RecoNet & EvalSMSI

Outils pour la SSI

Michel Dubois

myshell.dubois@gmail.com

http://reconet.sourceforge.net
http://evalsmsi.sourceforge.net

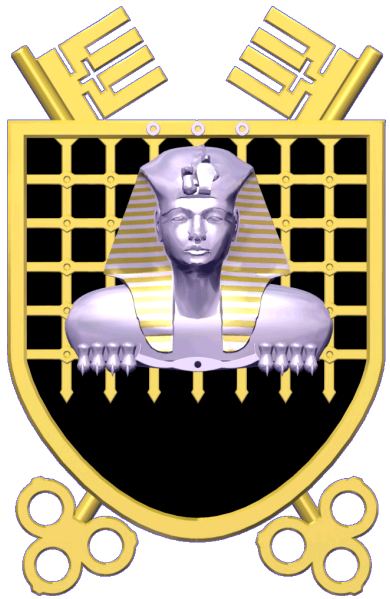
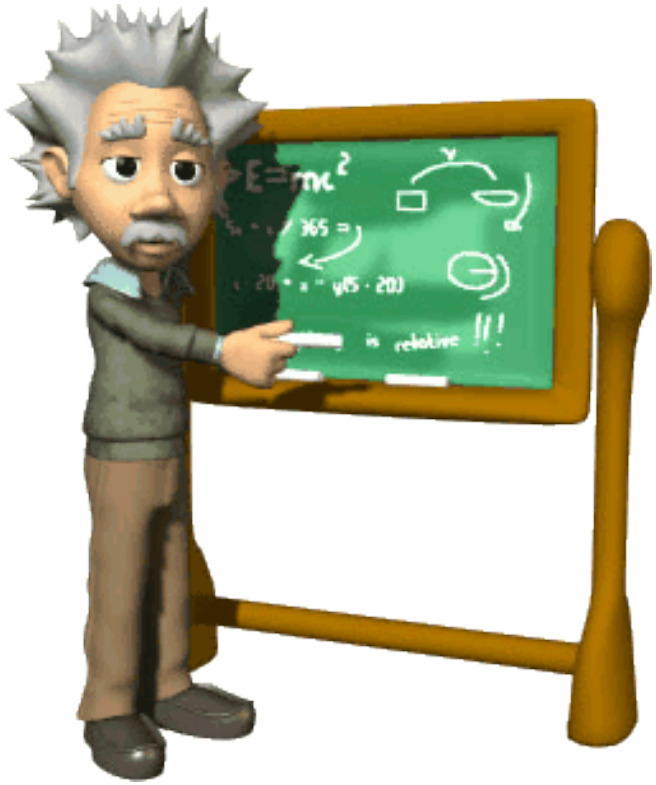


Table des matières

1. Reconet
   - Tests d'intrusions
   - Automatisation...
   - l'outil RecoNet
2. EvalSMSI
   - ISO 27001 & SMSI
   - l'application EvalSMSI

Reconet

1 Reconet
- Tests d'intrusions
- Automatisation...
- l'outil RecoNet



Définition & Objectifs

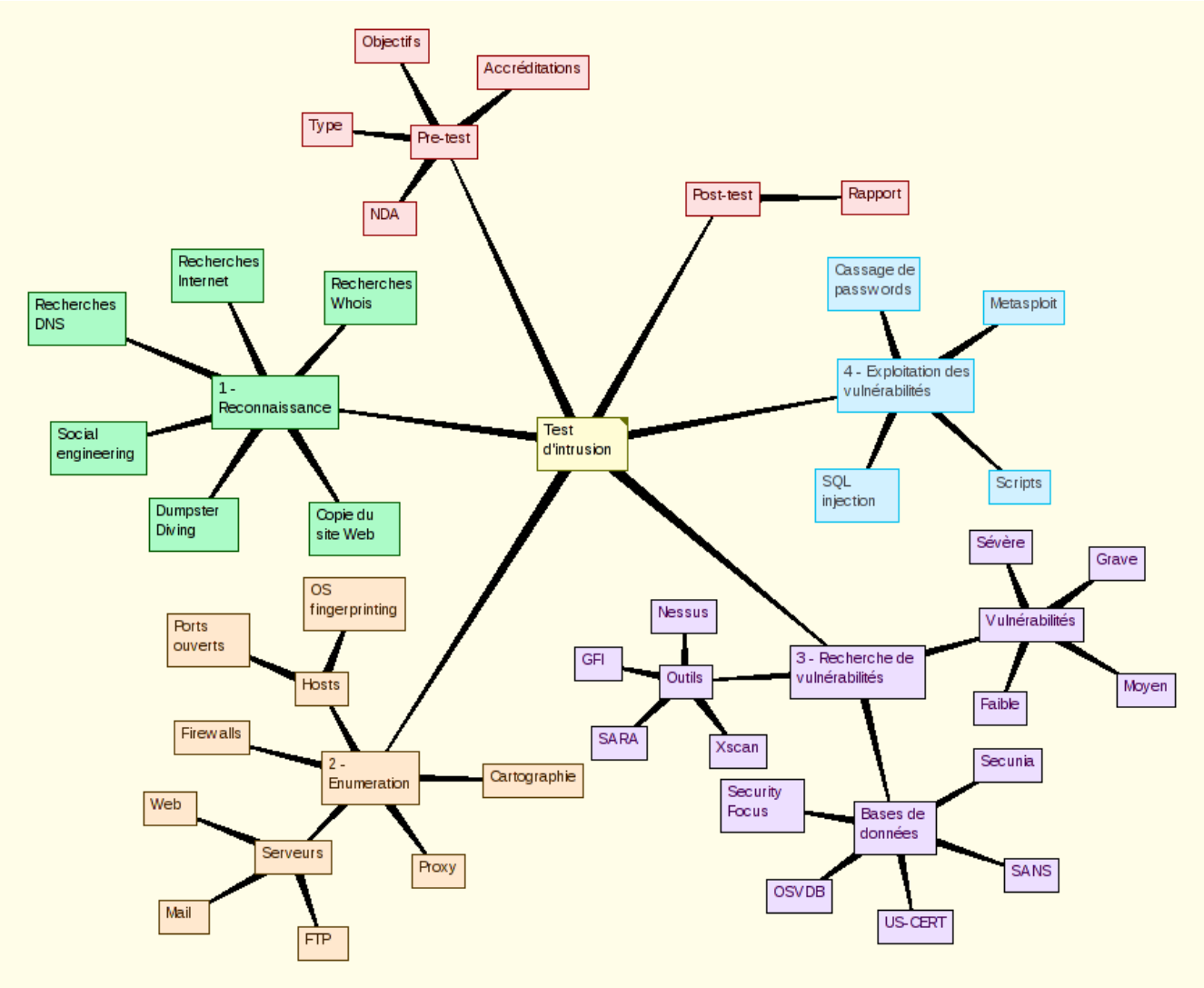
Définition

Un test d'intrusion est une méthode d'**évaluation de la sécurité d'un système d'information** basée sur la simulation d'une attaque, interne ou externe, par un cybercriminel.

Il s'agit de déterminer :

- la faisabilité d'une attaque
  - sur un système cible
  - à un instant donné
- la gravité de l'impact sur le SI
  - gravité d'une attaque potentielle
  - niveau technique estimé pour réaliser l'attaque

Logigramme d'un test



4 phases

- **Phase 1** : reconnaissance active et passive
- **Phase 2** : énumération et cartographie
- **Phase 3** : recherche de vulnérabilités
- **Phase 4** : exploitation des vulnérabilités

4 phases

- **Phase 1** : reconnaissance active et passive
- **Phase 2** : énumération et cartographie
- **Phase 3** : recherche de vulnérabilités
- **Phase 4** : exploitation des vulnérabilités

4 phases

- **Phase 1** : reconnaissance active et passive
- **Phase 2** : énumération et cartographie
- **Phase 3** : recherche de vulnérabilités
- **Phase 4** : exploitation des vulnérabilités

4 phases

- **Phase 1** : reconnaissance active et passive
- **Phase 2** : énumération et cartographie
- **Phase 3** : recherche de vulnérabilités
- **Phase 4** : exploitation des vulnérabilités

Automatisation ?

Constats

- Augmentation du nombre de demandes de tests
- Ressources en experts insuffisantes
- Durée d'un test relativement longue
- Travail sur un environnement en production
- Grande diversité des SI

Conséquence

Besoin de gagner du temps

Possibilité d'automatiser certaines parties du test ?

Automatisation ?

Constats

- Augmentation du nombre de demandes de tests
- Ressources en experts insuffisantes
- Durée d'un test relativement longue
- Travail sur un environnement en production
- Grande diversité des SI

Conséquence

Besoin de gagner du temps

Possibilité d'automatiser certaines parties du test ?

Automatisation ?

Constats

- Augmentation du nombre de demandes de tests
- Ressources en experts insuffisantes
- Durée d'un test relativement longue
- Travail sur un environnement en production
- Grande diversité des SI

Conséquence

Besoin de gagner du temps

Possibilité d'automatiser certaines parties du test ?

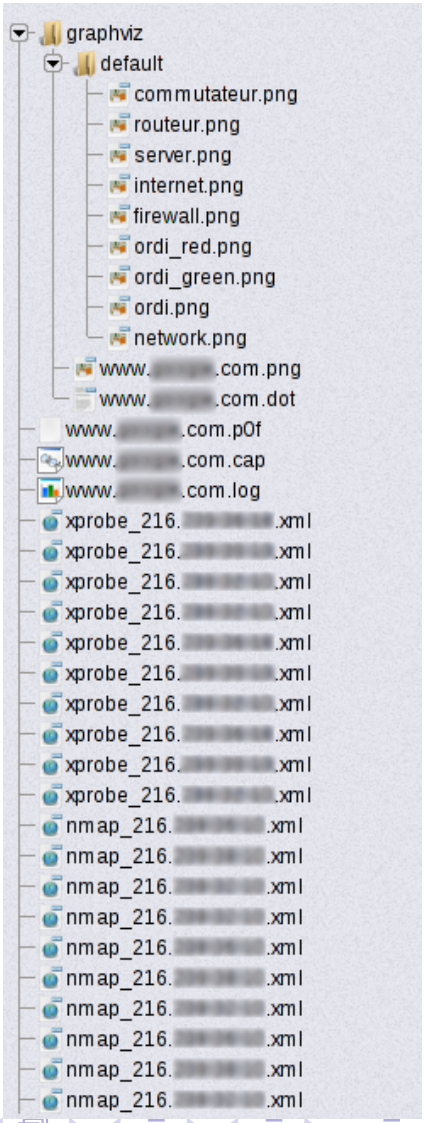
Description de reconet

RECONET

- automatisation des phases 1 et 2
- logiciel écrit en python
- cartographie du réseau étudié
- fichier de logs détaillé

Résultats obtenus

- un fichier de log
- un fichier HTML généré par netcraft
- fichiers `nmap` & `xprobe`
- un fichier généré par `p0f`
- un fichier de capture `tcpdump`
- un fichier `graphviz`



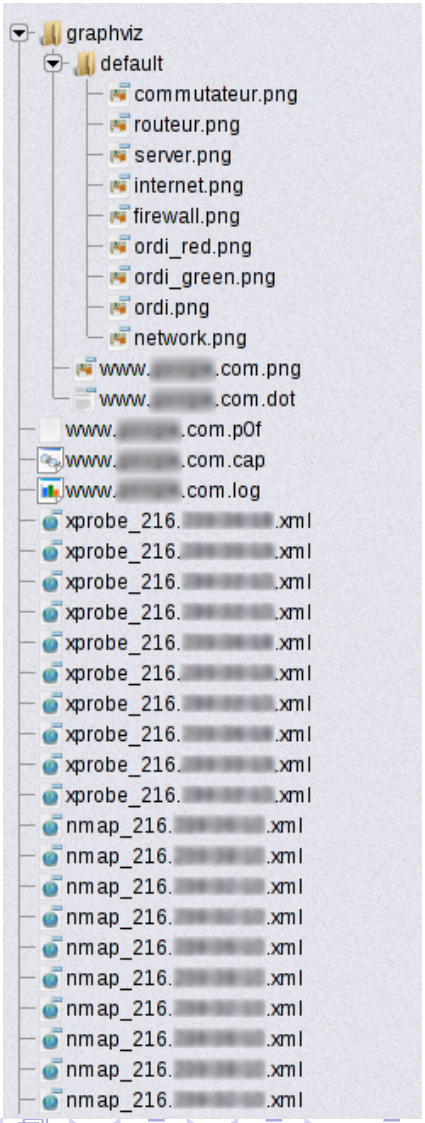
Description de reconet

RECONET

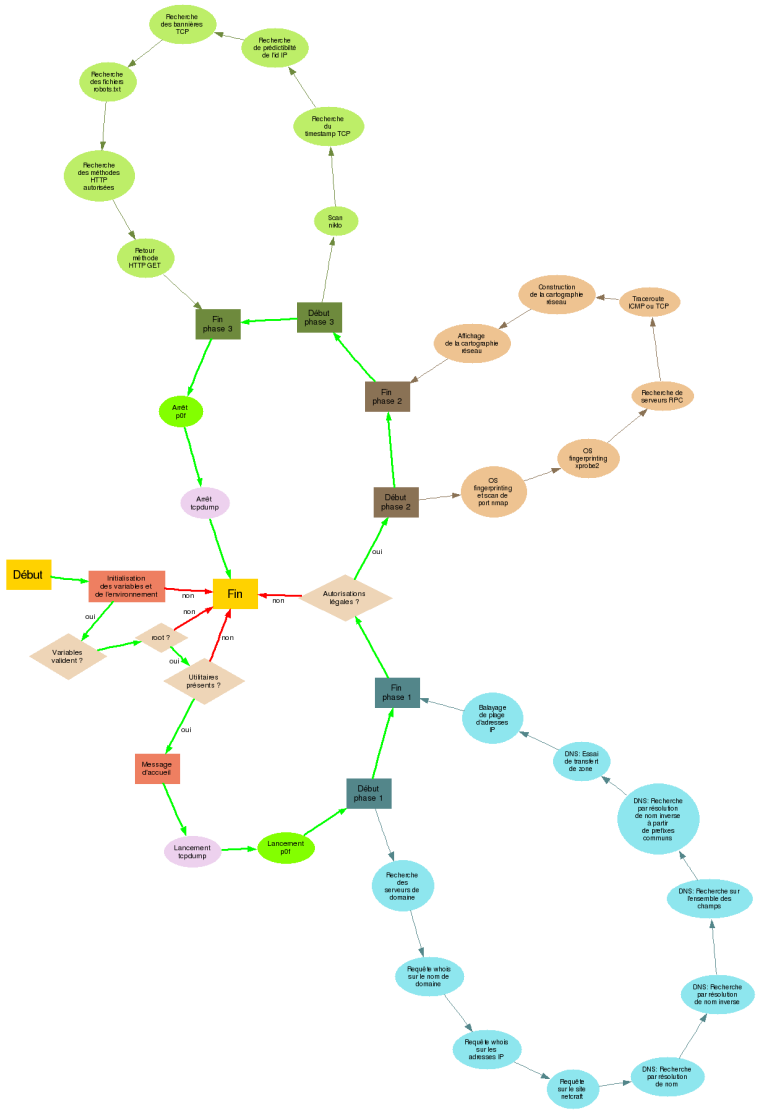
- automatisation des phases 1 et 2
- logiciel écrit en python
- cartographie du réseau étudié
- fichier de logs détaillé

Résultats obtenus

- un fichier de log
- un fichier HTML généré par netcraft
- fichiers `nmap` & `xprobe`
- un fichier généré par `p0f`
- un fichier de capture `tcpdump`
- un fichier `graphviz`



Fonctionnement de reconet



Détails...

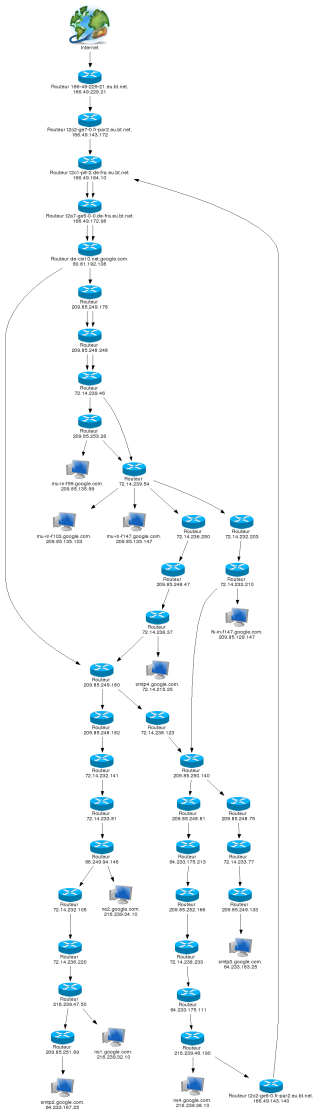
Ligne de commande :

```
# ./reconet.py
Michel Dubois -- reconet.py -- (c) 2007
Syntaxe:        reconet.py [-h -v] -s <server>
Options:        -h [--help]     affichage de l'aide
                -v [--verbose]  mode verbose
                -s [--server]   URL du site Web

# ./reconet.py -v -s www.google.com
```

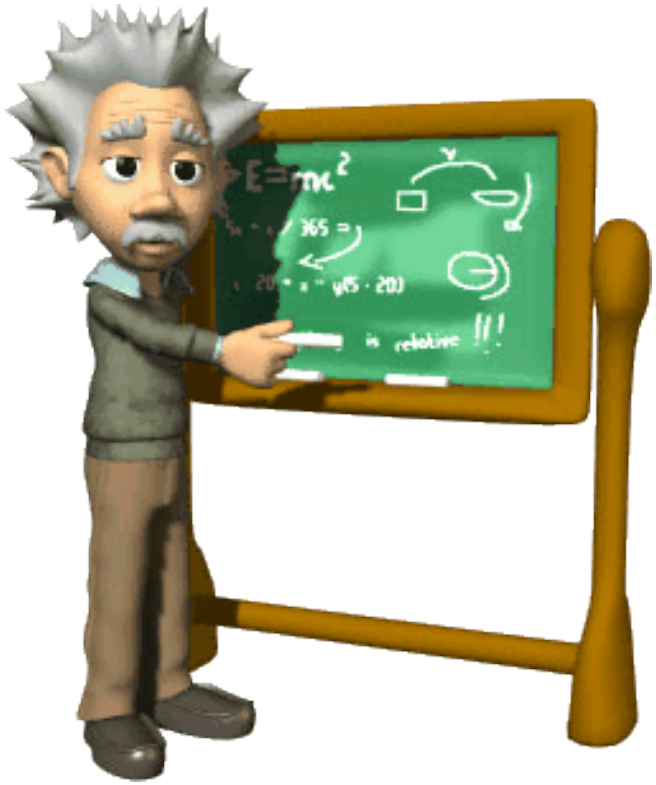
- initialisation de l'environnement
- test de la présence des utilitaires
- lancement tcpdump & p0f
- énumération : DNS, whois, netcraft, transfert de zones, balayage de préfixes communs, scan plage d'adresses IP
- Fingerprinting : nmap, xprobe2
- scan de ports
- traceroute ICMP et TCP
- construction de la carte (graphviz)

Détails...



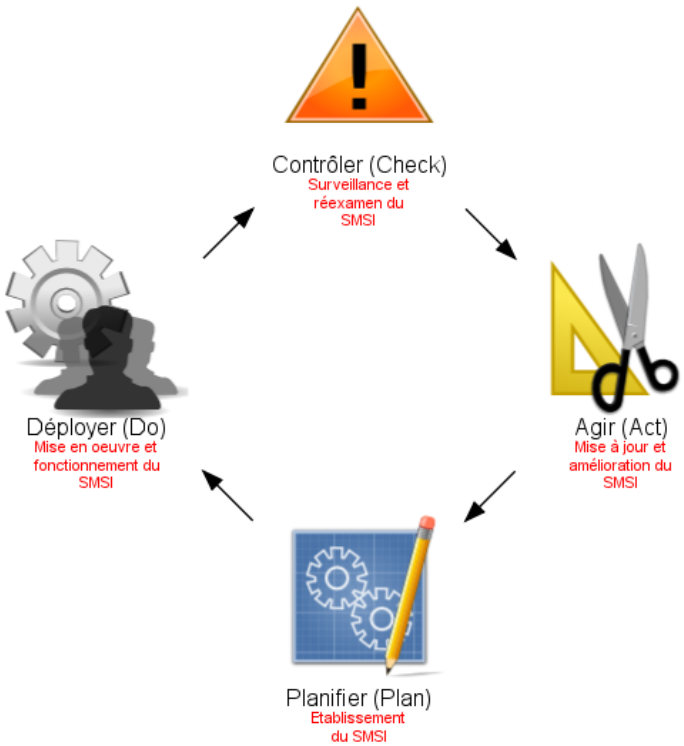
- Scan `nikto`
- Timestamp TCP, prédictibilité id IP (`hping`)
- Recherche bannière TCP, robots.txt (`netcat`)
- Recherche méthode HTTP autorisées,retour méthode GET,...

EvalSMSI



2 EvalSMSI
- ISO 27001 & SMSI
- l'application EvalSMSI

Objectifs



ISO 27001 *Source HSC*

Il s'agit de spécifier les `exigences` pour

- mettre en place
- exploiter
- améliorer

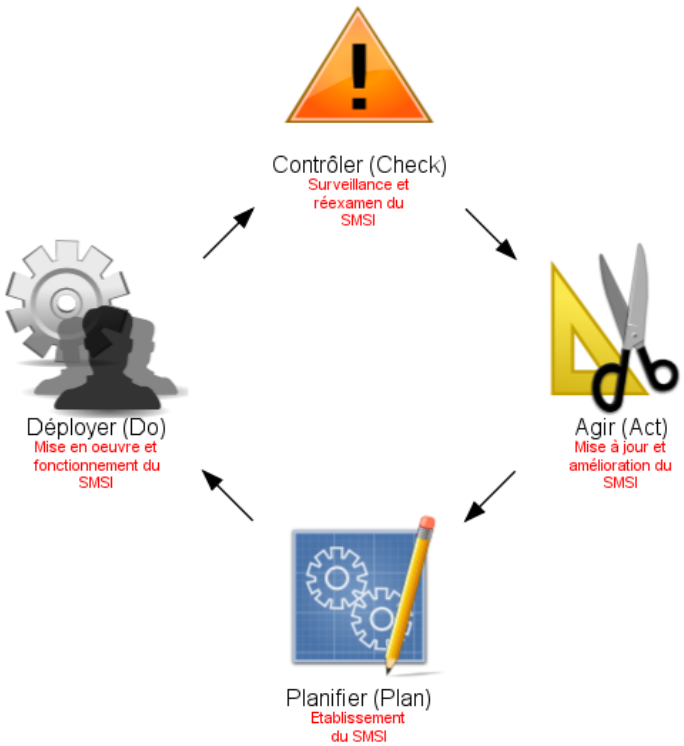
un `SMSI`

SMSI *Source HSC*

Un système de management est un système permettant

- de définir une politique
- d'établir des objectifs
- d'atteindre ces objectifs

Objectifs



ISO 27001 *Source HSC*

Il s'agit de spécifier les `exigences` pour

- mettre en place
- exploiter
- améliorer

un `SMSI`

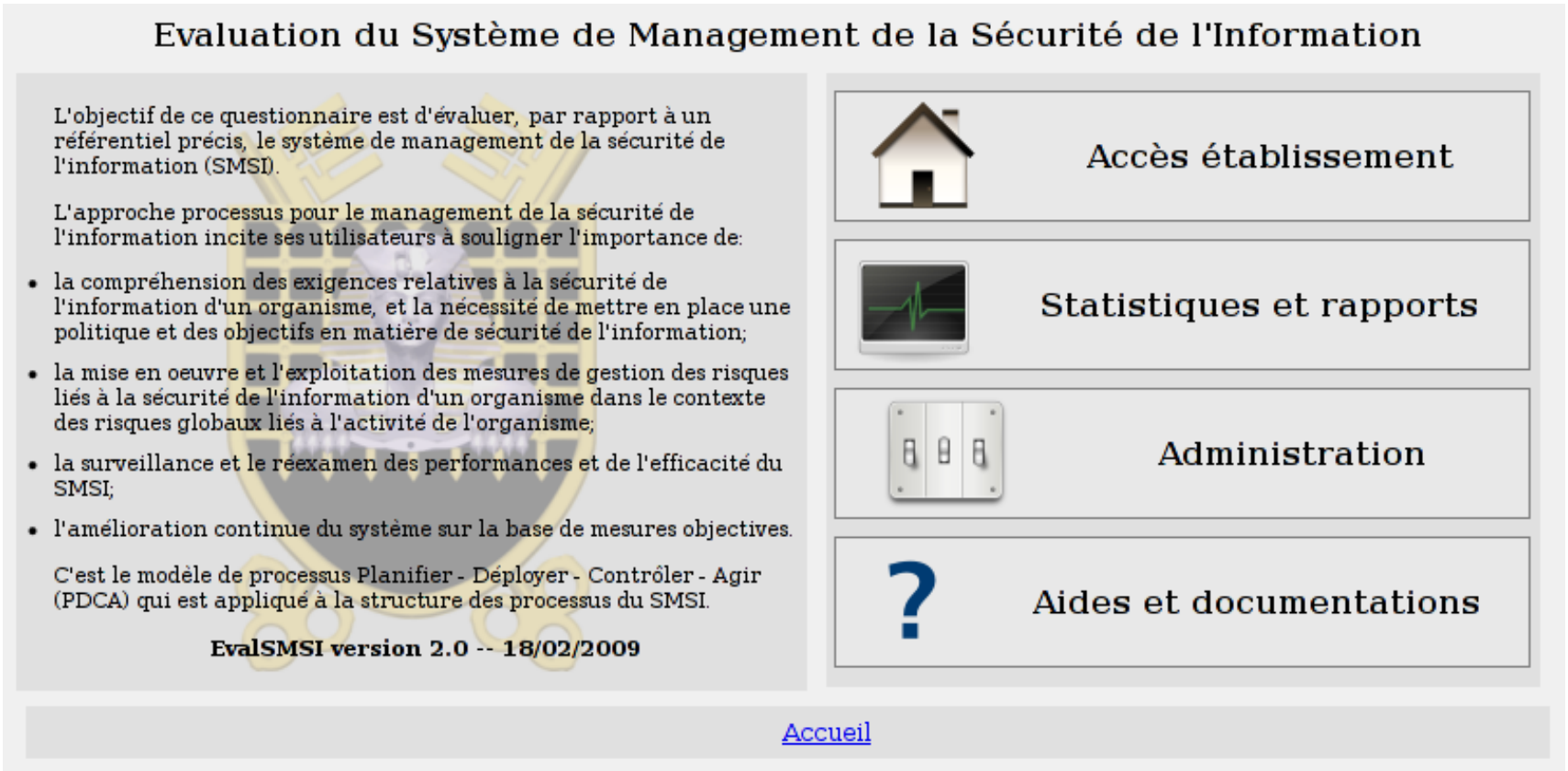
SMSI *Source HSC*

Un système de management est un système permettant

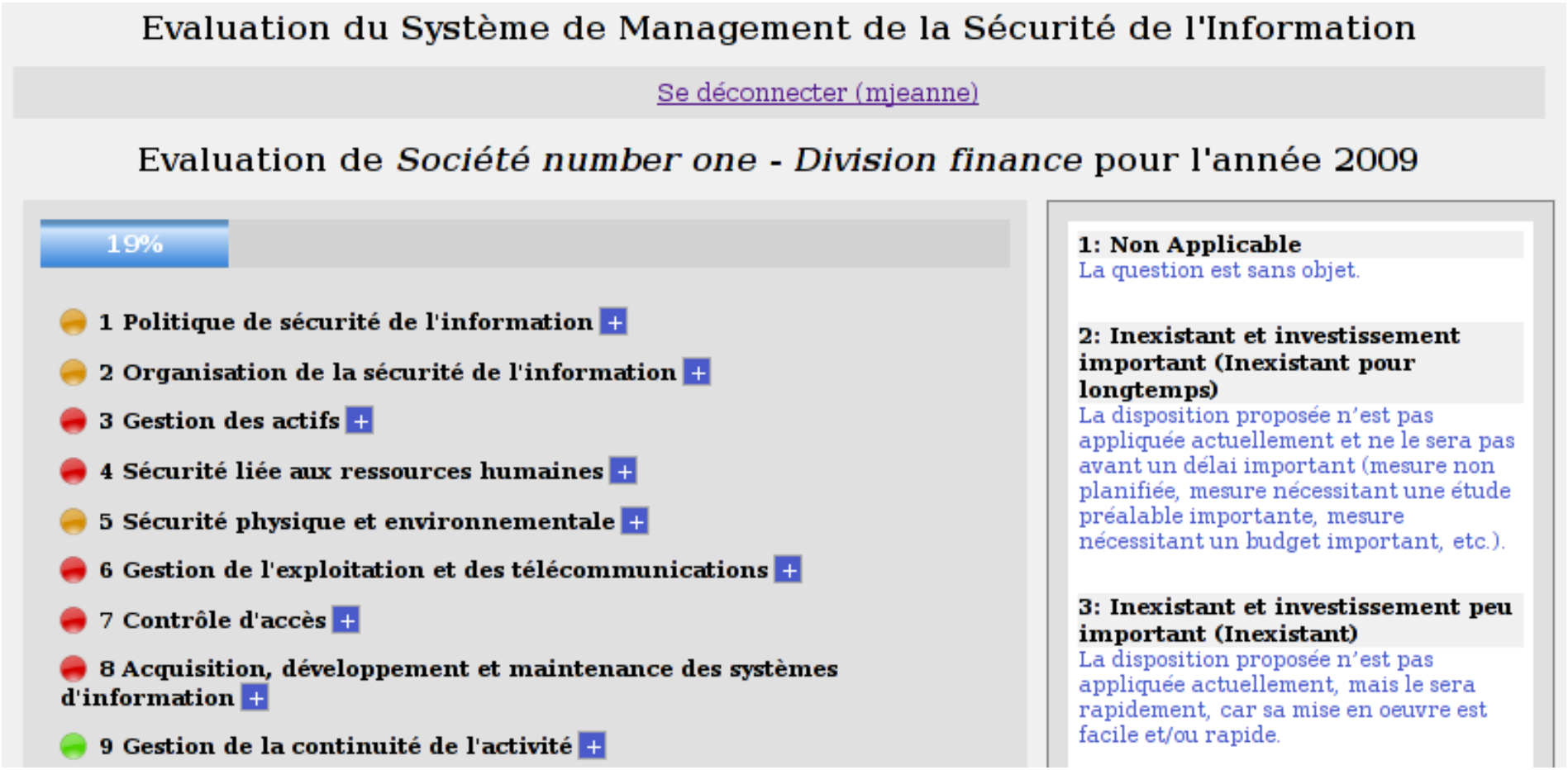
- de définir une politique
- d'établir des objectifs
- d'atteindre ces objectifs

Justification

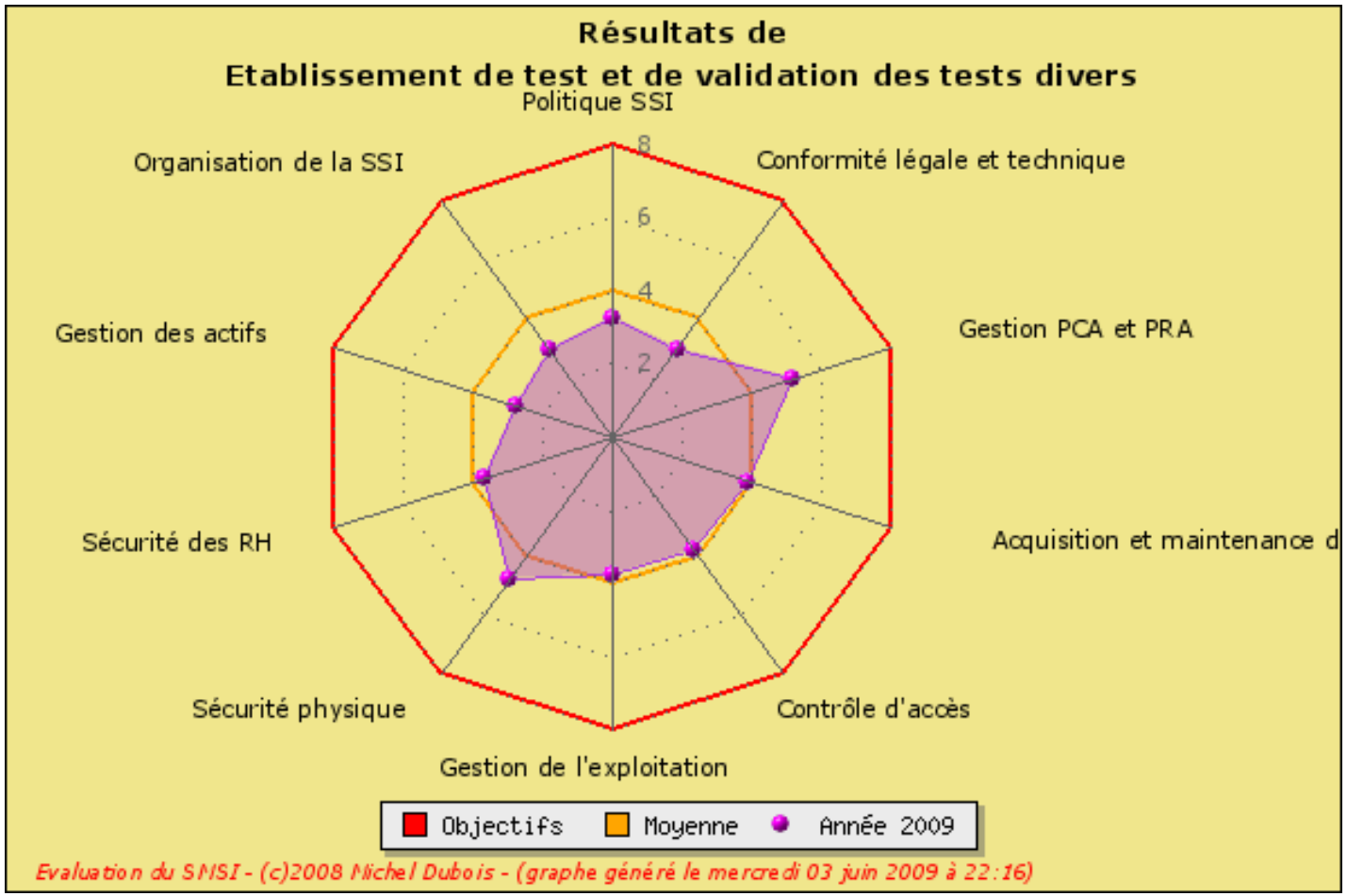
Faciliter les opérations d'`audit interne` et de `suivi des actions` liées au management de la sécurité de l'information.



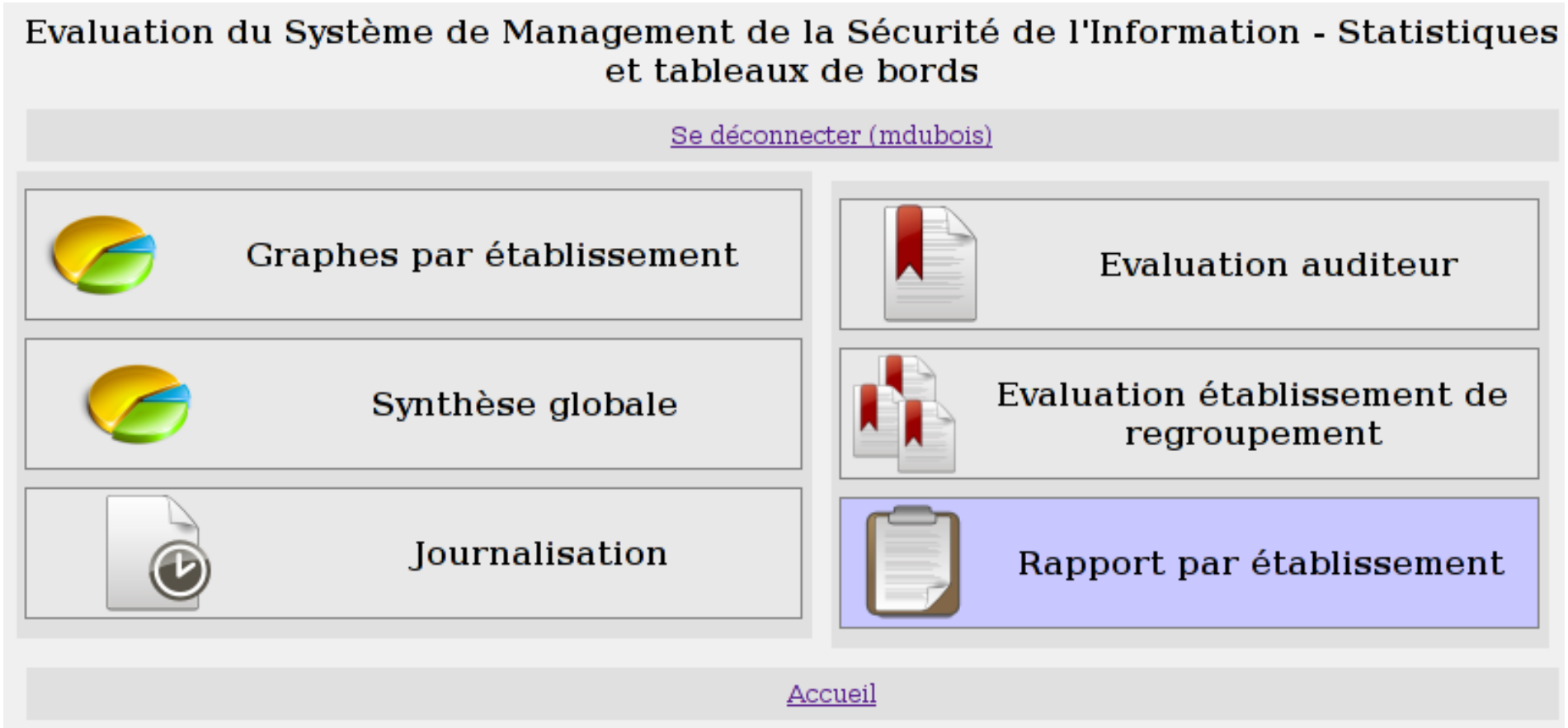
Fonctionnement — évaluation interne par questionnaire



Fonctionnement — génération de graphes



Fonctionnement — tableau de bord évaluateur



Fonctionnement — génération automatique de rapport

Rapport d'évaluation du
Système de Management de la Sécurité de l'Information
Etablissement de test et de validation des tests divers

Michel Dubois – RSSI

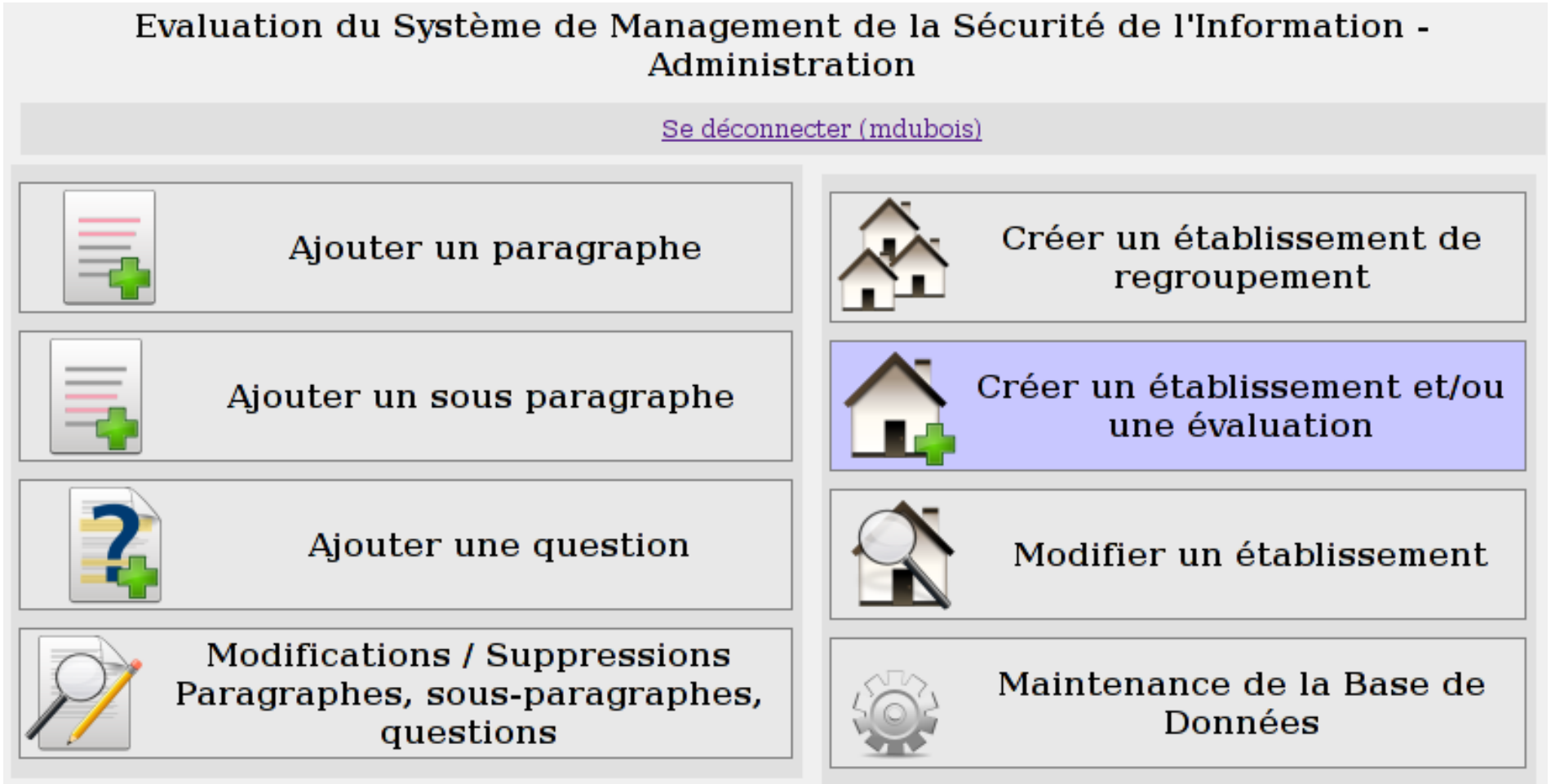
3 juin 2009

Résumé

Ce rapport décrit le résultat de l'évaluation du Système de Management de la Sécurité de l'Information (SMSI) réalisé par *Etablissement de test et de validation des tests divers* en 2009. L'évaluation initiale a été contrôlée le 3 juin 2009 par Michel Dubois – Responsable Sécurité des Systèmes d'Information (RSSI). Cette évaluation repose sur un questionnaire établit conformément aux normes ISO 27001 et ISO 27002.

- Directeur de l'établissement : *Monsieur Jean Aymard de la ssi*
- RSSI de l'établissement : *Monsieur Louis Dupont*

Fonctionnement — administration de l'application



Questions ?