Cible de Sécurité CSPN

6TZEN

Version	Date	Description	Rédacteurs
1.0	26/06/2015	Version initiale	Adminext, Oppida
1.1	02/07/2015	Modification du chapitre « Argumentaire du produit », Relecture	Adminext
1.2	06/07/2015	Relecture, modification du chapitre « description des fonctions de sécurité »	Oppida
1.3	01/09/2015	- désactivation webdav - retrait des parties destinées aux guides utilisateurs	Adminext
1.4	28/10/2015	Mise en forme et commentaires.	Oppida
1.5	02/11/2015	- Modifications de la figure 5 (architecture fonctionnelle) et 6	Adminext

		(schéma réseau) - Extraction de la liste des paramètres de la configuration d'évaluation vers un autre document que la cible.	
2.0	25/02/2016	- Prise en compte des remarques de l'ANSSI	Adminext
3.0	08/03/2017	- Suppression des mauvaises références de version	Adminext

1. SOMMAIRE

2. INTRODUCTION

2.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN, du produit 6Tzen développé par la société Adminext.

2.2. REFERENCES

Référence	Nom du document	Version
CER-I-02.1	Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau ANSSI-CSPN-CER-I-02/1.1	2
CRYPTO	Mécanismes cryptographiques du produit 6TZen	1.2
INSTALL	6Tzen : Prérequis & installation	1
GUIDES	Livret d'utilisation : démo assistée du Portail Usager (ref : 2015-00002493) Livret d'utilisation : Administration du portail de démarches, 10/09/2015	2 1
PARAM	ST_Annexe_Paramètre	2

3. IDENTIFICATION DU PRODUIT

Cette cible de sécurité a été élaborée en vue d'une évaluation Certification Sécurité de Premier Niveau (CSPN).

Organisation éditrice	Adminext
Lien vers l'organisation	http://www.6tzen.fr/
Nom commercial du produit	6TZEN
Numéro de la version évaluée	Le produit est constitué des trois composants logiciels : • HUB version 1.0.36.FINAL • DEMATREE version 1.05.08.FINAL2 • ADMIMAIL version 3.02.09.FINAL2
Catégorie de produit	Identification, authentification, contrôle d'accès

4. ARGUMENTAIRE DU PRODUIT

4.1. DESCRIPTION GENERALE DU PRODUIT

6Tzen est une solution intégrée de dématérialisation des échanges, qui s'adresse à la fois aux citoyens par le biais d'un portail de démarches en ligne, et aux agents publics par le biais d'une application de gestion et d'instruction des demandes.

La solution met à disposition des utilisateurs les deux interfaces suivantes : **6Tzen Portail** et **6Tzen Admin**.

4.1.1. 6Tzen Portail

Il s'agit du portail destiné aux usagers pour :

- Accéder à une liste de démarches en ligne,
- Effectuer une démarche / remplir un formulaire en ligne,
- Soumettre la demande à l'administration,
- Suivre l'état de la demande en temps réel,
- Échanger avec les agents directement sur le portail,
- Gérer son porte-documents et y stocker ses pièces justificatives,
- Accéder aux réponses de l'Administration.

Figure 1: Page d'accueil de 6Tzen portail

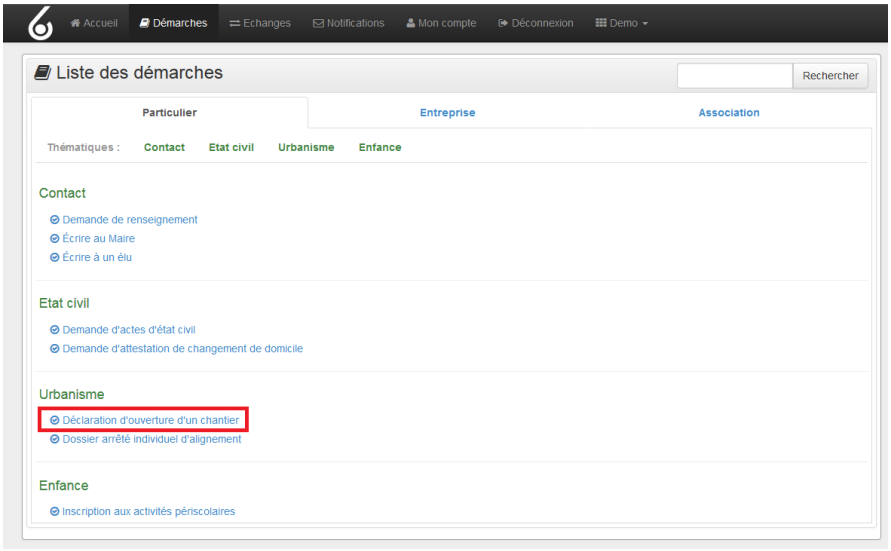

Figure 2 : Écran de liste des démarches du portail destiné aux citoyens

4.1.2. 6Tzen Admin

Il s'agit du portail mis à disposition des agents publics pour :

- Prendre en charge les demandes entrantes,
- Les qualifier et les diffuser pour traitement à un agent instructeur,
- Échanger avec l'usager directement via l'application,
- Piloter le portefeuille de demandes,
- Instruire la demande en gérant notamment un statut,
- Communiquer le statut des demandes à l'usager.

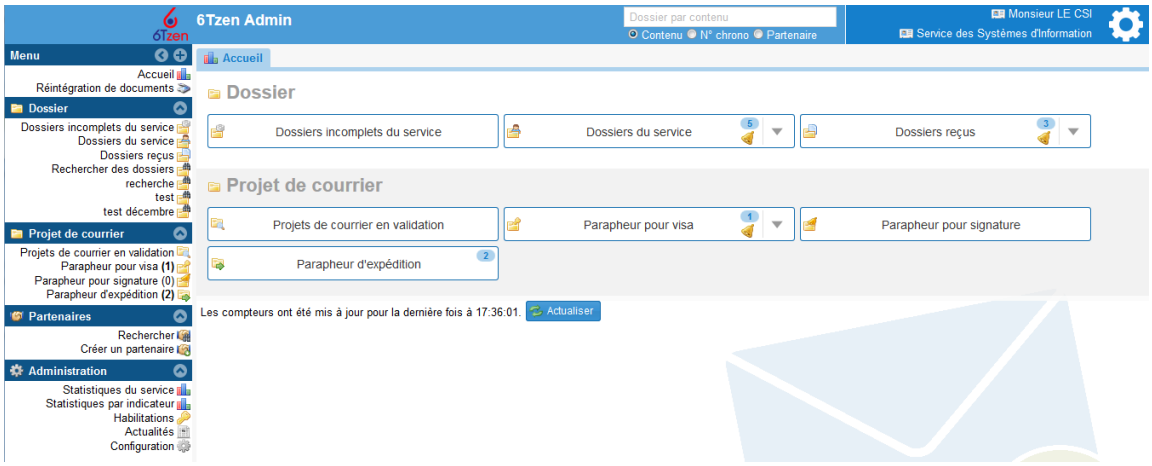

Figure 3: Page d'accueil de l'application 6Tzen Admin

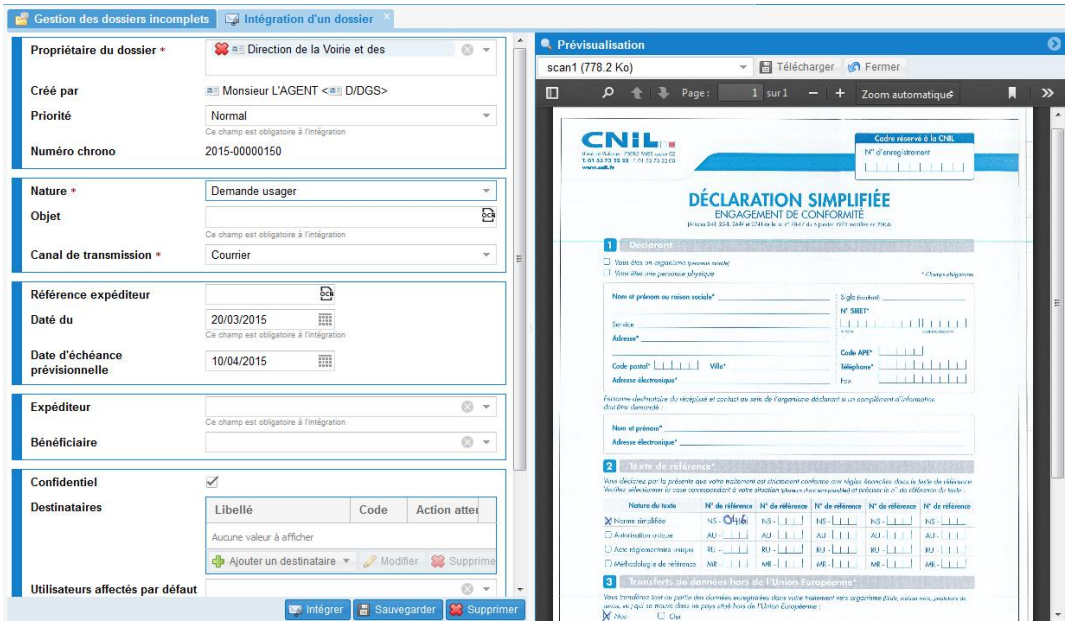

Figure 4: Exemple d'édition d'une demande

4.2. UTILISATEURS TYPIQUES DU PRODUIT

Deux catégories de profils se distinguent :

1. Les utilisateurs du portail 6Tzen Portail (les usagers)
2. Les utilisateurs du portail 6Tzen Admin

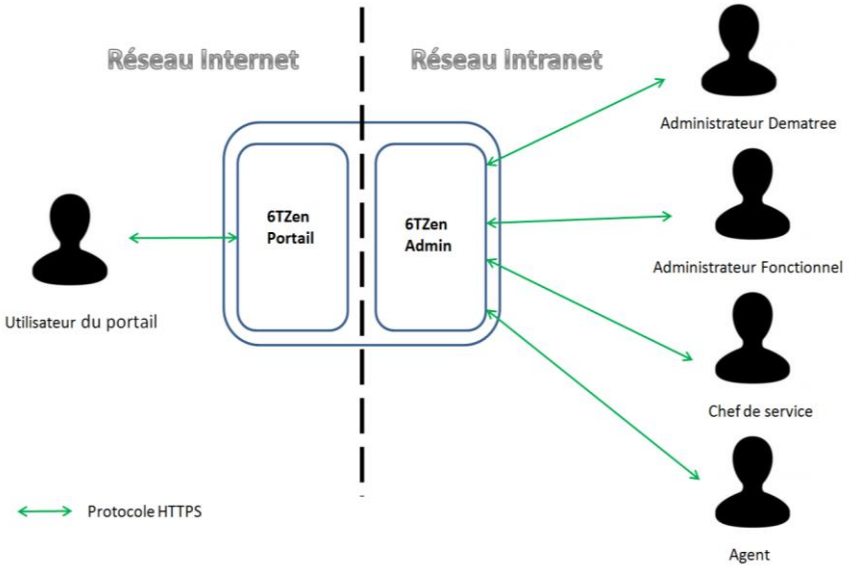

Figure 5 : Architecture fonctionnelle

4.2.1. Utilisateurs du portail 6Tzen Portail

L'utilisateur du portail (l'usager) réalise des démarches sur le portail :

- Il peut se créer un compte,
- Il peut gérer son compte : modifier ses données personnelles, changer son mot de passe selon la politique de mot de passe, visualiser ses connexions précédentes.
- Il peut effectuer des démarches via son compte;
- Il peut visualiser ses démarches et leur état d'avancement.

4.2.2. Utilisateurs du portail 6Tzen Admin

L'Administrateur Dematree gère :

- les profils des agents, des chefs de service : il peut créer, modifier ou supprimer les profils des agents et des chefs de services,
- les profils des autres administrateurs fonctionnels : il peut créer, modifier ou supprimer les profils des autres administrateurs fonctionnels,
- les services : créer, modifier ou supprimer des services,

Remarque : Il existe un administrateur Dematree unique qui ne peut être supprimé et ses droits ne peuvent être restreints.

L'Administrateur fonctionnel gère les paramètres fonctionnels de 6TZen.

Les paramètres fonctionnels sont des paramètres de personnalisation du produit comme par exemple les listes de références, la typographie des dossiers, la liste des démarches, etc. La liste de ces paramètres est en annexe.

Un **Chef de service** gère un ou des services :

- Il peut affecter des dossiers à des agents de son service,
- Il peut envoyer le dossier à un autre service,
- Il peut réaliser une opération sur un dossier :
- Créer le dossier,
- Diffuser le dossier,
- Consulter le dossier,
- Modifier le dossier,
- Supprimer le dossier.
- Etc

Un **Agent** est attaché à un ou des services.

- Il traite les dossiers auxquels il a été affecté au sein d'un service,
- Il peut visualiser les dossiers à accès public ouvert des services auxquels il appartient.

Remarque : Toutes ces opérations sont tracées dans le dossier sauf l'opération de consultation. Toutes les personnes traitant un dossier peuvent visualiser les traces des actions réalisées sur ce dossier.

4.2.3. Administrateur technique

Un autre type d'utilisateur qui n'est ni un utilisateur du portail 6Tzen Portail, ni un utilisateur du portail 6Tzen Admin se distingue : **l'administrateur technique**.

Il correspond à l'administrateur du socle technique sur lequel s'exécute la cible d'évaluation. Ce rôle n'est pas géré par le produit.

4.3. PERIMETRE DE L'EVALUATION

La cible de l'évaluation est constituée des modules logiciels ADMIMAIL, DEMATREE et HUB.

ADMIMAIL est le module qui met en œuvre le portail 6TZen Portail et qui permet la gestion des dossiers.

DEMATREE est le module qui permet la gestion des rôles de l'intranet ; à savoir les administrateurs Dematree, les administrateurs fonctionnels, les chefs de service et les agents.

HUB est le module responsable de l'envoi des mails sur instruction du module ADMIMAIL.

4.4. ENVIRONNEMENT D'UTILISATION

Les modules logiciels objets de l'évaluation doivent être déployés dans une infrastructure classique de mise à disposition de services web.

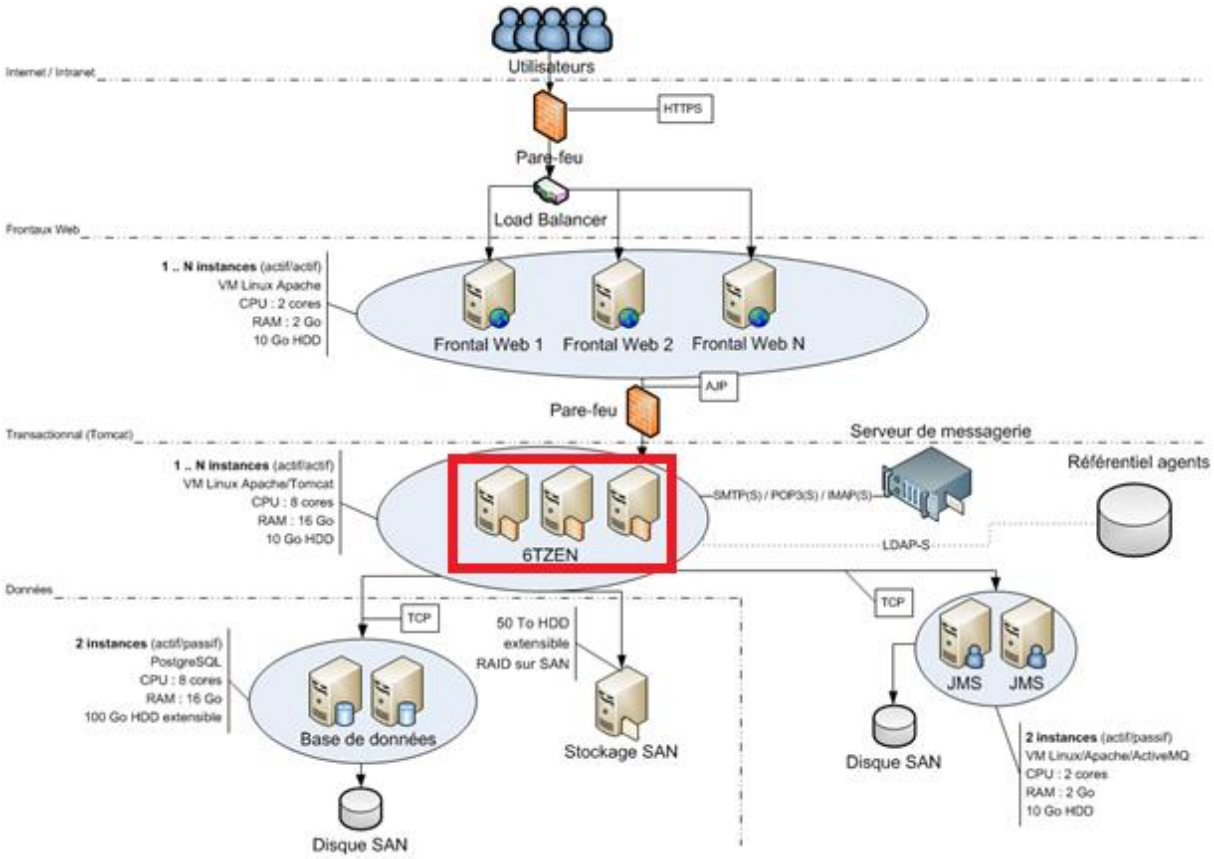

Figure 6: Déploiement classique de la solution 6TZEN (en rouge le périmètre du produit évalué)

4.5. DEPENDANCES DU PRODUIT A DES MATERIELS, LOGICIELS ET/OU DES MICROPROGRAMMES DU SYSTEME

Les modules ADMIMAIL, DEMATREE et HUB ont besoin pour fonctionner des composants suivants :

- un système d'exploitation de type Linux,
- un serveur web Apache,
- un serveur d'application Tomcat,
- un serveur de base de données PostgreSQL,
- un serveur ActiveMQ pour le dépôt de messages par l'application,
- un serveur STMP pour l'envoi des mails.

4.6. HYPOTHESES SUR L'ENVIRONNEMENT

4.6.1. Hypothèses sur l'environnement physique du produit

La plateforme est installée dans des locaux sécurisés et seuls les administrateurs techniques peuvent y accéder.

4.6.2. Hypothèses sur les utilisateurs du produit

Les administrateurs techniques et les administrateurs fonctionnels sont considérés comme étant formés, compétents et de confiance.

Les utilisateurs du portail respectent les procédures décrites dans les guides fournis [GUIDES].

4.7. ENVIRONNEMENT TECHNIQUE DE L'EVALUATION

4.7.1. Conditions d'évaluation

Les dépendances techniques retenues pour la plateforme d'évaluation sont :

- Système d'exploitation Debian version 7 64 bits
- Serveur Apache version 2.2
- Serveur Tomcat version 7
- Serveur PostgreSQL version 9.1
- Serveur ActiveMQ version 5.13

Une architecture de type 3-tiers sera installée pour la plateforme d'évaluation :

- Frontal web Apache,
- Serveur transactionnel Tomcat sur lequel sont installés les modules logiciels ADMIMAIL, DEMATREE et HUB,
- Serveur de base de données PostgreSQL,
- Serveur de messagerie SMTP.

4.7.2. Configuration d'évaluation

Pour l'évaluation, une démarche type a été configurée. La configuration des modules logiciels évalués est décrite dans le document annexe [PARAM].

5. BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Le produit doit protéger les données suivantes :

- **Données usagers** : identifiants, empreintes des mots de passe et données envoyées par les usagers.
  Protection : Intégrité et Confidentialité
- **Dossiers** : un dossier est composé de la demande des usagers et de l'instruction correspondante.
  Protection : Intégrité et Confidentialité
- **Organigramme** : il contient les droits des chefs de service sur les services et sur les dossiers ainsi que les droits des agents sur les dossiers. Les identifiants et empreintes des mots de passe des agents et chefs de service entrent aussi dans cette catégorie de biens sensibles.
  Protection : Intégrité et Confidentialité

6. DESCRIPTION DES MENACES

6.1. SOURCES DE MENACES

Les sources menaçantes considérées pour l'évaluation sont :

- Un internaute malveillant : une personne présente sur internet, sans compte valide sur l'application,
- Un usager malveillant : un utilisateur ayant un compte temporaire ou valide sur le portail.
- Un agent malveillant,
- Un chef de service malveillant.

6.2. LISTE DES MENACES RETENUES

6.2.1. Menaces liées à un internaute malveillant

- M1. Usurpation d'identité d'un usager

Un internaute malveillant se connecte sur le compte d'un usager.

Biens impactés : données usagers (en confidentialité et en intégrité)

- M2. Usurpation d'identité d'un agent, d'un chef de service ou d'un administrateur fonctionnel

Un internaute malveillant se connecte sur le compte d'un agent, d'un chef de service ou d'un administrateur fonctionnel.

Biens impactés : dossiers et organigramme (en confidentialité et en intégrité)

6.2.2. Menaces liées à usager malveillant

- M3. Usurpation d'identité d'un autre usager

Un usager malveillant se connecte sur le compte d'un autre usager.

Biens impactés : données usagers (en confidentialité et en intégrité)

- M4. Usurpation d'identité d'un agent, d'un chef de service ou d'un administrateur fonctionnel

Un usager malveillant se connecte sur le compte d'un agent, d'un chef de service ou d'un administrateur fonctionnel.

Biens impactés : dossiers et organigramme (en confidentialité et en intégrité)

6.2.3. Menaces liées à un agent ou un chef de service malveillant

- M5. Usurpation d'identité d'un usager

Un agent ou un chef de service malveillant se connecte sur le compte d'un usager.

Biens impactés : données usagers (en confidentialité et en intégrité)

- M6. Usurpation d'identité d'un agent, d'un chef de service ou d'un administrateur fonctionnel

Un agent ou un chef de service malveillant se connecte respectivement sur le compte d'un autre agent ou d'un autre chef de service ou d'un administrateur fonctionnel.

Biens impactés : dossiers et organigramme (en confidentialité et en intégrité)

- M7. Élévation de privilèges

Un chef de service malveillant ou un agent malveillant réussit à s'octroyer des droits illégitimes.

Biens impactés : dossiers et organigramme (en confidentialité et en intégrité)

6.2.4. Menaces liées à tous les agents menaçants

- M8.accès illégitime

Un agent menaçant réalise une opération illégitime sur un dossier. Une opération illégitime correspond à la création, diffusion, modification ou suppression d'un dossier sans avoir les droits nécessaires.

Biens impactés : dossiers (en confidentialité et en intégrité)

- M9.MITM

Un agent menaçant réussit à écouter ou altérer un flux de communication :

  - communication entre un usager et le portail 6Tzen Portail,
  - communication entre un administrateur fonctionnel, un chef de service ou un agent et le portail d'administration 6Tzen Admin.

Biens impactés : tous les biens (données usagers, dossiers, organigrammes) qui circulent entre les utilisateurs et les portails (en confidentialité et en intégrité)

7. DESCRIPTION DES FONCTIONS DE SECURITE

7.1. LISTE DES FONCTIONS DE SECURITE

Le périmètre d'évaluation couvre les fonctions de sécurité suivantes du produit :

7.1.1. F1.Authentification des usagers

Les utilisateurs du portail (usagers) se connectent à leur compte avec un identifiant et un mot de passe.

7.1.2. F2.Communications sécurisées

Les flux de communication entre les utilisateurs du produit et le produit sont protégés par un tunnel TLS avec authentification du portail (authentification serveur).

7.1.3. F3.Authentification des administrateurs fonctionnels, des chefs de service et des agents

Les administrateurs fonctionnels, les chefs de service et les agents se connectent à leur compte avec un identifiant et un mot de passe.

7.1.4. F4.Gestion des droits

Une gestion fine des droits est mise en place.

Un chef de service est affecté sur un ou plusieurs services :

- Il peut créer, consulter, modifier ou supprimer ou transférer à un autre service le dossier.
- Il peut affecter un dossier à un agent.

Un agent peut faire partie d'un ou plusieurs services :

- selon ses droits, un agent peut créer, consulter, modifier ou supprimer un dossier.
- selon le type de document

Chaque utilisateur peut déléguer ses droits, sur une période qu'il définit, à un autre utilisateur.

7.1.5. F5.Traçabilité

Toutes les opérations effectuées sur les dossiers (sauf la simple consultation) sont tracées dans le dossier.

Toutes les opérations réalisées par les usagers sur leur compte sont tracées.

7.2. ARGUMENTAIRE DES FONCTIONS DE SECURITE

Le tableau ci-dessous indique comment chaque menace identifiée est couverte par les fonctions de sécurité évaluées.

Tableau 1: Tableau de couverture des menaces par les fonctions de sécurité

Sources de menaces	**Menaces**	**Fonctions de sécurité permettant de contrer les menaces**
Internaute malveillant	M1	F1, F2
	M2	F2, F3
Usager malveillant	M3	F1, F2, F5
	M4	F2, F3, F5
Agent, chef de service malveillant	M5	F1, F2
	M6	F2, F3
	M7	F4
Tous les agents malveillants	M8	F4, F5
	M9	F2