exaprotect

EXAPROTECT SECURITY MANAGEMENT SOLUTION

Cible de Sécurité

TYPE :	Critères Communs
REDACTEUR :	L. Pautet, C. Pommier
VALIDATEUR :	L. Pautet
ETAT :	Final
REFERENCE :	SMSSecurityTarget-fr
VERSION :	1.8
DIFFUSION :	DCSSI, Publique

Fiche de contrôle du document

Résumé :	Ce document constitue la cible de sécurité du produit ExaProtect Security Management Solution.

Fichier source :	partner-SMSSecurityTarget-18-fr.doc
Date de création :	23/11/2005
Date de dernière modification :	15/07/2008 16:32

Validation :	

Version	Date	Auteur(s)	Commentaire(s)
0.1	23/11/2005	L. Pautet	Version initiale
0.2	14/12/2005	L. Pautet	Mise à jour suite à relecture
0.3	17/01/2006	L. Pautet	Ajout des chapitres Critères Communs
1.0	25/04/2006	L. Pautet	Mise à jour après relecture
1.1	19/04/2006	L. Pautet	Mise à jour après retour DCSSI
1.2	27/04/2006	L. Pautet	Petites corrections
1.3	15/05/2006	L. Pautet	Mise à jour après retour DCSSI
1.4	05/02/2007	C. Pommier	Mise à jour des terminologies utilisées Mise à jour après retour CESTI
1.5	06/07/2007	C. Pommier	Mise à jour suite au rapport technique intermédiaire de l'évaluateur
1.6	11/07/2007	C. Pommier	Petites corrections
1.7	04/07/2008	C. Pommier	Petites corrections
1.8	15/07/2008	C. Pommier	Petites corrections sur les algorithmes de chiffrement

Sommaire

I Introduction

I.1 Objectif du document

Le présent document constitue la **cible de sécurité** du produit **ExaProtect Security Management Solution** (SMS) de la société ExaProtect. La version prise en compte est 2.7 :

- Nom de ce document : ExaProtect Security Management Solution – Cible de sécurité
- Version : 1.7
- Identifiant de la TOE : ExaProtect Security Management Solution (ou ExaProtect SMS)
- Version : 2.7
- Référence Critères Commun : Version 2.3 d'Août 2005

Ce document précise les exigences de sécurité en termes fonctionnels et en termes de tâches d'évaluation qui doivent être satisfaites par le produit évalué (la cible de l'évaluation - la TOE) afin de faire face aux menaces potentielles en exploitation.
La cible de sécurité indique également comment le produit évalué répond à ces exigences.

I.2 Organisation du document

- Le **Chapitre 1** constitue l'introduction du document.
- Le **Chapitre 2** décrit dans un langage naturel les services fournis par le produit évalué (la TOE) ainsi que son architecture.
- Le **Chapitre 3** précise les conditions prévues d'exploitation du produit évalué ; en particuliers les menaces auxquelles le produit aura à faire face.
- Le **Chapitre 4** indique les objectifs de sécurité à atteindre par le produit et par son environnement d'exploitation pour contrer les menaces identifiées.
- Le **Chapitre 5** détaille les exigences de sécurité à satisfaire pour atteindre ces objectifs de sécurité : exigences fonctionnelles et exigences d'assurance.
- Le **Chapitre 6** indique les fonctionnalités présentes dans le produit évalué pour répondre aux exigences fonctionnelles et les mesures mises en place pour répondre aux exigences d'assurance.
- Le **Chapitre 7** indique si le produit évalué se veut également conforme aux exigences spécifiées dans un profil de protection (PP).
- Le **Chapitre 8** regroupe tous les argumentaires permettant de s'assurer notamment de la couverture complète des menaces par les objectifs de sécurité et les exigences de sécurité ou de la couverture des exigences fonctionnelles par les fonctionnalités du produit.
- Le **Chapitre 9** contient un glossaire des termes techniques et autres acronymes utilisés dans le document.
- Le **Chapitre 10** contient les références précises des documents mentionnés dans le document.

I.3 Conformité aux critères communs

Le présent document est conforme aux exigences des Critères Communs 2.3 [CC] relatives aux cibles de sécurité.

II Description du produit évalué

Le présent chapitre précise le périmètre logique et physique de la cible de l'évaluation (la TOE).

II.1 Services fournis par le produit

La solution ExaProtect SMS permet de répondre aux challenges de supervision de la sécurité que l'on peut résumer de la manière suivante :

- Gérer un grand nombre de dispositifs de sécurité répartis sur l'ensemble du système d'information
- Traiter la masse d'information générée par les dispositifs
- Enrichir les évènements (réduction des faux positifs, prise en compte du contexte « métier »)
- Corréler les évènements provenant de différents dispositifs et générer des alertes
- Automatiser le processus de diagnostic
- Focaliser l'expertise humaine sur la menace la plus importante
- Proposer des contre mesures lorsque c'est possible
- Fournir une vue synthétique et globale sur le risque et la menace

Ces services sont réalisés par les deux composants principaux **ExaProtect Security Management Agent** (SMA) et **ExaProtect Security Management Platform** (SMP). L'analyse des évènements de sécurité et la configuration de la solution est réalisé via la console **ExaProtect Security Management Console** (SMC) depuis un poste avec un navigateur Web.

La terminologie employée dans la solution ExaProtect SMS est la suivante :

Equipement :	Elément du système d'information générant au cours de son fonctionnement des entrées de log susceptibles de contenir des informations intéressantes d'un point de vue sécurité (firewall, IDS, proxy, systèmes Unix/Windows, application Web …).
Entrée de log:	Message enregistré par une application, un système d'exploitation ou un dispositif de sécurité. Cela peut être une ligne de fichier texte décrivant l'échec d'une tentative de connexion ou un enregistrement dans une base de données indiquant qu'un utilisateur s'est authentifié avec succès.
Log brut :	Enregistrement généré optionnellement par le SMA étant la représentation fidèle au format texte d'une entrée de log.
Evènement :	Objet de données standardisé (IDMEF) représentant une entrée de log, créé par un Security Management Agent.
Alertes :	Evènement IDMEF agrégé, corrélé, enrichi ou modifié (évènement traité par le moteur de corrélation). Les alertes sont créées sur le Security Management Platform.
Corrélation :	Mise en relation d'information de différents types, provenant de sources différentes (évènement provenant d'un scanner, évènement provenant d'un IDS, base de vulnérabilités, règles de corrélation…).
Alerte de corrélation :	Alerte générée par le serveur ExaProtect SMP regroupant des évènements et/ou des alertes.

Incident :	Container d'alertes au format IODEF qui permet d'assurer le suivi du traitement de ces alertes en précisant notamment la cause, les actions à effectuer (interfaçage possible avec un logiciel de gestion de tickets tiers).

La solution ExaProtect SMS fournit les services suivants :

La collecte de logs de sécurité : Depuis des agents installés sur des équipements intégrés aux systèmes d'information (pare-feu, routeur, serveur,..) les entrées de log sont collectées. Les mécanismes de collecte mis en œuvres dans la solution ExaProtect SMS utilisent plusieurs modes : collecte dans un fichier à plat, dans une base de données, via Syslog ou bien également à l'aide de protocoles propriétaires (ex : OPSEC). Les échanges agent-serveur sont sécurisés par des certificats dont la racine de confiance est située sur le serveur SMP.

La consolidation : La consolidation des entrées de log s'effectue par les agents, en les filtrant, les normalisant dans un format basé sur IDMEF, tout en leur attribuant un label issu d'une taxonomie d'évènements. Les évènements normalisés sont ensuite centralisés via une communication sécurisée sur un serveur central (ExaProtect SMP).

L'analyse : Les évènements sont regroupés, enrichis et corrélés, des alertes de corrélation sont générées de façon à être facilement et humainement traitables par les analystes sécurité. Ce module constitue l'intelligence de la solution ExaProtect SMS et sa véritable valeur ajoutée. Le processus de traitement de la solution ExaProtect SMS contribue à diminuer très significativement le nombre d'alertes à traiter par l'analyste sécurité (de plusieurs millions à quelques dizaines) et à augmenter leur pertinence.

L'audit et l'expertise *:* L'investigation et l'acquittement de chacune des alertes critiques ainsi que le suivi des incidents (traitement d'un ensemble d'alertes) sont réalisés par un analyste sécurité au travers de l'interface de la solution ExaProtect SMS (SMC).

Le compte rendu : Enfin, les tableaux de bord orientés « sécurité » et « organisation » sont destinés aux analystes sécurités et à la direction de l'organisation. Ils prennent en compte des indicateurs métiers de l'entreprise. Ce module de l'application ExaProtect SMS permet de synthétiser l'ensemble des informations traitées préalablement et de les présenter de manière organisée, pertinente et orientée métier.
Ce service ne fait pas partie du périmètre de l'évaluation.

Le schéma ci-dessous présente la vision globale du concept ExaProtect SMS.

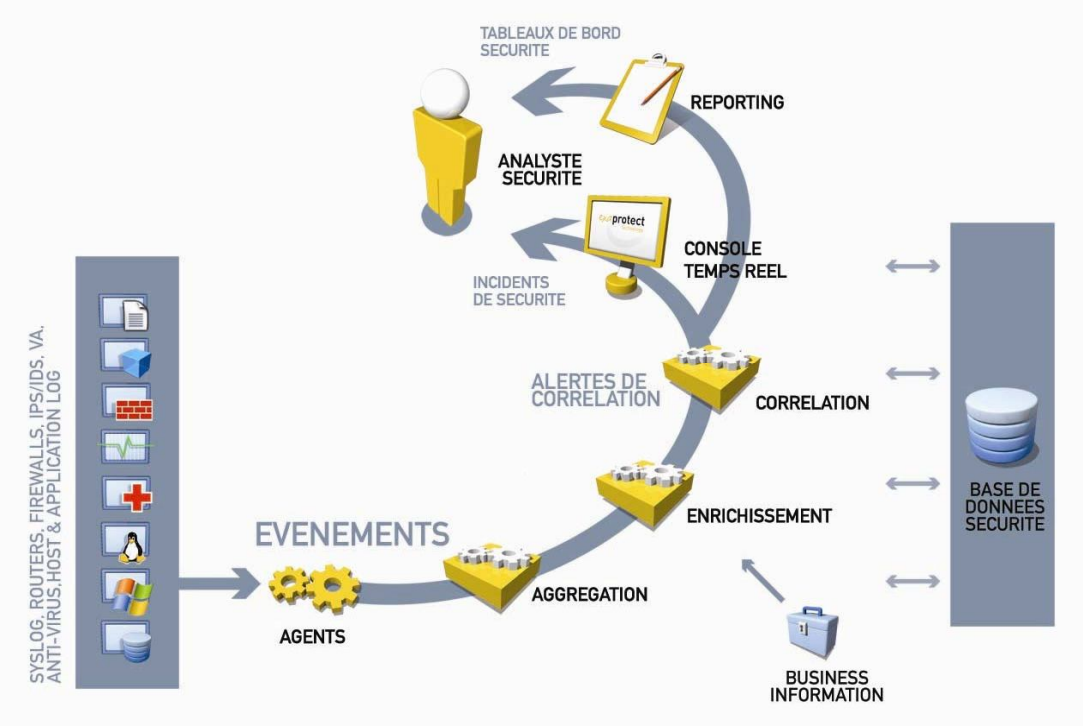

Figure 1: Concept de la solution ExaProtect SMS

II.2 Biens sensibles

II.2.1 Biens sensibles internes à la TOE

Il s'agit des biens nécessaires au fonctionnement des fonctions de sécurité de la TOE et qui doivent être protégés pour assurer le fonctionnement et la sécurité du produit ExaProtect SMS.

Les fichiers de configurations placés sur le serveur ExaProtect SMP.

- **Les fichiers de paramétrage des règles de corrélation** (scénario, regroupements d'évènements, traitement spécifique d'une alerte). Ces données peuvent être modifiées au travers de l'interface homme-machine du produit.
  Ce bien est sensible vis-à-vis de l'intégrité et de la disponibilité.

- **Les fichiers de paramétrage du traitement des incidents** (ex : exécution d'un script à la clôture d'un incident).
  Ce bien est sensible du point de vue de l'intégrité.

- **Le fichier de paramétrage propre du serveur ExaProtect SMP** (base de données sur laquelle se connecter, login et mot de passe utilisé sur la base de données, services du produit à lancer…)
  Ce bien est sensible vis-à-vis de la confidentialité (divulgation du mot de passe de la base, de l'intégrité et de la disponibilité.

- **Les fichiers de paramétrage du traitement des évènements et des alertes** (durée de traitement autorisé, plages horaires, gestion du spooler de réception des évènements)
  Ce bien est sensible vis-à-vis de l'intégrité.

- **Les fichiers de configuration de la sauvegarde,** en particulier l'heure à laquelle l'archive est créée.
  Ce bien est sensible vis-à-vis de l'intégrité.

- **La base d'état des agents.**
  Ce bien est sensible vis-à-vis de l'intégrité et de la disponibilité.

Les fichiers de configurations placés sur les agents. Ils sont définis préalablement sur le serveur avant d'être répliqués sur l'agent via une connexion sécurisée.

- **Les fichiers de paramétrages spécifiques** à l'utilisation de l'agent (ex : adresse du serveur central).
  Ce bien est sensible vis-à-vis de l'intégrité (modification du comportement de l'agent) et dans une moindre mesure de la disponibilité et de la confidentialité.

- **Les fichiers de règles de transcription** contiennent ce qui est nécessaire pour définir comment un agent va transformer les entrées de log en évènement et filtrer les évènements générés.
  Ce bien est sensible vis-à-vis de l'intégrité et de la disponibilité (modification du comportement de l'agent à cause de la modification ou de la destruction du fichier).

Les biens liés aux utilisateurs du produit ExaProtect SMS.

- **La liste des utilisateurs autorisés** à utiliser la solution (stockés dans la base de données avec leur mot de passe associé).
  Ce bien est sensible vis-à-vis de l'intégrité, de la confidentialité et de la disponibilité.

Les biens liés à la protection des communications entre les agents et le serveur.

- **Bi-clé de l'autorité de certification** utilisée par le serveur dont l'autorité racine est située sur le serveur SMP
  Ce bien est sensible vis-à-vis de l'intégrité, de la confidentialité et de la disponibilité.

- **Bi-clé de l'agent** pour communiquer avec le serveur
  Ce bien est sensible vis-à-vis de l'intégrité, de la confidentialité et de la disponibilité.

- **Bi-clé du serveur**
  Ce bien est sensible vis-à-vis de l'intégrité, de la confidentialité et de la disponibilité.

Les biens liés à la protection des communications entre la console d'administration et le serveur ExaProtect SMP.

- **Bi-clé du serveur Web** TOMCAT
  Ce bien est sensible vis-à-vis de l'intégrité, de la confidentialité et de la disponibilité.

Les biens générés par la TOE et utilisés par les fonctions de sécurité.

- **Les alertes créées soit par l'utilisateur soit par le serveur** (alertes de corrélation) et stockées dans la base de données.
  Ce bien est sensible vis-à-vis de l'intégrité, de la confidentialité et de la disponibilité.

- **Les incidents** créés soit par l'utilisateur, soit par le moteur de corrélation et stockés dans la base de données
  Ce bien est sensible vis-à-vis de l'intégrité, de la confidentialité et de la disponibilité.

II.2.2 Biens sensibles externes à la TOE

Il s'agit des biens sensibles exploités par la TOE pour rendre son service.

- **Les évènements et les logs bruts remontés par les agents** et qui sont stockés dans la base de données du serveur et parfois (temporairement) sur l'agent lorsque la liaison agent-serveur est rompue (mécanisme de spool).
  Ce bien est sensible vis-à-vis de l'intégrité, de la confidentialité et de la disponibilité.

- **La base d'information :** modélisation des actifs de l'entreprise avec leur niveau de criticité, ce qui comprend les machines du parc supervisé, et les vulnérabilités associées.
  Ce bien est sensible vis-à-vis de l'intégrité et de la disponibilité, et parfois de la confidentialité lorsque les clients finaux du produit considèrent la liste de ses actifs comme confidentielle. Néanmoins, la TOE ne protège pas ces informations.

- **La base de vulnérabilité** embarquée contenant une liste de vulnérabilités connues sur des produits avec leurs références associées (CVE, Bugtraq ID).
  Ce bien est sensible vis-à-vis de l'intégrité et de la disponibilité.

II.3 Rôles

Le produit ExaProtect SMS s'appuie sur quatre rôles caractérisés par des droits d'accès différents aux fonctionnalités du produit et au paramétrage des fonctions de sécurité.

- Le rôle « **Viewer** » : ce rôle ne permet que la visualisation des informations via les différents écrans du produit (sur la console SMC).

- Le rôle « **Analyst** » : ce rôle permet de visualiser les alertes mais également de les acquitter. Ce rôle permet également d'activer ou de désactiver un agent mais pas de la configurer.

- Le rôle « **Administrator** » : ce rôle dispose des mêmes droits que le rôle « analyst » mais avec en plus la possibilité de configurer via la console SMC les agents et les règles de corrélation Par contre, ce rôle ne peut créer et configurer des utilisateurs ayant pour rôle « viewer » ou « analyst ».

- Le rôle « **Superuser** » : ce rôle dispose des mêmes droits que le rôle « administrator » mais avec en plus la possibilité de créer et de configurer tous les utilisateurs du produit.

Un cinquième rôle n'ayant pas de droits définis au sein de l'application existe : il s'agit de l' « **administrateur système** » qui installe le produit.

II.4 Architecture du produit évalué

II.4.1 Présentation des composants de la solution

L'architecture de la solution ExaProtect SMS repose sur le modèle CIDF[1] formalisant les systèmes de traitements d'événements de sécurité. CIDF distingue les fonctions suivantes :

- E-Box : Générateurs d'événements
- A-Box : Module d'analyse des événements
- D-Box : Base de données des événements
- R-Box : Unité de réponse et de contre mesure

La solution ExaProtect SMS reprend les composants décrits dans le modèle CIDF et les positionne sur plusieurs niveaux :

- Les **agents ExaProtect SMA** – il s'agit de composants logiciels se positionnant, soit directement sur l'équipement soit à proximité, et qui assurent la fonction de collecte et de normalisation des événements de sécurité (E-Box).
- Le **serveur ExaProtect SMP** – il s'agit d'un *appliance* dédié à l'analyse et la contre mesure (A-Box, D-Box et R-Box), il est généralement déployé sur le réseau d'administration de l'organisation.
- La **console ExaProtect SMC** – il s'agit de l'interface utilisateur de la solution ExaProtect SMS, celle-ci est accessible via un navigateur Web.
- Les **équipements** – il s'agit de tous équipements assurant des fonctions de sécurité (active ou passive) ou bien susceptibles d'envoyer des informations intéressantes d'un point de vue sécurité. Ces composants ne font pas partie de l'offre d'ExaProtect puisque ce sont les équipements qui sont supervisés par la solution ExaProtect SMS.

[1] http://gost.isi.edu/cidf/

La figure ci-après présente l'architecture standard composée d'agents déployés « au plus proche » des équipements, d'un serveur ExaProtect SMP et de postes d'accès à la console ExaProtect SMC. Il est également représenté sur le schéma un mode de déploiement avec des serveurs relais. Dans le cas d'une communication serveur vers serveur, le serveur émettant l'alerte est vu comme un agent par le serveur récepteur (les mêmes mécanismes de remontées d'alertes sont mis en œuvre comme pour un agent classique mais ne nécessitent pas de configuration particulière).

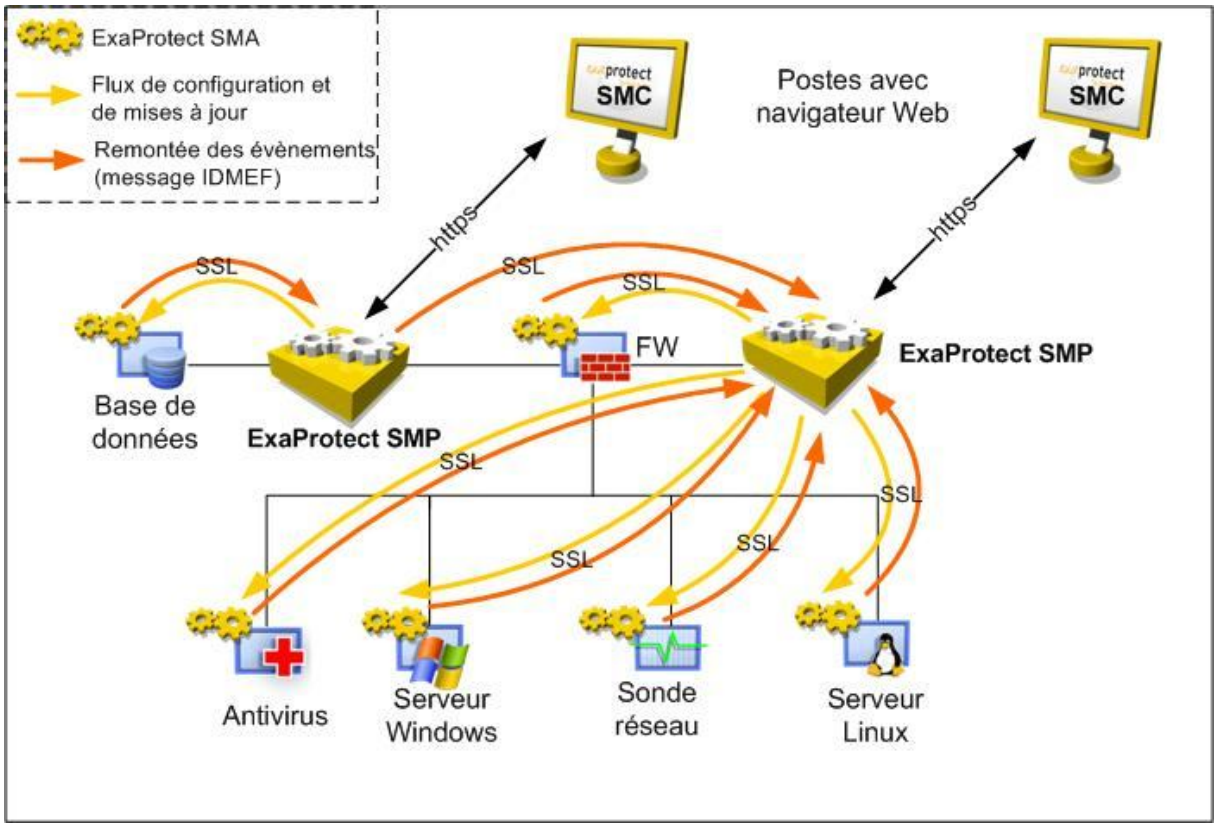

Figure 2: Exemple d'architecture standard

II.4.2 Serveur ExaProtect SMP

Le serveur ExaProtect SMP fonctionne sous le système d'exploitation RedHat Entreprise Linux 3.0, il intègre des composants issus du monde libre (logiciel libre) tels que Tomcat, MySQL. La technologie de corrélation développée par ExaProtect constitue le cœur de la solution et assure les fonctions de corrélation, de réaction et de présentation (temps réel et reporting).

Le serveur ExaProtect SMP est composé de sous-ensembles :

- Le collecteur
- La base de données des évènements, des alertes de sécurité et des incidents
- Le corrélateur
- Le module de réaction
- L'interface de supervision
- L'interface de *reporting*
- La base d'information décrivant les actifs, le périmètre supervisé et les vulnérabilités associées

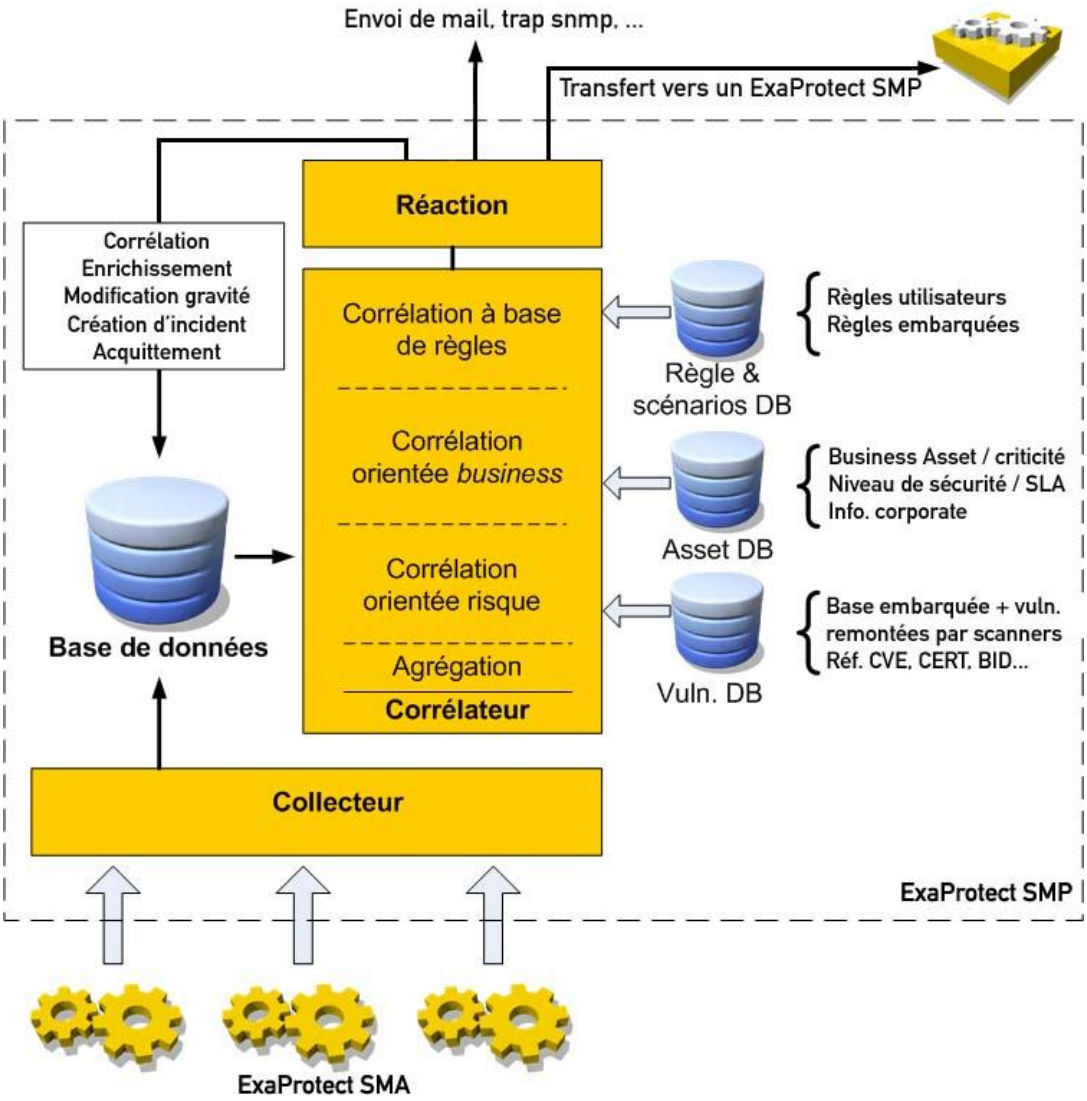

Figure 3: Architecture interne du serveur ExaProtect SMP

Le collecteur de messages
Ce composant a pour mission de récupérer les évènements IDMEF envoyés par les agents. Les évènements sont récupérés par un canal de communication dédié et sécurisé. Une fois que l'évènement a été reçu, il est stocké dans la base de données (D-box) et envoyé au moteur de corrélation (A-box).

La base de données
Ce composant a pour mission de stocker les évènement et alertes de sécurité. L'application ExaProtect SMS offre des fonctionnalités de sauvegarde, restauration et d'archivage automatiques des informations qu'elle contient.

Le corrélateur de messages (A-Box)
Ce composant récupère les nouveaux évènements puis les analyse à l'aide des différents mécanismes de corrélation (règles et scénarios de corrélation, base de vulnérabilités, criticité des assets…).

Le module de réaction (R-Box)
Ce composant permet d'exécuter des actions en fonction des résultats des traitements effectués précédemment. Les actions possibles sont :

- Génération d'alertes de corrélation
- Ajustement automatique du niveau de gravité de l'alerte
- Acquittement automatique des alertes
- Création d'un incident
- Emission de mail
- Exécution de commande (ex. émission d'une *trap* SNMP)

II.4.3 Console ExaProtect SMC

L'interface utilisateur (IHM) est accessible via un navigateur Web (Mozilla Firefox et IE) à travers une connexion HTTPs (SSL) authentifiée. Elle offre une supervision temps réel et permet d'acquitter et d'investiguer l'ensemble des alertes de sécurité depuis une console unique. C'est aussi via cette console que la configuration de la solution SMS est réalisée.

La vue principale de l'interface utilisateur permet de suivre en temps réel les alertes remontées. La mise en place de filtres permet de spécifier des critères (type d'équipements, site …) et donc de limiter le nombre d'alertes à afficher.

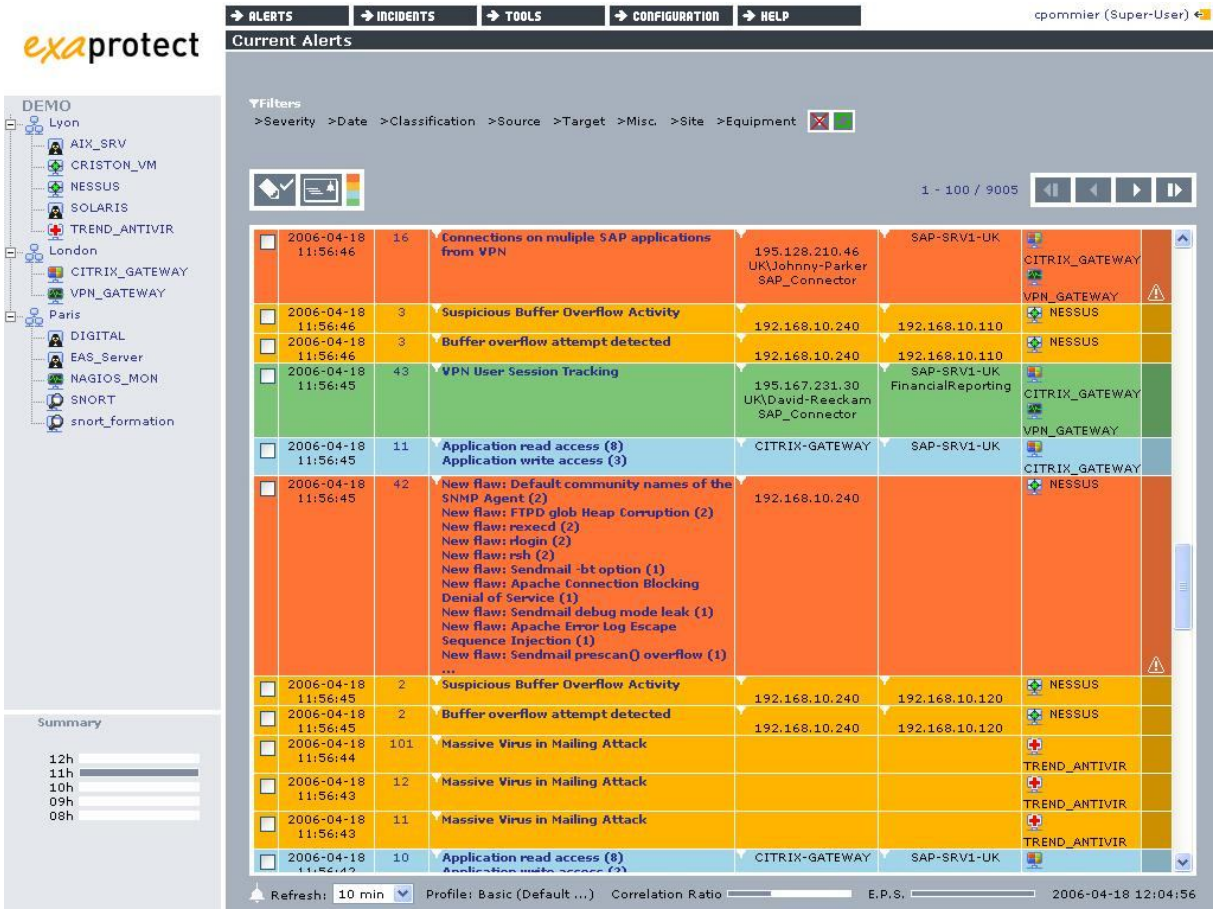

Figure 4: Capture d'écran de l'interface utilisateur

Des permissions peuvent être attribuées aux utilisateurs selon les quatre profils définis précédemment.

L'interface de *reporting*

L'interface utilisateur permet également d'accéder aux fonctions de génération de rapport. Les rapports traitent des informations concernant les événements de sécurité (ex : gravité, type, quantité) mais également concernant le travail des analystes de sécurité (temps de traitement d'un événement, durée d'investigation, respect du SLA…). La pertinence du paramétrage des équipements peut également être mise en évidence aux travers d'indicateurs spécifiques (faux positifs, confiance accordée aux équipements …).

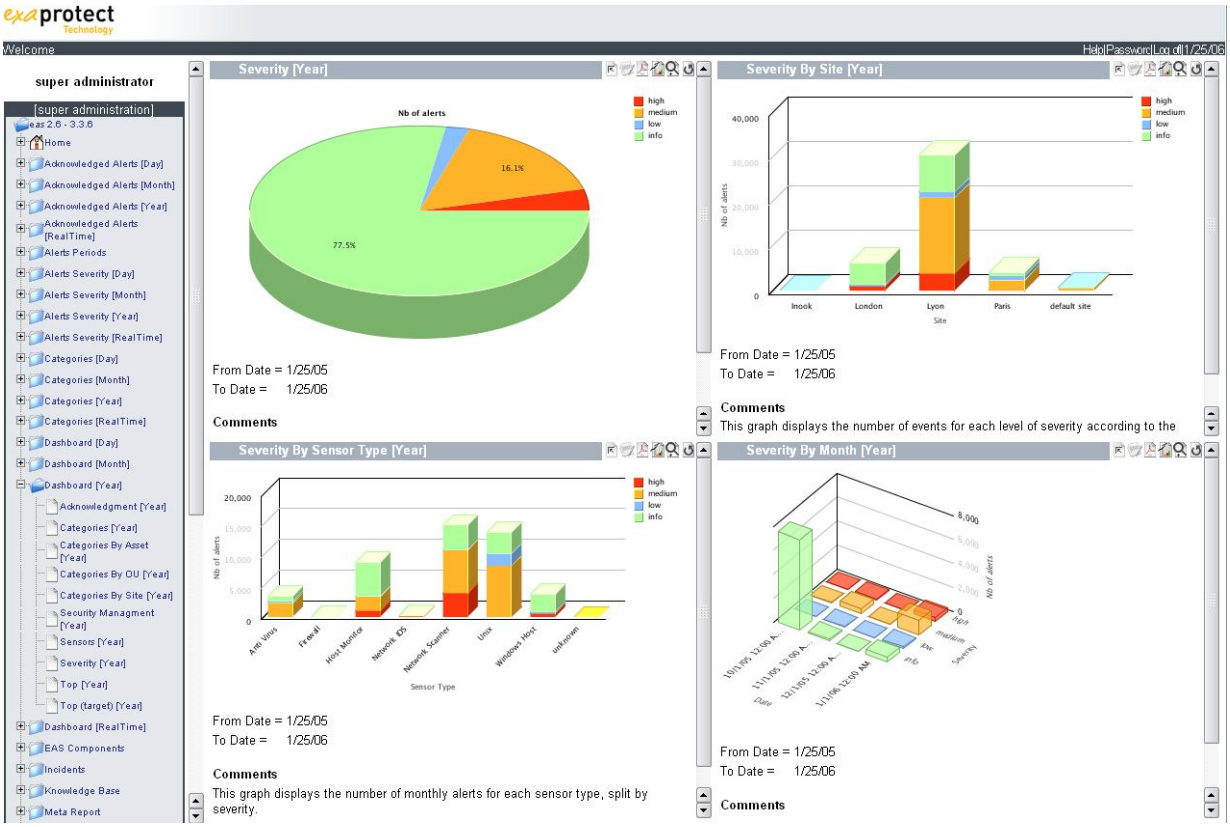

Figure 5: Exemples de graphiques fournis

II.4.4 Agents ExaProtect SMA

Les agents assurent la collecte des entrées de log générés par les équipements via des modules appelés collecteurs. L'agent convertit ces entrées de log en évènement (normalisation lexicale et syntaxique) via des *converters* et envoie ces évènements sous forme de message dans un format basé sur IDMEF au server ExaProtect SMP. Il existe différent types de *converter* :

- Log : pour la collecte des entrées de log dans des fichiers texte ou via le protocole Syslog
- WELF : pour la collecte des entrées de log dans des fichiers au format WELF (*Webtrend Log Export Format*)
- Database : pour la collecte des entrées de log dans une base de données
- OPSEC : pour la collecte des entrées de log sur un serveur de management Checkpoint via l'API OPSEC
- WMI : pour la collecte des Event Logs Windows
- RDEP : pour la collecte des sondes d'intrusion CISCO

- SCANNER : pour interfaçage spécifique avec les scanners de vulnérabilité (gestion différentielle des scans)
- Multi-line : pour la collecte des entrées de log dans des fichiers texte ou via le protocole Syslog dont l'information constituant un message est découpé sur plusieurs lignes.
- RSA : pour la collecte des entrées de log d'une base de données RSA ACE en utilisant l'API RSA admin toolkit.

Ces modules sont intégrés dans l'agent ExaProtect SMA, celui-ci peut utiliser simultanément plusieurs *converter*. La conversion des entrées de log en évènements format IDMEF s'effectue à l'aide de fichiers de règles de transcription (requêtes ou expressions régulières). Lié aux évènements, l'agent peut aussi générer optionnellement des logs bruts, étant la représentation fidèle au format texte des entrées de log.
Les agents sécurisent la transmission des informations en créant un tunnel SSL avec le serveur ExaProtect SMP, de sorte que l'intégrité et la confidentialité des évènements puissent être conservées.

De plus, les agents intègrent des mécanismes de tolérance aux pannes :

- Un **mode hors ligne**, permettant de sauvegarder dans des fichiers temporaires locaux les messages en attendant le rétablissement de la ligne communication avec le serveur. Dans le cas où la taille limite stockage est atteinte, l'agent supprime par défaut le fichier temporaire le plus ancien.
- Une **fonction de priorisation** des événements dans une file d'attente permettant en cas de réception d'un nombre trop importants d'évènements (congestion) de prioriser les évènements de plus grande gravité.

Enfin, il est possible au niveau de l'agent d'appliquer des filtres pour ignorer à la source certains types d'événements.

Les types d'équipement actuellement supportés par l'application ExaProtect SMS sont listés ci-dessous.

- Network based Intrusion Detection (ex : Snort IDS)
- Firewalls
- Host-based Intrusion Detection (ex : Tripwire agent)
- Operating Systems Logs (ex: FreeBSD, Windows, Linux,…)
- Routers / Switches
- VPN
- Anti-virus
- Vulnerability Assessment (ex : Nessus)
- Physical Monitoring (ex : APC UPS)
- Intrusion Prevention (ex : Portsentry)
- Database Server
- Monitoring
- Remote Control
- Mail Sever
- Honeypot
- Operating Systems hardening (ex : Grsec)
- Web Servers
- Ftp Servers
- Proxy servers
- Authentication (ex : Radius)

Une liste de tous les produits supportés par la solution ExaProtect SMS est disponible sur le site web (www.exaprotect.com).

L'architecture évolutive permet d'intégrer de nouveaux équipements ou de nouvelles applications facilement en quelques jours.

Les agents ExaProtect SMA sont supportés sur les systèmes d'exploitation suivants:

- Linux : RedHat 7.1 ou sup., Red Hat EL 3 ou sup., Debian 3.0 (kernel 2.4) ou sup.
- Windows XP, 2000, 2003
- SUN-Solaris 2.8 ou sup.
- DEC TRU64 4.0f ou sup.
- IBM-AIX 5.1 ou sup.

II.4.5 Archivage des logs bruts issues des équipements

Afin de constituer des preuves légales de qualité, la solution ExaProtect SMS propose d'archiver les logs bruts (avant toute transformation), et de les réunir dans des fichiers d'archives sur une base d'un fichier d'archive par jour.

Par défaut, ce fichier est signé lors de sa génération. Cette signature s'effectue à l'aide d'un mécanisme à clef publique, la clef publique étant disponible dans l'interface utilisateur.

Par ailleurs, il est possible de chiffrer ces mêmes fichiers dans un souci de confidentialité des informations contenues. Ce chiffrement s'effectue lui aussi grâce à un algorithme à clef publique, laquelle doit être fournie par l'administrateur (droit super-user) dans l'interface d'administration du produit.

Les fichiers d'archives sont téléchargeables à travers l'interface du produit.

II.4.6 Périmètre de l'évaluation

Le périmètre de l'évaluation est le suivant:

- La collecte des évènements et logs bruts par le serveur SMP envoyés par l'agent SMA
- La corrélation des évènements et des alertes de sécurité.
- L'analyse des alertes de sécurité au travers de fonctions d'audit accessibles via la console SMC
- Les communications entre les agents et le serveur
- Les communications entre la console et le serveur, y compris le mécanisme d'authentification et de contrôle d'accès des utilisateurs
- L'archivage des logs bruts issus des équipements.

Les éléments suivants ne font pas partie du périmètre de l'évaluation :

- Les mécanismes de « reporting » à partir des évènements et des alertes de sécurité stockées dans la base de données.
  Ceci correspond à un module de génération de statistiques et de rapport d'activité à destination du management de la SSI au sein d'une entreprise. Il n'y a pas de fonction d'audit associée.
- La collecte des entrées de log sur l'équipement, leur communication vers un agent, et leur transformation en évènements et logs bruts.
  Il sera fait l'hypothèse dans le cadre de l'évaluation, que l'équipement à l'origine des entrées de log de sécurité envoie des messages fondés et non altérés en direction de l'agent.

Le schéma ci-après présente le périmètre de l'évaluation associé aux composants du produit.

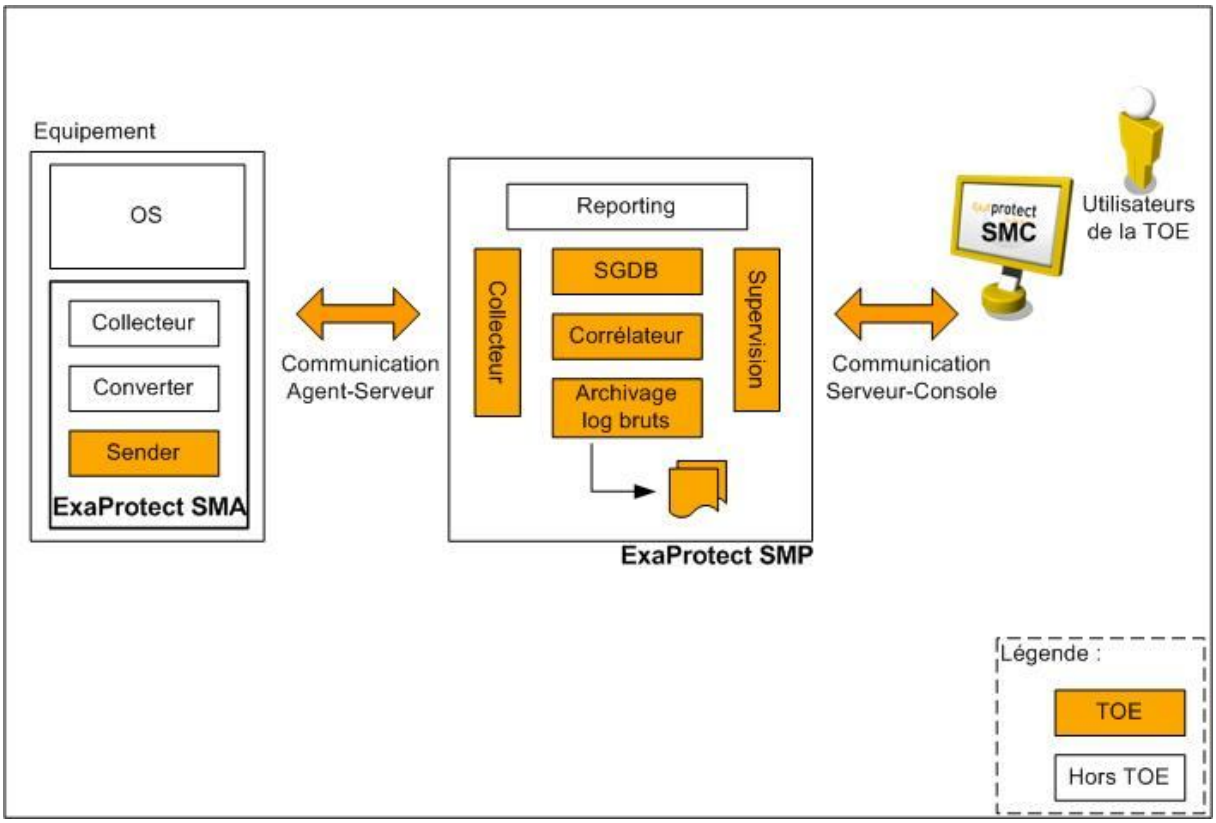

Figure 8 : Périmètre de la TOE

III Environnement de sécurité du produit évalué

Ce chapitre précise les aspects de sécurité de l'environnement dans lequel il est prévu d'utiliser la TOE.

III.1 Hypothèses

H.PROTECT_HARDWARE

Le poste d'accès à la console SMC et le serveur SMP sont placés dans des locaux sécurisés.

Cette hypothèse écarte les menaces devant mettre en œuvre au préalable un accès physique aux machines.

H.EXPORT_BASE

Dans le cadre du service d'archivage des logs bruts, il est supposé que les moyens permettant le déchiffrement et la vérification de la signature des archives hors de la TOE sont gérés de manière sûre.

Cette hypothèse écarte les menaces liées à la qualité des moyens permettant la récupération de manière sûre des bases de données exportées.

H.TRUE_AGENT

Il est supposé que l'agent transforme de façon cohérente et fidèle les entrées de log des différents équipements supportés en évènements.

Cette hypothèse écarte les menaces liées à la malformation volontaire des évènements remontés par les agents.

H.SAFE_CONFIG_AGENT

Les agents ExaProtect SMA sont installés et exploités sur des systèmes sains et sécurisés par des personnels de confiance, ces systèmes protégeant la configuration des agents (fichiers de paramétrage, bi-clé).

Cette hypothèse écarte les menaces de piégeage et d'altération des équipements sur lesquels les agents ExaProtect SMA sont installés et par conséquent les menaces d'accès par un attaquant à la configuration des agents (fichier de paramétrage, bi-clé).

H.TIME

Les équipements et le serveur s'appuient sur une base de temps synchronisée mise à disposition par l'environnement de la TOE.

Cette hypothèse écarte les menaces de dysfonctionnement du moteur de corrélation à cause de décalages dans les logs.

H.FIREWALL

Le serveur est protégé par un dispositif de filtrage des communications.

Cette hypothèse écarte les menaces de piratage distant du serveur via des protocoles non-autorisés.

H.CRYPTO

Les bi-clés, utilisés pour le chiffrement des archives des logs bruts, mis en oeuvre dans le cadre de la TOE sont conformes au référentiel cryptologique de la DCSSI pour des produits qualifiés au niveau « standard ».

Cette hypothèse écarte les menaces sur la crypto employée dans le cadre du produit.

H.ADMIN_HOST_NOEVIL

Tous les utilisateurs de la machine qui héberge le serveur ExaProtect SMP sont de confiance.

Cette hypothèse écarte les menaces de piégeage ou d'action malveillante sur le serveur par un individu ayant des droits sur le système d'exploitation hôte du logiciel ExaProtect SMP.

H.USER_FORMATION

L'ensemble des rôles utilisant le produit ExaProtect SMS sont formés aux fonctionnalités du produit et sont sensibilisés aux conséquences de leurs actes (en particulier sur l'acquittement des alertes), ainsi que sur les procédures de sécurité associées à l'utilisation du produit (surveillance de la taille des logs, purge de la base de données, archivage).

Cette hypothèse écarte les menaces de mauvaise utilisation du produit et participe à couvrir les menaces dont les mesures de protection nécessitent une vigilance de la part des utilisateurs.

H.SERVEUR_CLEAN

L'appliance du serveur SMP ne contient aucun autre service (applications tierces) que ceux installés initialement.

Cette hypothèse écarte les menaces d'attaques distantes ou locales sur des services non utilisés par le produit ExaProtect SMP.

III.2 Menaces

III.2.1 Agents menaçants

Les agents menaçants sont les personnes ayant accès au LAN, celles ayant accès à la console SMC (personnes avec un rôle « Viewer », « Analyst », « Administrator » ou « Superuser »), les utilisateurs ayant accès à une machine sur laquelle un agent SMA est installé.
Dans la suite du document, on considère un attaquant une des personnes précédemment énumérées. Le potentiel d'attaque des agents menaçant est au minimum considéré comme « basique » au sens des CC.

III.2.2 Menaces causant l'interruption du service

M.ALTER_PARAM_AGENT

Le **fichier de paramétrage spécifique** d'un agent ExaProtect SMA est détruit ou modifié : soit intentionnellement par un attaquant, soit accidentellement à la suite d'une erreur de manipulation sur l'équipement hôte de l'agent ExaProtect SMA. Cette menace rend le service indisponible, l'agent ExaProtect SMA n'étant plus en mesure de transmettre les informations au serveur ExaProtect SMP.

III.2.3 Menaces causant l'altération du service

M.ALTER_TRANSCRIPT_AGENT

Le **fichier de règles de transcription** d'un agent ExaProtect SMA est détruit ou modifié : soit intentionnellement par un attaquant, soit accidentellement à la suite d'une erreur de manipulation sur l'équipement hôte de l'agent ExaProtect SMA. Cette menace peut conduire à l'altération du service, les évènements devant être normalement remontés vers le serveur ExaProtect SMP pouvant être filtrées au niveau de l'agent ExaProtect SMA.

M.ALTER_PARAM

Un des fichiers de paramétrage (**fichier de paramétrage propre du serveur ExaProtect SMP, fichier de paramétrage des règles de corrélation du serveur ExaProtect SMP, fichier de paramétrage des incidents, fichier de paramétrage de traitement des évènements, données de configuration de la sauvegarde, la base de données d'état des agents**) est détruit ou modifié intentionnellement par un attaquant. Cette menace peut changer le comportement du produit et conduire à une utilisation non sécurisée.

M.FORGE_ALERT

Un attaquant forge une attaque à l'intérieur d'une entrées de log qui est récupérée par un équipement et transmis au serveur via un agent, dans le but d'exécuter des commandes dans les bases de données du serveur.

III.2.4 Menaces causant l'altération de données sensibles

M.ALTER_USERS

Un attaquant réussit à s'introduire sur le serveur ExaProtect SMP afin d'y modifier **la liste des utilisateurs autorisés** à utiliser la solution ExaProtect SMS. Cette menace peut permettre à un attaquant de se connecter en « superuser » et de modifier profondément le paramétrage du produit.

M.ALTER_BASES

Un attaquant modifie intentionnellement les bases de données (**base des actifs, base de vulnérabilité, base des alertes et incidents**).

III.2.5 Menaces causant la divulgation de données sensibles

M.DIVULG_PARAM_SERVEUR

Le **fichier de paramétrage propre du serveur ExaProtect SMP** est divulgué suite à une attaque intentionnelle du serveur. Cette menace peut concerner la divulgation du mot de passe permettant de se connecter à la base de données du serveur ExaProtect SMP.

M.DIVULG_KEYS_SERVER

Les bi-clés utilisées pour protéger les communications avec le serveur ExaProtect SMP (**bi-clé de l'AC, bi-clé du certificat du serveur ExaProtect SMP, bi-clé du serveur Web TOMCAT**) sont compromises suite à une attaque sur le serveur ExaProtect SMP. Cette menace peut mettre en péril la confidentialité des communications avec le serveur ExaProtect SMP.

III.3 Politique de sécurité de l'organisation

OSP.CRYPTO

Le produit ExaProtect SMS utilise des mécanismes cryptographiques conformes au référentiel cryptographique de la DCSSI.

OSP.QUALIF

Le produit ExaProtect SMS est évalué selon les Critères Communs selon le paquet d'assurance EAL2+ de la qualification standard.

OSP.CORRELATION_AUDIT

Le produit ExaProtect SMS effectue une corrélation des évènements de sécurité remontés par les agents et génère des alertes de sécurité. Le produit ExaProtect SMS fournit à ses utilisateurs des moyens d'audit pour exploiter ces alertes.

OSP.SPOOL_ALERTES

Le produit ExaProtect SMS permet de transmettre de manière asynchrone **les évènements remontés par les agents** vers le serveur ExaProtect SMP lorsque la liaison entre l'agent et le serveur est rétablie après une coupure. La coupure est elle-même signalée à l'utilisateur par l'intermédiaire d'un évènement spécifique, de même que la perte d'évènements suite à saturation du spool d'évènement est signalée.

OSP.PROTECTION_ALERTES_SERVEUR

Le produit ExaProtect SMS protège les **alertes créées par le serveur** ainsi que les **incidents** contre la modification et la divulgation.

OSP.COMM_AGENT

Le produit ExaProtect SMS protège les **communications agent-serveur** contre la modification et la divulgation et l'usurpation d'identité.

OSP.COMM_CONSOLE

Le produit ExaProtect SMS protège les **communications console d'administration-serveur** contre la modification, la divulgation et l'usurpation d'identité.

OSP.ROLES_ACCESS

Le produit ExaProtect SMS gère des rôles utilisateurs permettant d'attribuer des droits d'accès différents aux fonctionnalités du produit. Ces rôles sont stockés dans la base de données sous la forme d'une liste des utilisateurs autorisés. Les rôles sont associés à des utilisateurs qui sont authentifiés leur donnant accès aux alertes à travers une interface d'administration distante.

OSP.EXPORT_BASE

Le produit ExaProtect SMS archive les logs bruts en les signant et en les chiffrant (optionnellement).

IV Objectifs de sécurité

Les objectifs de sécurité reflètent l'intention déclarée et sont à même de contrer toutes les menaces identifiées et de couvrir toutes les politiques de sécurité organisationnelles et les hypothèses identifiées.

IV.1 Objectifs de sécurité pour la TOE

OT.CONFIG_SYNCHRO

La TOE doit se prémunir d'une perte ou d'une modification du fichier de paramétrage spécifique d'un agent ExaProtect SMA en effectuant une synchronisation de ces fichiers avec ceux de référence stockés.

OT.AGENT_CONNECT

La TOE doit détecter une perte de liaison réseau entre l'agent ExaProtect SMA et le serveur ExaProtect SMP.

OT.HEART_BEAT

Les agents ExaProtect SMA doivent signaler au serveur ExaProtect SMP de manière régulière leur bon fonctionnement (liaison applicative).

OT.CTL_SERV_ASSETS

La TOE doit mettre en œuvre un contrôle d'accès sur les ressources du serveur ExaProtect SMP (bases de données, fichiers de paramétrages, bi-clés,…).

OT.CTL_SGBD

La TOE doit mettre en œuvre un contrôle d'accès sur les ressources de la base de données.

OT.ALERTES_AGENT

La TOE doit être capable de générer et de collecter à partir des agents : les évènements issus des équipements et les évènements internes au fonctionnement de l'agent (perte d'évènements,...).

OT.ALERTES_SERVEUR

La TOE doit être capable, à partir du serveur ExaProtect SMP, de générer des évènements internes au fonctionnement du serveur (spooler plein, erreur sur la liaison agent serveur, authentification, changement de mot de passe, création de compte, génération d'un backup).

OT.CORRELATION

La TOE doit être capable de relier entre elles plusieurs évènements par des critères particuliers afin de générer une alerte de corrélation.

OT.AUDIT

La TOE doit fournir les moyens d'auditer l'ensemble des évènements et alertes (y compris les alertes de corrélation et les alertes propres au serveur) enregistrées.

OT.ASYNC_TRANSMIT

La TOE doit permettre de stocker les évènements sur les agents lors d'une rupture de liaison avec le serveur ExaProtect SMP et de les transmettre à nouveau lorsque la liaison est rétablie.

OT.PROTECT_COMM_AGENT

La TOE doit fournir les moyens de chiffrement et de scellement des informations échangées entre les agents ExaProtect SMA et le serveur ExaProtect SMP.

OT.PROTECT_COMM_CONSOLE

La TOE doit fournir les moyens de chiffrement et de scellement des informations échangées entre la console utilisateur et le serveur ExaProtect SMP.

OT.ROLES

La TOE doit définir et gérer des droits d'accès aux fonctions d'audit de la TOE en fonction de rôles correspondants à différents profils de droits d'accès pour les utilisateurs authentifiées de la TOE.

OT.I&A_USERS

La TOE doit être en mesure d'identifier et d'authentifier les utilisateurs de la TOE qui accèdent au serveur ExaProtect SMP via la console.

OT.CRYPTO_BASE

La TOE doit être en mesure de chiffrer et de signer les bases de données exportées.

OT.CTL_PARAM_BASE

La TOE doit mettre en œuvre un mécanisme de contrôle des paramètres des requêtes passées aux bases de données.

IV.2 Objectifs de sécurité pour l'environnement de la TOE

OE.PROTECT_HARDWARE

Le poste d'accès à la console SMC et le serveur SMP doivent être installés dans un local sécurisé.

OE.EXPORT_BASE

Dans le cadre du service d'archivage des logs bruts, il est supposé que les moyens permettant le déchiffrement et la vérification de la signature des archives hors de la TOE sont gérés de manière sûre.

OE.TRUE_AGENT

La TOE doit se reposer sur des agents qui transforment de façon fiable et cohérente les entrées de log remontées par les équipements.

OE.ADM_NO_EVIL

L'organisme doit recruter des personnels de confiance comme administrateurs des systèmes d'exploitation qui hébergent les agents ExaProtect SMA et comme administrateurs du serveur ExaProtect SMP.

OE.HOST_CLEAN

Les équipements sur lesquels sont installés les agents SMA doivent être sécurisés selon des procédures de durcissement et mis à jour en fonction des vulnérabilités spécifiques découvertes sur le système d'exploitation et les applications installées sur ces équipements.

OE.SERVER_CLEAN

L'appliance sur lequel le serveur SMP est installé ne doit pas contenir d'autres services (applications tierces) que ceux installés initialement.

OE.USR_AWARE

Les utilisateurs de la TOE doivent être formés à l'utilisation de la TOE et être sensibilisés à la sécurité, en particulier aux conséquences de leurs actes lorsqu'ils traitent et acquittent des alertes.

OE.CRYPTO

La TOE doit utiliser des mécanismes cryptographiques conformes au référentiel de la DCSSI pour les produits qualifiés au niveau « standard ».

OE.QUALIF

La TOE doit être évaluée au niveau EAL2+ correspondant à une qualification de niveau « standard ».

OE.TIME

Le temps de référence de la TOE doit être synchronisé avec une base de temps mise à disposition par l'environnement.

OE.FIREWALL

L'environnement de la TOE doit inclure un dispositif de filtrage des communications placé devant le serveur ExaProtect SMP.

OE.CTL_AGENT_ASSETS

Les systèmes sur lesquels les agents sont installés doivent mettre en œuvre un contrôle d'accès sur les ressources des agents (fichiers de paramétrage, bi-clé).

V Exigences de sécurité

V.1 Exigences fonctionnelles pour la TOE

V.1.1 Résumé

Composant	Intitulé
FPT_TRC.1	Internal TSF consistency
FPT_TST.1*	TSF Agent connection testing
FDP_ACC.1_filesystem	Subset access control
FDP_ACF.1_filesystem	Security attribute based access control
FMT_MSA.3_filesystem	Static attribute initialisation
FDP_ACC.1_SGBD	Subset access control
FDP_ACF.1_SGBD	Security attribute based access control
FMT_MSA.3_SGBD	Static attribute initialisation
FDP_ACC.1_Console	Subset access control
FDP_ACF.1_Console	Security attribute based access control
FMT_MSA.3_Console	Static attribute initialisation
FMT_MSA.1	Management of security attributes
FMT_SMR.1	Security roles
FMT_SMF.1	Specification of Management Functions
FAU_GEN.1_Agent	Audit data generation
FAU_GEN.1_Serveur	Audit data generation
FAU_SAA.4	Complex attack heuristics
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_STG.2	Guarantees of audit data availability
FAU_STG.4	Prevention of audit data loss
FPT_ITT.1_CommAgent	Basic internal TSF data transfer protection
FTP_TRP.1	Trusted path
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FIA_AFL.1	Authentication failure handling
FCS_COP.1/Console	Cryptographic operations
FCS_COP.1/Communications	Cryptographic operations
FCS_COP.1/Bases	Cryptographic operations
FDP_IFF.1	Simple Security Attribute
FDP_IFC.1	Subset information flow control

Toutes les exigences fonctionnelles pour la TOE sont extraites de la partie 2 des Critères Communs [CC] sauf l'exigence présentée ci-dessous issue du composant FPT_TST.1 et notée FPT_TST.1* dont les caractéristiques sont les suivantes :

FPT_TST.1* TSF agent connection testing

Hierarchical to: No other components.

Dependencies: None

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of the TSF operation of [selection: [assignment: parts of TSF], the TSF].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF data].

V.1.2 Détail des exigences fonctionnelles pour la TOE

Le texte extrait des Critères Commun est en caractères normaux. Les attributions (« assignments ») et les sélections (« selections ») sont en **caractères gras**. Les raffinements (« refinements ») sont en *caractères italiques*.

FPT_TST.1* TSF agent connection testing

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] **periodically during normal operation** to demonstrate the correct operation of the TSF operation of [selection: [assignment: parts of TSF], the TSF] **des agents**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF data] de **la connexion entre les agents et le serveur**.

FPT_TRC.1 Internal TSF consistency

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [assignment: list of SFs dependent on TSF data replication consistency] **F_AUDIT_AGENT**.

FDP_ACC.1_filesystem Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] **Discretionary Access Access Policy** on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]. **Sujets: les comptes utilisateurs du système hôte ; Objets : les fichiers de paramétrage et de configuration des serveurs.**

FDP_ACF.1_filesystem Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] **Discretionary Access Access Policy** to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

- **L'identité et l'appartenance à un groupe associées au sujet (un compte utilisateur du système hôte)**
- **Les privilèges du système de fichier hôte (lecture, écriture, exécution) associés aux objets (les fichiers de paramétrage et de configuration stockés sur le serveur ExaProtect SMP)**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]. **L'objet doit être accédé uniquement par un sujet ayant les droits adéquats**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]. **Pas de règle additionnelle.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]. **Pas de règle**.

FMT_MSA.3_filesystem Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] **Discretionary Access Access Policy** to provide [selection, choose one of: restrictive, permissive,[assignment: other property]] **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: the authorised identified roles] **aucun rôle (initialisation à l'installation)** to specify alternative initial values to override the default values when an object or information is created**.**

FDP_ACC.1_SGBD Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] **SGBD Access Policy** on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]. **Sujets: les comptes utilisateurs des bases de données ; Objets : les tables des bases de données.**

FDP_ACF.1_SGBD Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] **SGBD Access Policy** to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

- **L'identité et l'appartenance à un groupe associées au sujet (un compte utilisateur de la base de données)**
- **Les privilèges (GRANT, ALTER, SELECT,…) associés aux objets (les tables de la base de données)**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]. **L'objet doit être accédé uniquement par un sujet ayant les droits adéquats**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]. **Pas de règle additionnelle.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]. **Pas de règle.**

FMT_MSA.3_SGBD Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] **SGBD Access Policy** to provide [selection, choose one of: restrictive, permissive,[assignment: other property]] **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: the authorised identified roles] **aucun rôle (initialisation à l'installation)** to specify alternative initial values to override the default values when an object or information is created**.**

FDP_ACC.1_Console Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] **Console Access Policy** on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]. **Sujets: les utilisateurs de la TOE ; Objets : les fonctionnalités de la TOE accessibles aux utilisateurs permettant de visualiser, acquitter les alertes, créer des comptes, purger la base de données.**

FDP_ACF.1_Console Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] **Console Access Policy** to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

- **L'identité et l'appartenance à un groupe associées au sujet (un utilisateur de la TOE)**
- **Les droits pour les sujets (d'exécuter ou non) associés aux objets (les fonctionnalités de la TOE accessibles aux utilisateurs permettant de visualiser, acquitter les alertes, créer des comptes, purger la base de données)**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]. **L'objet doit être accédé uniquement par un sujet ayant les droits adéquats**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]. **Pas de règle additionnelle.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]. **Pas de règle.**

FMT_MSA.3_Console Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] **Console Access Policy** to provide [selection, choose one of: restrictive, permissive,[assignment: other property]] **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: the authorised identified roles] **administrator et superuser** to specify alternative initial values to override the default values when an object or information is created**.**

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] **Console Access Policy** to restrict the ability to [selection: change_default, query, modify, delete,[assignment: other operations]] **modify** the security attributes [assignment: *list of security attributes*] **les droits pour les sujets (d'exécuter ou non)** to [assignment: *the authorised identified roles*] **administrator et superuser.**

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorised identified roles]. **Viewer, Analyst, Administrator, Superuser.**

FMT_SMR.1.2 The TSF shall be able to associate users with roles**.**

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF] **création/suppression de comptes utilisateurs, attribution des rôles, purge de la base de données, attribution des droits d'accès.**

FAU_GEN.1_Agent Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection, choose one of: minimum,basic,detailed,not specified] **not specified** level of audit; and
- [assignment: other specifically defined auditable events] **tous les entrées de log disponibles sur les équipements.**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information] **no other audit relevant information**.

FAU_GEN.1_Serveur Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection, choose one of: minimum,basic,detailed,not specified] **not specified** level of audit; and
- [assignment: other specifically defined auditable events] **tous les entrées de log disponibles sur le serveur y compris les traces internes de l'utilisation du produit.**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information] **no other audit relevant information**.

FAU_SAA.4 Complex attack heuristics

FAU_SAA.4.1 The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] **all sequences of system events whose occurrence are representative of known penetration scenarios** and the following signature events [assignment: a subset of system events] **all system events** that may indicate a potential violation of the TSP.

FAU_SAA.4.2 The TSF shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of [assignment: the information to be used to determine system activity] **informations contenues dans le format IDMEF des évènements** .

FAU_SAA.4.3 The TSF shall be able to indicate an imminent violation of the TSP when system activity is found to match a signature event or event sequence that indicates a potential violation of the TSP.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [assignment: authorised users] **les viewer, les analyst, les administrator et les super-user** with the capability to read [assignment: list of audit information] **toutes les informations d'audit** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: searches,sorting,ordering] **searches, sorting et ordering** of audit data based on [assignment: criteria with logical relations] **date, type d'évènement, équipement**.

FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [selection, choose one of: prevent,detect] **prevent** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [assignment: metric for saving audit records] **100% des** audit records will be maintained when the following conditions occur: ou [refinement] *continuer à enregistrer sur l'agent les évènements dans un spooler* [selection: *audit storage exhaustion,failure,attack*] **si la communication entre les agents et le serveur est interrompue**.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [selection, choose one of: "ignore auditable events","prevent auditable events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"] **ignore auditable events** and [assignment: other actions to be taken in case of audit storage failure] **et émettre une alerte si le spooler d'alerte est plein** if the audit trail is full.

FPT_ITT.1_CommAgent Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [selection: disclosure, modification] **disclosure, modification** when it is transmitted between separate parts of the TOE.

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: remote, local] **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure**.**

FTP_TRP.1.2 The TSF shall permit [selection: the TSF, local users, remote users] **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: initial user authentication,[assignment: other services for which trusted path is required]] **initial user authentication and review of audit trails**.

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated allowing any other TSF-mediated actions on behalf of that user.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] **3** unsuccessful authentication attempts occur related to [assignment: list of authentication events] **authentification des intervenants**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list of actions] **bloquer le compte utilisateur**.

FCS_COP.1/Console Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] **du chiffrement et de la signature sur les communications entre la console et le serveur** in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] **SSL_RSA_WITH_3DES_EDE_CBC_SHA pour le chiffrement, SHA1withRSA pour la signature** and cryptographic key sizes [assignment: cryptographic key sizes] **2048bits pour le SHA1withRSA, 128 bits pour 3DES** that meet the following: [assignment: list of standards]. **SSL pour le chiffrement, X509 V1 pour la signature.**

FCS_COP.1/Communications Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] **du chiffrement et de la signature sur les communications entre les agents et le serveur** in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] **TLS_RSA_WITH_AES_128_CBC_SHA pour le chiffrement, SHA1withRSA pour la signature** and cryptographic key sizes [assignment: cryptographic key sizes] **2048bits pour le SHA1withRSA, 128 bits pour AES** that meet the following: [assignment: list of standards].**TLS pour le chiffrement, X509 V1 pour la signature.**

FCS_COP.1/Bases Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] **du chiffrement et de la signature sur les bases exportées** in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] **3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH pour le chiffrement, DSA pour la signature** and cryptographic key sizes [assignment: cryptographic key sizes] **1024 pour la signature et de 768 à 2048 bits pour la clé de chiffrement** that meet the following: [assignment: list of standards] **no standard**.

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] **CTL_BASE SFP** based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes] **le contenu des commandes passées à la base de données**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes**] le contenu des commandes passées à la base de données ne doit pas contenir d'autres commandes imbriquées qui peuvent être interprétées par le moteur de la base de données**.

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules] **pas d'autre règle**.

FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities] **pas d'autre capacité**.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows] **les commandes passées à la base de données qui ne contiennent pas d'autres commandes imbriquées**.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows] **pas de règles**.

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] **CTL_BASE SFP** on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP] **sujets : commandes passées à la base de données, information : le contenu des commandes, opération : passage de la commande à la base**

V.1.3 Niveau minimal de résistance des fonctions de sécurité

Le niveau minimal exigé de résistance des fonctions de sécurité de la TOE (SOF-Claim)[2] est : **élevé** (**SOF-high**).

[2] Niveau de résistance intrinsèque d'une fonction face à des attaques. Ce niveau ne doit pas être confondu avec le niveau de résistance global de la TOE (niveau défini par le composant AVA_VLA) qui prend en compte des attaques altérant ou rendant inopérantes des fonctions de la TOE.

V.2 Exigences d'assurance pour la TOE

Exigences	Intitulés
Classe ACM : Configuration Management	
ACM_CAP.2	Configuration items
Classe ADO : Delivery and Operation	
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
Classe ADV : Development	
ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_LLD.1[3]	Descriptive low-level design
ADV_IMP.1[4]	Subset of the implementation of the TSF
ADV_RCR.1	Informal correspondence demonstration
Classe AGD : Guidance Documents	
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
Classe ALC : Life Cycle Support	
ALC_DVS.1	Identification of security measures
ALC_FLR.3	Systematic flaw remediation
ALC_TAT.1[5]	Well-defined development tools
Classe ATE : Tests	
ATE_FUN.1	Functional testing
ATE_COV.1	Evidence of coverage
ATE_IND.2	Independent testing - sample
Classe AVA : Vulnerability Assessment	
AVA_MSU.1	Examination of guidance
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.2	Independent vulnerability analysis

Toutes les exigences d'assurance pour la TOE sont extraites de la partie 3 des Critères Communs [CC].
Le niveau visé est EAL2 augmenté des composants ADV_HLD.2, ADV_LLD.1, ADV_IMP.1, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1, AVA_MSU.1 et AVA_VLA.2.
Ce niveau est le niveau demandé pour la qualification (OSP.QUALIF).

Le niveau de résistance intrinsèque des fonctions de sécurité demandé pour la qualification est élevé.

V.3 Exigences pour l'environnement technique de la TOE

La TOE ne requiert pas de mécanisme particulier pour son environnement technique.

[3] Pour les modules répondant aux exigences fonctionnelles de la classe FCS.
[4] Pour l'implémentation répondant aux exigences fonctionnelles de la classe FCS.
[5] Pour l'implémentation répondant aux exigences fonctionnelles de la classe FCS.

VI Spécifications du produit évalué

VI.1 Fonctions de sécurité

F_I&A_Util

Cette fonction de sécurité permet d'identifier et d'authentifier les utilisateurs qui se connectent à la console du produit ExaProtect SMS afin de gérer les alertes. L'authentification est basée sur un identifiant et un mot de passe attribué à chaque utilisateur. Le login/mot de passe est géré dans la base de données du serveur ExaProtect SMP. Il est saisi au niveau de la console et envoyé au serveur via un formulaire web dans un flux https.

F_CTL_Gere_access_Util

Cette fonction de sécurité gère les quatre profils utilisateurs (viewer, analyst, administrator, super-user) et accorde des droits en fonction d'une table des droits. Le niveau de droit de chaque utilisateur est inscrit dans la base de données du serveur avec le login, le hash du password (MD5 du nom du login concaténé au password), et la date de dernière connexion.

F_CTL_Access_ressources_Serveur

Cette fonction de sécurité permet la protection et le contrôle d'accès aux fichiers de paramétrage du serveur. Cette fonction s'appuie pour cela sur les droits d'accès et les comptes utilisateurs du système d'exploitation sur lequel est installé le serveur ExaProtect SMP.

F_CTL_Base_de_données

Cette fonction de sécurité permet la protection et le contrôle d'accès aux tables des bases de données du serveur. Cette fonction s'appuie pour cela sur les droits d'accès et les comptes utilisateurs du système de base de données utilisé par le serveur ExaProtect SMP, ainsi que sur un mécanisme de filtrage des commandes passées à la base de données.

F_IMP_Agent

Cette fonction de sécurité collecte les évènements et les logs bruts des équipements et ceux internes au fonctionnement de l'agent (perte d'évènements,...).

F_IMP_Serveur

Cette fonction de sécurité collecte les évènements internes au fonctionnement du serveur ExaProtect SMP (spooler plein, erreur sur la liaison agent serveur, authentification, changement de mot de passe, création de compte, génération d'un backup, ...). Les logs du serveur se trouvent dans un fichier texte qui est analysé par un agent local. Cette fonction impute également les évènements propres à l'application (ex : création de comptes utilisateurs, accès à l'application…).

F_AUD_Audit

Cette fonction de sécurité permet l'audit des évènements collectés au niveau des agents et du serveur (y compris les évènements internes au serveur). Elle permet en particulier l'acquittement des alertes par un utilisateur du produit ExaProtect SMS.

F_FID_Synchro

Cette fonction de sécurité permet de synchroniser la configuration des agents au démarrage et également à la demande d'un utilisateur autorisé.

F_FIA_Liaison

Cette fonction de sécurité effectue la prévention d'une rupture de liaison avec l'agent. Elle met en œuvre un mécanisme de surveillance du lien réseau et un mécanisme de "heartbeat" qui vérifie le bon fonctionnement de l'agent et qui génère une alerte en cas de rupture.

F_ECH_AgentServeur

Cette fonction de sécurité assure la confidentialité et l'intégrité des échanges entre le serveur et ses agents. Elle met en oeuvre un flux TLS/SSL chiffré et signé basé sur des certificats clients et serveurs signés par une CA propre à ExaProtect SMS (CA hors TOE).

F_ECH_ConsoleServeur

Cette fonction de sécurité assure la confidentialité et l'intégrité des échanges entre la console et le serveur. Elle met en oeuvre un flux https basé sur des certificats serveurs signés par une CA propre à ExaProtect SMS (CA hors TOE).

F_EXPORT_BASE

Cette fonction de sécurité assure la confidentialité et l'intégrité des archives de logs bruts. Elle met en œuvre un mécanisme de chiffrement (optionnel) et de signature des bases.

VI.2 Niveau de résistance des fonctions

Les fonctions suivantes sont réalisées par des mécanismes de type probabilistiques ou permutationnels :

- F_I&A_Util

Le niveau de résistance intrinsèque[6] de ces fonctions est : **élevé** (**SOF-high**).

VI.3 Mesures d'assurance

GESTION DE CONFIGURATION

Le développeur utilise un système de gestion de configuration qui permet notamment de générer une liste de configuration.

LIVRAISON ET EXPLOITATION

Des procédures de livraison et d'installation de la TOE sont disponibles.

CONCEPTION

Le développeur dispose d'une documentation technique décrivant la conception de la TOE.

GUIDES

Une documentation d'utilisation est disponible pour la TOE.

[6] Niveau de résistance intrinsèque d'une fonction face à des attaques de type force brute. Ce niveau ne doit pas être confondu avec le niveau de résistance global de la TOE (niveau défini par le composant AVA_VLA) qui prend en compte des attaques altérant ou rendant inopérantes des fonctions de la TOE.

SUPPORT AU CYCLE DE VIE

Le développement est réalisé dans un environnement sécurisé.
Il existe un support technique assurant la maintenance corrective et évolutive du produit.

TESTS FONCTIONNELS

Des tests fonctionnels sont réalisés pour toutes les versions de la TOE.

ANALYSE DE VULNERABILITES

Les vulnérabilités connues pour ce type de produit ont été prises en compte lors du développement du produit.

VII Conformité à un profil de protection

La présente cible de sécurité ne se revendique pas conforme à un profil de protection.

VIII Argumentaires

VIII.1 Argumentaire des objectifs de sécurité

VIII.1.1 Récapitulatif

	OE.PROTECT_HARDWARE	OE.EXPORT_BASE	OE.TRUE_AGENT	OE.HOST_CLEAN	OE.SERVER_CLEAN	OE.ADM_NO_EVIL	OE.USR_AWARE	OE.CRYPTO	OE.QUALIF	OE.TIME	OE.FIREWALL	OE.CTL_AGENT_ASSETS	OT.CONFIG_SYNCHRO	OT.AGENT_CONNECT	OT.HEART_BEAT	OT.CTL_SERV_ASSETS	OT.CTL_SGBD	OT.ALERTES_AGENT	OT.ALERTES_SERVER	OT.CORRELATION	OT.AUDIT	OT.ASYNC_TRANSMIT	OT.PROTECT_COMM_AGENT	OT.PROTECT_COMM_CONSOLE	OT.ROLES	OT.I&A_USERS	OT.CRYPTO_BASE	OT.CTL_PARAM_BASE
H.PROTECT_HARDWARE	X																											
H.EXPORT_BASE		X																										
H.TRUE_AGENT			X																									
H.SAFE_CONFIG_AGENT				X		X						X																
H.TIME										X																		
H.FIREWALL											X																	
H.CRYPTO								X																				
H.ADMIN_HOST_NOEVIL						X																						
H.USER_FORMATION							X																					
H.SERVEUR_CLEAN					X																							
M.ALTER_PARAM_AGENT												X	X	X	X													
M.ALTER_PARAM						X	X									X												
M.ALTER_TRANSCRIPT_AGENT				X		X						X	X															
M.ALTER_USERS																X	X											
M.ALTER_BASE																	X											
M.DIVULG_PARAM_SERVEUR																X												
M.DIVULG_KEYS_SERVEUR																X												
M.FORCE_ALERT			X																									X
OSP.CRYPTO								X																				
OSP.QUALIF									X																			
OSP.CORRELATION_AUDIT																		X	X	X	X							
OSP.SPOOL_ALERTES														X	X				X			X						
OSP.PROTECTION_ALERTES_SERVEUR				X		X										X												
OSP.COMM_AGENT								X															X					
OSP.COMM_CONSOLE								X																X				
OSP.ROLES_ACCESS																				X					X	X		
OSP.EXPORT_BASE		X						X																			X	

VIII.1.2 Argumentaire détaillé

VIII.1.2.1 Couverture des menaces

M.ALTER_PARAM_AGENT

Pour prévenir la menace, la TOE doit:

- Vérifier que la connexion applicative entre l'agent et le serveur est correcte (OT.HEART_BEAT).
- Bénéficier d'un mécanisme de contrôle d'accès aux fichiers de paramétrage de l'agent (OE.CTL_AGENT_ASSETS)

Pour se protéger, la TOE doit:

- Mettre en place un mécanisme de synchronisation des fichiers de configuration des agents, toutes modifications d'un de ces fichiers sur l'agent sera écrasées à la prochaine synchronisation avec le serveur SMP (OT.CONFIG_SYNCHRO)

Pour détecter l'occurrence de la menace, la TOE doit:

- Etre en mesure de détecter une rupture de communication entre le l'agent et le serveur (OT.AGENT_CONNECT)

M.ALTER_PARAM

Pour prévenir la menace, la TOE doit:

- Etre administrée par des personnels de confiance (OE.ADM_NO_EVIL) et formés (OE.USER_AWARE)

Pour se protéger, la TOE doit:

- Mettre en place un mécanisme de contrôle d'accès aux fichiers de paramétrages stockés sur le serveur (OT.CTL_SERV_ASSETS)

Pour détecter l'occurrence de la menace, la TOE doit:

- Rien

M.ALTER_TRANSCRIPT_AGENT

Pour prévenir la menace, la TOE doit:

- Etre administrée par des personnels de confiance (OE.ADM_NO_EVIL)
- Avoir été installée selon des procédures de durcissement de la sécurité (OE.HOST_CLEAN)
- Bénéficier d'un mécanisme de contrôle d'accès aux fichiers de paramétrage de l'agent (OE.CTL_AGENT_ASSETS)

Pour se protéger, la TOE doit:

- Mettre en œuvre un mécanisme de synchronisation des configurations (OT.CONFIG_SYNCHRO)

Pour détecter l'occurrence de la menace, la TOE doit:

- Rien

M.ALTER_USERS

Pour prévenir la menace, la TOE doit:

- Rien

Pour se protéger, la TOE doit:

- Mettre en place un mécanisme de contrôle d'accès aux fichiers de paramétrages stockés sur le serveur (OT.CTL_SERV_ASSETS)
- Mettre en place un mécanisme de contrôle d'accès aux tables des bases de données utilisées par le serveur (OT.CTL_SGBD)

Pour détecter l'occurrence de la menace, la TOE doit:

- Rien

M.ALTER_BASE

Pour prévenir la menace, la TOE doit:

- Rien

Pour se protéger, la TOE doit:

- Mettre en place un mécanisme de contrôle d'accès aux tables des bases de données utilisées par le serveur (OT.CTL_SGBD)

Pour détecter l'occurrence de la menace, la TOE doit:

- Rien

M.DIVULG_PARAM_SERVEUR

Pour prévenir la menace, la TOE doit:

- Rien

Pour se protéger, la TOE doit:

- Mettre en place un mécanisme de contrôle d'accès aux fichiers de paramétrages stockés sur le serveur (OT.CTL_SERV_ASSETS)

Pour détecter l'occurrence de la menace, la TOE doit:

- Rien

M.DIVULG_KEYS_SERVER

Pour prévenir la menace, la TOE doit:

- Rien

Pour se protéger, la TOE doit:

- Mettre en place un mécanisme de contrôle d'accès aux fichiers contenant les bi-clés stockés sur le serveur (OT.CTL_SERV_ASSETS)[7]

Pour détecter l'occurrence de la menace, la TOE doit:

- Rien

[7] Il n'y a pas de mécanisme de révocation de certificat, en cas de renouvellement ou compromission le certificat est simplement remplacé.

M.FORGE_ALERT

Pour prévenir la menace, la TOE doit:

- Rien

Pour se protéger, la TOE doit:

- Utiliser des agents qui transcrivent de manière sûre et fiable les évènements de sécurité récupérés sur les équipements (OE.TRUE_AGENT)
- Mettre en place un mécanisme de contrôle des paramètres passés à la base de données (OT.CTL_PARAM_BASE)

Pour détecter l'occurrence de la menace, la TOE doit:

- Rien

VIII.1.2.2 Couverture des OSP

OSP.CORRELATION_AUDIT

Pour mettre en œuvre la politique la TOE:

- Offre un mécanisme de collecte des évènements au niveau des agents (OT.ALERTES_AGENT)
- Offre un mécanisme de collecte des évènements au niveau du serveur (OT_ALERTES_SERVEUR)
- Offre un mécanisme de corrélation des évènements collectés (OT.CORRELATION)

Pour garantir la mise en œuvre de la politique la TOE:

- Rien

Pour contrôler la mise en œuvre de la politique la TOE :

- Offre la possibilité d'exploiter les journaux d'alertes grâce à un mécanisme d'audit (OT.AUDIT)

OSP.CRYPTO

Pour mettre en œuvre la politique la TOE:

- S'appuie sur des mécanismes cryptographiques conformes aux recommandations de la DCSSI (OE.CRYPTO)

Pour garantir la mise en œuvre de la politique la TOE:

- Rien

Pour contrôler la mise en œuvre de la politique la TOE :

- Rien

OSP.QUALIF

Pour mettre en œuvre la politique la TOE:

- S'appuie sur le processus de qualification standard de la DCSSI (OE.QUALIF)

Pour garantir la mise en œuvre de la politique la TOE:

- Rien

Pour contrôler la mise en œuvre de la politique la TOE :

- Rien

OSP.SPOOL_ALERTES

Pour mettre en œuvre la politique la TOE :

- Offre un mécanisme de spool des évènements sur l'agent lorsque la connexion entre l'agent et le serveur est rompue. (OT.ASYNC_TRANSMIT)

Pour garantir la mise en œuvre de la politique la TOE:

- Dispose d'un mécanisme de détection de rupture de connexion entre un agent et le serveur (OT.AGENT_CONNECT)
- Dispose d'un mécanisme de surveillance régulier de la connexion entre l'agent et le serveur (OT.HEART_BEAT)

Pour contrôler la mise en œuvre de la politique la TOE :

- Génère une alerte au niveau du serveur lorsqu'une rupture de connexion est constatée (OT_ALERTES_SERVEUR)

OSP.PROTECTION_ALERTES_SERVEUR

Pour mettre en œuvre la politique la TOE:

- Offre un mécanisme de contrôle d'accès aux fichiers d'imputation (OT.CTL_SERV_ASSETS)

Pour garantir la mise en œuvre de la politique la TOE:

- Est administrée par des personnels de confiance (OE.ADM_NO_EVIL)
- A été installée selon des procédures de durcissement de la sécurité (OE.HOST_CLEAN)

Pour contrôler la mise en œuvre de la politique la TOE :

- Rien

OSP.COMM_AGENT

Pour mettre en œuvre la politique la TOE:

- Offre un mécanisme de chiffrement et de contrôle d'intégrité des flux entre un agent ExaProtect SMA et le serveur ExaProtect SMP (OT.PROTECT_COMM_AGENT)
- S'appuie sur des mécanismes cryptographiques conformes aux recommandations de la DCSSI (OE.CRYPTO)

Pour garantir la mise en œuvre de la politique la TOE:

- Rien

Pour contrôler la mise en œuvre de la politique la TOE :

- Rien

OSP.COMM_CONSOLE

Pour mettre en œuvre la politique la TOE:

- Offre un mécanisme de chiffrement et de contrôle d'intégrité des flux entre la console et le serveur ExaProtect SMP (OT.PROTECT_COMM_CONSOLE)
- S'appuie sur des mécanismes cryptographiques conformes aux recommandations de la DCSSI (OE.CRYPTO)

Pour garantir la mise en œuvre de la politique la TOE:

- Rien

Pour contrôler la mise en œuvre de la politique la TOE :

- Rien

OSP.ROLES_ACCESS

Pour mettre en œuvre la politique la TOE:

- Dispose d'un mécanisme d'authentification basé sur un couple login/mot de passe (OT.I&A_USERS)
- Définis des rôles aux utilisateurs de la TOE chaque rôle disposant de droits d'accès particuliers aux biens de la TOE (OT.ROLES)

Pour garantir la mise en œuvre de la politique la TOE:

- Rien

Pour contrôler la mise en œuvre de la politique la TOE :

- Mets en œuvre des traces d'audit (OT.AUDIT).

OSP.EXPORT_BASE

Pour mettre en œuvre la politique la TOE:

- S'appuie sur des mécanismes cryptographiques conformes aux recommandations de la DCSSI (OE.CRYPTO)
- Mets en oeuvre des mécanismes de chiffrement et de signature des bases de données exportées (OT.CRYPTO_BASE)

Pour garantir la mise en œuvre de la politique la TOE:

- Rien

Pour contrôler la mise en œuvre de la politique la TOE :

- Utilise des outils de vérification de signature et de déchiffrement sûrs et fiables (OE.EXPORT_BASE)

VIII.1.2.3 Couverture des hypothèses

H.PROTECT_HARDWARE

L'objectif d'environnement OE.PROTECT_HARWARE couvre cette hypothèse par l'installation de la TOE dans des locaux sécurisés.

H.EXPORT_BASE

L'objectif d'environnement OE.EXPORT_BASE couvre cette hypothèse par l'utilisation d'outils de vérification et de déchiffrement sûrs.

H.TRUE_AGENT

L'objectif d'environnement OE.TRUE_AGENT couvre cette hypothèse par l'utilisation d'agents sûrs et fiables pour la transmission des évènements vers le serveur.

H.SAFE_CONFIG_AGENT

L'objectif d'environnement OE.HOST_CLEAN couvre cette hypothèse par l'installation sécurisée et la mise à jour des systèmes d'exploitation mettant en oeuvre les agents.

L'objectif d'environnement OE.ADM_NO_EVIL couvre cette hypothèse par l'emploi d'installateurs des agents dignes de confiance.

L'objectif d'environnement OE.CTL_AGENT_ASSETS couvre cette hypothèse par l'emploi d'un mécanisme de contrôle d'accès sur les ressources des agents.

H.ADMIN_HOST_NOEVIL

L'objectif d'environnement OE.ADM_NO_EVIL couvre cette hypothèse par l'emploi d'utilisateurs dignes de confiance.

H.CRYTO

L'objectif d'environnement OE.CRYPTO couvre cette hypothèse par l'emploi de mécanismes cryptographiques conformes aux recommandations de la DCSSI.

H.FIREWALL

L'objectif d'environnement OE.FIREWALL couvre cette hypothèse par l'emploi d'un dispositif de filtrage devant le serveur.

H.TIME

L'objectif d'environnement OE.TIME couvre cette hypothèse par la synchronisation des agents et du serveur avec une base de temps fournie par l'environnement.

H.USER_FORMATION

L'objectif d'environnement OE.USR_AWARE couvre cette hypothèse par l'emploi d'utilisateurs de la TOE digne de confiance.

H.SERVEUR_CLEAN

L'objectif d'environnement OE.SERVER_CLEAN couvre cette hypothèse par la non-installation de service tiers sur l'appliance du serveur SMP après son installation.

VIII.2 Argumentaire des exigences de sécurité

VIII.2.1 Récapitulatif

	FPT_TRC.1	FPT_TST.1*	FDP_ACC.1_filesystem	FDP_ACF.1_filesystem	FMT_MSA.3_filesystem	FDP_ACC.1_SGBD	FDP_ACF.1_SGBD	FMT_MSA.3_SGBD	FAU_GEN.1_Agent	FAU_GEN.1_Serveur	FAU-SAA.4	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FAU_STG.2	FAU_STG.4	FPT_ITT.1_CommAgent	FTP_TRP.1	FDP_ACC.1_Console	FDP_ACF.1_Console	FMT_MSA.3_Console	FMT_MSA.1	FMT_SMR.1	FMT_SMF.1	FIA_UID.2	FIA_UAU.2	FIA_AFL.1	FCS_COP.1/Console	FCS_COP.1/Communications	FCS_COP.1/Bases	FDP_IFF.1	FDP_IFC.1
OT.CONFIG_SYNCHRO	X																															
OT.AGENT_CONNECT		X																														
OT.HEART_BEAT		X																														
OT.CTL_SERV_ASSETS			X	X	X																											
OT.CTL_SGDB						X	X	X																								
OT.ALERTES_AGENT									X																							
OT.ALERTES_SERVEUR										X																						
OT.CORRELATION											X																					
OT.AUDIT												X	X	X																		
OT.ASYNC_TRANSMIT															X	X																
OT.PROTECT_COMM_AGENT																	X												X			
OT.PROTECT_COMM_CONSOLE																		X										X				
OT.ROLES																			X	X	X	X	X	X								
OT.I&A_USERS																									X	X	X					
OT.CRYPTO_BASE																														X		
OT.CTL_PARAM_BASE																															X	X

VIII.2.2 Argumentaire détaillé

OT.CONFIG_SYNCHRO

Cet objectif est réalisé par le composant FPT_TRC.1 qui assure une cohérence entre les données séparées de la TSF.

OT.AGENT_CONNECT

Cet objectif est réalisé par le composant FPT_TST.1* qui permet de s'assurer de la disponibilité des évènements remontés par les agents en effectuant régulièrement un test sur la connexion agent-serveur.

OT.HEART_BEAT

Cet objectif est réalisé par le composant FPT_TST.1* qui permet de s'assurer la disponibilité des agents en émettant régulièrement à destination du serveur un message indiquant le bon fonctionnement de l'agent.

OT.CTL_SERV_ASSETS

Cet objectif est réalisé par les composants FDP_ACC.1_filesystem et FDP_ACF.1_filesystem qui utilisent un mécanisme de contrôle d'accès sur le serveur, ainsi que par l'objectif FMT_MSA.3_filesystem qui initialise à l'installation du produit les attributs de sécurité des biens protégés par le contrôle d'accès (les fichiers de paramétrages).

OT.CTL_SGBD

Cet objectif est réalisé par les composants FDP_ACC.1_SGBD et FDP_ACF.1_SGBD qui utilisent un mécanisme de contrôle d'accès sur les tables des bases de données, ainsi que par l'objectif FMT_MSA.3_SGBD qui initialise à l'installation du produit les attributs de sécurité des biens protégés par le contrôle d'accès (les droits sur les tables).

OT.ALERTES_AGENT

Cet objectif est réalisé par le composant FAU_GEN.1_Agent qui permet la génération et la collecte d'évènements de sécurité et des logs bruts (les entrées de log des équipements et ceux spécifiques à l'agent) sur les agents.

OT.ALERTES_SERVEUR

Cet objectif est réalisé par le composant FAU_GEN.1_Serveur qui permet la génération et la collecte d'évènements de sécurité (les logs spécifiques au serveur) sur le serveur.

OT.CORRELATION

Cet objectif est réalisé par le composants FAU_SAA.4 qui réalise une analyse complexe de l'enchaînement et du contenu des évènements remontés par les équipements et par le serveur dans le but d'en effectuer une corrélation.

OT.AUDIT

Cet objectif est réalisé par le composant FAU_SAR.1 qui définit la revue des fichiers d'audit issus du mécanisme de corrélation du produit. L'objectif impose également l'accès à la revue d'audit par des utilisateurs authentifiés. Ceci est réalisé par le composant FAU_SAR.2.

Enfin l'objectif demande que les revues d'audits soient effectuées de manière sélective en fonction de critères, ceci est réalisé par le composant FAU_SAR.3

OT.ASYNC_TRANSMIT

Cet objectif est réalisé par le composant FAU_STG.2 qui permet de s'assurer que les évènements continuent à être crées même en cas de rupture de connexion entre l'agent et le serveur par stockage dans un spooler. Cet objectif est également réalisé par le composant FAU_STG.4 qui émet une alerte lorsque le spooler est plein prévenant que l'agent n'est plus en mesure de stocker les nouveaux évènements.

OT.PROTECT_COMM_AGENT

Cet objectif est réalisé par le composant FPT_ITT.1_Comm_Agent qui assure la protection en confidentialité et en intégrité des données échangées entre un agent et un serveur, ainsi que par le composant FCS_COP.1/Communications qui mets en œuvre les mécanismes de chiffrement et de signature des communications entre les agents et le serveur.

OT.PROTECT_COMM_CONSOLE

Cet objectif est réalisé par le composant FTP_TRP.1 qui garantit l'utilisation d'un chemin de confiance entre l'interface utilisateur située sur la console et le serveur ExaProtect SMP, ainsi que par le composant FCS_COP.1/Console qui mets en œuvre les mécanismes de chiffrement et de signature des communications entre la console et le serveur.

OT.ROLES

Cet objectif est réalisé par le composant FMT_SMR.1 qui définit les rôles (viewer, analyst, administrator, super-user). Les rôles sont gérés grâce au composant FMT_SMF.1. Ces rôles sont associés à des droits d'accès sur les fonctionnalités offertes par la console, droits d'accès qui sont définis, initialisés et gérés grâce aux composants FDP_ACC.1_Console, FDP_ACF.1_Console, FMT_MSA.3_Console et FMT_MSA.1.

OT.I&A_USERS

Cet objectif est réalisé par les composants FIA_UID.2 et FIA_UAU.2 qui définissent un mécanisme d'authentification avant toute action sur la TOE, ainsi que par le composant FIA_AFL.1 qui gère la manière dont est traitée une mauvaise authentification.

OT.CRYPTO_BASE

Cet objectif est réalisé par le composant FCS_COP.1/Bases qui met en œuvre les mécanismes de chiffrement et de signature des bases de données exportées.

OT.CTL_PARAM_BASE

Cet objectif est réalisé par les composants FDP_IFF.1 et FDP_IFC.1 qui mettent en œuvre un mécanisme de contrôle des paramètres passés aux bases de données.

VIII.2.3 Satisfaction de dépendances

Composant	Intitulé	Dépendances	Respect
FPT_TRC.1	Internal TSF consistency	FPT_ITT.1	Oui
FPT_TST.1*	TSF Agent connection testing	-	
FDP_ACC.1_filesystem	Subset access control	FDO_ACF.1_filesystem	Oui
FDP_ACF.1_filesystem	Security attribute based access control	FDP_ACC.1_filesystem	Oui
		FMT.MSA.3_filesystem	Oui
FMT_MSA.3_filesystem	Static attribute initialisation	FMT_MSA.1	Initialisation définitive des attributs de sécurité à l'installation
		FMT_SMR.1	Pas de gestion de rôles
FDP_ACC.1_SGBD	Subset access control	FDP_ACF.1_SGBD	Oui
FDP_ACF.1_SGBD	Security attribute based access control	FDP_ACC.1_SGBD	Oui
		FMT_MSA.3_SGBD	Oui
FMT_MSA.3_SGBD	Static attribute initialisation	FMT_MSA.1	Initialisation définitive des attributs de sécurité à l'installation
		FMT_SMR.1	Pas de gestion de rôles
FDP_ACC.1_Console	Subset access control	FDP_ACF.1_Console	Oui
FDP_ACF.1_Console	Security attribute based access control	FDP_ACC.1_Console	Oui
		FMT_MSA.3_Console	Oui
FMT_MSA.3_Console	Static attribute initialisation	FMT_MSA.1	Oui
		FMT_SMR.1	Oui
FMT_MSA.1	Management of security attributes	FDP_ACC.1_filesystem FDP_ACF.1_filesystem FDP_ACC.1_SGBD FDP_ACF.1_SGBD FDP_ACC.1_Console FDP_ACF.1_Console	Oui
		FMT_SMF.1	Oui
		FMT_SMT.1	Oui
		FMT_SMR.1	Oui
FMT_SMR.1	Security roles	FIA_UID.1	Oui
FMT_SMF.1	Specification of Management Functions	-	Oui
FAU_GEN.1_Agent	Audit data generation	FPT_STM.1	La TOE n'est pas à l'origine d'une base de temps fiable puisque l'environnement fournit ce service.
FAU_GEN.1_Serveur	Audit data generation	FPT_STM.1	La TOE n'est pas à l'origine d'une base de temps fiable puisque l'environnement fournit ce service.
FAU_SAA.4	Complex attack heuristics	-	Oui
FAU_SAR.1	Audit review	FAU_GEN.1	Oui
FAU_SAR.2	Restricted audit review	FAU_SAR.1	Oui
FAU_SAR.3	Selectable audit review	FAU_SAR.1	Oui
FAU_STG.2	Guarantees of audit data availability	FAU_GEN.1	Oui
FAU_STG.4	Prevention of audit data loss	FAU_STG.1	Oui
FPT_ITT.1_CommAgent	Basic internal TSF data transfer protection	-	Oui
FTP_TRP.1	Trusted path	-	Oui
FIA_UID.2	User identification before any action	-	Oui
FIA_UAU.2	User authentication before any action	FIA_UID.1	Oui
FCS_COP.1/Console	Cryptographic operation	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes	Pas de génération ni de destruction des clés selon des mécanismes cryptographiques. Les bi-clés sont générées hors de la TOE, la révocation s'effectue par simple effacement du fichier. Le contrôle des valeurs sûres des algorithmes utilisés pour

Composant	Intitulé	Dépendances	Respect
			la génération des clés est fait hors TOE.
FCS_COP.1/Communications	Cryptographic operation	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes	Pas de génération ni de destruction des clés selon des mécanismes cryptographiques. Les bi-clés sont générées hors de la TOE, la révocation s'effectue par simple effacement du fichier. Le contrôle des valeurs sûres des algorithmes utilisés pour la génération des clés est fait hors TOE.
FCS_COP.1/Bases	Cryptographic operation	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes	Pas de génération ni de destruction des clés selon des mécanismes cryptographiques. Les bi-clés sont générées hors de la TOE, la révocation s'effectue par simple effacement du fichier. Le contrôle des valeurs sûres des algorithmes utilisés pour la génération des clés est fait hors TOE.
FIA_AFL.1	Authentification failure handling	FIA_UID.1	Oui
FDP_IFF.1	Simple Security Attributes	FDP_IFC.1 FMT_MSA.3	Pas de FMT_MSA.3 car aucune initialisation statique des attributs de sécurité
FDP_IFC.1	Subset information flow control	FDP_IFF.1	Oui

VIII.2.4 Pertinence du niveau de résistance des fonctions exigé

Le niveau de résistance exigé SOF-high se justifie par le niveau des informations (informations sensibles) qui seront manipulées par le produit.

VIII.3 Argumentaire des spécifications globales

VIII.3.1 Récapitulatif

	FPT_TRC.1	FPT_TST.1*	FDP_ACC.1_filesystem	FDP_ACF.1_filesystem	FMT_MSA.3_filesystem	FDP_ACC.1_SGBD	FDP_ACF.1_SGBD	FMT_MSA.3_SGBD	FAU_GEN.1_Agent	FAU_GEN.1_Serveur	FAU-SAA.4	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FAU_STG.2	FAU_STG.4	FPT_ITT.1_CommAgent	FTP_TRP.1	FDP_ACC.1_Console	FDP_ACF.1_Console	FMT_MSA.3_Console	FMT_MSA.1	FMT_SMR.1	FMT_SMF.1	FIA_UID.2	FIA_UAU.2	FIA_AFL.1	FCS_COP.1/Console	FCS_COP.1/Communications	FCS_COP.1/Bases	FDP_IFF.1	FDP_IFC.1
F_FID_Synchro	X																															
F_FIA_Liaison		X																														
F_CTL_Access_ressources_Serveur			X	X	X																											
F_CTL_Base_de_données						X	X	X																							X	X
F_IMP_Agent									X						X	X																
F_IMP_Serveur										X																						
F_AUD_Audit									X	X	X	X	X	X																		
F_ECH_AgentServeur																	X												X			
F_ECH_ConsoleServeur																		X										X				
F_CTL_Gere_access_Util																			X	X	X	X	X	X								
F_I&A_Util																									X	X	X					
F_EXPORT_BASE																														X		

VIII.3.2 Argumentaire détaillé

F_FID_Synchro

Cette fonction est réalisée par le composant FPT_TRC.1 qui assure une cohérence entre les données séparées de la TSF.

F_FIA_Liaison

Cette fonction est réalisée par le composant FPT_TST.1* qui permet de s'assurer la disponibilité des agents en émettant régulièrement à destination du serveur un message indiquant le bon fonctionnement de l'agent.

F_CTL_Access_ressources_Serveur

Cette fonction est réalisée par les composants FDP_ACC.1_filesystem et FDP_ACF.1_filesystem qui utilisent un mécanisme de contrôle d'accès sur le serveur, ainsi que par l'objectif FMT_MSA.3_filesystem qui initialise à l'installation du produit les attributs de sécurité des biens protégés par le contrôle d'accès (les fichiers de paramétrages).

F_CTL_Base_de_données

Cette fonction est réalisée par les composants FDP_ACC.1_SGBD et FDP_ACF.1_SGBD qui utilisent un mécanisme de contrôle d'accès sur les tables des bases de données, ainsi que par le composant FMT_MSA.3_SGBD qui initialise à l'installation du produit les attributs de sécurité des biens protégés par le contrôle d'accès (les droits sur les tables), et aussi les composants FDP_IFF.1 et FDP_IFC.1 qui mettent en œuvre un mécanisme de contrôle des paramètres passés aux bases de données.

F_IMP_Agent

Cette fonction est réalisée par le composant FAU_GEN.1_Agent qui permet la génération et la collecte d'évènements de sécurité et des logs bruts (les entrées de log des équipements et ceux spécifiques à l'agent) sur les agents.

Cette fonction est réalisée par le composant FAU_STG.2 qui permet de s'assurer que les évènements continuent à être crées même en cas de rupture de connexion entre l'agent et le serveur par stockage dans un spooler. Cette fonction est également réalisée par le composant FAU_STG.4 qui émet une alerte lorsque le spooler est plein prévenant que l'agent n'est plus en mesure de stocker les nouveaux évènements.

F_IMP_Serveur

Cette fonction est réalisée par le composant FAU_GEN.1_Serveur qui permet la génération et la collecte d'évènements de sécurité (les logs spécifiques au serveur) sur le serveur.

F_AUD_Audit

Cette fonction est réalisée par le composant FAU_SAR.1 qui définit la revue des fichiers d'audit issus du mécanisme de corrélation du produit. La fonction impose également l'accès à la revue d'audit par des utilisateurs authentifiés. Ceci est réalisé par le composant FAU_SAR.2.

Enfin la fonction demande que les revues d'audits soient effectuées de manière sélective en fonction de critères, ceci est réalisé par le composant FAU_SAR.3

De plus, cette fonction est réalisée par le composants FAU_SAA.4 qui réalise une analyse complexe de l'enchaînement et du contenu des évènements remontés par les équipements et par le serveur dans le but d'en effectuer une corrélation. Suite à cette corrélation, des alertes de sécurité sont générées. Ceci est réalisé par les composants FAU_GEN.1_Agent et FAU_GEN.1_Serveur.

F_ECH_AgentServeur

Cette fonction est réalisée par le composant FPT_ITT.1_Comm_Agent qui assure la protection en confidentialité et en intégrité des données échangées entre un agent et un serveur, ainsi que par le composant FCS_COP.1/Communications qui mets en œuvre les mécanismes de chiffrement et de signature des communications entre les agents et le serveur.

F_ECH_ConsoleServeur

Cette fonction est réalisée par le composant FTP_TRP.1 qui garantit l'utilisation d'un chemin de confiance entre l'interface utilisateur située sur la console et le serveur ExaProtect SMP, ainsi que par le composant FCS_COP.1/Console qui mets en œuvre les mécanismes de chiffrement et de signature des communications entre la console et le serveur.

F_CTL_Gere_access_Util

Cette fonction est réalisée par le composant FMT_SMR.1 qui définit les rôles (viewer, analyst, administrator, super-user). Les rôles sont gérés grâce au composant FMT_SMF.1. Ces rôles sont associés à des droits d'accès sur les fonctionnalités offertes par la console, droits d'accès qui sont définis, initialisés et gérés grâce aux composants FDP_ACC.1_Console, FDP_ACF.1_Console, FMT_MSA.3_Console et FMT_MSA.1.

F_I&A_Util

Cette fonction est réalisée par les composants FIA_UID.2 et FIA_UAU.2 qui définissent un mécanisme d'authentification avant toute action sur la TOE, ainsi que par le composant FIA_AFL.1 qui gère la manière dont est traitée une mauvaise authentification.

F_EXPORT_BASE

Cette fonction est réalisée par le composant FCS_COP.1/Bases qui met en œuvre les mécanismes de chiffrement et de signature des bases de données exportées.

VIII.4 Argumentaire pour les exigences d'assurance

VIII.4.1 Mesures de l'environnement de développement

VIII.4.1.1 Méthodes et outils de gestion de configuration

Le système de gestion de configuration couvre la gestion et le contrôle du développement, de la production et de la maintenance d'ExaProtect SMS. Son application permet d'affecter un identifiant unique à chaque version de la TOE et d'établir une liste des versions des composants qui constituent une version donnée.

Le commanditaire documente les procédures du système de gestion de configuration et fournit une liste de configuration pour chaque version de la TOE présentée.

L'évaluateur évalue la documentation et contrôle, sur les versions de la TOE qui lui sont livrées par le commanditaire, que le système de gestion de configuration est bien appliqué tel que décrit dans la documentation (pas d'audit de l'environnement de développement sous ce critère).

Argumentaire : ces procédures satisfont à l'exigence ACM_CAP.2

VIII.4.1.2 Sécurité de l'environnement de développement

Les mesures de sécurité appliquées pour le développement et la maintenance d'ExaProtect SMS garantissent l'intégrité du code exécutable de la TOE et la confidentialité des documents de développement associés.

Le commanditaire documente les mesures de sécurité de l'environnement de développement en identifiant précisément le périmètre de cet environnement, et fournit des traces de l'application de ces mesures.

L'évaluateur évalue la documentation et procède à un audit de l'environnement afin de vérifier et d'apprécier l'application des mesures, et d'interviewer les personnels concernés sur leur connaissance des mesures.

Argumentaire : ces procédures satisfont à l'exigence ALC_DVS.1.

VIII.4.1.3 Procédures de livraison

Les procédures et mesures mises en place pour transférer ExaProtect SMS du développeur chez l'utilisateur final garantissent l'authenticité et l'intégrité de la TOE lors du transfert.
Le commanditaire documente les procédures de livraison.
L'évaluateur évalue la documentation et procède à un audit de l'environnement afin de vérifier et d'apprécier l'application des mesures, et d'interviewer les personnels concernés sur leur connaissance des mesures.

Argumentaire : ces procédures satisfont à l'exigence ADO_DEL.1.

VIII.4.1.4 Procédures de correction des anomalies

Des procédures de correction des anomalies sont mises en place au niveau du laboratoire et du service support pour assurer une gestion et un contrôle des anomalies de sécurité découvertes en interne ou soumises par les exploitants, ainsi que la distribution des correctifs associés, une fois les anomalies résolues.

Le commanditaire documente les procédures visant à la correction des anomalies, et fournit les documents donnant des lignes directrices aux exploitants pour lui soumettre les anomalies.

L'évaluateur évalue la documentation (pas d'audit de l'environnement de développement sous ce critère).

Argumentaire : ces procédures satisfont à l'exigence ALC_FLR.3.

VIII.4.1.5 Documentation et outils de développement des fonctions de sécurité

Le commanditaire fournit les documents permettant d'assurer un niveau de qualité compatible avec les exigences liées au paquet d'assurance sécurité : spécifications fonctionnelles, conception de haut niveau, conception de bas niveau, documentation des outils et techniques de développement (compilateurs, makefiles, …) et code source. Ces documents forment les niveaux successifs de représentation de la fonctionnalité de sécurité.

Des correspondances entre ces niveaux sont établies, en commençant par les fonctions de sécurité des TI spécifiées de manière informelles dans ce document.

L'évaluateur évalue la documentation, et vérifie que les exigences fonctionnelles de sécurité du se reflètent bien dans les différents niveaux de représentation de la fonctionnalité de sécurité.

Argumentaire : ces mesures satisfont aux exigences ADV_FSP.1, ADV_HLD.2, ADV_LLD.1, ALC_TAT.1, , ADV_IMP.1 et ADV_RCR.1.

VIII.4.2 Test des fonctions de sécurité

VIII.4.2.1 Procédures de test du développeur

Le commanditaire fournit les documents produits à l'occasion des tests qu'il a effectués sur la TOE. Ces documents doivent décrire le plan et les procédures de tests suivies et montrer le degré de couverture des spécifications fonctionnelles par les tests. Ils doivent inclure les résultats effectifs des tests et démontrer que les fonctions de sécurité se comportent bien de la manière spécifiée dans les spécifications fonctionnelles.

Le commanditaire met également à disposition de l'évaluateur une TOE se prêtant au repassage des tests qu'il a effectués sur la TOE.

L'évaluateur évalue la documentation et repasse une partie des tests du développeur.

Argumentaire : ces procédures satisfont aux exigences ATE_FUN.1, ATE_COV.1 et à une partie d'ATE_IND.2 (repassage des tests).

VIII.4.2.2 Test indépendant par l'évaluateur

Le commanditaire met à disposition de l'évaluateur une TOE se prêtant à l'exécution de tests indépendants.

Sur la base des spécifications fonctionnelles et de la documentation de test, l'évaluateur conçoit des tests complémentaires des fonctions de sécurité, afin de valider des comportements de sécurité de la TOE que le commanditaire n'aurait pas testés.

Argumentaire : ces mesures satisfont à une partie de l'exigence ATE_IND.2 (test indépendant).

VIII.4.3 Documentation d'exploitation

VIII.4.3.1 Procédures d'installation et de démarrage

Ces procédures permettent l'installation et le démarrage de la TOE dans des conditions qui garantissent une exécution satisfaisante de ses fonctions de sécurité.

Afin de prévenir les risques d'utilisation impropre, la documentation d'installation et de démarrage doit spécifiquement identifier tous les modes d'exécution possibles de la TOE ainsi que leur impact sur la sécurité. Elle doit être claire, complète, cohérente, et accessible à l'audience visée. Elle doit enfin énumérer toutes les hypothèses relatives à l'environnement d'exploitation prévu et les exigences sur les mesures de sécurité (TI ou non-TI) qui doivent être présentes dans l'environnement.

Le commanditaire documente les procédures d'installation et de démarrage sûrs de la TOE.
L'évaluateur évalue la documentation, au besoin en ré-appliquant les procédures ou une partie d'entre elles.

Argumentaire : ces procédures satisfont aux exigences ADO_IGS.1 et AVA_MSU.1 (concernant la documentation d'installation et de démarrage).

VIII.4.3.2 Documentation d'administration

La documentation d'exploitation à destination des administrateurs doit décrire le comportement des fonctions de sécurité et refléter les hypothèses sur l'environnement d'exploitation, dans une optique de configuration, de maintenance et de maintien en condition opérationnelle corrects des fonctions de sécurité. Elle doit également décrire les différents types d'événements relatifs à la sécurité susceptibles de survenir, et fournir des lignes directrices sur la manière de les prendre en compte.

Des exigences spécifiques à la prévention de l'utilisation impropre, similaires à celles sur la documentation d'installation et de démarrage, pèsent également sur la documentation d'administration

Le commanditaire fournit la documentation d'administration.
L'évaluateur évalue la documentation d'administration.

Argumentaire : ces mesures satisfont aux exigences AGD_ADM.1 et AVA_MSU.1 (concernant la documentation d'administration).

VIII.4.3.3 Documentation utilisateur

La documentation d'exploitation à destination des utilisateurs doit décrire le comportement des fonctions de sécurité qu'ils ont besoin de connaître, et refléter les hypothèses sur l'environnement d'exploitation et les responsabilités qui les concernent (et notamment les situations qui nécessitent d'en référer à l'administrateur).

Des exigences spécifiques à la prévention de l'utilisation impropre, similaires à celles sur la documentation d'installation et de démarrage et d'administration, peuvent également peser sur la documentation utilisateur, sous réserve de leur pertinence et de leur applicabilité aux utilisateurs.

Le commanditaire fournit la documentation utilisateur.
L'évaluateur évalue la documentation utilisateur.

Argumentaire : ces mesures satisfont aux exigences AGD_USR.1 et AVA_MSU.1 (concernant la documentation utilisateur).

VIII.4.4 Estimation de la vulnérabilité

Cette tâche s'appuie sur les résultats de toutes les tâches précédentes et sur des sources publiques et également sur les outils spécifiques que l'évaluateur peut développer pour identifier les vulnérabilités susceptibles de causer la réalisation de menaces identifiées dans la présente cible de sécurité ou des infractions aux règles de politiques de sécurité organisationnelles de la présente cible de sécurité. La résistance des mécanismes de sécurité de nature combinatoire ou probabiliste aux attaques directes est également estimée.

Le commanditaire doit fournir une analyse de vulnérabilités énonçant toutes les vulnérabilités qu'il a décelées au cours du développement, montrant qu'elles ne sont pas exploitables et justifiant que la cible d'évaluation résiste aux attaques de pénétration requérant une compréhension minimale de son fonctionnement.

Une analyse de la résistance des mécanismes pour lesquels une annonce de résistance des fonctions a été faite dans la présente cible de sécurité doit également être fournie par le commanditaire.

L'évaluateur rédige une analyse indépendante de vulnérabilités (à destination exclusive de l'organisme de certification), sur la base des autres fournitures de l'évaluation, afin de confirmer ou d'infirmer les résultats des analyses du commanditaire. Il procède d'autre part à des tests de pénétration dans le but d'estimer les moyens nécessaires à la mise en oeuvre des vulnérabilités (compétence technique, temps, expertise, etc.). Cette tâche permet de confirmer ou d'infirmer que le niveau minimum de moyens nécessaires estimés, mesurés selon une métrique décrite dans les Critères Communs, est strictement supérieur à ceux correspondant à un potentiel d'attaque élevé.

Argumentaire : ces mesures satisfont aux exigences AVA_SOF.1 et AVA_VLA.2.

IX Glossaire

Acquittement :	Tâche réalisée par un analyste consistant à valider la prise en compte d'une alerte.
Agent :	Composant de la solution ExaProtect SMS chargé de collecter les entrées de log générées par les équipements et de les convertir en évènement (normalisation lexical et syntaxique), ces évènements sont ensuite envoyés sous forme de message IDMEF au server ExaProtect SMP.
Agrégation :	Mécanisme de regroupement de plusieurs alertes ayant un ou plusieurs critères identiques (même nom, même machine cible, …).
Alerte :	Evènement IDMEF agrégé, corrélé, enrichi ou modifié (évènement traité par le moteur de corrélation). Les alertes sont créées sur le Security Management Platform.
Evènement :	Objet de données standardisé (IDMEF) représentant une entrée de log, créé par un Security Management Agent.
Alerte corrélée :	Alerte intégrée dans une alerte de corrélation.
Alerte de corrélation :	Alerte générée par le serveur ExaProtect SMP regroupant des évènements et des alertes.
Converter :	Regroupement de plusieurs règles de transcription de même type : Log (fichiers de logs), Database (base de données), WELF (fichier de logs), OPSEC (checkpoint), WMI (windows), RDEP (cisco), SCANNER, Multi_Line (fichiers de logs) ou RSA (base de données).
Corrélation :	Mise en relation d'information de différents types, provenant de sources différentes (alertes provenant d'un scanner, alertes provenant d'un IDS, base de vulnérabilités, règles de corrélation…).
Equipement :	Elément du système d'information générant au cours de son fonctionnement des entrées de log susceptible de contenir des informations intéressantes d'un point de vue sécurité (firewall, IDS, proxy, systèmes Unix/Windows, application Web …).
Entrée de log :	Message enregistré par une application, un système d'exploitation ou un dispositif de sécurité. Cela peut être une ligne de fichier texte décrivant l'échec d'une tentative de connexion ou un enregistrement dans une base de données indiquant qu'un utilisateur s'est authentifié avec succès..
ExaProtect SMA :	*ExaProtect Security Management Agent* : Composant logiciel se positionnant, soit directement sur un équipement, soit à proximité, et qui assurent la collecte et la normalisation des entrées de log en évènements avant de les transmettre à un ExaProtect SMP.
ExaProtect SMC :	*ExaProtect Security Management Console* : Console Web utilisateur de la solution ExaProtect SMS.
ExaProtect SMP :	*ExaProtect Security Management Platform* : Appliance dédié à la collecte et à l'analyse des alertes de sécurité. C'est le composant central de la solution ExaProtect SMS.
ExaProtect SMS :	*ExaProtect Security Management Solution*
Faux positif :	Evènement ou alerte correspondant à une erreur de détection des équipements.
Gravité :	Importance de l'alerte, les différents niveaux sont : "high", "medium", "low", "info", "unknown".
Heartbeats :	Message envoyé par un agent au serveur pour lui signaler son activité.
IDMEF :	*Intrusion Detection Message Exchange Format* : Format ouvert dédié à l'échange de messages de sécurité entre équipements de sécurité (standard issu de l'IETF : *Internet Engineering Task Force*).

IODEF :	*Incident Object Description Exchange Format* : Format ouvert dédié à la gestion des évènements de sécurité.
Incident :	Container d'alertes au format IODEF qui permet d'assurer le suivi du traitement de ces alertes en précisant notamment la cause, les actions à effectuer (interfaçage possible avec un logiciel de gestion de tickets tiers).
OSVDB :	*Open Source Vulnerability Database* : Base de vulnérabilités open source, ayant pour but de référencer l'ensemble des vulnérabilités connues grâce aux contributions de la communauté sécurité.
Règle de corrélation :	Description de critères (conditions et exceptions) permettant d'effectuer des actions prédéfinies en fonction des informations contenues dans les alertes suivant une plage de temps définie et du nombre d'alertes concernées.
SLA :	*Service Level Agreement* : Indicateur spécifiant le délai d'acquittement maximum d'une alerte (en minute) calculé en fonction de la gravité de l'alerte, de la criticité de la machine impactée, du niveau de sécurité courant et des plages horaires de travail de l'analyste.

X Références

[CC] Common Criteria for Information Technology Security Evaluation version 2.3, August 2005
Part 1 : Introduction and general model, réf. CCIMB-2005-08-001
Part 2 : Security functional requirements, réf. CCIMB-2005-08-002
Part 3 : Security Assurance Requirements ; réf. CCIMB-2005-08-003

[QUALIF] Règles relatives à la qualification des produits de sécurité par la DCSSI version 1.1, réf. N°000451/SGDN/DCSSI/SDR, SGDN/DCSSI, 26/02/2004 et
Processus de qualification d'un produit de sécurité - niveau standard - version 1.0, réf. N°001591/SGDN/DCSSI/SDR, SGDN/DCSSI, 28/07/2003