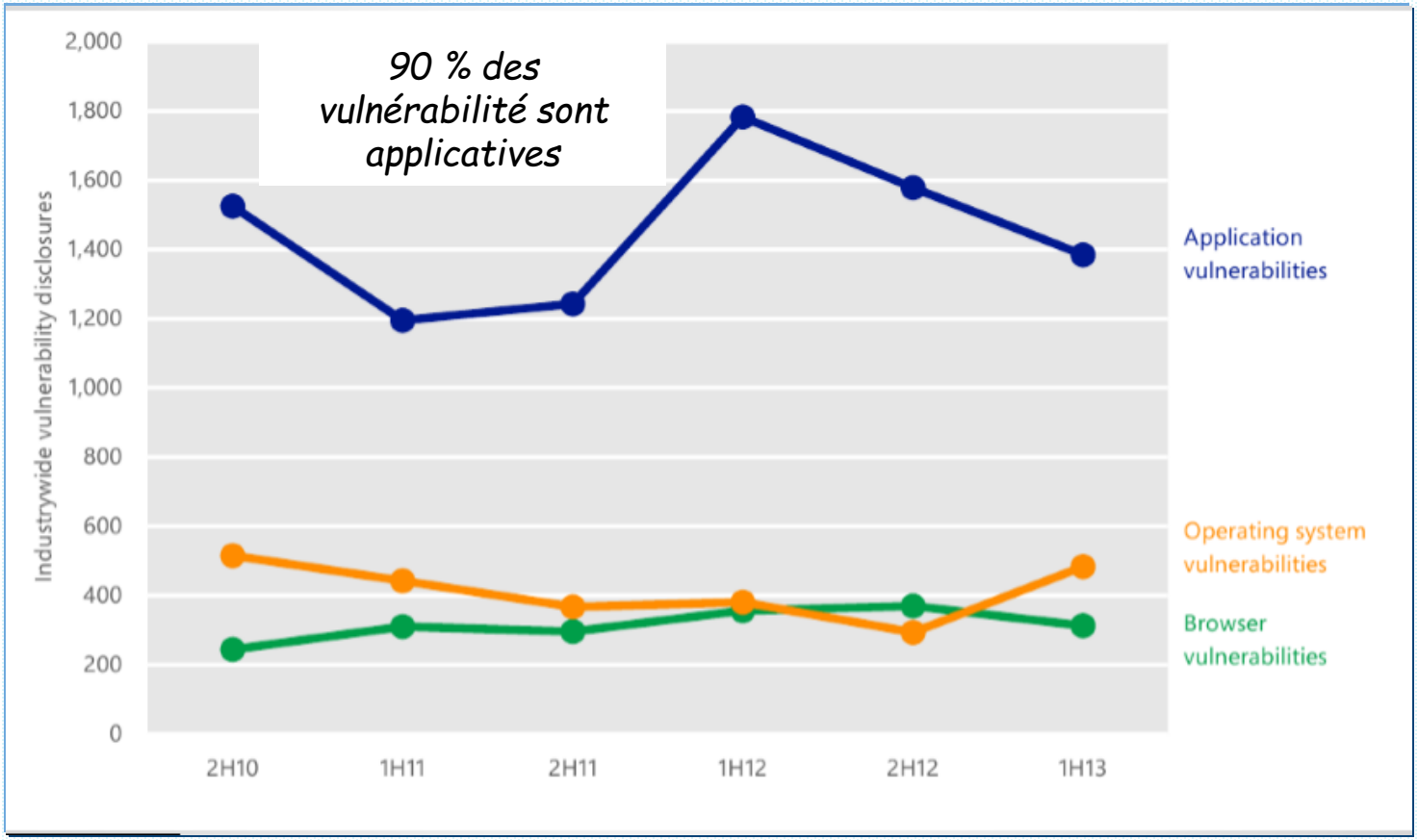
1. Besoin de sécurité
2. Analyse de risque
3. Les exigences réglementaires
4. Les spécifications des mesures de sécurité
5. La sécurisation des développements
6. **Les tests et recettes de sécurité**
7. La sécurisation de l'exploitation
8. La sécurisation de la sous-traitance
9. Le suivi des risques résiduels et induits

Tests et recette de sécurité

- Stratégie de test
- Rapport de test
- Quizz

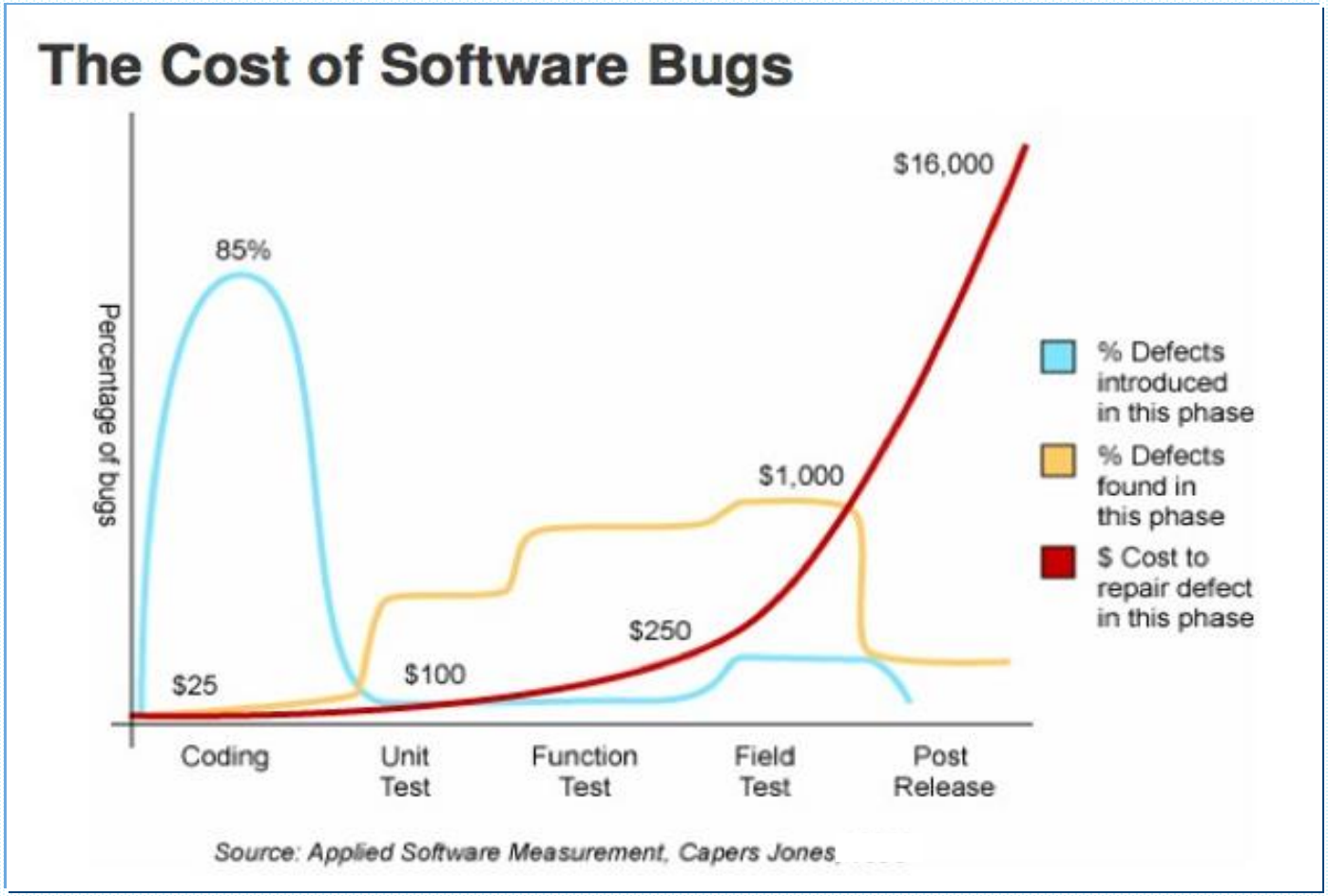
Les tests et recettes de sécurité

Stratégie de test



Les tests et recettes de sécurité

Stratégie de test



Les tests et recettes de sécurité

Stratégie de test

Etape 1 – Scénarios d'attaques / menaces

- Source : interne, externe, averti, …
- Vecteur : réseau, application, …
- Cibles : données, commande, …
- Objectifs : accès, prise de main

Etape 2 – Choix des tests

- Revue de vulnérabilité
- Tests d'intrusion
- Tests fonctionnels
- …

Les tests et recettes de sécurité

Stratégie de test

⇨ Les tests et recette de sécurité peuvent s'appuyer sur tout ou partie des investigations suivantes :

CS1	**Contrôler les Infrastructures**	➔ Analyse d'architecture ➔ Contrôle de configuration ➔ Tests d'intrusion
CS2	**Contrôler les Applications**	➔ Analyse de code ➔ Tests des fonctions de sécurité ➔ Tests de vulnérabilités
CS3	**Contrôler les Process**	➔ Contrôle environnements ➔ Contrôle des procédures ➔ Contrôle des méthodes

Les tests et recettes de sécurité

Stratégie de test : choix

Top10 Web	Tests d'intrusion	Analyse du code
A1 - Injection	++	+++
A2 – Violation de Session / Authentification	++	+
A3 – Cross Site Scripting	+++	+++
A4 – Référence Directes	+	+++
A5 – Mauvaise configuration	+	++
A6 – Exposition de données	++	+
A7 – Probleme d'habilitation fonctionnelle	+	+
A8 - CSRF	++	+
A9 – Utilisation de Composants vulnérables		+++
A10 – Redirection et transferts	+	+

Les tests et recettes de sécurité

Stratégie de test : choix

1 – Tests d'intrusion

- Facile à réaliser
- Fournit une preuve de la vulnérabilité, …
- Compétence moindre
- Dépend des scénarios testés

2 – Revue de code

- Vue exhaustive
- Vérifie l'efficience des contrôle
- S'assure de la mise en œuvre des contrôle
- Vérifie qu'une fonction piégée n'est pas présente
- S'intègre facilement dans le cycle de développement

Les tests et recettes de sécurité

Rapport de test

⇨ **Le Rapport de test** :

- Périmètre
- Liste des recommandations
- Liste des vulnérabilités
  - Niveau de risque
  - Description
  - Probabilité
  - Impact
  - Recommandation
- Annexe décrivant les étapes pour reproduire chaque vulnérabilité

Les tests et recettes de sécurité

Quizz

Un test de non régression pour la cyber sert principalement à assurer :

- Que le système fonctionne conformément aux exigences du Métier
- Qu'un nouveau système peut fonctionner dans l'environnement cible
- Que les normes de développement ont été appliquées
- Que les évolutions apportées n'ont introduit aucune nouvelle faille

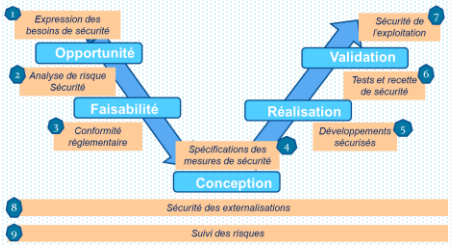
LES MESURES DE DEVELOPPEMENT SECURISÉ

Quizz

Durant la phase de test d'un projet de développement d'application, un auditeur doit examiner :

- Les spécifications du design et de la conception
- Le contrat vendeur
- Les rapports d'erreur
- Les demandes de modification de programme

Les activités ISP



1. Besoin de sécurité
2. Analyse de risque
3. Les exigences réglementaires
4. Les spécifications des mesures de sécurité
5. La sécurisation des développements
6. Les tests et recettes de sécurité
7. **La sécurisation de l'exploitation**
8. La sécurisation de la sous-traitance
9. Le suivi des risques résiduels et induits

LES MESURES DE SECURITE OPERATIONNELLES

Les principaux processus

- Gestion de la sécurité des réseaux
- Gestion des vulnérabilités des assets
- Gestion des enregistrements (logs)
- Gestion des incidents et surveillance du SI

LES MESURES DE SECURITE OPERATIONNELLES

Gestion de la sécurité des réseaux

Installer et gérer des pare-feu pour protéger des zones du SI

Les pare-feu sont des dispositifs qui contrôlent le trafic autorisé entre le réseau d'une entreprise (interne) et les réseaux non approuvés (externes), ainsi que le trafic entrant et sortant dans des zones plus sensibles du réseau interne d'une société.

L'environnement des données sensibles est un exemple de zone plus sensible au sein du réseau approuvé d'une entreprise.

Tous les systèmes doivent être protégés contre les accès non autorisés depuis un réseau non approuvé, que ce soit en entrée via Internet ou via les réseaux sans fil

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des vulnérabilités

Maintien du Niveau de sécurité : la gestion des patchs -correctifs

- Doit s'accompagner d'un inventaire exhaustif et à jour des biens, systèmes utilisés, versions, administrateur responsable
- Doit s'accompagner d'une veille technologique sur les nouvelles vulnérabilités et leur gravité
- Doit s'accompagner d'une procédure complète de mise à jour, test et recette des correctifs
- Doit être documenté et faire l'objet d'un suivi via des indicateurs

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des vulnérabilités

Maintien du Niveau de sécurité : le Standard CVSS

La qualification peut être effectuée en se basant sur le standard CVSS (Common Vulnerability Scoring System) qui s'appuie sur 3 natures de métriques :

- **Basique,** qui prend en compte les caractéristiques techniques immuables de la vulnérabilité :
  - Exécution locale ou à distance de la faille,
  - Difficulté des conditions d'exploitation,
  - Impact
- **Temporel**, qui prend en compte les caractéristiques d'évolution de la vulnérabilité :
  - Exploitabilité inexistante,
  - Proof of Concept, exploit publié, exploit non nécessaire …),
  - Moyens de son exploitation (existence d'un correctif de sécurité)
- **Environnemental**, qui prend en compte les caractéristiques propres au SI

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des vulnérabilités

Maintien du Niveau de sécurité : La démarche

Réception

Réception quotidienne par mail des vulnérabilités

1er filtrage des vulnérabilités

Analyse
de la vulnérabilité

Analyse et requalification de la CRITICITE

- criticité => Normal | Urgent | Prioritaire

CVSS

Analyse de la PERTINENCE pour les alertes prioritaires et urgentes : le PERIMETRE est-il impacté?

Résultat

3 cas :

- La vulnérabilité est **HORS PERIMETRE**
- Dans les autres cas, la vulnérabilité est **NOTIFIEE**
- Si la vulnérabilité est **PRIORITAIRE** **cellule de TRAVAIL**

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des vulnérabilités

Maintien du Niveau de sécurité : La qualification

CVSS

Score de BASE

-
basé sur ce que fourni le prestataire de veille
évaluation de l'impact maximum théorique de la vulnérabilité

Score TEMPOREL

pondère le score de base en fonction du risque actuel
=> programme d'exploitation, correctif

Score ENVIRONNEMENTAL

pondère le score temporel, en fonction du périmètre particulier
=> dégâts collatéraux, distribution, impact

Score final

Note entre 0 et 10

Seuils

Normal	Urgent	Prioritaire
0 à 6	6 à 8	8 à 10

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des vulnérabilités

Maintien du Niveau de sécurité : Le durcissement

Certains systèmes embarquent **par défaut** des faiblesses qui ne peuvent être décrites comme des vulnérabilités.

Le durcissement se traduit par :

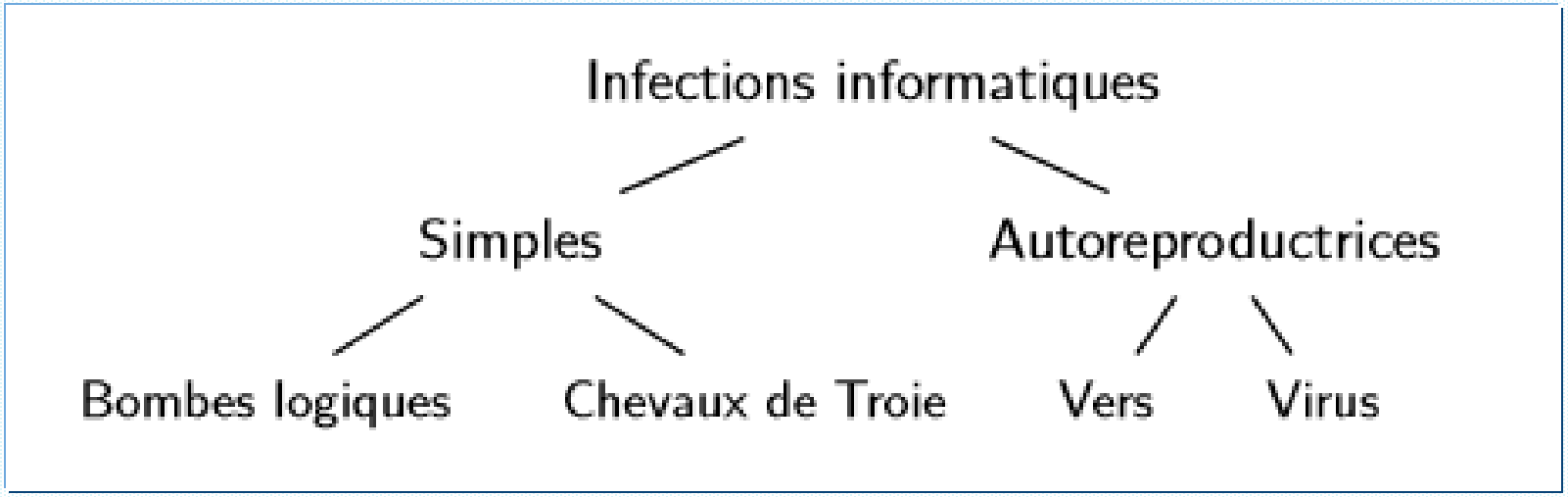
- La suppression de fonctions inutiles
- L'activation de paramètres de sécurité
- Le renforcement d'une stratégie de sécurité
- Le rajout de modules de sécurité
- …

Des dizaines de guides de durcissement sont disponibles sur Internet

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des vulnérabilités

La lutte anti virales



LES MESURES DE SECURITE OPERATIONNELLES

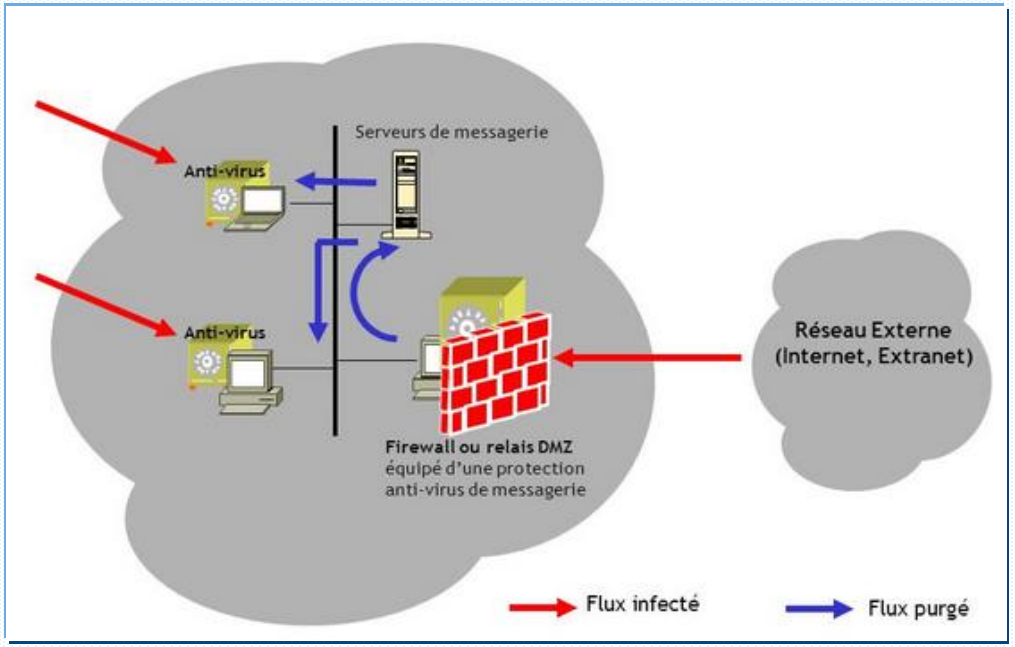
Gestion des vulnérabilités

La lutte anti virales : les modes de propagation

Modes de propagation

- ⇨ Echange de données
- ⇨ Vulnérabilité logicielle
- ⇨ Intervention de maintenance
- ⇨ ….

Positionnement des moyens de détection sur les points de passage de la propagation : messagerie, passerelle de connexion, poste de travail, …



LES MESURES DE SECURITE OPERATIONNELLES

Gestion des vulnérabilités

La lutte anti virales : les modes de détection

La détection par la signature

- ⇨ l'Antivirus interroge sa base de données de référence pour savoir à qui il a affaire et prendre les mesures qui s'imposent.

La détection par le comportement

- ⇨ l'Antivirus intervient quand un programme a un comportement inhabituel ou non approprié.

La détection par le contrôle de l'intégrité.

- ⇨ l'Antivirus vérifie si les fichiers n'ont pas été modifiés depuis leur installation, s'ils sont bien dans leur version originale (vérification des date / heure et taille).

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des enregistrements

Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données

Les mécanismes de journalisation et le suivi des activités des utilisateurs sont essentiels pour prévenir, détecter ou minimiser l'impact d'une altération des données.

La présence de journaux dans tous les environnements permet de suivre de près, d'émettre des alertes et d'analyser les incidents éventuels.

En l'absence de journaux retraçant les activités du système, il est très difficile, sinon impossible, de déterminer la cause d'une anomalie.

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des enregistrements

Le SIEM

La gestion et la corrélation des évènements sécurité est classiquement réalisé par un SIEM : Security Information and Event Management

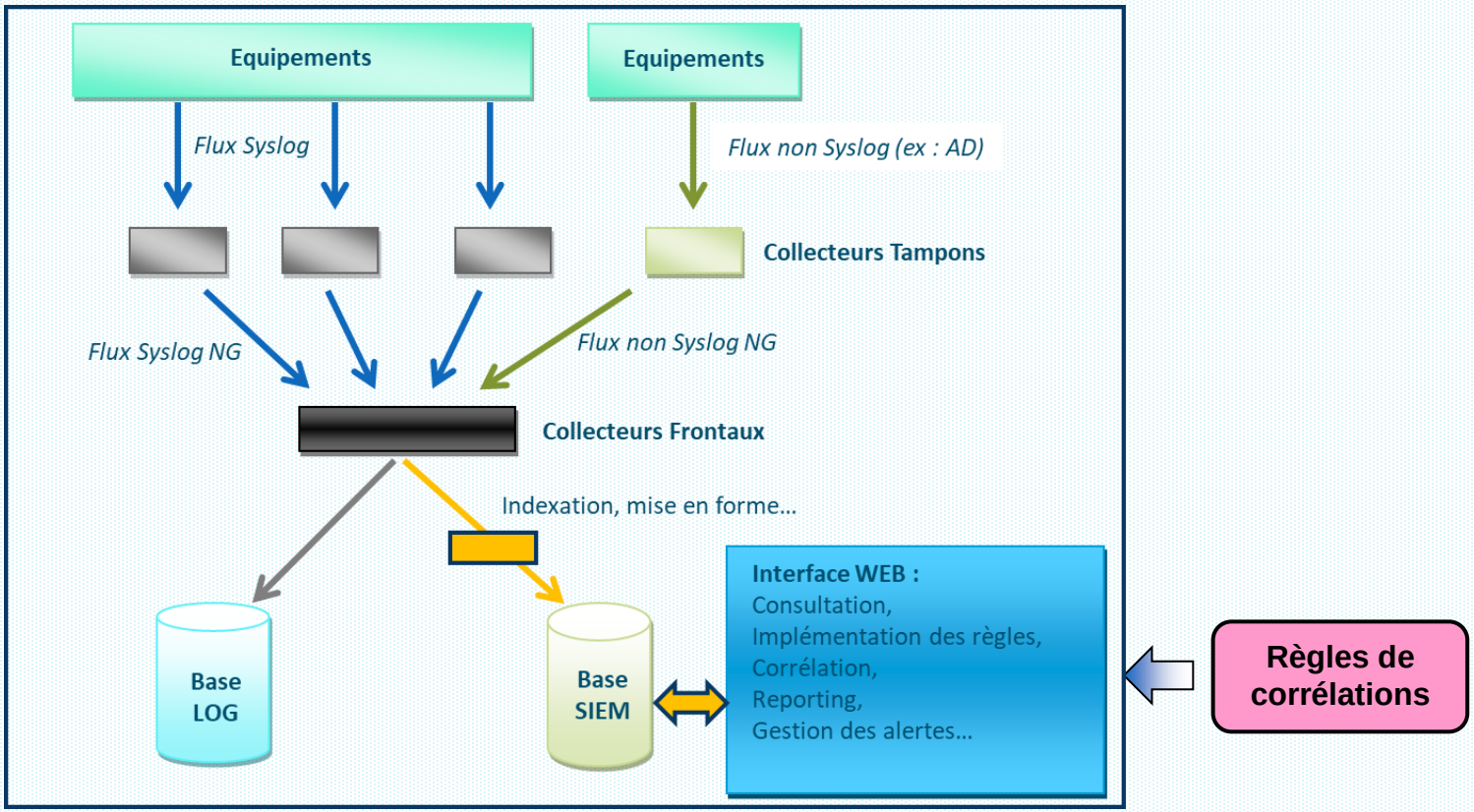
Les SIEM doivent permettent la gestion des enregistrements avec :

- la collecte
- l' analyse (la corrélation)
- l'alerte
- l'archivage sécurisé
- la preuve

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des enregistrements

Le SIEM



LES MESURES DE SECURITE OPERATIONNELLES

Gestion des enregistrements

Exemples d'événements « anormaux » / « suspects »

- Logins simultanés
- Flux non autorisés
- Activités hors horaires « normaux »
- Adresses IP non connues
- impossibilité de se connecter à la machine
- système de fichiers endommagé
- signature de binaires modifiée
- connexions ou activités inhabituelles
- activité importante
- modification intempestive du fichier de mots de passe, date de modification suspecte

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des incidents et surveillance

Type d'incidents de sécurité a détecter

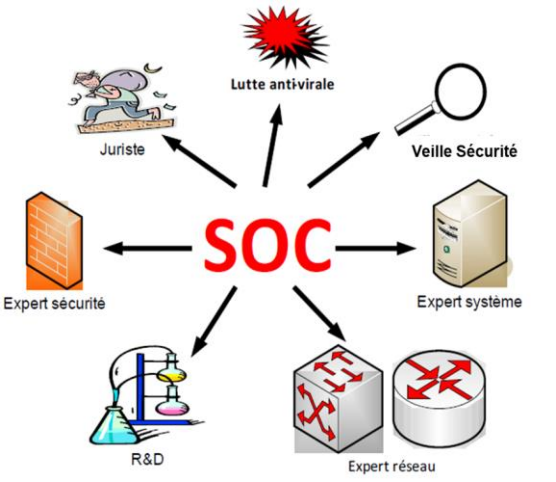
- exploitation d'une vulnérabilité
- élévation de privilèges
- exfiltration de données
- propagation virale
- mécanisme de persistance (APT)
- déni de service
- accès non autorisé à une ressource
- usurpation d'identité
- actions non conformes à la politique de sécurité

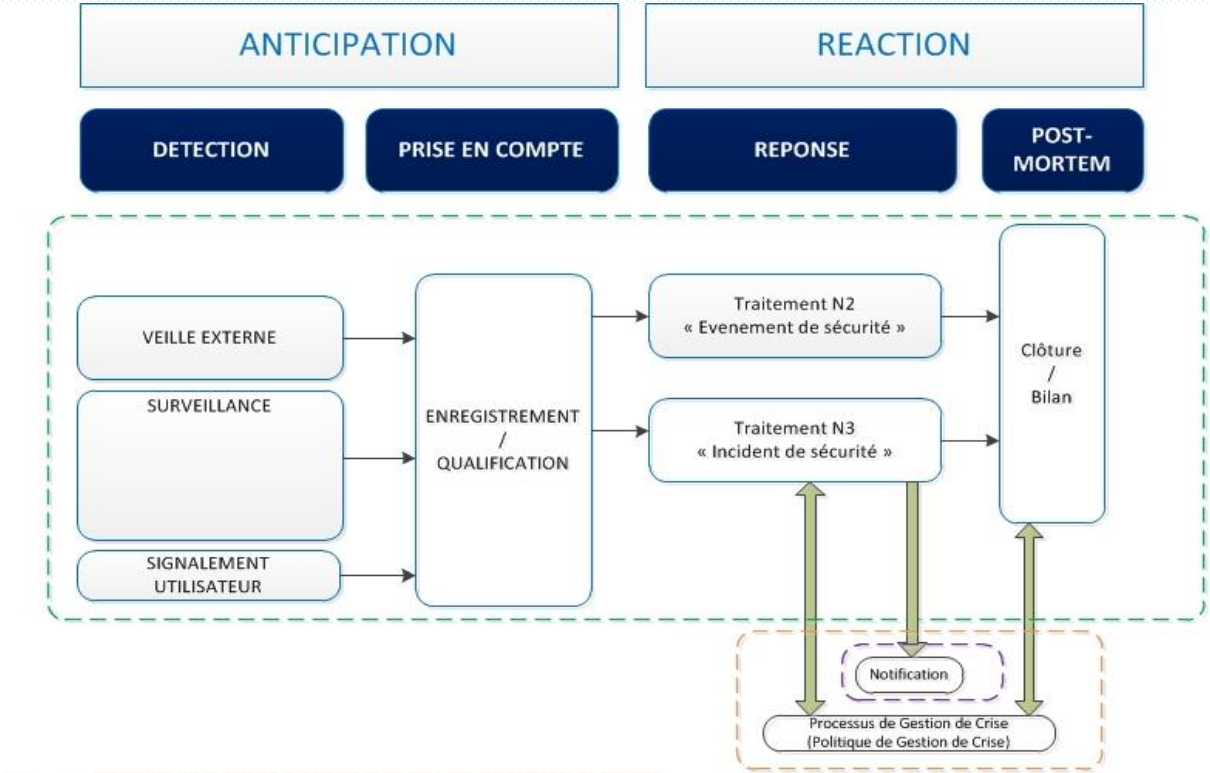
Source ANSSI / ISO 27035

LES MESURES DE SECURITE OPERATIONNELLES

Gestion des incidents et surveillance

Le SOC





LES MESURES DE SECURITE OPERATIONNELLES

QUIZZ

Une organisation a récemment installé un correctif de sécurité, qui a provoqué un arrêt du serveur de production. Pour réduire les risques que cela se reproduise de nouveau, il faudrait ?

- ❑ appliquer le correctif selon les notes documentaires du correctif.
- ❑ s'assurer qu'un bon processus de gestion du changement est place.
- ❑ évaluer correctement te correctif avant sa migration en production.
- ❑ approuver le correctif après une analyse des risques.

LES MESURES DE SECURITE OPERATIONNELLES

QUIZZ

Citer une bonne pratique de configuration de son antivirus :

- ❑ Avoir un antivirus d'un éditeur connu
- ❑ Avoir un jour installé un antivirus
- ❑ Tenir son antivirus à jour (mise à jour des signatures et du moteur)
- ❑ Interdire l'analyse antivirale à certains répertoires ou périphériques

LES MESURES DE SECURITE OPERATIONNELLES

QUIZZ

Sélectionner la (ou les) proposition(s) vraie(s) parmi les suivantes. Un antivirus :

- ❑ Peut détecter tous les virus et programmes malveillants, y compris ceux non découverts ;
- ❑ Protège de toutes les menaces ;
- ❑ Ne peut détecter que les virus qui sont connus dans sa base de signatures ;
- ❑ Doit être actif, et à jour pour être utile

LES MESURES DE SECURITE OPERATIONNELLES

QUIZZ

Mon antivirus me protège suffisamment. Je suis à l'abri de tous les virus, y compris des virus à paraitre non encore détectés (0-day) ?

- ❑ Vrai
- ❑ Faux

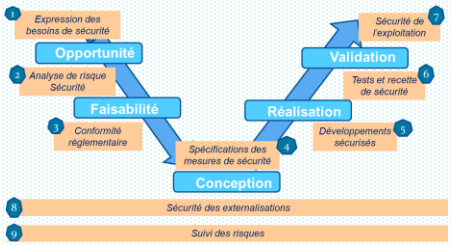
LES MESURES DE SECURITE OPERATIONNELLES

QUIZZ

Quel élément composant l'antivirus lui permet de détecter les codes malveillants connus ?

- ❑ Le nom de l'éditeur (Sophos, Trend Micro, McAfee. . .)
- ❑ La matrice de flux
- ❑ La base de données des signatures
- ❑ Le moteur de chiffrement

Les activités ISP



1. Besoin de sécurité
2. Analyse de risque
3. Les exigences réglementaires
4. Les spécifications des mesures de sécurité
5. La sécurisation des développements
6. Les tests et recettes de sécurité
7. La sécurisation de l'exploitation
8. **La sécurisation de la sous-traitance**
9. Le suivi des risques résiduels et induits

SÉCURISATION DE LA SOUS-TRAITANCE

Activités informatiques

- Introduction
- Démarche
- Outils
- Quizz

SÉCURISATION DE LA SOUS-TRAITANCE
Activités informatiques

Sous-traitance classique

- **L'hébergement des systèmes**
  Une entreprise fait héberger ses serveurs chez un hébergeur. Il lui loue des m² et des capacités techniques: climatisation, adduction électrique, accès réseau, sécurité physique,…
  L'entreprise dispose d'un accès à ses équipements qui lui appartiennent.

- **Les développements**
  Une entreprise fait développer une application par des équipes externes. Ces dernière vont lui livrer les sources et les exécutables selon des modalités à définir

- **Tierce Maintenance Applicative. (TMA)**
  L'entreprise confie la maintenance corrective (et souvent évolutive) des ses applications informatiques..

SÉCURISATION DE LA SOUS-TRAITANCE
Activités informatiques

Sous-traitance avec accès à distance

⇨ **MCO – Maintien en Conditions Opérationnelles**.

L'entreprise confie la maintenance corrective (et souvent évolutive) de ses équipements. Ce dernier s'assure de la maintenabilité des équipements :

- Mise à jour logiciel,
- Patch de sécurité
- Configuration

⇨ **Télé-administration /télé exploitation**

L'entreprise confie la gestion opérationnelle de ses équipements :

- Sauvegarde
- Supervision,

SÉCURISATION DE LA SOUS-TRAITANCE
Activités informatiques

Sous-traitance complète

⇨ **Télé-service**

Externalisation complète d'un service informatique, qui est opéré en externe (hébergement, application, exploitation, …).

Exemple : utilisation d'une application en mode SaaS

Modalité « extrême » : Le cloud computing.

l'entreprise va externaliser un service en recherchant une très forte fiabilité et une grande disponibilité des données, et sans visibilité du comment et du où.

SÉCURISATION DE LA SOUS-TRAITANCE
Activités informatiques

⇨ Une prestation externalisée engendre des vulnérabilités :

- Contrats souvent abusifs, avec clauses « standard »
- Définition de niveaux de service (SLA) sans pénalités
- Problématique de la protection des données personnelles : localisation, traçabilité, …
- Sous-traitance en cascade

Le recours a une prestation externalisée ne dégage pas l'entreprise de ses obligations (CNIL, Bâle II, CRBF,…) ni de ses responsabilités

SÉCURISATION DE LA SOUS-TRAITANCE
Activités informatiques

Accès au SI par des tiers

Impact

- Vol de 40 millions de données cartes bancaires et de 70 millions d'identités clients
- Plus de 250 M$ de coût pour la chaîne de magasins, une forte dégradation de l'image de marque

Mode opératoire

- Décembre 2013 : les attaquants cherchent à pénétrer le SI de Target en utilisant son sous-traitant gérant la climatisation : Fazio Mechanical Services
- Le portail de gestion des achats protégé par un mot de passe, facilement volé chez FMS, servant de porte d'entrée

SÉCURISATION DE LA SOUS-TRAITANCE
Activités informatiques

Application vulnérable fournie par un sous-traitant

Cause

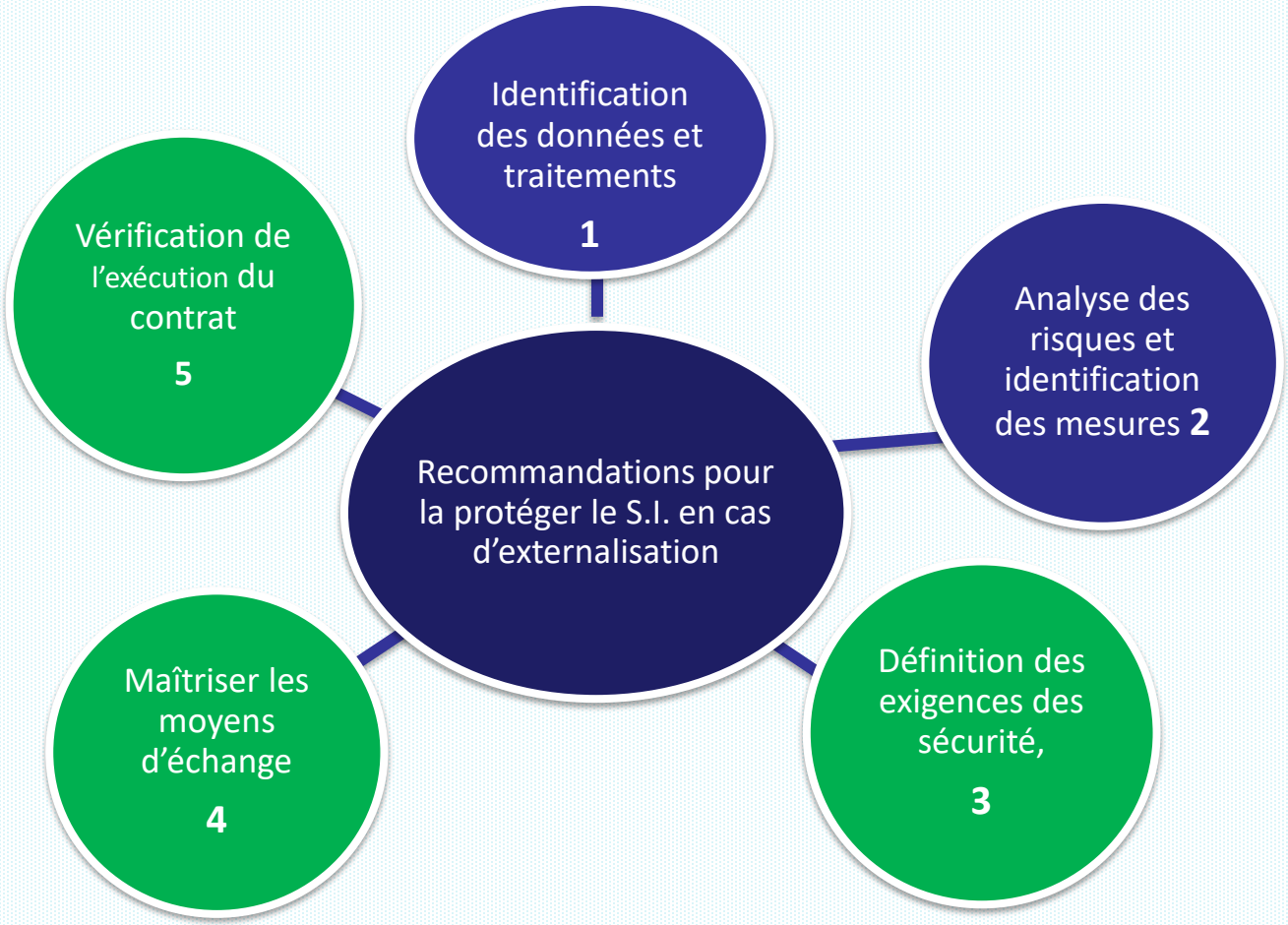
- La CNIL a infligé une amende de 100 000 euros à Darty pour un formulaire non-sécurisé accessible dans sa GRC de SAV sous Eptica

Amende de 100 000 euros

Mode opératoire

- Manque de sécurité dans un formulaire de saisie en ligne. Une vulnérabilité permet d'accéder à l'ensemble des formulaires et à des données des clients qui utilisent ce service.

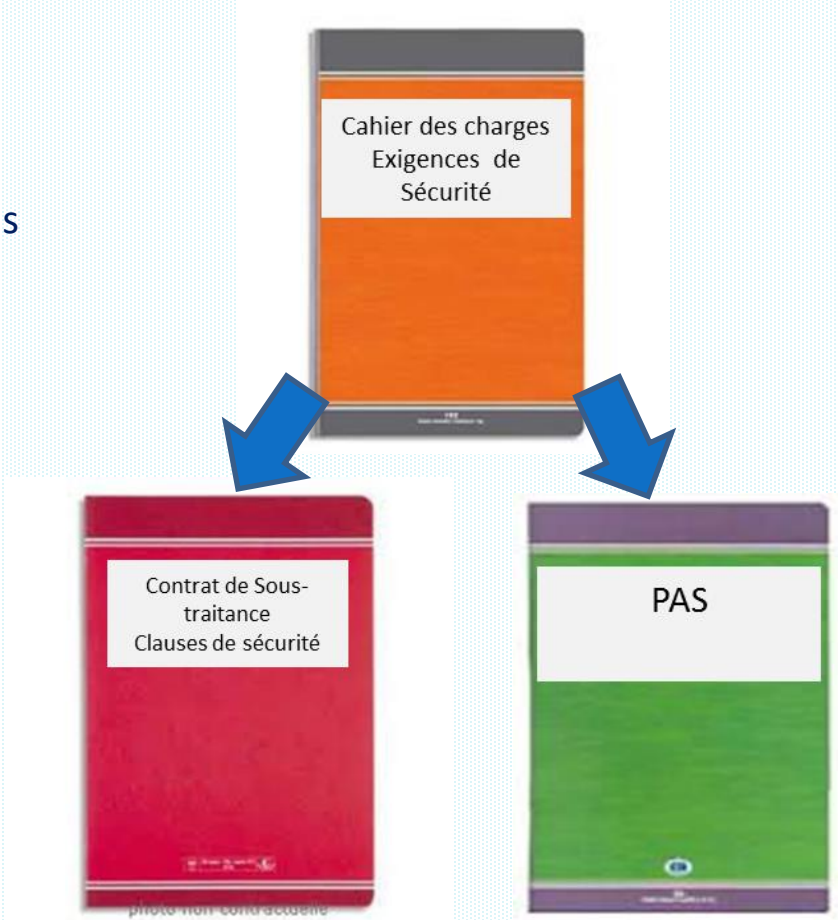
SÉCURISATION DE LA SOUS-TRAITANCE
Démarche



SÉCURISATION DE LA SOUS-TRAITANCE
Démarche

⇨ Définir ses propres exigences de sécurité:

- Intégrer ses propres exigences de sécurité dans le cahier des charges
- Rédiger les clauses contractuelles afférentes à la sécurité
- Elaborer **un Plan d'Assurance Sécurité (PAS)** conjointement avec le Prestataire
- Elaborer un PCA (si justifié)



SÉCURISATION DE LA SOUS-TRAITANCE
Outils

- Clauses réglementaires et/ou juridiques
  - Respect des principes français en matière de protection des DCP
  - Durée de conservation des données
  - Destruction ou restitution des données
  - Localisation des données
  - Respect de la réglementation métier
- Clauses de Sécurité et de confidentialité
  - Certification
  - Réversibilité
  - Traçabilité
  - Auditabilité
  - Continuité de service, sauvegarde et intégrité
  - Confidentialité
- Droit a l'audit

SÉCURISATION DE LA SOUS-TRAITANCE
Outils

Définit les exigences de sécurité vis-à-vis du tiers :

- ⇨ Exigences de sécurité pour réaliser la prestation
- ⇨ Exigences de protection de l'information
- ⇨ Exigences de communication d'incidents

Le PAS est annexé au contrat de sous-traitance et consolide les exigences de la société vis-à-vis du prestataire/partenaire

SÉCURISATION DE LA SOUS-TRAITANCE
Outils

Partie 1 : description de la prestation

SÉCURISATION DE LA SOUS-TRAITANCE

Outils

Partie 2

3	Plan d'Assurance Sécurité Système d'Information
3.1	**OS - Organisation de la sécurité de la prestation**
3.1.1	OS1 - Identification des acteurs et instances de pilotage Λ
3.1.2	OS2 - Documentation de sécurité Λ
3.1.3	OS3 - Indicateurs et enregistrements de sécurité Λ
3.1.4	OS4 - Sous-traitants ou autres tiers du prestataire/partenaire Λ
3.2	**SF - Sensibilisation et formation du personnel**
3.2.1	SF1 - Sensibilisation du personnel Λ
3.2.2	SF2 - Formation des développeurs
3.3	**PI - Protection de l'information et des ressources supports**
3.3.1	PI1 - Classification de l'informations et inventaire Λ
3.3.2	PI2 - Marquage des ressources supports Λ
3.3.3	PI3 - Protection des informations sensibles sous forme papier ou orale Λ
3.3.4	PI4 - Remise de ressources supports contenant des informations sensibles
3.3.5	PI5 - Partage des informations électroniques sensibles
3.3.6	PI6 - Protection logique du stockage des informations sensibles Λ
3.3.7	PI7 - Suppression des informations sensibles et des ressources supports Λ
3.3.8	PI8 - Gestion des mécanismes de chiffrement
3.4	**CA - Contrôle d'accès**
3.4.1	CA1 - Gestions des droits d'accès (accréditations) Λ
3.4.2	CA2 - Séparation des taches sensibles Λ
3.4.3	CA3 - Séparation des taches sensibles Λ
3.4.4	CA4 - Identification des accédant au SI Λ
3.4.5	CA5 - Mesures d'authentification Λ
3.4.6	CA6 - Règles de l'utilisation de mots de passe Λ
3.4.7	CA7 - Règles de gestion des accès distants au SI LBP Λ
3.4.8	CA8 - Traçage des accès distants Λ

SÉCURISATION DE LA SOUS-TRAITANCE
Outils

Partie 2

3.5	**SP - Sécurité des projets de développements**
3.5.1	SP1 - Organisation du développement sécurité
3.5.2	SP2 - Bonnes pratiques de développement
3.5.3	SP3 - Environnement de développement sécurisé
3.5.4	SP4 - Test de sécurité
3.5.5	SP5 - Recette de sécurité des applications
3.5.6	SP6 - Traitement des vulnérabilités des produits fournis
3.6	**GI - Gestion des incidents SSI**
3.6.1	GI1 - Activités de la gestion des incidents SSI Λ
3.6.2	GI2 - Processus d'alerte des incidents Λ
3.7	**GE - Gestion de l'exploitation SSI**
3.7.1	GE1 - Isolement des plates-formes
3.7.2	GE2 - Pollutions informatiques Λ
3.7.3	GE3 - Configuration et durcissement des applications et systèmes d'exploitation
3.7.4	GE4 - Configuration des équipements et sécurité logique de niveau de réseau
3.7.5	GE5 - Maintien du niveau de sécurité des équipements et logiciels Λ
3.7.6	GE6 - Sauvegarde et restauration
3.7.7	GE7 - Politique concernant les données de production Λ
3.7.8	GE8 - Journalisation / Collecte des traces
3.7.9	GE9 - Archivage
3.8	**AS - Audits de sécurité programmés Λ**
3.9	**CP - Contrôle permanent de sécurité**

SÉCURISATION DE LA SOUS-TRAITANCE
Quizz

Lequel des points suivants est le plus important pour valider un processus de sélection d'un fournisseur :

- ❑ Le fournisseur choisi propose le plus bas prix.
- ❑ Le fournisseur choisi propose le prix le plus élevé.
- ❑ Le fournisseur a été choisi avant la définition des critères de sélection.
- ❑ Certains fournisseurs n'ont pas répondu à la demande d'offre.

SÉCURISATION DE LA SOUS-TRAITANCE
Quizz

En ce qui concerne l'externalisation des services IT, laquelle de conditions suivantes devraient avoir de la plus grande importance ?

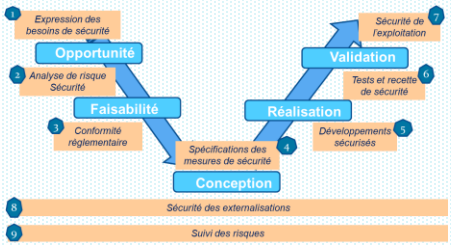
- Les activités externalisées sont au cœur des activités métiers et fournissent un avantage appréciable à l'organisation.
- La renégociation périodique est spécifiée dans le contrat d'externalisation.
- Les activités semblables sont externalisées à plus d'un fournisseur.

SÉCURISATION DE LA SOUS-TRAITANCE
Quizz

Un auditeur SI examine le nouveau contrat de sous-traitance d'un fournisseur de services IT. Quel élément manquant doit le préoccuper le PLUS ?

- Une clause assurant un « droit à l'audit »
- Une clause définissant des paiements de pénalité pour performances pauvres
- Des exigences en matière de niveau de service
- Une clause à propos de la limitation de fiabilité du fournisseur

Les activités ISP



1. Besoin de sécurité
2. Analyse de risque
3. Les exigences réglementaires
4. Les spécifications des mesures de sécurité
5. La sécurisation des développements
6. Les tests et recettes de sécurité
7. La sécurisation de l'exploitation
8. La sécurisation de la sous-traitance
9. **Le suivi des risques résiduels et induits**

SUIVI DES RISQUES RÉSIDUELS
La Théorie

Analyse de risque et besoins

Risques potentiels

Risques maîtrisé

Risques Résiduels

Livraison du projet

Risques potentiels

Risques maîtrisé

Risques Résiduels

SUIVI DES RISQUES RÉSIDUELS

La Pratique

Analyse de risque et besoins

Risques potentiels

Risques maîtrisé

Risques Résiduels

Livraison du projet

Risques potentiels

Risques maîtrisé

Risques Résiduels

SUIVI DES RISQUES RÉSIDUELS

Attention aux risques résiduels qui persistent …