Cible de Sécurité

DISCO

Version 01.05p du 23/10/2020

Réf : DISCO_Cible de sécurité

Historique

Version	Date	Origine de la mise à jour	Rédigée par	Validée par
V01.00	23/08/2019	Création du document	Claire GRANDSIRE Esteban BOUILLARD	Synacktiv
V01.01	27/08/2019	Ajout documents référencés Complétion du chapitre 3.6	Claire GRANDSIRE Esteban BOUILLARD	Synacktiv
V01.02	13/09/2019	Modification suite aux retours de l'ANSSI	Esteban BOUILLARD	Frédéric GOURMANDIN
V1.03	23/09/2019	Modification suite aux retours ANSSI et SYNACKTIV	Esteban BOUILLARD	Claire GRANDSIRE
V1.04	16/07/2020	Mise à jour du document en prévision de l'entrée en CSPN	Esteban BOUILLARD	Claire GRANDSIRE
V1.05	07/10/2020	Mise à jour suite à la première évaluation	Esteban BOUILLARD	Claire GRANDSIRE
V1.05p	23/10/2020	Mise à jour du document pour publication	Esteban BOUILLARD	Jean-Vincent GAIFFAS

Sommaire

1. Introduction

1.1. Objet du document

Ce document est réalisé dans le cadre de la demande d'évaluation au CSPN du produit TSCAP auprès de l'ANSSI. La cible de sécurité décrit :

- Le produit ;
- L'environnement d'utilisation et d'évaluation ;
- Les hypothèses ;
- Les biens sensibles et cryptographiques;
- Les menaces ;
- Les fonctions de sécurité du produit.

1.2. Documents applicables

Ref.	Description
[CER-I-01.1]	Méthodologie pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau. N°1416/ANSSI/SR du 30 mai 2011.
[CER-I-02.1]	Critères pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau. N°1417/ANSSI/SR du 30 mai 2011.

Tableau 1 – Documents applicables

1.3. Documents référencés

Ref.	Nom du document
[REF1]	Suivi des briques externes
[REF4]	Manuel utilisateur TSCAP

Tableau 2 – Documents référencés

1.4. Glossaire

Acronymes	Définitions
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CSPN	Certification de Sécurité de Premier Niveau
TOE	Target Of Evaluation (Cible d'évaluation)
NIST	National Institute of Standard and Technologies
CIS	Center for Internet Security

PSSI	Politique de Sécurité du Système d'Informations
AD	Active Directory
LDAP	Lightweight Directory Access Protocol
Framework	Boite à outils de développement
Contrôles techniques	Tests tels que définis dans la norme OVAL en version 5.10
TMSAD	Trust Model for Security Automation Data
SCAP	« Security Content Automation Protocol » Le protocole SCAP est un protocole d'audit de sécurité des SI, maintenu par l'agence américaine NIST.
TSCAP	Trusted SCAP
WinRM	« Windows Remote Management » repose sur du HTTP et il est l'implémentation chez Microsoft du standard WS-Management, basé sur SOAP.
API	Application Programming Interface

Tableau 3 - Glossaire

2. Identification du produit

Organisation éditrice	Sopra Steria Group
Nom commercial du produit	TSCAP
Nom de code pour l'évaluation	DISCO
Version propose à l'évaluation	Version 1.1.0
Identification du produit soumis à l'évaluation	cpe:2.3:a:SOPRA_STERIA:TSCAP:1.1.0:*:*:fr:*:windows:*:*
Catégorie du produit	Administration et supervision de la sécurité

Tableau 4 - Identification du produit

TSCAP est fourni pour évaluation dans sa version 1.1.0. Il est à noter que la version de TSCAP est identifiée de la manière suivante : <majeur>.<mineur>.<correctif>, avec :

- Numéro de version majeure : Ce numéro évolue uniquement lorsqu'une fonctionnalité majeure est apportée à TSCAP ;
- Numéro de version mineure : Ce numéro évolue lorsque des fonctionnalités mineures sont apportées à TSCAP ;
- Numéro de version corrective : Ce numéro évolue lorsqu'un correctif est apporté à TSCAP, ou que les autorités de confiance (voir chapitre autorités de confiance) sont modifiées dans le magasin TSCAP.

Les hashs permettant d'identifier l'ensemble des fichiers composants cette version sont disponibles dans le fichier de clé permettant l'exécution de TSCAP.

Le hash SHA-256 de ce fichier de clé permettant de vérifier l'intégrité de la version 1.1.0 est fourni dans le changelog de l'application. Ce changelog est fourni avec TSCAP lors de l'entrée en évaluation.

3. Description du produit

3.1. Description générale

3.1.1. SCAP

Security Content Automation Protocol (SCAP) est un protocole d'audit de sécurité des systèmes d'informations. Ce protocole est maintenu par le NIST et le CIS, deux agences américaines de normalisation et de sécurité. Il décrit plusieurs cas d'utilisation :

- Vérification de la conformité du système audité à la PSSI ;
- Recherche de vulnérabilité sur le système audité ;
- Vérification de l'application de patchs sur le système audité ;
- Recherche de composants installés sur le système audité.

SCAP est basé sur des contenus au format XML, normalisés par le langage XCCDF, permettant de définir des checklists de tests à effectuer en fonction de profils, et le langage OVAL, permettant de définir les tests à exécuter sur le système audité.

Il est possible d'effectuer des signatures électroniques sur les contenus SCAP, afin de prouver leur authenticité. Cette fonctionnalité de signature est définie par la norme TMSAD, qui établit un modèle de confiance autour des contenus SCAP.

3.1.2. TSCAP

TSCAP (Trusted SCAP) est un outil permettant, à partir d'entrées SCAP, d'auditer des systèmes et de produire des rapports aux formats XML et HTML. Ces rapports donnent un état de conformité du système audité à la politique de sécurité en vigueur, et mettent en exergue les non-conformités du système audité.

Les résultats SCAP sont issus d'un calcul entre le résultat attendu de l'état du système, défini par l'auditeur, et l'état réel du système, donné par le système via des sondes de collecte.

TSCAP prend en entrée un fichier SCAP pouvant contenir une ou plusieurs signatures XML telles que formalisées dans la norme TMSAD en version 1.0, vérifie ces signatures et génère une erreur en cas d'incohérence.

3.1.3. Intervenants TSCAP

a. Producteur de contenu SCAP

Le producteur de contenu SCAP est une personne qui écrit un contenu SCAP offrant un fichier de paramétrage déterminant les actions à mener sur le système (quels tests, comment sont-ils organisés…). On appelle ces fichiers de paramétrage « entrées SCAP ».

Le producteur SCAP :

- peut être issu d'une communauté publique ;
- n'a cependant aucun privilège sur le système sur lequel est exécuté TSCAP ;

- conserve sa clé privée permettant de signer l'entrée SCAP.

b. Autorités de confiance

Les autorités de confiance sont fixées à la compilation, par demande contractuelle dans le cahier des charges du produit, afin d'empêcher toute diffusion de ce produit en dehors du cadre de démonstration dans lequel il est prévu de fonctionner. De plus, il est à noter que la capacité de révocation des certificats pouvant être proposée par les autorités n'est pas gérée dans TSCAP.

Autorités de confiance SCAP

Ces autorités sont des autorités de certification qui ont approuvé la signature d'un contenu SCAP. Par exemple, lorsque le NIST crée un contenu, celui-ci est signé par l'un des membres du NIST, dont la clé publique est certifiée par l'autorité NIST.

Autorité de confiance TSCAP

L'autorité TSCAP est une autorité de confiance gérant la création des certificats permettant la signature et la vérification de signature des entrées SCAP passées à TSCAP. Cette signature permet d'assurer l'intégrité des entrées SCAP.

3.2. Description de l'utilisateur typique : l'Auditeur

L'auditeur est la personne en charge d'exécuter TSCAP afin de réaliser l'audit d'un système. Il dispose d'un accès privilégié sur sa machine (administrateur local), afin de pouvoir lancer les composants nécessitant un accès privilégié (tel que la collecte).

Lorsqu'il souhaite faire un audit à distance, l'auditeur donne à TSCAP un accès privilégié ainsi qu'un accès non privilégié sur la machine distante, afin de pouvoir collecter les données selon le principe du moindre privilège.

Les secrets gardés par l'auditeur sont les suivants :

- Secret du compte privilégié du système audité ;
- Secret du compte non privilégié du système audité.

L'auditeur peut aussi utiliser TSCAP afin de vérifier l'intégrité d'un rapport produit par lui-même ou un autre auditeur.

3.3. Description de l'utilisation : Cas d'usage de l'outils.

TSCAP fonctionne de la manière suivante :

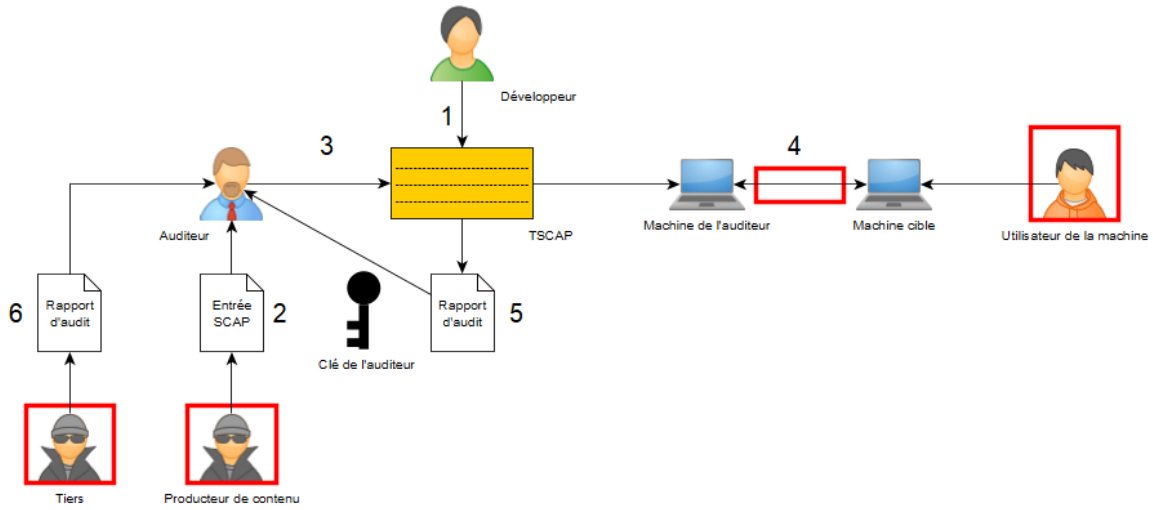

Figure 1 – Fonctionnement de TSCAP

Dans ce schéma de fonctionnement, les encadrés rouges indiquent les endroits où un attaquant pourrait intervenir.

1) Le Développeur fournit TSCAP à l'Auditeur ;
2) Le producteur de contenus fournit à l'auditeur une entrée SCAP. Ce producteur de contenu est supposé malveillant pour prendre en compte le pire scénario (M3) et le contenu qu'il produit ne peut être supposé sain ;
3) L'Auditeur exécute TSCAP en fournissant l'entrée SCAP et ses paramètres. L'Auditeur est réputé de confiance. Egalement, sa machine est considérée comme non compromise.
4) La machine de l'Auditeur communique avec la machine auditée au travers d'un canal WinRM. Le réseau sur lequel passe ce canal n'est pas considéré comme sûr. Egalement, l'Utilisateur de la machine cible n'est pas administrateur de la machine et n'est pas considéré comme de confiance. Cependant, il est supposé qu'il n'a pas réussi à élever ses privilèges sur la machine. Toutefois, il peut tenter d'utiliser les failles pouvant être induites par l'utilisation TSCAP pour élever ses privilèges ;
5) TSCAP produit un rapport d'audit, signé avec la clé privée de l'Auditeur, et le fournit à l'Auditeur. Il est à noter que les rapports d'audit sont au format XML (OVAL, XCCDF ou ARF) ou HTML. Seuls les rapports au format XML sont signés, et font l'objet d'une vérification de sécurité. Les rapports HTML ne sont utilisés que pour analyser les résultats de rapport. Egalement, les rapports ARF ne font pas l'objet d'une vérification des contraintes métier définies via Schematron ;
6) L'auditeur vérifie le rapport XML fourni par un tiers. Le tiers n'est pas réputé de confiance et le rapport peut être malveillant. TSCAP permet de vérifier l'innocuité de ce rapport, et une vérification de la signature XML permet de déterminer si le rapport a été modifié depuis sa production.

TSCAP est indépendant du système sur lequel il est exécuté, c'est-à-dire qu'aucune dépendance non standard n'est nécessaire à son exécution. Il peut être exécuté après un simple copier-coller sur le système de fichier local ou directement depuis un support amovible (clé USB par exemple).

Après exécution de TSCAP, il est obligatoire de suivre la procédure de nettoyage documentée dans le manuel utilisateur [REF4] afin d'assurer que TSCAP ne laisse aucune trace sur le poste auditeur. Cette procédure se base sur un script fourni dans le package de TSCAP.

3.3.1. Architecture du produit TSCAP

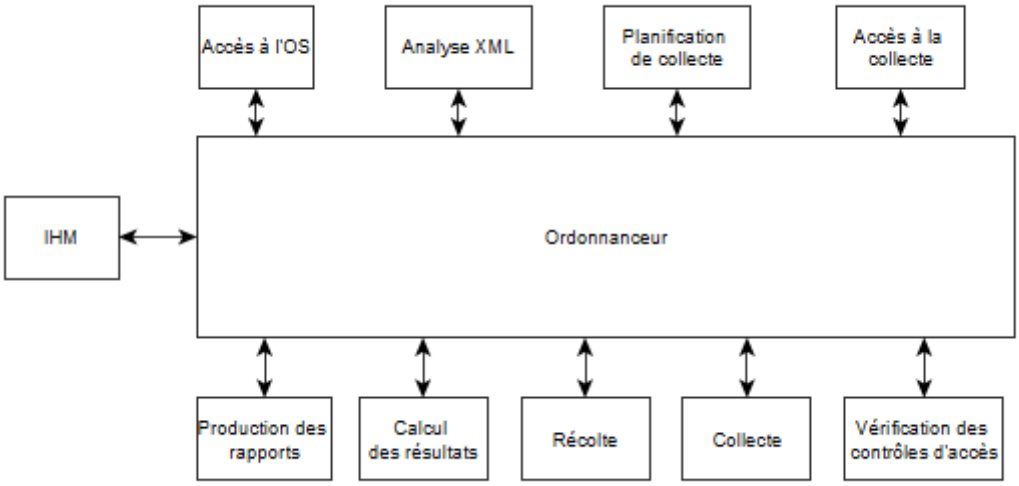

Figure 2 – Architecture TSACP

TSCAP est conçu à la manière d'une application micro-services. L'ordonnanceur joue le rôle de contrôleur de micro-services, et communique avec les composants via un composant de communication. Chacun des composants est exécuté selon le principe de moindres privilèges.

TSCAP prend en entrée une commande utilisateur, qui référence une entrée SCAP et permet de donner des directives sur le workflow à suivre. En sortie, TSCAP fournit un état du système au format XML (OVAL system characteristics, OVAL results, XCCDF results ou ARF selon le cas d'utilisation) ou HTML. Le rapport produit permet à l'auditeur d'identifier les failles (vulnérabilité, non-respect de la PSSI, logiciel malveillant) sur le système.

3.3.2. Workflow du produit

L'entrée SCAP est passée à l'ordonnanceur par l'IHM, qui déclenche le workflow suivant :

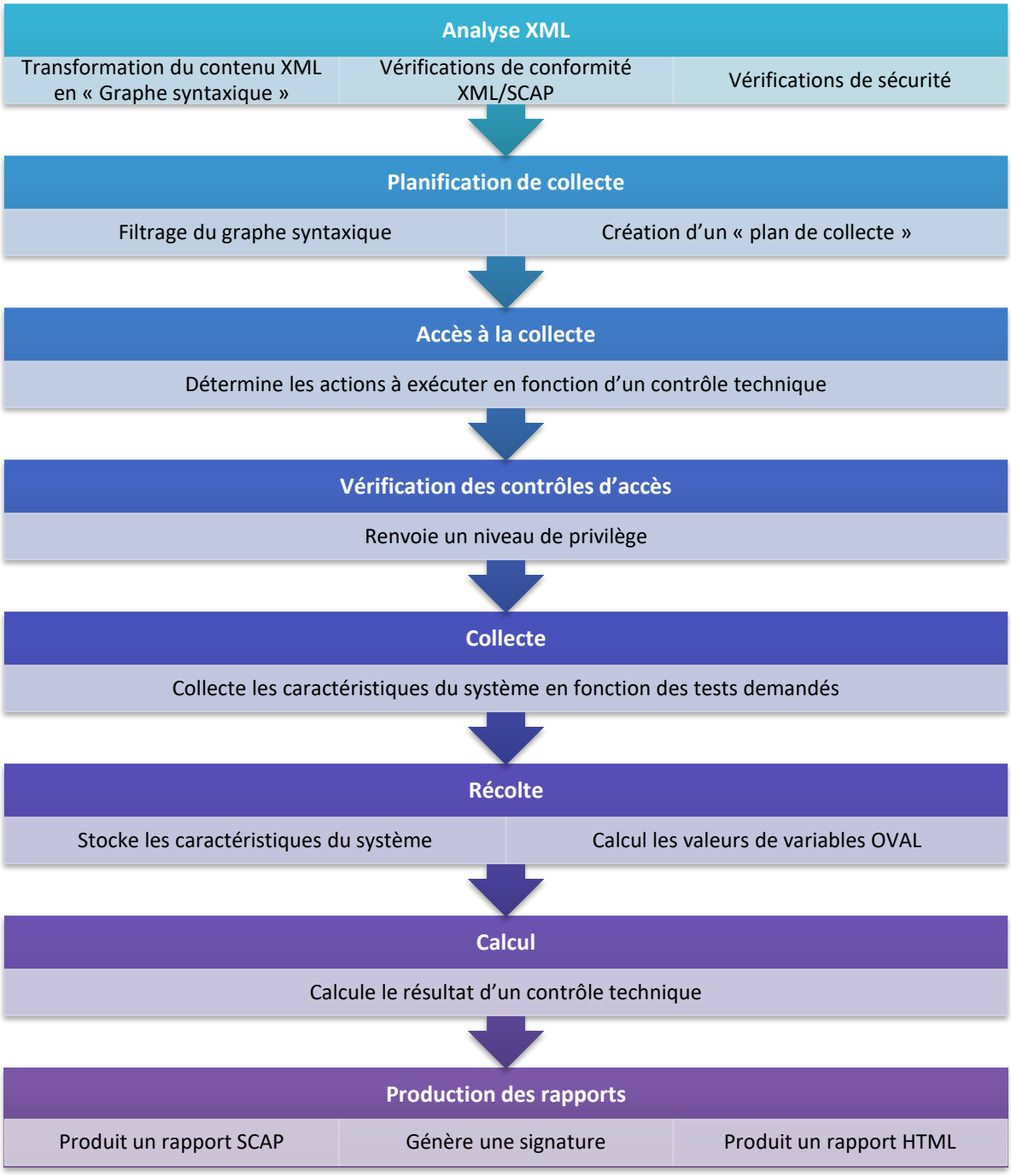

Figure 3 - Workflow Ordonnanceur TSCAP

3.4. Description de l'environnement prévu pour son utilisation

TSCAP a vocation à fonctionner sur les versions de Windows suivantes :

- Windows 10 1809 64 bits x86 ;
- Windows 8.1 32 bits x86 ;
- Windows server 2016 64 bits x86;
- Windows server 2012 R2 64 bits x86.

Afin de pouvoir faire fonctionner l'ensemble des fonctionnalités de TSCAP, le système d'exploitation doit remplir les conditions suivantes :

- WinRM doit être configuré afin de pouvoir communiquer avec une machine distante ;
- La machine de l'auditeur doit avoir accès à l'annuaire LDAP ou AD auquel la machine auditée est connectée, dans le cas de contrôles techniques le nécessitant.
- TSCAP nécessite d'être lancée depuis un compte privilégié (administrateur du système local) et depuis une fenêtre PowerShell exécutée en tant qu'Administrateur afin de pouvoir s'exécuter dans des conditions nominales.

3.5. Description des dépendances

TSCAP est programmé en C++ et RUST.

Outre l'ensemble des dépendances nécessaires à la compilation, TSCAP a besoin d'un environnement Windows avec PowerShell dans les versions installées par défaut sur les versions compatibles de Windows pour s'exécuter dans des conditions nominales.

La liste des CVE des produits utilisés ainsi que leurs applicabilités à TSCAP est dans le document [REF1] de la cible de sécurité.

3.6. Description du périmètre de l'évaluation

TSCAP peut permettre d'auditer un poste local ou des postes distants.

La TOE est évaluée en tant qu'auditeur d'un poste distant.

TSCAP est prévu pour fonctionner dans un cadre de démonstration sur une plateforme où est installé un ensemble d'autorités de certifications. Ces autorités de certification sont aussi fixées dans TSCAP à la compilation pour éviter une utilisation en dehors du cadre de démonstration. Aussi, dans le cadre de l'évaluation, l'autorité de certification du NIST est fournie, ainsi qu'une autorité DISCO, permettant de vérifier la validité des contenus SCAP issus du NIST ou des rapports générés avec le certificat fourni sur la plateforme d'évaluation.

4. Environnement technique de fonctionnement du produit

L'environnement technique retenu pour l'évaluation est un ensemble de deux postes de travail chacun disposant d'un OS Windows 10 x86 64 bits durci selon le guide de durcissement du CIS. Les règles de durcissement du CIS sont cependant assouplies pour permettre la communication WinRM entre les deux machines physiques. Ces postes de travail sont fournis par le commanditaire de l'évaluation à l'évaluateur.

Afin de respecter les conditions de l'utilisation prévue, le produit est à évaluer dans ses fonctions de sécurité dans le cadre d'audits sur un poste de travail distant, soit entre les deux machines physiques.

5. Mesures d'environnement

5.1. Description des hypothèses sur l'environnement

H.1 : L'auditeur est de confiance et suit l'ensemble des directives données dans le manuel utilisateur.

H.2 : Le poste auditeur est sain, durci selon les bonnes pratiques et préconfiguré pour permettre une communication distante via WinRM (voir documentation Microsoft).

H.3 : Le poste audité est sain dans le sens où aucun malware ne modifie le comportement nominal des commandes système. Egalement, le poste audité est préconfiguré pour permettre une communication distante avec le poste auditeur (voir documentation Microsoft).

H.4 : Les fonctions de vérification et production de signature XML offertes par l'API Windows sont supposées de confiance. Egalement, l'implémentation TLS fournie par le système Windows est supposée de confiance.

6. Biens sensibles de la TOE

6.1. Biens essentiels informationnels

		Confidentialité	Intégrité	Disponibilité	Authentification
BS.1	Données de collecte	X	X		X
BS.2	Rapports		X		X
BS.3	Machine auditée		X		
BS.4	Machine auditeur		X		

Tableau 5 – Biens Sensibles

BS.2 - La clé auditeur permet de signer les rapports et ainsi garantir leur intégrité dans le temps.

6.2. Biens cryptographiques

		Confidentialité	Intégrité	Disponibilité	Authentification
BSC.1	Secret du compte privilégié du système audité	X	X		
BSC.2	Secret du compte non privilégié du système audité	X	X		
BSC.3	Clé Auditeur permettant de signer les rapports		X		X

Tableau 6 – Biens Sensibles - Cryptographiques

7. Description des menaces

7.1. Agents menaçants

AM.1 : Producteur de contenu SCAP.

AM.2 : Utilisateur de la machine audité.

AM.3 : Attaquant sur le réseau en position d'interception.

AM.4 : Attaquant en capacité de fournir un rapport malveillant à l'auditeur.

7.2. Menaces

M.1 : Un attaquant porte atteinte à l'intégrité et la confidentialité des données de collecte

Scénarios de menace envisagé : une escalade de privilèges de l'utilisateur (ou toute autre personne ayant un accès non privilégié à la machine auditée) de la machine auditée sur son système pour récupérer des traces laissées par TSCAP.

M.2 : Un attaquant modifie le rapport

Scénarios de menace envisagé : Modification du rapport tout au long de son cycle de vie (création à suppression) par un utilisateur autre que l'auditeur.

M.3 : Un attaquant porte atteinte à l'intégrité du système auditée

Scénarios de menace envisagé :

- Un producteur de contenu SCAP pourrait chercher à produire une entrée SCAP contenant des injections de code arbitraire, l'entrée SCAP interprétée pourrait alors permettre par exemple la fuite d'information, réaliser des dénis de service, etc.
- Un attaquant positionné sur le réseau modifie les commandes envoyées par TSCAP pour porter atteinte à l'intégrité des systèmes audités.

M.4 : Un attaquant porte atteinte à l'intégrité du système auditeur

Scénarios de menace envisagé :

- Un producteur de contenu SCAP pourrait chercher à produire une entrée SCAP contenant des injections de code arbitraire, l'entrée SCAP interprétée pourrait alors permettre par exemple la fuite d'information, réaliser des dénis de service, etc.

- Un attaquant positionné sur le réseau modifie les données collectées par TSCAP pour porter atteinte à l'intégrité du système auditeur.

	M.1 Atteinte à l'intégrité des données de collecte	M.2 Modification du rapport	M.3 Atteinte à l'intégrité du système audité	M.4 Atteinte à l'intégrité du système auditeur
BS.1 Données de collecte	X	X		
BS.2 Rapport	X	X		
BS.3 Machine auditée			X	X
BS.4 Machine auditeur				X

Tableau 7 – Menace sur les biens supports

8. Spécification des fonctions dédiées à la sécurité

8.1. Fonctions de sécurité

FS.1 : Chiffrement des communications réseau

TSCAP nécessite de communiquer au travers du réseau entre le poste auditeur et le poste audité. En effet, le poste auditeur envoie des commandes vers le poste audité.

Pour cela, il est nécessaire de protéger les communications réseau entre le poste auditeur et le poste audité.

Afin de respecter le principe de moindre privilèges, l'auditeur doit exécuter les commandes sur le poste audité avec le moins de privilèges requis possible. Pour cela, il dispose aussi d'un accès sur le système audité avec un compte non privilégié. Cet accès est effectué selon les mêmes modalité que pour le compte privilégié.

FS.2 : Signature du rapport produit par TSCAP avec la clé auditeur

TSCAP permet de signer les rapports produits, afin d'en assurer l'intégrité et l'authentification. Ces rapports sont signés à l'aide de la clé de l'auditeur, récupérée dans son certificat, passé en paramètre de TSCAP avec le paramètre --userkey.

Une vérification est effectuée sur la clé de l'auditeur afin de s'assurer que cette clé est conforme.

Ensuite, une signature est générée pour l'ensemble du document. Cette signature est au format tel que décrit dans la norme TMSAD en version 1.0.

Les suites de chiffrement autorisées sont celles indiquées dans le document référentiel SCAP. Il est à noter que la norme TMSAD autorise le hashage du contenu signé via SHA-1, mais que TSCAP refuse cet algorithme pour la signature.

FS.3 : Vérification de la signature du contenu SCAP passé en entrée

TSCAP permet de vérifier les signatures présentes dans un rapport passé en entrée, afin d'en assurer l'intégrité et l'authentification. Ces rapports sont signés selon les spécifications de la norme TMSAD en version 1.0.

Les suites de chiffrement autorisées sont celles indiquées dans le document référentiel SCAP. Il est à noter que la norme TMSAD autorise le hashage du contenu signé via SHA-1, mais que TSCAP refuse cet algorithme pour la signature.

FS.4 : Composant d'analyse XML

Les entrées utilisateur correspondent aux contenus des documents XML fournis en entrée à TSCAP, aussi appelés « entrées SCAP », aux divers champs de la GUI et aux paramètres de la ligne de commande, aussi appelés « instructions d'audit ».

Pour chaque entrée utilisateur, le composant approprié effectue d'abord une vérification par liste blanche, puis une vérification par liste noire. Ces vérifications permettent notamment de se protéger

contre les vulnérabilités liées aux injections susceptibles de se trouver dans un contenu SCAP produit par un potentiel attaquant.

Après que les entrées utilisateurs soient passées par les composants de validation des entrées, elles sont utilisées en paramètre des fonctions sécurisées dans la suite du code pour construire les appels aux interpréteurs visés (le système par exemple).

8.2. Concordances fonctions de sécurité, hypothèses et menaces

Fonctions de sécurité et hypothèses	M.1 Atteinte à l'intégrité des données de collecte	M.2 Modification du rapport	M.3 Atteinte à l'intégrité du système audité	M.4 Atteinte à l'intégrité du système auditeur
FS.1 : Chiffrement des communications réseau	X		X	X
FS.2 : Signature du rapport produit par TSCAP avec la clé auditeur		X		
FS.3 : Vérification de la signature du contenu SCAP passé en entrée			X	X
FS.4 : Composant d'analyse XML			X	X
H.1 : L'auditeur est de confiance		X		
H.2 : Le poste auditeur est sain	X			
H.3 : Le poste audité est sain	X			
H.4 : Les APIs Windows de signature sont de confiance		X		

Tableau 8 – Concordances fonctions de sécurité, hypothèses et menaces