

RÉFÉRENTIELS

Atelier n° 4: sécurité

21 avril 2016

Christophe JODRY - Cédric BERTRAND

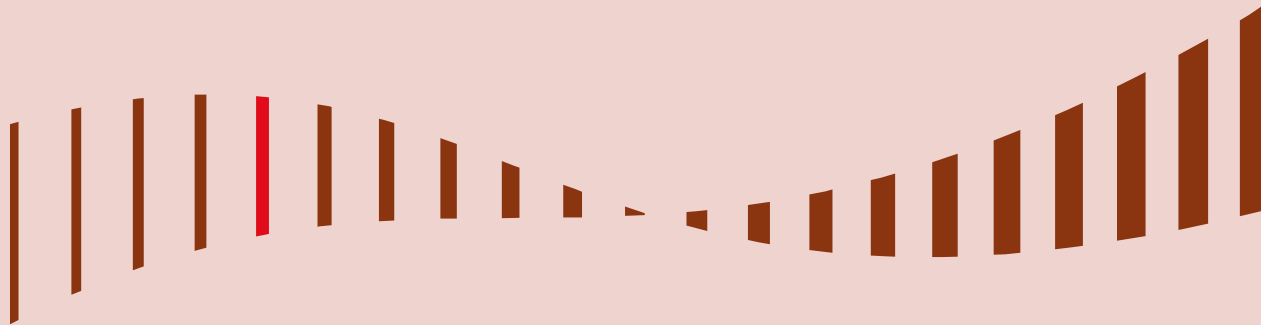
Atelier n° 4: sécurité

Sommaire

- A. Fondamentaux en SSI
- B. Etude sécurité en maison et centre de santé
- C. PGSSI-S: principes et focus sur l'authentification
- D. IGC Santé

E. Sécurité opérationnelle

Concepts fondamentaux en SSI



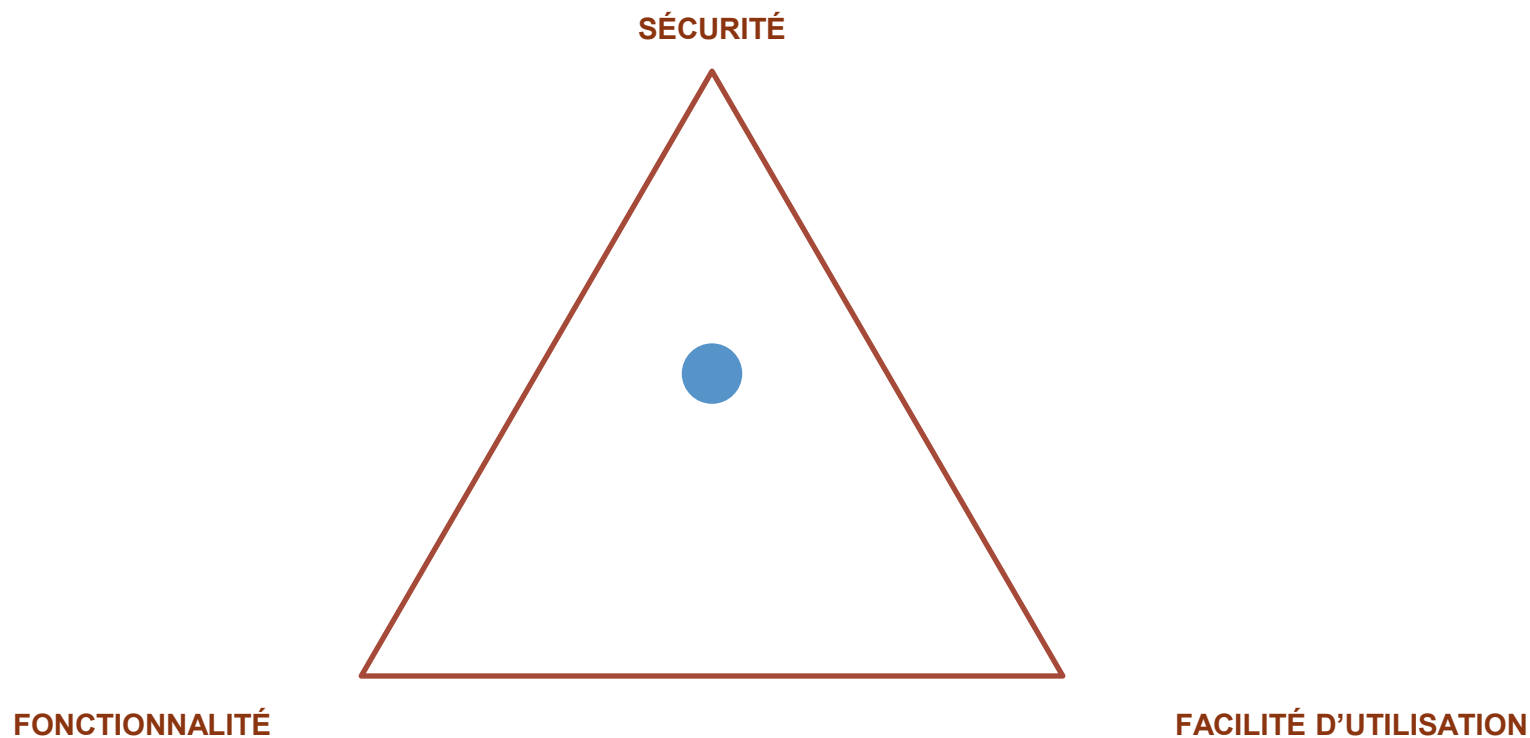
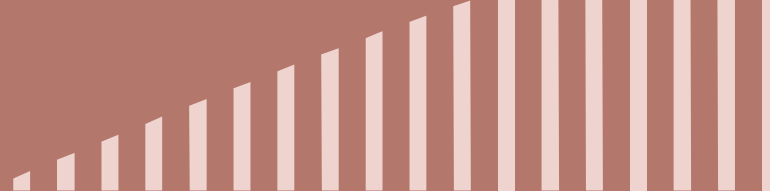
UN SI?

Le **système d'information** (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information. (Wikipédia)

Deux sous-systèmes:

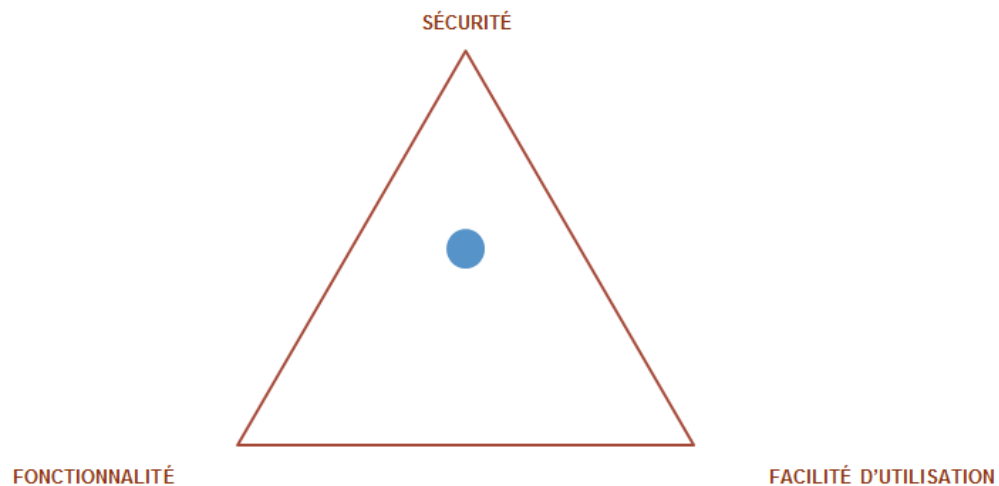
- un sous-système social: structure organisationnelle et personnes concernées par le SI;
- Un sous-système technique: technologies et processus concernés par le SI.

SSI: d'abord du bon sens



Mettons en application

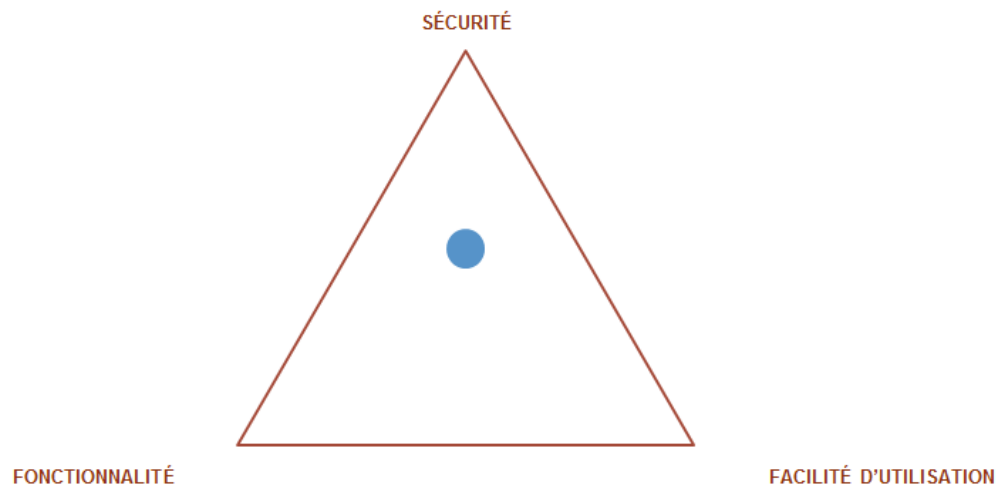
LE TRIANGLE DE LA SÉCURITÉ



L'exemple du logiciel

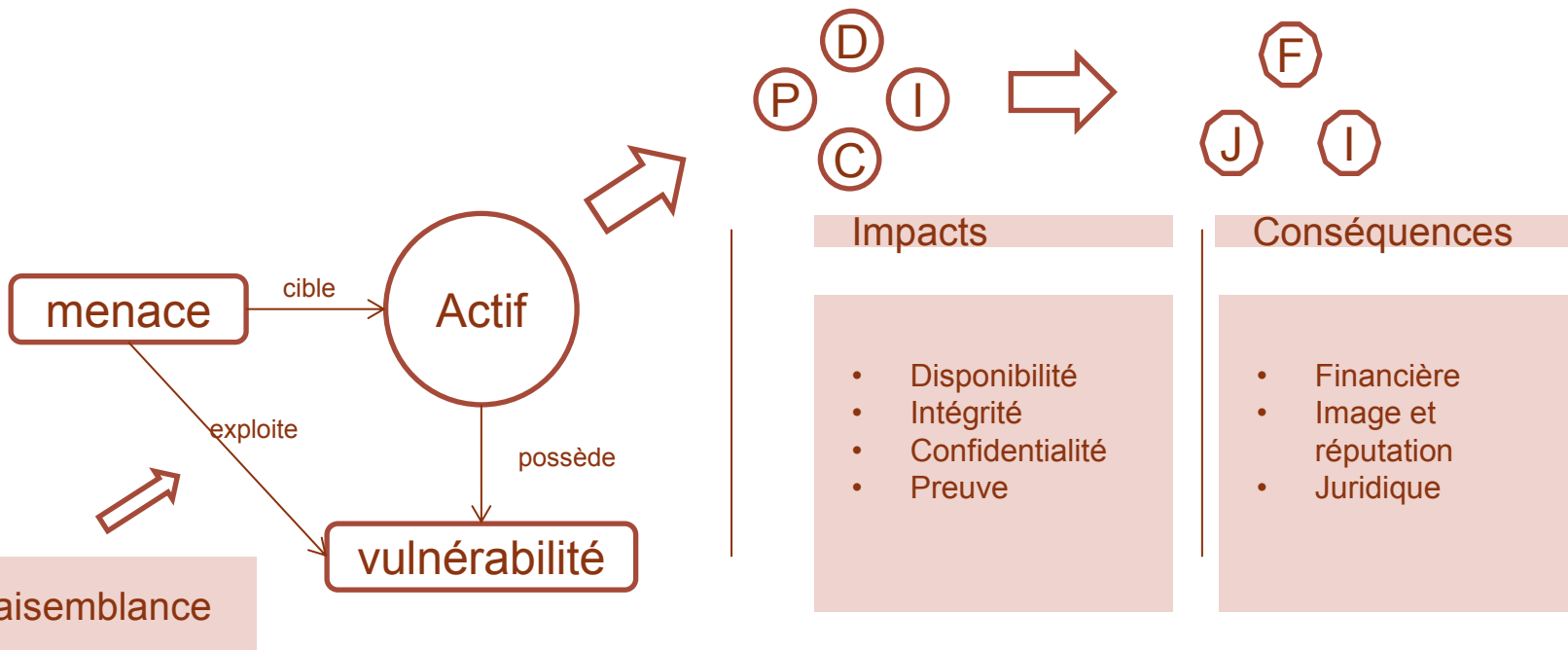
Mettons en application

LE TRIANGLE DE LA SÉCURITÉ



D'autres exemples?

ANALYSER LES RISQUES. COMMENT FAIRE?

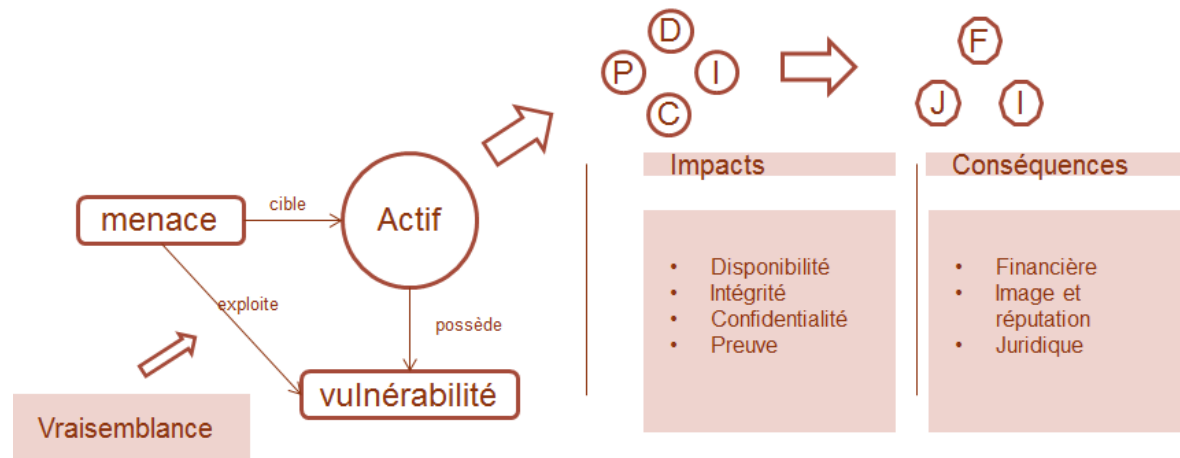
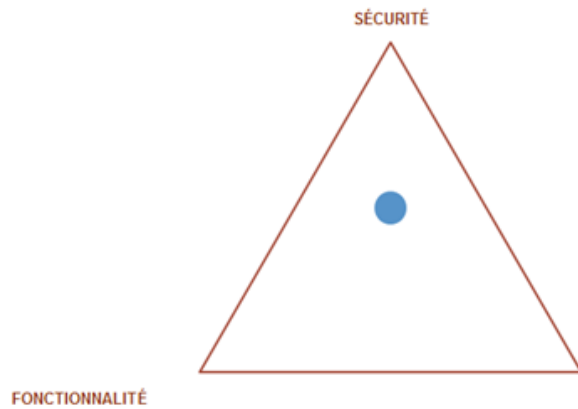


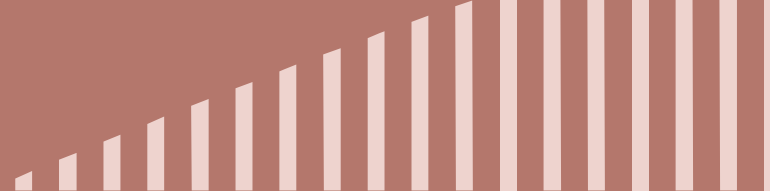
Menaces ou vulnérabilités?

- 1/ Lignes de communication non protégées: **V**
- 2 /Erreur de l'équipe opérationnelle: **M**
- 3/ Défaut de maintenance du logiciel: **V**
- 4/ Erreur d'utilisation: **M**
- 5/ Politique de mot de passe faible: **V**
- 6/ Transfert du mot de passe en clair: **V**
- 7/ Absences de mises à jour de sécurité: **V**
- 8/ Infection virale: **M**

- 9/ Jeu de règles de filtrage IP laxiste: **V**
- 10/ Corruption de données: **M**
- 11/ Présence en zone inondable: **V**
- 12/ Crue: **M**
- 13/ Espionnage: **M**
- 14/ Abus de droit: **M**
- 15/ Absence de procédure de gestion du changement: **V**
- 16/ Portabilité: **V**
- 17/ Incendie: **M**

SSI: bon sens et gestion des risques





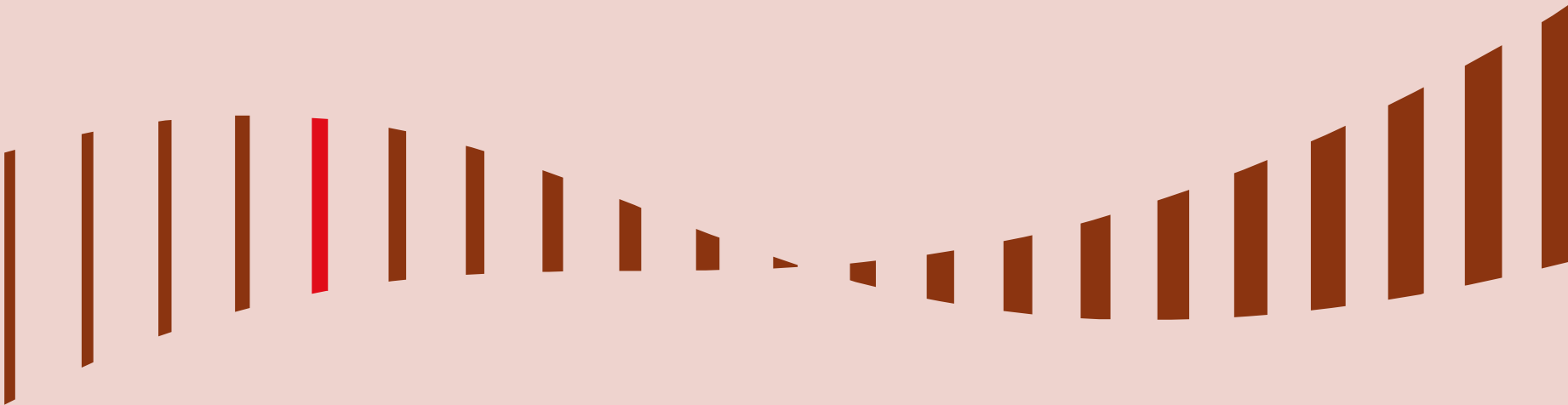
NOUS PENSONS DÉSORMAIS DE MANIÈRE IDENTIQUE ET AVONS LE MÊME LANGAGE.

NOUS POUVONS DONC CONTINUER.

RÉFÉRENTIELS

Les risques SSI en maison et centre de santé

Retour de l'étude réalisée en février-mars 2016



Présentation de l'étude PGSSI-S en maison et centre de santé

Une étude sur l'applicabilité de la PGSSI-S en maison et centre de santé a eu lieu de février à mars 2016.

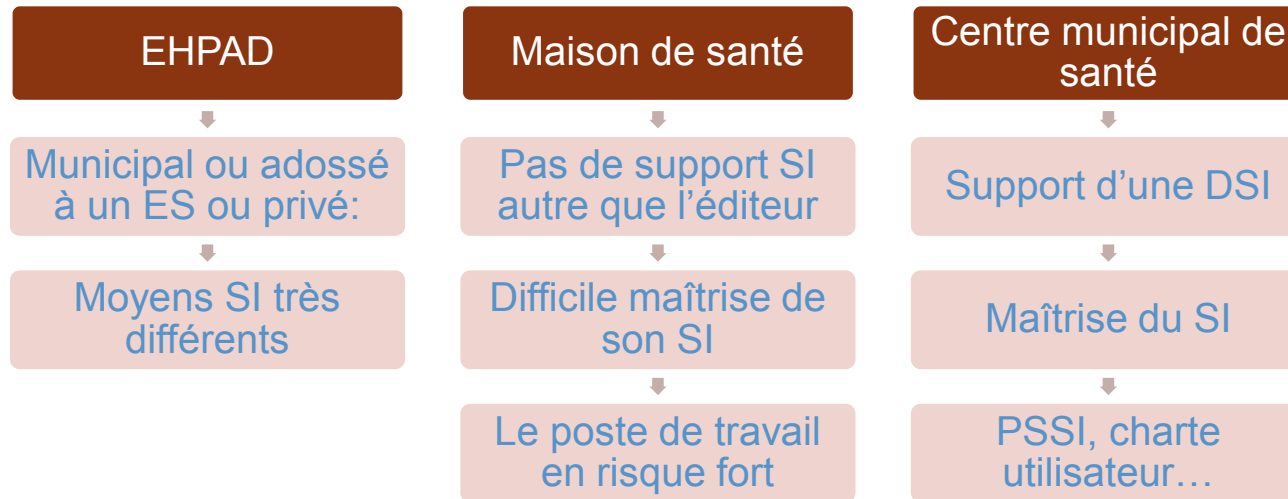
Objectif

- **Confronter certains guides PGSSI-S à la réalité terrain du contexte 2.**
- **Liste des documents:**
 - **Guide d'élaboration d'une PSSI pour les non-experts**
 - **Guide de gestion des habilitations**
- **structures sélectionnées par la Direction des Affaires Médicales de l'ASIP Santé.**

Méthode

- **2h à 2h30 d'entretien (difficile de mobiliser plus les structures);**
- **pour éviter aux structures visitées le sentiment d'être auditées, l'interlocuteur de l'ASIP Santé se présente plutôt comme un avant-vente avec ses produits « PGSSI-S » ;**
- **3 temps dans l'entretien:**
 - **prise de contexte;**
 - **échange sur le guide habilitation;**
 - **échange sur le memento PSSI et charte utilisateur.**

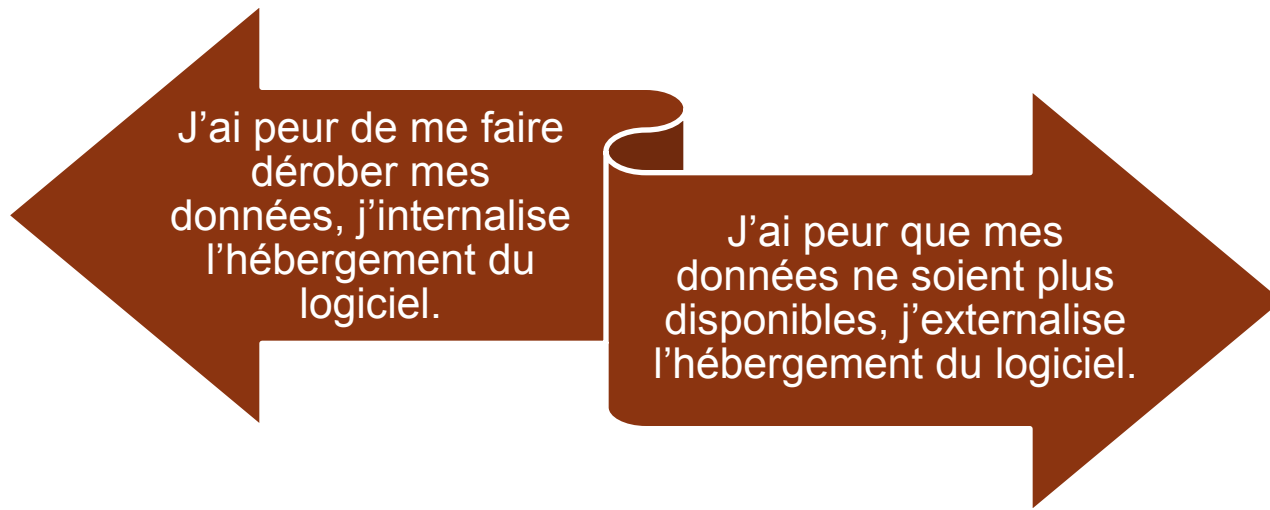
3 niveaux de maturité SSI ?

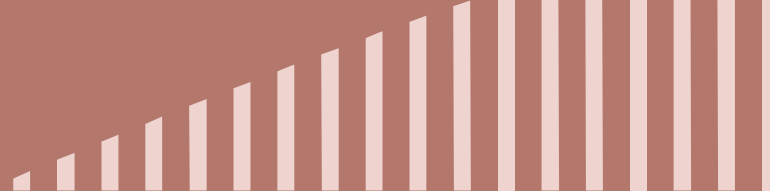


Votre logiciel au centre du SI

Le logiciel est la brique essentielle du Système d'Information de ces structures.

Aucun autre actif n'a la même valeur.





Les risques liés à l'externalisation

?

Les risques liés à l'internalisation

?

C'est l'histoire d'un médecin coordinateur en EHPAD qui avait laissé ses clés sur une table basse...

Et l'intégrité?



Des craintes sur la disponibilité et sur la confidentialité. Mais l'intégrité des données?

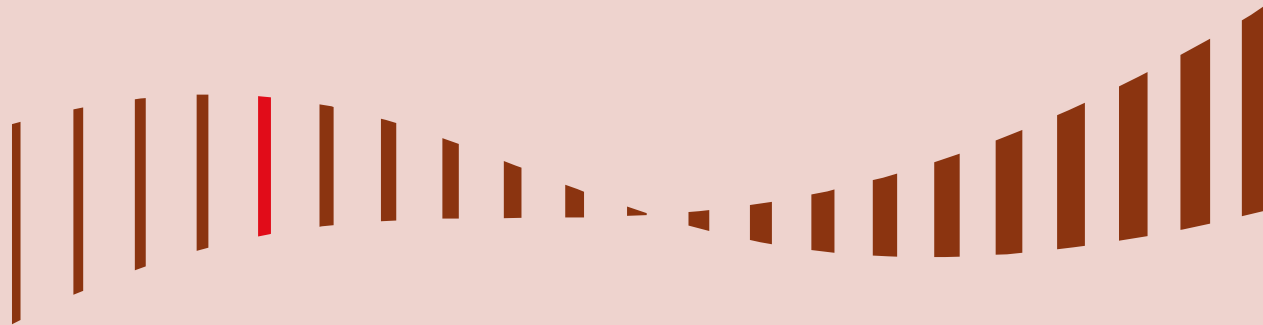
C'est l'histoire de milliers de Français qui en se connectant au site des impôts en 2013 ont pu consulté le dossier d'un autre citoyen...mais pas le leur.

C'est l'histoire d'un oncologue qui n'a pas le bon nombre d'heures d'exposition aux rayons depuis le début du traitement de son patient...

RÉFÉRENTIELS

PGSSI-S

PGSSI-S: Principes



Définitions

La PGSSI-S n'est pas une politique de sécurité.

La PGSSI-S est un corpus documentaire.

La PGSSI-S ne garantit pas un niveau de sécurité.

La PGSSI-S organise la sécurité.

Quels sont les textes auxquels vous êtes soumis?

- **LOI INFORMATIQUE ET LIBERTE**
- **CODE DE LA SANTE PUBLIQUE**
incluant la nouvelle loi santé promulguée le 26 janvier.

- **RGS de l'ANSSI**
- **PSSI-E et PSSI-MCAS**
- **PGSSI-S**

Impacts de la nouvelle loi santé sur la sécurité:

- **Usage du NIR pour identifier les patients (travaux en cours)**
- **Déclaration d'incident sécurité (travaux en cours)**

Le cadre normatif et juridique

Dans le cadre d'un développement de solution e-santé, je souhaitais prendre contact avec l'ASIP pour connaître les règles que doit respecter mon application (aussi bien web que apps) afin d'être aux "normes".

Si une partie de vos futurs clients sont des établissements publics du secteur santé, vos produits devront être conformes à la Politique de sécurité des Systèmes d'information de l'Etat (PSSIE) et de la Politique de Sécurité des Systèmes d'Information pour les Ministères en Charge des Affaires Sociales (PSSI-MCAS). La PGSSIS-S est la déclinaison opérationnelle de ces deux référentiels.

PSSI – MCAS : Politique de Sécurité des Systèmes d'Information pour les Ministères en Charge des Affaires Sociales

<http://www.legifrance.gouv.fr/eli/arrete/2015/10/1/AFSZ1523362A/jo>

PSSIE - Politique de Sécurité des Systèmes d'Information de l'Etat (ANSSI). http://www.ssi.gouv.fr/uploads/IMG/pdf/pssie_anssi.pdf

De ce fait, je vous invite à prendre connaissance des guides de la PGSSIS-S, en commençant notamment par les référentiels d'identification et d'authentification des acteurs de santé, ainsi que le référentiels d'imputabilité et le guide accès tiers.

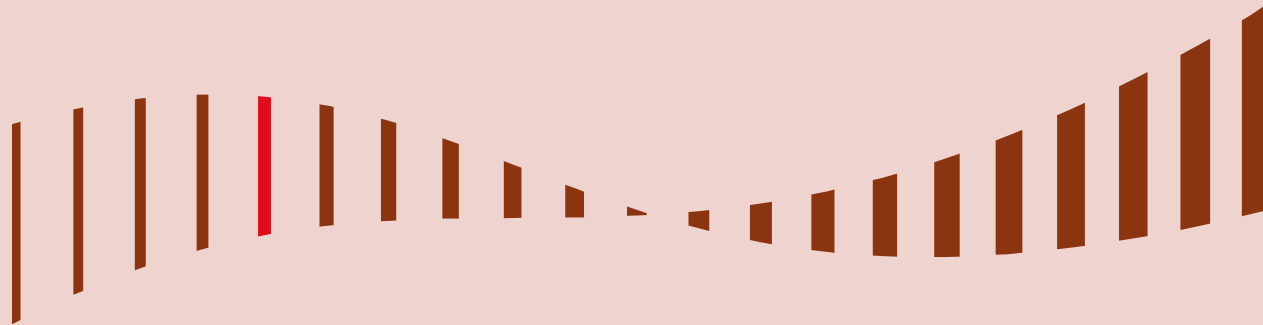
<http://esante.gouv.fr/pgssi-s/espace-publication>

Il est de la responsabilité de l'hébergeur données de santé de reporter sur ses clients l'obligation d'un code source sécurisé. Ce sera donc le cas de votre futur hébergeur qui vous imposera par une clause au contrat un développement dans les règles de l'art (le référentiel Owasp pouvant représenter les règles de l'art dans votre cas de figure par exemple).

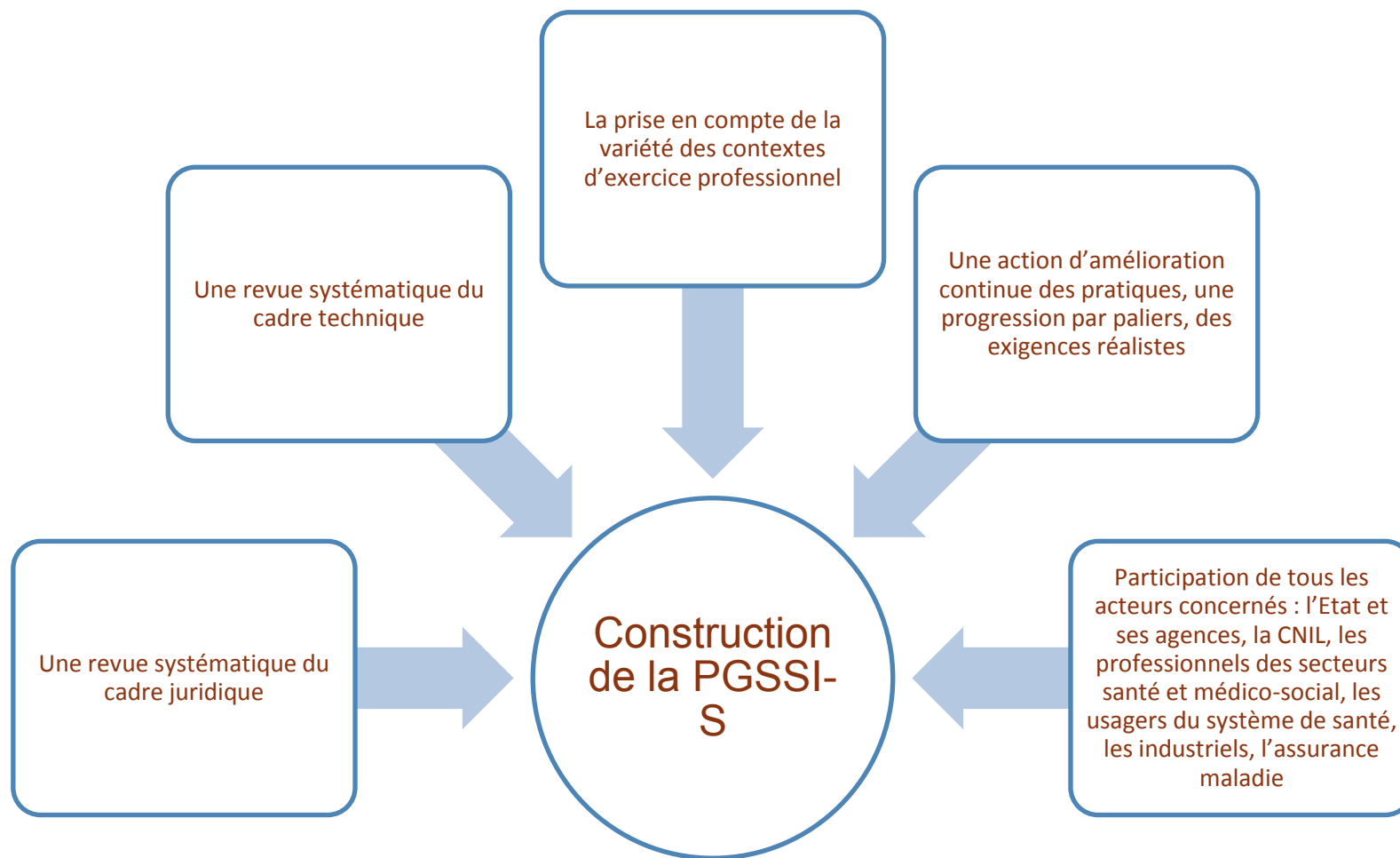
Enfin, vos applications traitant des données personnelles, vous êtes soumis aux règles émises par la CNIL, notamment le guide nommé "la sécurité des données personnelles". Notamment la fiche 16 concernant le développement.

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf

Démarche de construction de la PGSSI-S



Démarche de construction de la PGSSI-S



GT

ROLE

- Contribution et relecture sur les documents initiés par l'ASIP
- Proposition de nouveaux documents

COMPOSITION :

- ASIP Santé
- Ministère (DSSIS)
- CNAM
- CNIL
- AFHADS
- LESSIS
- FEHAP
- FEIMA
- SYNTEC
- Représentants ES, GCS, Université, CHU etc...

• ...

Comité de pilotage

ROLE:

- Orientations stratégiques
- Validation des travaux des GT pour la concertation

COMPOSITION:

- Ministère (DSSIS)
- Ministère (DGOS, DGS)
- ASIP Santé
- CNL
- CNAM

Comité de concertation

ROLE:

- Validation pour passage en concertation privée et publique

COMPOSITION:

- Ministère (DSSIS)
- ASIP Santé
- CNAM
- CNIL
- AFHADS
- FEIMA
- FEHAP
- SYNTEC
- Représentants ES
- ...

GT

ROLE

- Contribution et relecture sur les documents initiés par l'ASIP
- Proposition de nouveaux documents

COMPOSITION :

- ASIP Santé
- Ministère (DSSIS)
- CNAM
- CNIL
- **AFHADS**
- **LESSIS**
- **FEHAP**
- **FEIMA**
- **SYNTEC**
- Représentants ES, GCS, Université, CHU etc

Comité de pilotage

ROLE:

- Orientations stratégiques
- Validation des travaux des GT pour la concertation

COMPOSITION:

- Ministère (DSSIS)
- Ministère (DGOS, DGS)
- ASIP Santé
- CNL
- CNAM

Comité de concertation

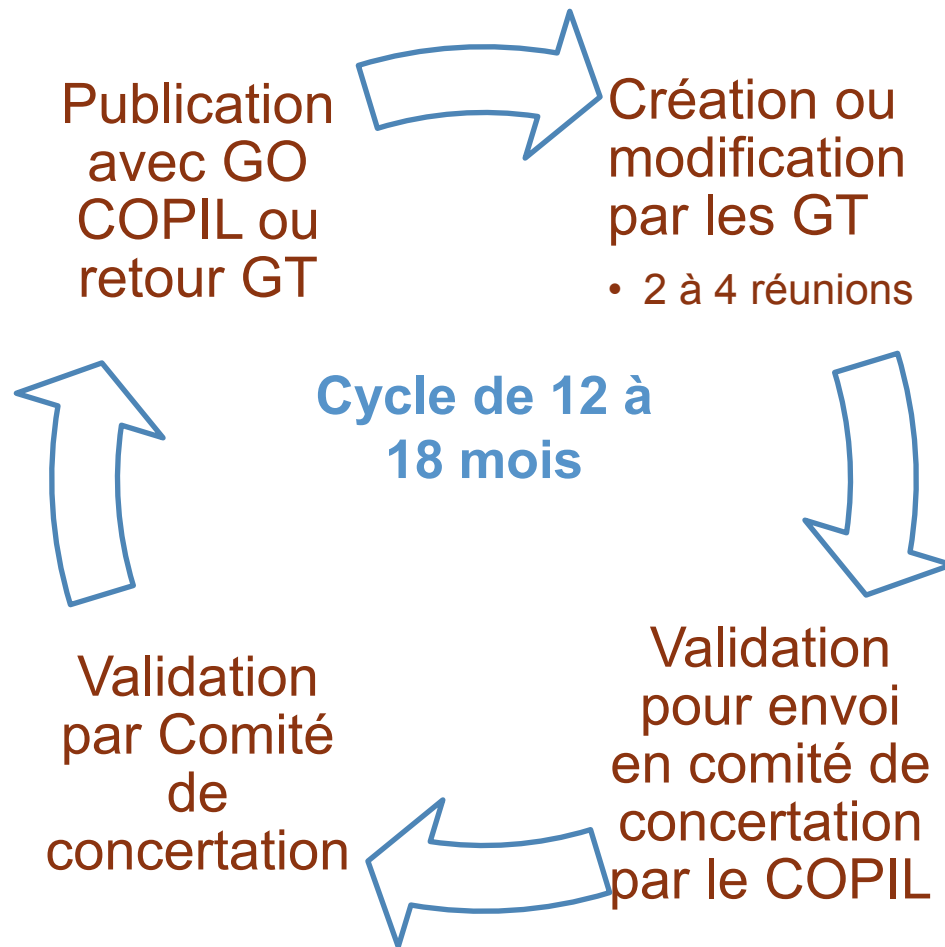
ROLE:

- Validation pour passage en concertation privée et publique

COMPOSITION:

- Ministère (DSSIS)
- ASIP Santé
- CNAM
- CNIL
- **AFHADS**
- **FEIMA**
- **FEHAP**
- **SYNTEC**
- Représentants ES
- ...

Cycle de création d'un document



La prochaine concertation début mai: donner votre avis!

**PGSSI-S - Politique générale de sécurité des systèmes
d'information de santé**
**Guide pratique Mécanismes de protection de l'intégrité
des données stockées**

V 0.3

**PGSSI-S - Politique générale de sécurité des systèmes
d'information de santé**
Guide Gestion des habilitations d'accès au SI

V 0.2

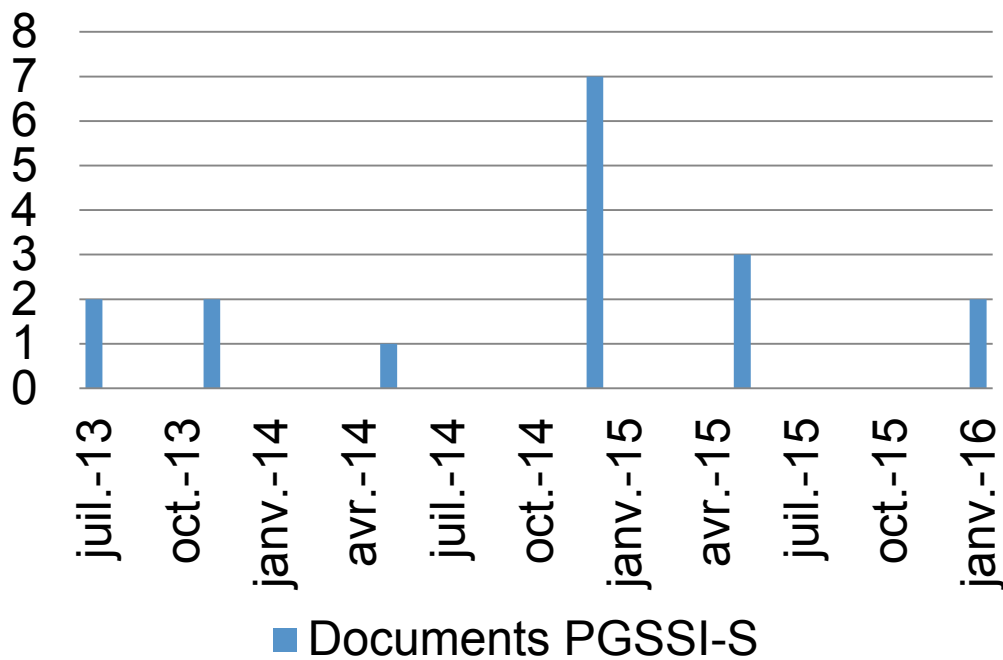
Les publications

Le rythme des publications

17 documents

575 pages

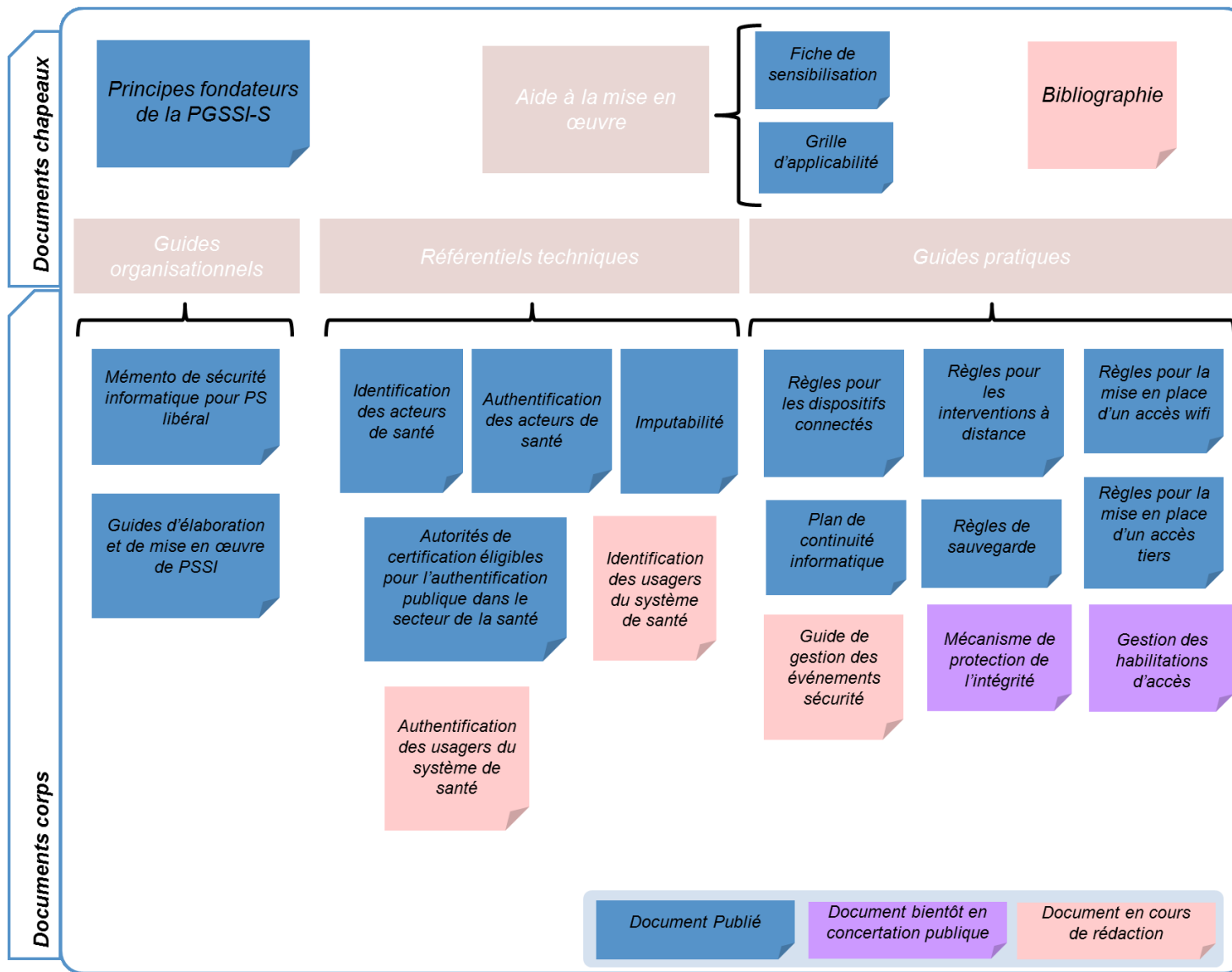
CHRONOLOGIE DE PUBLICATION



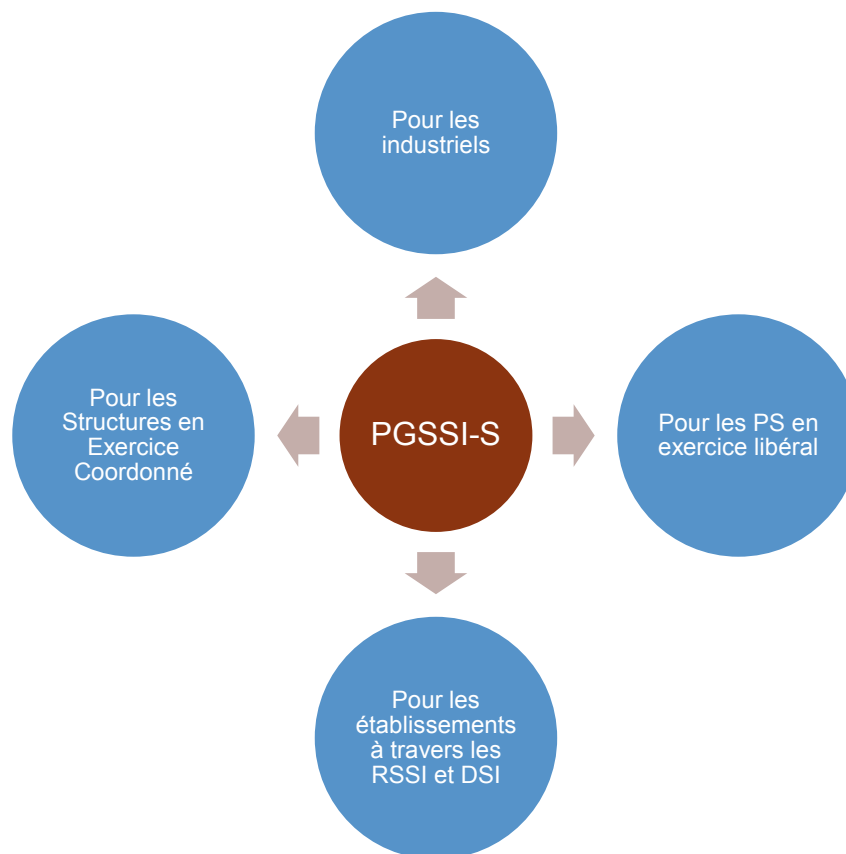
Les publications

Titre	pages	Date 1ère publication	Date dernière publication	type
Principes fondateurs	20	juil-13	juil-13	Chapeau
Règles pour les dispositifs connectés	20	nov-13	nov-13	Pratique
Règles pour la mise en place d'un accès wifi	12	mai-14	mai-14	Pratique
Règles pour les interventions à distance sur les Systèmes d'Information de Santé	20	déc-14	déc-14	Pratique
Destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé (SIS)	16	déc-14	déc-14	Pratique
Règles de sauvegarde des Systèmes d'Information de Santé	20	déc-14	déc-14	Pratique
Authentification des acteurs de santé	28	juil-13	déc-14	Référentiel
Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé	7	déc-14	déc-14	Référentiel
Imputabilité	32	déc-14	déc-14	Référentiel
Identification des acteurs sanitaires et médico-sociaux	24	déc-14	déc-14	Référentiel
Guide d'élaboration et de mise en œuvre de PSSI (et canevas de PSSI et de PAS associés)	270	mai-15	mai-15	organisationnel
Grille d'applicabilité des référentiels de la PGSSI-S	12	mai-15	mai-15	Hors Corpus
Fiche de sensibilisation à la sécurité des systèmes d'information de santé	4	mai-15	mai-15	Hors Corpus
Règles pour la mise en place d'un accès tiers	25	janv-16	janv-16	Pratique
Système d'Information et Plan de Continuité Informatique	45	janv-16	janv-16	Pratique

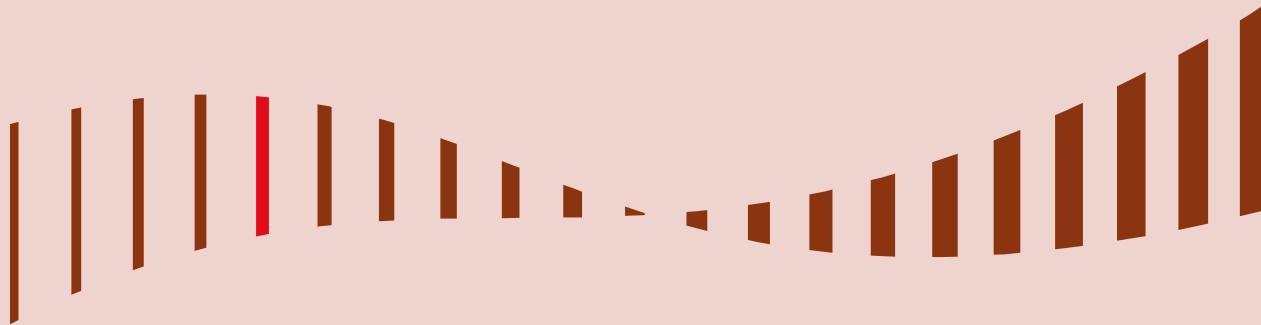
Les publications



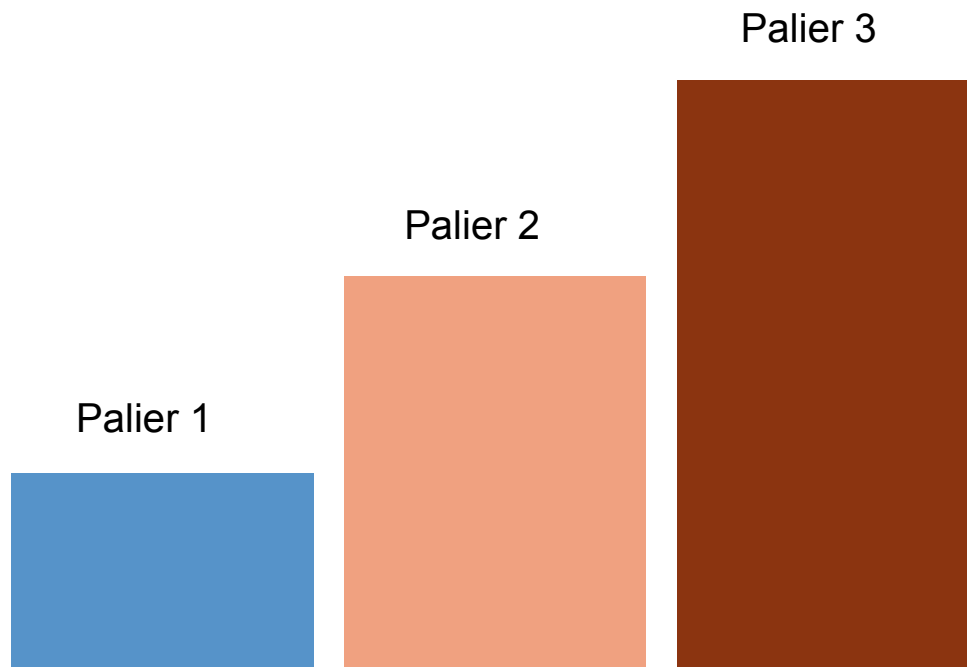
Un corpus documentaire de référence à destination de tous les acteurs du secteur sanitaire et, à terme, du secteur social:



Des mises en œuvre différentes pour des contextes différents



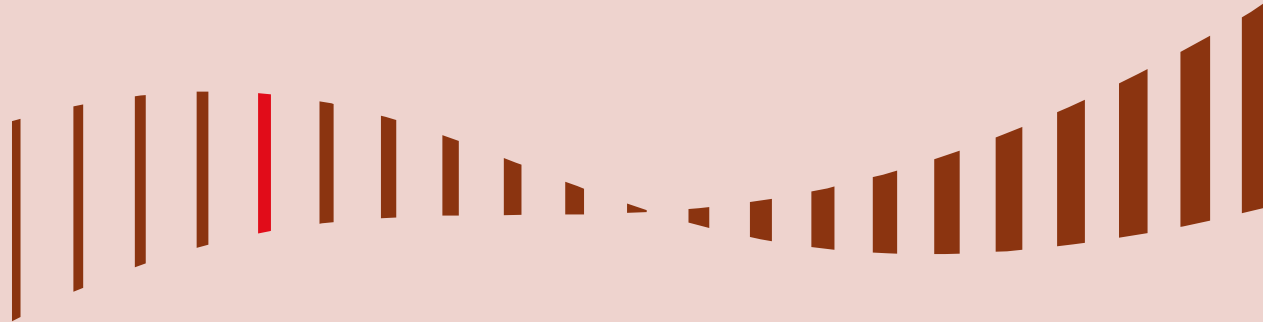
Pour une grande partie des guides et référentiels, il est proposé une trajectoire en 3 paliers.



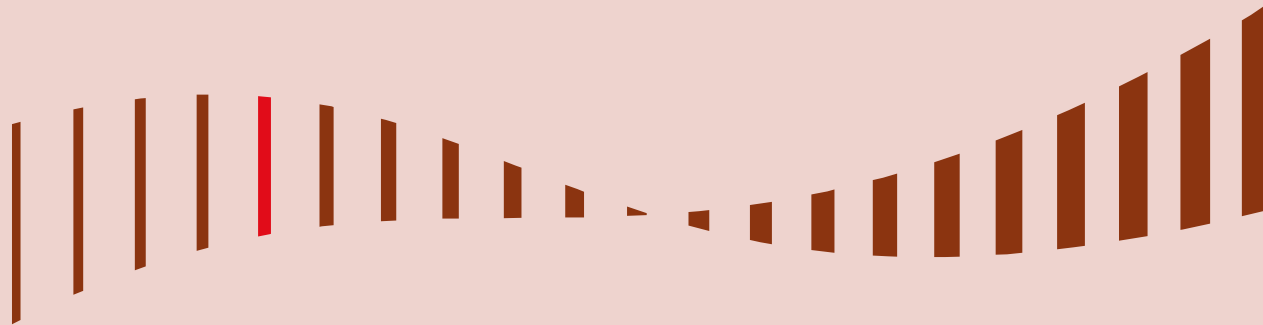
Des contextes dissociés

CONTEXTE	EXEMPLES
<u>Contexte 1</u> : exercice individuel pour lequel les accès au système d'information sont sous le contrôle du professionnel de santé	Médecin en exercice individuel
<u>Contexte 2</u> : exercice collectif pour lequel les accès au système d'information sont chacun sous le contrôle d'un utilisateur	cabinet , Maison de santé
<u>Contexte 3</u> : exercice collectif pour lequel au moins une partie du système d'information est mutualisée entre plusieurs utilisateurs	Etablissement de santé, centres municipaux de santé
<u>Contexte 4</u> : téléservices avec enregistrement préalable des utilisateurs	Mode SAAS
<u>Contexte 5</u> : téléservices sans enregistrement préalable des utilisateurs	DMP
<u>Contexte 6</u> : documents de santé électroniques quand ils sont amenés à sortir du SIS producteur pour échange ou mise en partage	Laboratoire

Les référentiels prochainement opposables



Identification des professionnels de santé



Guide identification des professionnels de santé

Date de publication:

Type de documents:

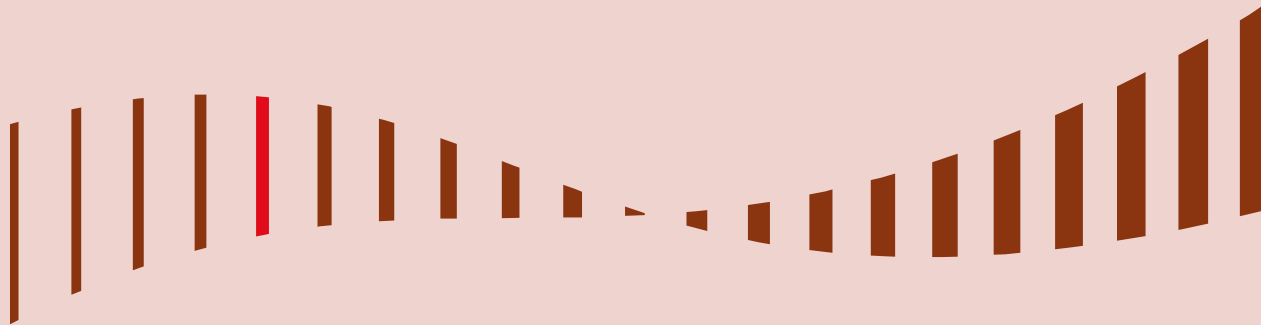
Périmètre d'application:

Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓	✓	✓	✓	✓
Commentaire						
La présente version du référentiel est applicable dans l'ensemble des domaines sanitaire et médico-social, dans la limite des procédures d'enregistrement existantes ¹ .						

SOMMAIRE

1. OBJET DU DOCUMENT.....	5
2. PÉRIMÈTRE D'APPLICATION DU RÉFÉRENTIEL	7
3. ENJEUX DE L'IDENTIFICATION DES ACTEURS SANITAIRES ET MÉDICO-SOCIAUX.....	8
4. DÉFINITIONS	9
4.1. Référentiels d'identité nationaux	
4.2. Identifiant opérationnel de portée nationale	
4.3. Autorité d'Enregistrement	
4.4. Gestionnaire de référentiel	
4.5. Identifiant	
4.6. Autorité d'affectation	
4.7. Type d'identifiant	
4.8. Données d'identité	
4.9. Traits d'identité	
4.10. Modes d'identification des personnes physiques	
5. PALIERS DE L'IDENTIFICATION DES ACTEURS SANITAIRES ET MÉDICO-SOCIAUX.....	12
5.1. Paliers de l'identification des personnes physiques	
5.2. Paliers de l'identification des personnes morales	
6. SYNTHÈSE DES PALIERS DE L'IDENTIFICATION	15
7. OFFRE INDUSTRIELLE.....	16
8. IMPACT SUR LES PRATIQUES PROFESSIONNELLES.....	17
ANNEXES	18
ANNEXE 1 – Traitement des identifiants	
ANNEXE 2 – Glossaire	
ANNEXE 3 – Documents de référence	

Authentification des professionnels de santé



Le Référentiel Général de Sécurité (RGS) définit l'authentification dans les termes suivants : « *L'authentification a pour but de vérifier l'identité dont se réclame une personne ou une machine (S'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité. L'authentification est généralement précédée d'une identification)*»

Le niveau de sécurité d'une fonction d'authentification est lié :

- au niveau de l'identifiant utilisé et de son processus d'attribution (assurance que l'identité préalablement enregistrée correspond à l'entité enregistrée et à elle seule) ;
- au niveau du dispositif d'authentification, de ses conditions d'attribution ainsi que de ses conditions d'emploi (assurance que le moyen d'authentification est utilisé par l'entité enregistrée).

(§3.2.a.1 du document « Référentiel Général de Sécurité » version 2.00).

Guide authentification des professionnels de santé

Date de publication: juillet 2013

Type de documents: référentiel (opposable)

Périmètre d'application:

Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓				
Commentaire						
La présente version du référentiel est applicable dans le cadre des usages santé ci-dessus. Le périmètre d'application sera élargi dans une version ultérieure du référentiel.						
Le mode d'exercice des acteurs ou encore le cycle de vie de la donnée n'ont pas d'incidence sur l'applicabilité des moyens définis.						

SOMMAIRE

SOMMAIRE	3
1. OBJET DU DOCUMENT	5
2. PÉRIMÈTRE D'APPLICATION DU RÉFÉRENTIEL	7
3. ENJEUX DE L'AUTHENTIFICATION DES ACTEURS DE SANTÉ	8
4. DÉFINITION DE L'AUTHENTIFICATION DES ACTEURS	9
4.1. Authentification	
4.2. Acteur de santé	
4.3. Portée d'un identifiant	
4.4. Facteur d'authentification	
4.5. Niveau d'authentification	
4.6. Authentification directe	
4.7. Architectures d'authentification (indirecte ou par délégation)	
5. PALIERS DE L'AUTHENTIFICATION DES ACTEURS DE SANTÉ	12
5.1. Paliers de l'authentification « publique » des acteurs de santé	
5.1.1. Palier 2 de l'authentification publique	
5.1.2. Palier 3 de l'authentification publique	
5.2. Paliers de l'authentification « privée » des acteurs de santé	
5.2.1. Palier 1 de l'authentification privée	
5.2.2. Palier 2 de l'authentification privée	
5.2.3. Palier 3 de l'authentification privée	
5.2.4. Socle commun de règles à respecter pour la mise en place de l'authentification « privée »	
6. SYNTHÈSE DES DISPOSITIFS D'AUTHENTIFICATION	18
7. OFFRE INDUSTRIELLE	19
8. IMPACT SUR LES PRATIQUES PROFESSIONNELLES	20
ANNEXES	21
ANNEXE 1 – Présentation et conditions d'emploi des dispositifs d'authentification	
A.1. Dispositifs d'authentification par carte CPS	
A.2. Dispositifs d'authentification par certificat logiciel de personne morale	
A.3. Dispositifs d'authentification par certificat logiciel de personne physique	
A.4. Dispositifs d'authentification par OTP	
ANNEXE 2 – Glossaire	
ANNEXE 3 – Documents de référence	

Les grands principes du guide

Portée d'un identifiant

L'identifiant utilisé dans le cadre d'une authentification peut avoir une portée locale ou nationale.

Pour mémoire, les identifiants de portée nationale (ou identifiants publics), sont attribués lors de l'enregistrement dans un référentiel d'identité national (RPPS, ADELI, FINESS, SIRET/SIREN, ...).

Tel que défini dans le référentiel d'identification des acteurs sanitaires et médico-sociaux.

Facteur d'authentification

- ce que la personne sait (ex. mot de passe) ;
- ce que la personne possède (ex. carte à puce, certificat électronique, token OTP, carte OTP, téléphone, tablette, boîte aux lettres de messagerie, etc.) ;
- ce que la personne est (ex. caractéristique physique de type biométrie) ;
- ce que la personne sait faire (ex. biométrie comportementale telle que la signature manuscrite ou la manière de taper sur un clavier d'ordinateur aussi appelée « frappologie »).

Authentification privée

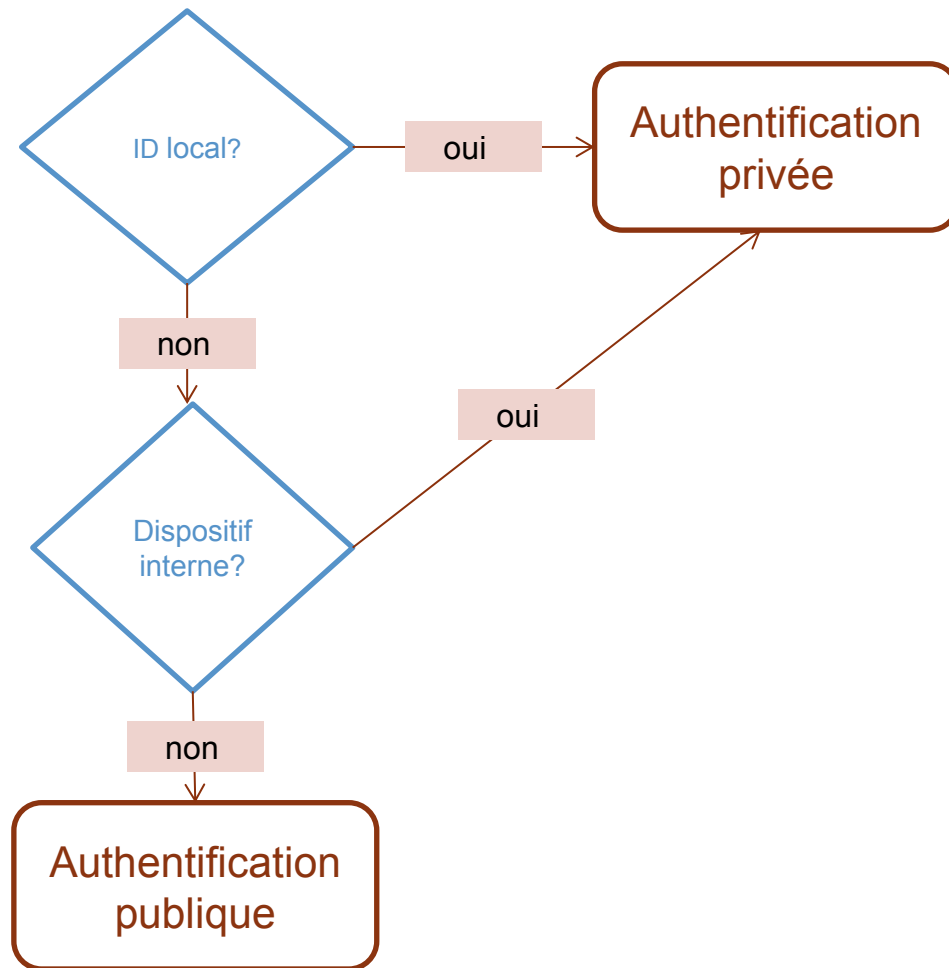
L'authentification est dite privée lorsque les dispositifs d'authentification utilisés sont diffusés pour une utilisation limitée à des systèmes d'information spécifiquement identifiés. Ils sont choisis par le responsable de traitement sur la base d'une analyse de risques. Ils peuvent être associés à des identifiants de portée nationale ou locale.

Authentification publique

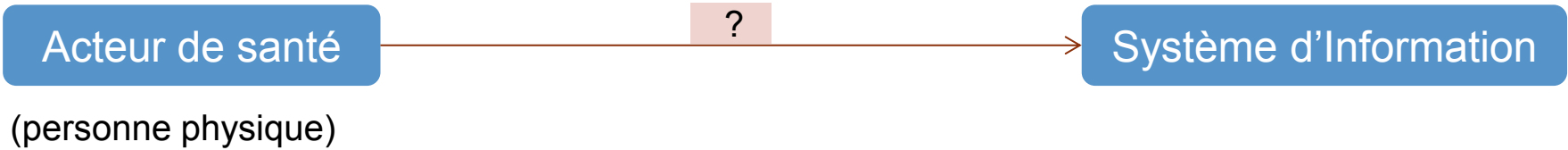
L'authentification est dite publique lorsque les dispositifs d'authentification utilisés sont associés à des identifiants de portée nationale (ou identifiants publics) et que leur utilisation n'est pas limitée à des systèmes d'information spécifiquement identifiés.

authentification privée ou publique?

- L'identifiant est-il de portée locale ou nationale?
- Le dispositif d'authentification (incluant l'enrôlement) fait partie du SI dans lequel se situe la personne physique cherchant à s'authentifier?



Typologie de l'authentification



3 variables:

Authentification privée →

Authentification publique →

Personne morale

(en intermédiaire)

1 règle:

Une personne morale ne peut pas utiliser une authentification privée.



Acteur de santé

(personne physique)

Authentification privée

Système d'Information

Acteur de santé

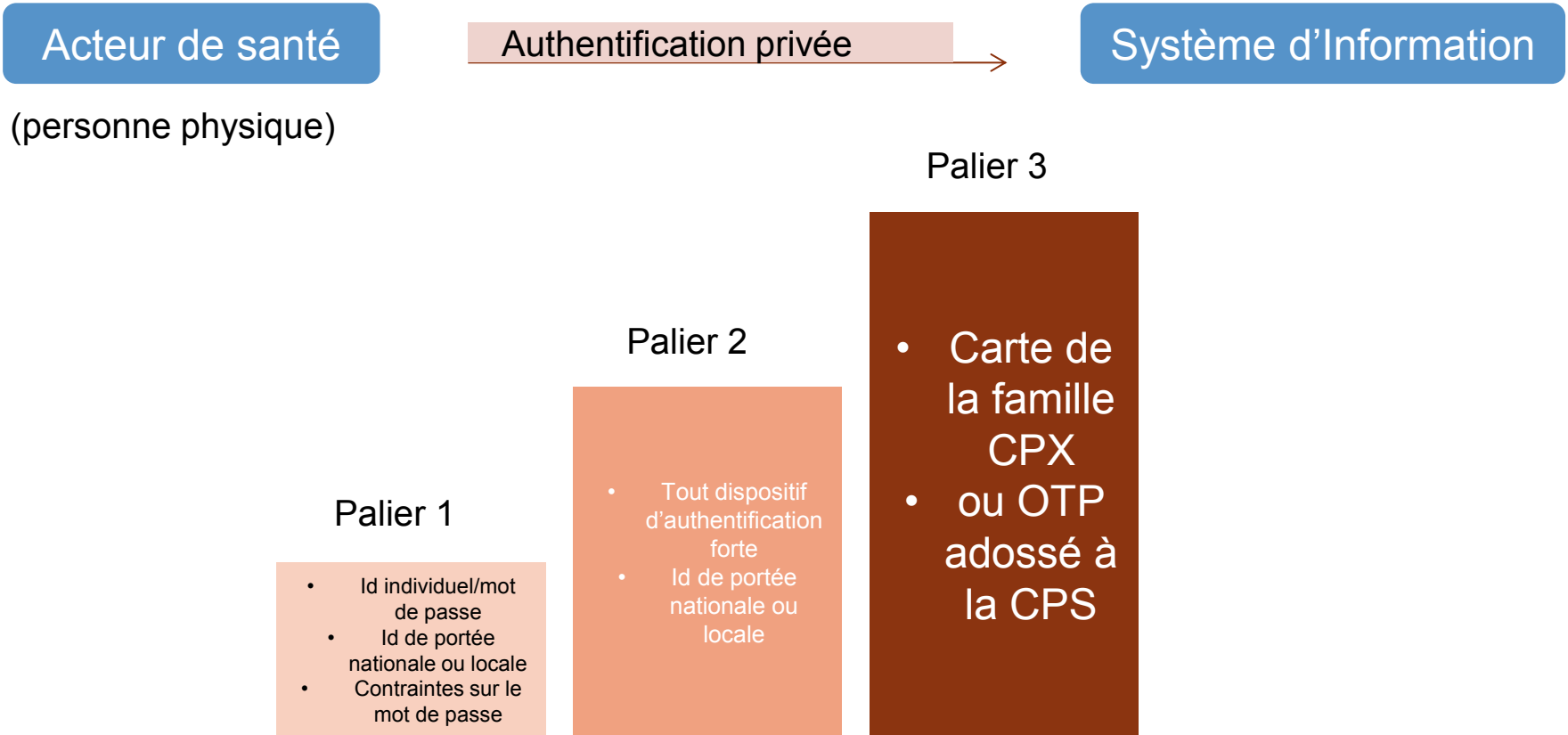
(personne physique)

Authentification publique

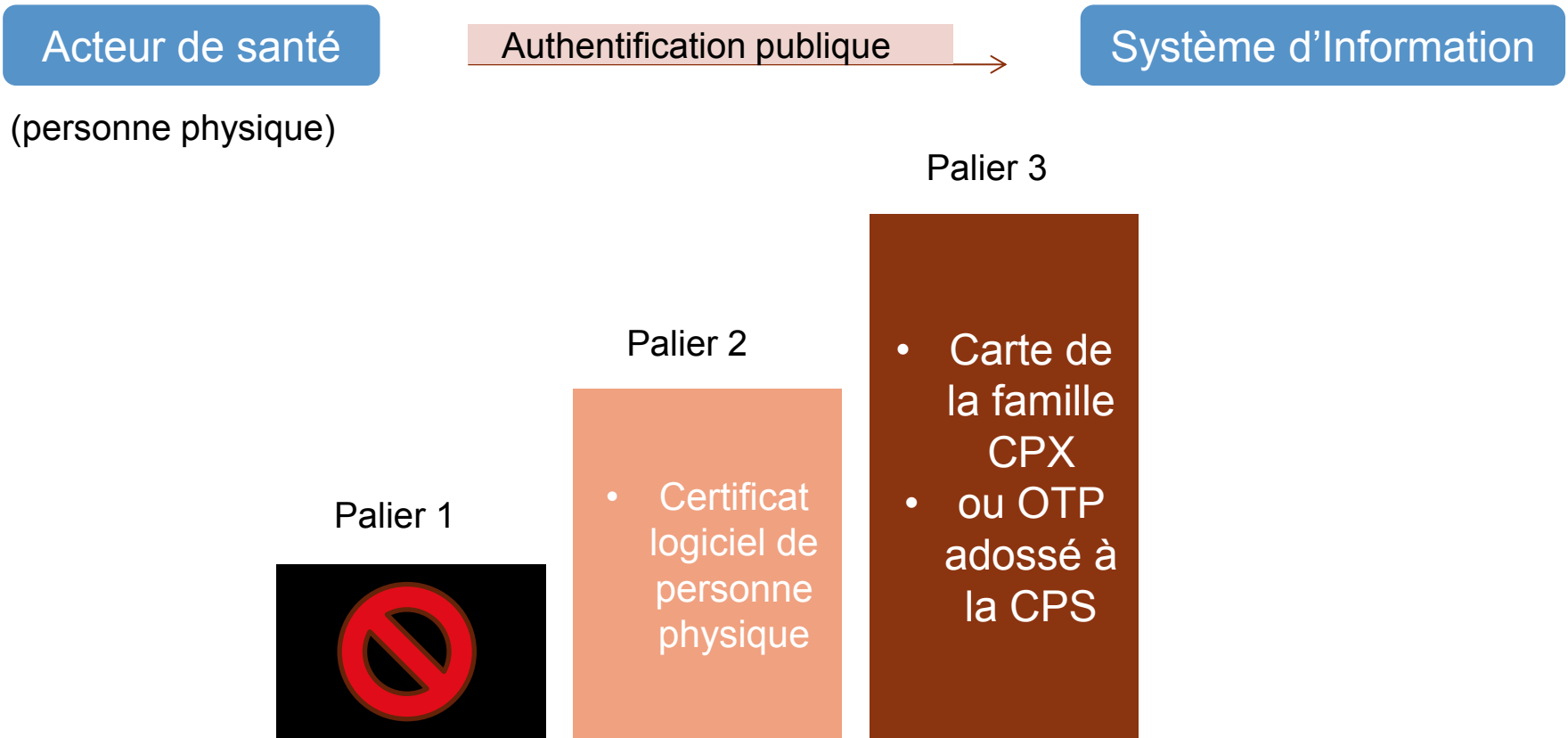
Système d'Information

Donc 2 types d'authentification **directe**.

Typologie de l'authentification



Typologie de l'authentification



Typologie de l'authentification

Acteur de
santé

Authentification
privée

Personne
morale

Authentification
publique

Système
d'Information

(personne physique)

Authentification **indirecte** = palier 2



Acteur de
santé

Authentification
publique

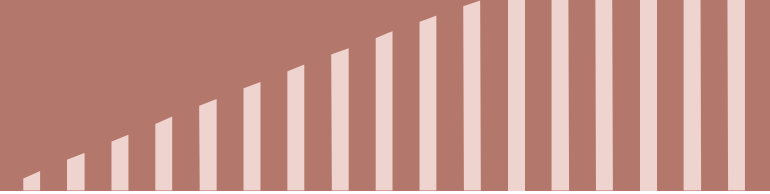
Personne
morale

Authentification
publique

Système
d'Information

(personne physique)

**Authentification par délégation =
palier 3**



Palier 1



Palier 2 = indirecte

Personne physique

- Tout dispositif d'authentification forte
- Id de portée nationale ou locale

Personne morale:

- Certificat serveur ou logiciel
- Id type FINESS, SIRET

Palier 3 = délégation

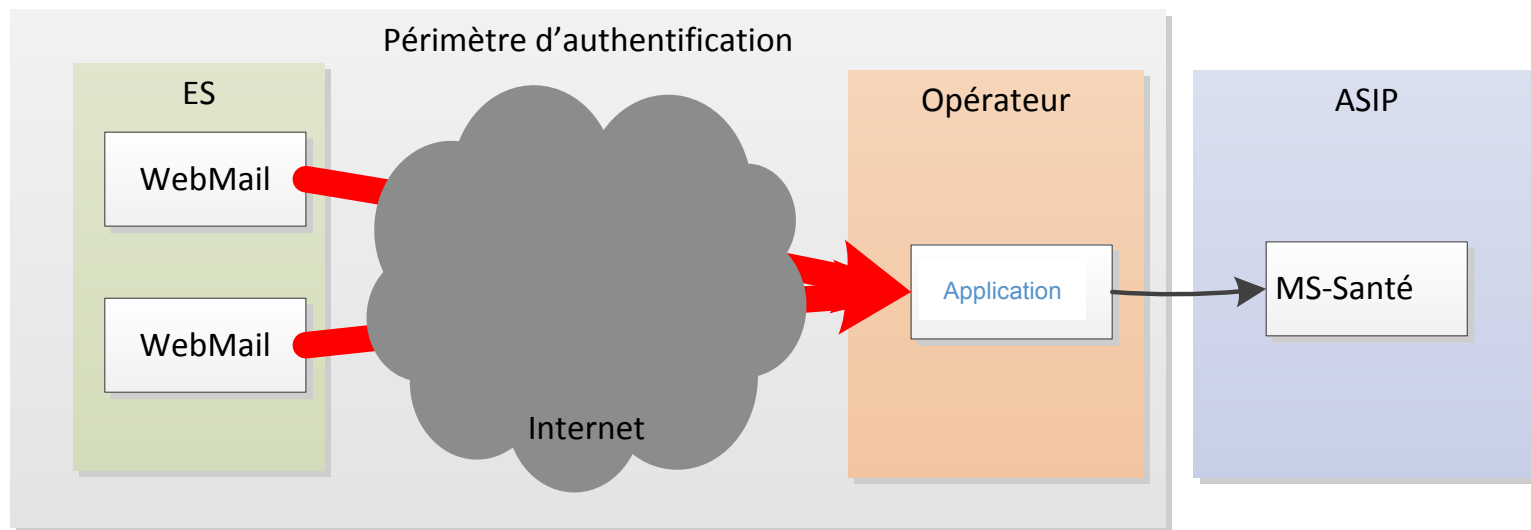
Personne physique:

- Carte de la famille CPX
- ou OTP adossé à la CPS

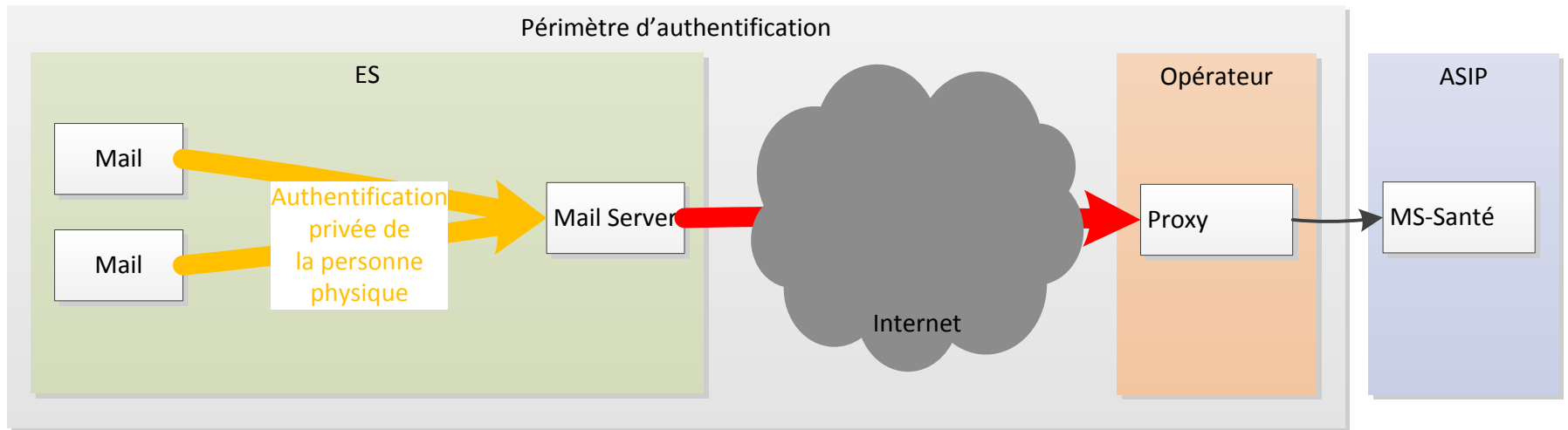
Personne morale:

- Certificat serveur ou logiciel et id type FINESS, SIRET

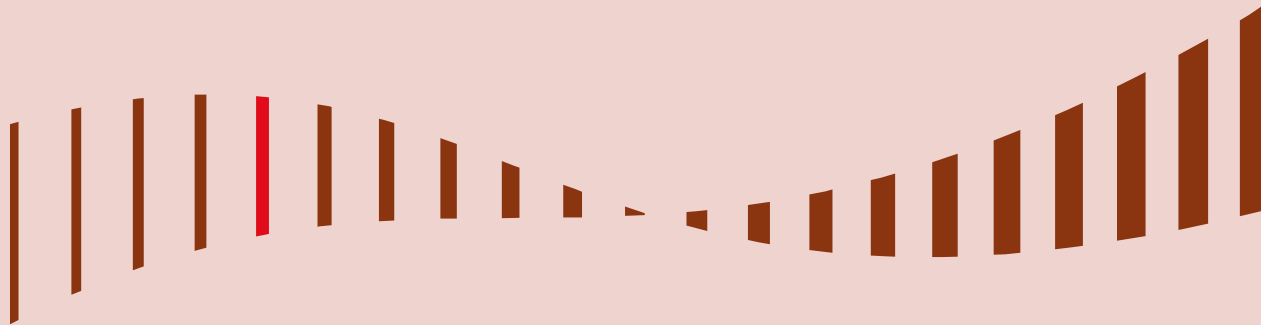
Exemples



Exemples



des exemples de guide pratique



Guide Accès web au SIS pour des tiers

Date de publication: janvier 2016

Type de documents: guide (non opposable)

Périmètre d'application:

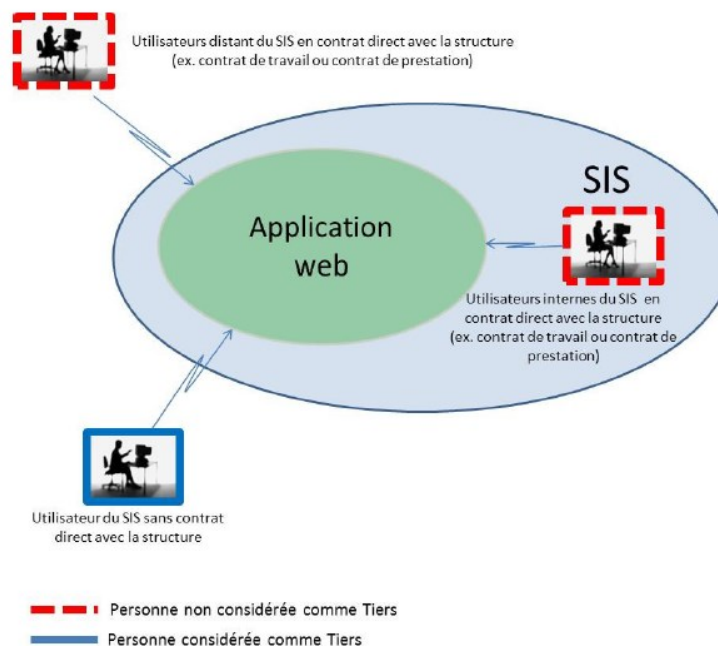
Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓	✓	✓	✓	✓
Commentaire						

Sommaire

1	INTRODUCTION	3
1.1	OBJET DU DOCUMENT	3
1.2	DEFINITIONS	5
1.3	CHAMP D'APPLICATION DU GUIDE	6
1.4	ENJEUX RELATIFS AUX ACCES AU SIS PAR DES TIERS VIA UNE APPLICATION WEB	8
1.5	REMARQUE PREALABLE	9
2	PRESENTATION DES DOCUMENTS DE REFERENCE	10
2.1	LES VINGT-NEUF RECOMMANDATIONS DE L'ANSSI POUR SECURISER VOTRE SITE WEB	10
2.2	LE " GUIDE DE REGLES ET DE RECOMMANDATIONS RELATIVES AU DEVELOPPEMENT D'APPLICATIONS DE SECURITE EN JAVA "	10
2.3	LES DIX VULNERABILITES DE SECURITE APPLICATIVES WEB LES PLUS CRITIQUES SELON L'OWASP	10
3	UTILISATION DU GUIDE	11
4	REGLES DE SECURITE	12
4.1	REGLES SPECIFIQUES A L'ACCES AUTHENTIFIE DE TIERS	12
4.2	BONNES PRATIQUES CONCERNANT L'ACCES A UNE APPLICATION VIA LE WEB	16
	ANNEXE 1 : GLOSSAIRE	22
	ANNEXE 2 : DOCUMENTS DE REFERENCE	24

Guide Accès web au SIS pour des tiers

- Les préconisations sont issues des bonnes pratiques en matière de Sécurité des Systèmes d'Information (SSI) et visent à traiter les principales vulnérabilités identifiées par des experts du domaine de la sécurisation web tels que l'Agence Nationale de la Sécurité des systèmes d'Information (ANSSI) et la communauté Open Web Application Security Project (OWASP).
- Elles concernent les phases de construction et de fonctionnement des services exposés. Il est rappelé que les structures publiques qui mettent en œuvre des services en ligne tels que des accès web doivent se conformer dans tous les cas au Référentiel Général de Sécurité .



Guide Plan de continuité Informatique

Date de publication: janvier 2016

Type de documents: guide (non opposable)

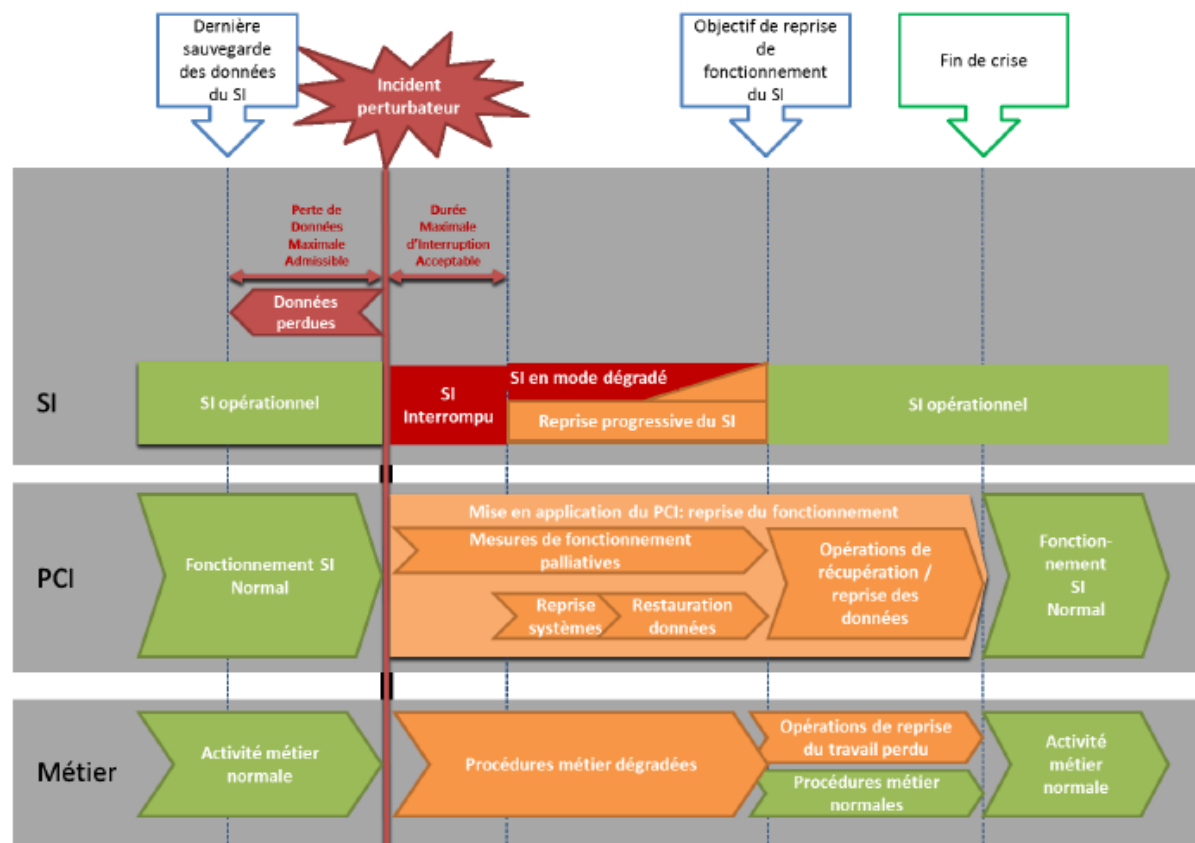
Périmètre d'application:

Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓	✓	✓	✓	✓
Commentaire						

Sommaire

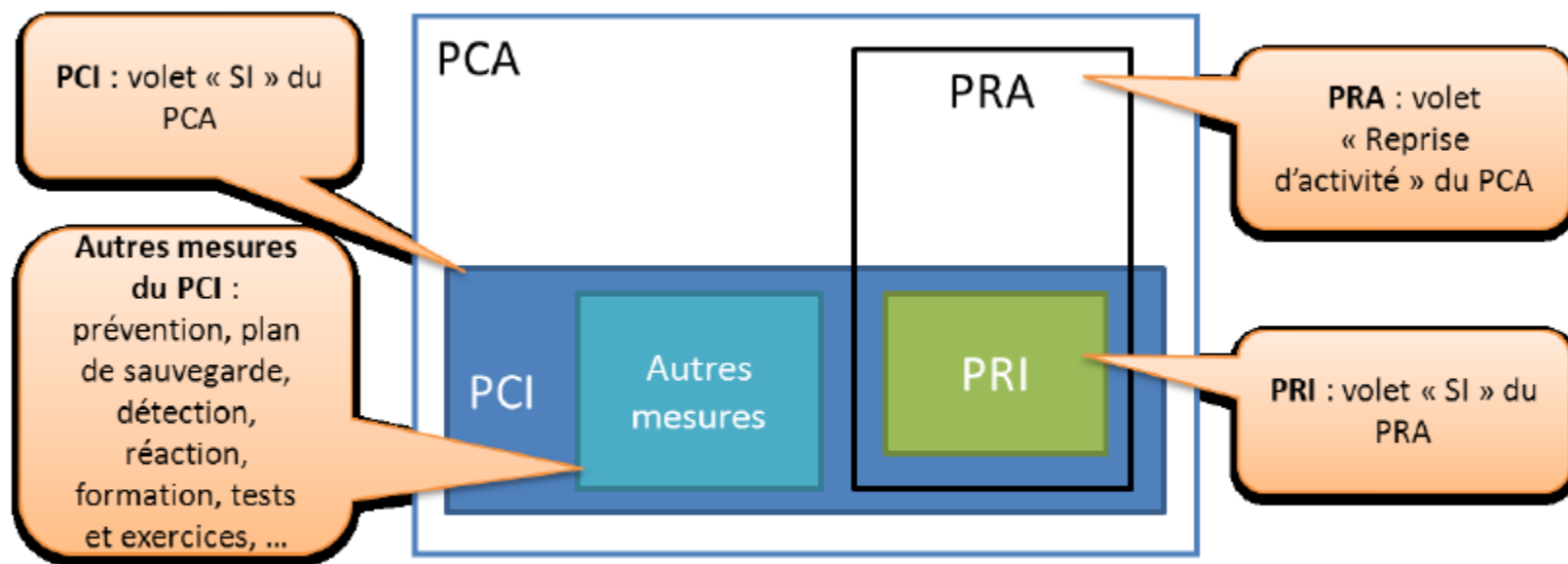
1	INTRODUCTION	5
1.1	OBJET DU DOCUMENT	5
1.2	CHAMP D'APPLICATION DU GUIDE PRATIQUE	6
1.3	ENJEUX RELATIFS A LA CONTINUITÉ DE FONCTIONNEMENT DES SYSTEMES D'INFORMATION DE SANTÉ	8
2	FONDEMENTS DU GUIDE	10
3	INTRODUCTION AU PCI	11
3.1	PCI ET PCA	11
3.2	TRAITEMENT D'UN INCIDENT QUI IMPACTE LA CONTINUITÉ DE FONCTIONNEMENT DU SI	12
3.3	DEFINITIONS LIEES A LA CONTINUITÉ DE FONCTIONNEMENT INFORMATIQUE	14
3.4	ORGANISATION NECESSAIRE	17
4	COMMENT ELABORER LE PCI DE VOTRE SI ?	18
4.1	SYNTHESE DE LA DEMARCHE	18
4.2	ORGANISATION	19
4.3	IDENTIFIER LES SCENARIOS D'INCIDENT A PRENDRE EN COMPTE	20
4.3.1	Incident affectant le SI	22
4.3.2	Incident affectant la structure	23
4.3.3	Incident affectant la structure et le SI	23
4.3.4	Interruption partielle et planifiée du SI	23
4.4	RECUEILLIR LE BESOIN METIER DE RETABLISSEMENT DES SERVICES	24
4.5	IDENTIFIER LES MOYENS DU SI CONCERNES ET LES MESURES EXISTANTES	26
4.6	ELABORER LES MESURES DE PREVENTION, LES MESURES PALLIATIVES ET LES MESURES DE SECOURS	28
4.6.1	Définitions	28
4.6.2	Mesures de prévention	28
4.6.3	Mesures palliatives	29
4.6.4	Mesures de secours	30
4.6.5	Impact des solutions prévues sur le reste des activités	30
4.6.6	Reversibilité et réintégration des données	32
4.6.7	Sélection des solutions	33
4.6.8	Documentation	34
4.7	PREPARER LES MOYENS NECESSAIRES AUX MESURES DE CONTINUITÉ ET TESTER LES SOLUTIONS	35
5	FAIRE VIVRE LE PCI	37
5.1	S'ENTRAINER ET VERIFIER REGULIEREMENT L'EFFICACITE DU PCI	37
5.2	MAINTENIR A JOUR LE PCI	39
5.3	IDENTIFIER LES LIMITES DU PCI	40
6	POUR ALLER PLUS LOIN	41
	ANNEXE 1 : EXEMPLE DE TABLEAU DE COLLECTE DES INFORMATIONS POUR LE PCI	42
	ANNEXE 2 : GLOSSAIRE	43
	ANNEXE 3 : DOCUMENTS DE REFERENCE	44

Guide Plan de continuité Informatique



Traitement d'un incident qui impacte la continuité de fonctionnement du SI

Guide Plan de continuité Informatique



Positionnements relatifs du PRI, PRA, PCI et PCA

All your base are belong to us

Sécurité opérationnelle – avril 2016

Sommaire

- A. Présentation
- B. Ça n'arrive pas qu'aux autres
- C. CTB-Locker
- D. Focus sur quelques failles
- E. Méthodologie / recommandations
- F. Synthèse
- G. Questions



Présentation

Ancien pentesteur

Certifié OSCP

Pentest : aka test d'intrusion. Méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique en simulant une attaque d'un utilisateur mal intentionné, voire d'un logiciel malveillant

Chargé de sécurité opérationnelle à l'ASIP

Toujours des tests d'intrusion mais mise en application des recommandations...

Ça n'arrive pas qu'aux autres



]HT[Hacked Team
@hackingteam

Suivre

Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1lhChT!rbB...
infotomb.com/eyyx0.torrent

Orange vous informe : rubrique mon compte

Cher(e) Client(e),

Orange a été la cible d'une intrusion informatique le 16 janvier 2014 à partir de la page « Mon Compte » de l'Espace Client du site orange.fr. Même si aucune action de votre part n'est requise, nous avons souhaité vous informer en toute transparence de l'existence et de la résolution de ce fait.

Vos mots de passe ne sont pas concernés, leur intégrité n'est pas mise en cause.

Organisation	Nombre de données volées	Type de violation	Secteur d'activité ciblé
Home Depot	109 000 000	Hacking du système	Commercial
JP Morgan Chase	83 000 000	Vol d'identité	Banque et finance
EBAY	145 000 000	Vol d'identité	Commercial
Korea Credit Bureau	104 000 000	Vol d'identité	Banque
Benesse Holdings	48 600 000	Vol d'identité	Education
Sites de jeux en ligne	27 000 000	Vol d'identité	Technologique - Jeux



Ça n'arrive pas qu'aux autres

Des données internes de la marque ETAM auraient été piratées

VTech victime d'un piratage informatique

Labio.fr piraté : demande de rançon et publication de résultats médicaux

Un hôpital américain totalement paralysé par un piratage depuis une semaine

PAR EMMANUEL GHESQUIER LE 17 FÉVRIER 2016 |  0

BUZZ | [LIRE + TARD](#)

Mairies françaises attaquées par un ransomware russe

Plusieurs centaines de sites du CNRS et des Restaurants du cœur piratés

CTB-Locker

Famille des **RansomWeb**

Le principe n'est plus de s'attaquer aux données d'un utilisateur, mais **au serveur de base de données d'un site web**

Modus operandi:

- 1- Détection d'une application web vulnérable et prise de contrôle avec une backdoor. **Aucun changement n'est aperçu sur le site.**
- 2- Modification du code de l'application utilisée afin de chiffrer les données envoyées en base de données ; Modification de la méthode de déchiffrement utilisée pour que les données restent encore lisibles. Clé de déchiffrement cachée sur un serveur
- 3- Attente de quelques mois, le temps que les sauvegardes des données chiffrées soient effectuées, et que celles-ci remplacent les sauvegardes non chiffrées
- 4- **Suppression de la clé de déchiffrement du code de l'application....**

RÉFÉRENTIELS

Focus sur quelques failles de sécurité

Généralités OWASP

OWASP : guide de sécurisation des applications web

OWASP Top Ten (2013)



Injections

Plusieurs types: sql, ldap, xml, etc.

Modification d'une requête existante pour afficher des données cachées, pour écraser des valeurs importantes, ou encore exécuter des commandes dangereuses.

➤ **Ne pas faire confiance aux données entrées par l'utilisateur !**

Topic : mossfon.com mail server SQLi ** [REDACTED]

share with each other but no leaks ,

vulnerable : https://web.mossfon.com/orion/orion_enLOGIN.asp

POST DATA :

UserId=11111%27+and+1=convert%28int,%28select+top+1+login+from+users+where+OrionID=1%29%29-- &Password=12345&submit=Login

webadmin;tuvani@900\$,id,1 webmaster;adawina_gonzales;id:2

www.elevage-connemara.fr/poney_nos-poneys-a-vendre_vahina-de-l-au-lne.phtml

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the correct syntax for statement 'SELECT pages_elements FROM pages, pages_elements, pages_profiles WHERE pages_profiles.accroche=fronte-l-aulne' AND pages.profil= ORDER BY pages_elements.position LIMIT 1You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the correct syntax for statement 'SELECT pages_elements FROM pages, pages_elements, pages_profiles WHERE pages_profiles.accroche=fronte-l-aulne' AND pages.profil= ORDER BY pages_elements.position LIMIT 1

```
[*] 200 for /flex2gateway/
[*] : :80 /flex2gateway/http 200
<?xml version="1.0" encoding="utf-8"?>
<amfx ver="3"><header name="AppendToGatewayUrl"><string>;jsessionid=3c3036d4f9cf40bf43b19104b51614c25650</string></header><body targetURI="/onResult" responseURL=""><object type="flex.messaging.messages.AcknowledgeMessage"><traits><string>timestamp</string><string>headers</string><string>body</string><string>correlationId</string><string>messageId</string><string>timeToLive</string><string>clientId</string><string>destination</string></traits><double>1.289047303817E12</double></object><traits><string>DSId</string></traits><string>BD1226D2-080E-409E-5E4D-B729314E52F</string></object><null/><string>root:x:0:0:root:/root:/bin/bash
in:x:1:1:bin:/bin:/sbin/nologin
aemon:x:2:2:daemon:/sbin:/sbin/nologin
dm:x:3:4:adm:/var/adm:/sbin/nologin
p:x:4:7:lp:/var/spool/lpd:/sbin/nologin
ync:x:5:0:sync:/sbin:/bin/sync
hutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
alt:x:7:0:halt:/sbin:/sbin/halt
ail:x:8:12:mail:/var/spool/mail:/sbin/nologin
ews:x:9:13:news:/etc/news:
ucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
```

Plusieurs sites pornos hackés, les données des clients déjà en vente sur le web

PAR EMMANUEL GHESQUIER LE 11 AVRIL 2016

www.comunicacao.sp.gov.br/%5C

Warning: PDOStatement::execute() [pdostatement.execute]: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the correct syntax for statement 'SELECT public_html/app/class/class.module_pagina.php on line 443

Upload de fichiers malicieux

Non trouvée par les scanners de sécurité

famille de vulnérabilités web permettant l'exécution de code arbitraire par un attaquant sur la machine visée

Survient quand on autorise les utilisateurs à envoyer des fichiers (avatars sur un forum, des photos sur une galerie, des pièces jointes sur un chat de support)

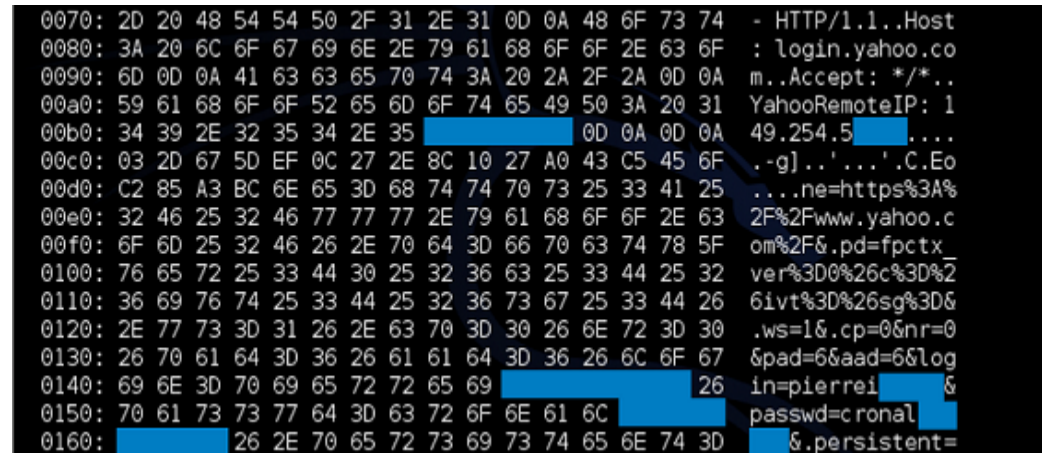
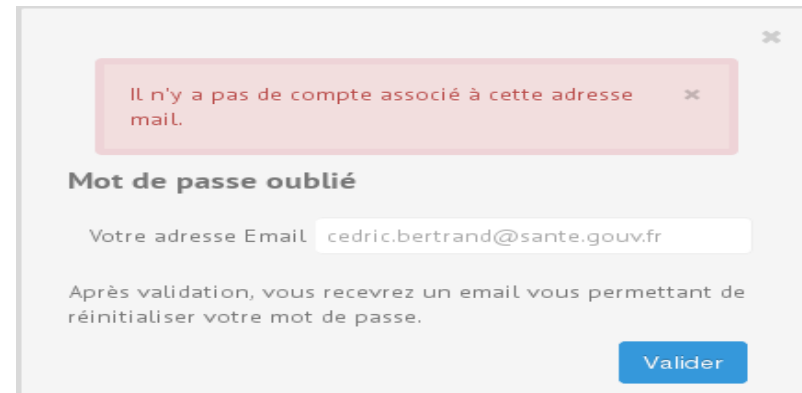
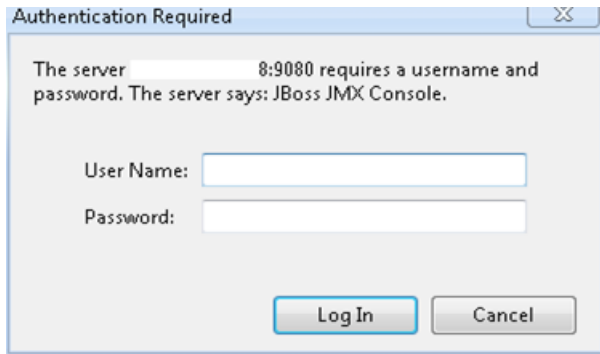


```
POST
/web/mss/formulaire-contact?p_p_id=suggestions_VWAR_suggestionsportlet_INSTANCE_8Ukm&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=
t.action=%2Fsuggestions%2Fenvoyersuggestion&_suggestions_VWAR_suggestionsportlet_INSTANCE_8Ukm_struts.portlet.mode=view HTTP/1.1
Host: cms.iso
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.1
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: https://cms.iso-production.mssante.fr/formulaire-contact?signaler=&
Content-Length: 369
Cookie: PAUTSESSIONID=F978BADFAD978819DEE47C5B6DF2178A.isop-paut-01.mss.asip.hst.fluxus.net; GUEST_LANGUAGE_ID=en_US; COOKIE_SUPPORT=
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

isExtensionValide=false&AutreDenomination=pentest&detail=test%252520extension%252520&demande=Service%20MSSant%C3%A9%20(Webmail)&ps.nom=
o16@gmail.com&ps.profil=Autre&ps.EmailMSS=&profession=&ps.civilite=M.&struts.enableJSONValidation=true&struts.validateOnly=true&enteredCaptchaText=TB1
```


Autres failles communes

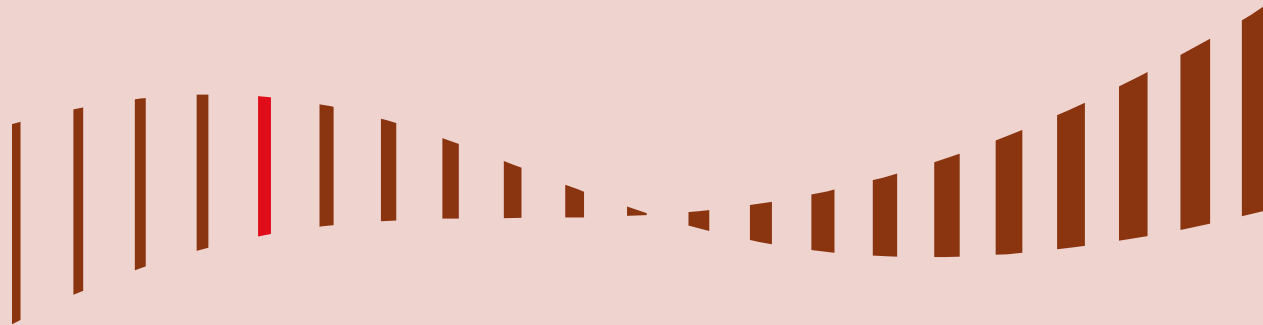
- Patch management
- Mots de passe faibles



Hackers actively exploiting JBoss vulnerability to compromise servers



Méthodologie et recommandations



Objectifs

- **Pas de « solution miracle » contre des attaquants compétents , possédant temps et ressources financières**
- **Utiliser les techniques des attaquants afin de les ralentir / décourager (outils automatisés, dorks google).**

Méthodologie test d'intrusion

1- Prise d'informations

2- Recherche de vulnérabilités

3- Exploitation de vulnérabilités

4- Post-Exploitation

5- Maintien de l'accès

Recherche d'informations

Rendre le moins d'informations accessibles

- Masquer bannières (versions, logiciels utilisés)
- Scans de ports (nmap – prix : gratuit)
- Brute-force des domaines accessibles
- Google dorks
- Analyse des documents accessibles publiquement (foca :
- Faire veille sur les logiciels utilisés (ex : vigilance)

The screenshot shows the OSINT Demo interface. On the left, a file tree is visible with a red box highlighting the 'Metadata' folder. The tree includes categories like Network, Domains, Roles, Vulnerabilities, and Metadata. The Metadata folder contains sub-folders for Documents (71/147), Metadata Summary, Users (23), Folders (29), Printers (0), Software (26), Emails (4), Operating Systems (4), Passwords (0), and Servers (0). On the right, a table lists attributes and their values.

Attribute	Value
All users found (23) - Times found	
Information Technology	22
Information Technology	13
Medical Device	2
Active Directory Windows A	2
Common Information Services	2
Gateway Services	1
Java	1
Database	3
Advertisement	4
Software Support G	1
Windows Security M	6
dm	1
Java	1
Office	2

Vigil@nce

analyse de vulnérabilités informatiques depuis 1999

The screenshot shows the SHODAN search interface. The search bar contains 'Apache/2.2.9'. Below the search bar, there are buttons for 'Exploits' and 'Maps'. The interface is dark-themed with a search bar and navigation buttons.

TOP COUNTRIES



Total results: 95,750

301 Moved Permanently

151.72.86.39

WIND Telecomunicazioni S.p.A

Added on 2016-04-11 20:15:42 GMT

Italy, Bitetto

Details

HTTP/1.1 301 Moved Permanently

Date: Mon, 11 Apr 2016 18:50:06 GMT

Server: Apache/2.2.9 (Unix) mod_ssl/2.2.9 OpenSSL/0.9.8o mod_wsgi/2.4 Python/2.6.2

Location: http://151.72.86.39/r41151,/playzone,/

Content-Length: 376

Content-Type: text/html; charset=iso-8859-1

Recherche de vulnérabilités

Utiliser les mêmes outils que les pirates

- Scanneur de vulnérabilités (ex : Nessus (1500€/an), OpenVAS)
- Scanneurs de vulnérabilités web (ex : acunetix, nikto, cms explorer)
- Protection (fail2ban)



Hosts > 192.168.15.13 > Vulnerabilities 129

Severity	Plugin Name	Plugin Family
CRITICAL	Apache 2.2.x < 2.2.15 Multiple Vulnerabilities	Web Servers
CRITICAL	OpenSSL Unsupported	Web Servers
CRITICAL	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities	CGI abuses
CRITICAL	PHP Unsupported Version Detection	CGI abuses
HIGH	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities	Web Servers

Acunetix Web Vulnerability Scanner (NFR Reseller Edition)

Scan Results: Scan Thread 1 (http://192.168.15.13)

Alerts (87)

- SQL Injection (31)
 - /Login.asp (6)
 - /Register.asp (12)
 - /Search.asp (1)
 - /showforum.asp (6)
 - /showthread.asp (6)

SQL Injection (High)

Vulnerability description

This script is possibly vulnerable to SQL injection attacks.

SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This vulnerability affects **/Login.asp**.

The impact of this vulnerability

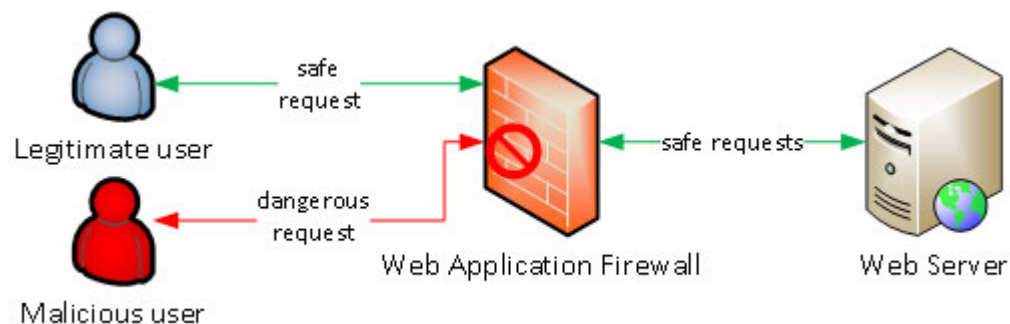
An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your

Activity Window

```
SQL injection "/showthread.asp" on parameter "id"
Test module: MultiRequest parameter manipulation (4 of 11)
MultiRequest parameter manipulation is preparing ...
MultiRequest parameter manipulation is executing on script "/Template.asp (1 of 6)" ...
MultiRequest parameter manipulation is executing on script "/Search.asp (2 of 6)" ...
MultiRequest parameter manipulation is executing on script "/Login.asp (3 of 6)" ...
```


Exploitation de vulnérabilités

- Bonnes pratiques de développement (OWASP)
- WAF (Web Application Firewall) (mod security Apache, CloudFlare, Barracuda)



OWASP

The Open Web Application Security Project

OWASP Top 10 - 2013

Les Dix Risques de Sécurité Applicatifs Web les Plus Critiques

Post-exploitation & maintien de l'accès

- Guide de durcissement de serveur web
- Sauvegardes
- Outils de monitoring (ex: tripwire, OSSEC, Rkhunter, logwatch)

Recovering from a `rm -rf /` [duplicate]

This question already has an answer here:

[Monday morning mistake: sudo rm -rf --no-preserve-root /](#) 5 answers

I run a small hosting provider with more or less 1535 customers and I use Ansible to automate some operations to be run on all servers. Last night I accidentally ran, on all servers, a Bash script with a `rm -rf {foo}/{bar}` with those variables undefined due to a bug in the code above this line.

All servers got deleted and the offsite backups too because the remote storage was mounted just before by the same script (that is a backup maintenance script).

How I can recover from a `rm -rf /` now in a timely manner?

Rule Name	Severity Level	Added	Removed	Modified
-----	-----	----	-----	-----
User binaries	66	0	0	0
Tripwire Binaries	100	0	0	0
Critical configuration files	100	0	0	0
Libraries	66	0	0	0
Operating System Utilities	100	0	0	0
Critical system boot files	100	0	0	0
File System and Disk Administration Programs	100	0	0	0
Kernel Administration Programs	100	0	0	0
Networking Programs	100	0	0	0
System Administration Programs	100	0	0	0
Hardware and Device Control Programs	100	0	0	0
System Information Programs	100	0	0	0
Application Information Programs				

Synthèse

- Durcissement du serveur web
- Sauvegardes
- Scan de vulnérabilités
- Patch management
- Veille sécurité
- Monitoring / WAF
- Pentest (si applications développées manuellement : OWASP)

Questions ?

