Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Bureau Qualifications et Agréments

Paris, le 03 AVR. 2019
N°1435 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU ELEMENTAIRE

SYSTEME DE DETECTION CYBELS SENSOR
composé de :
SONDE DE DETECTION 1.8.X,
CENTRE DE GESTION VERSION 1.8.X,
CENTRE D'EXPLOITATION VERSION 1.8.X

THALES SIX GTS FRANCE

RCS 383 470 937

4, avenue de Louvresses
92 622 Gennevilliers Cedex

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit.

Fiche 2 : Conditions et limites de la qualification.

Fiche 3 : Base documentaire de la qualification.

Le Premier ministre,

Vu le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », notamment son article 1er ;

Vu le décret du 27 mars 2014 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Vu la décision du 22 octobre 2014 portant délégation de signature (secrétariat général de la défense et de la sécurité nationale) ;

Vu le processus de qualification d'un produit, référence QUAL-PROD-PROCESS, version en vigueur ;

Vu le dossier de demande de qualification déposé par THALES SIX GTS France le 4 octobre 2017 ;

Vu le rapport technique d'évaluation du 14 décembre 2018 ;

Vu le rapport d'évaluation métier du 28 février 2019 ;

Vu le rapport des tests d'intrusion du 30 novembre 2018,

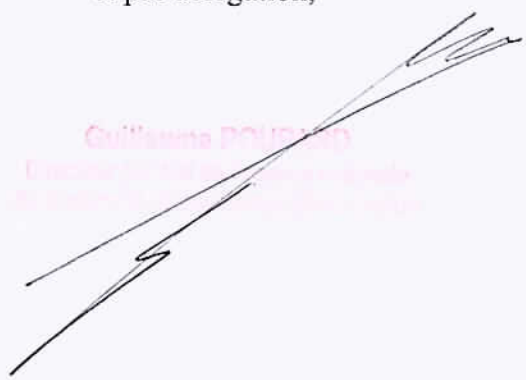
Décide :

Art. 1 – Le système de détection des évènements susceptibles d'affecter la sécurité des systèmes d'information portant le nom CYBELS SENSOR, et constitué des composants sonde de détection en version 1.8.X, du centre de gestion version 1.8.X, du centre d'exploitation version 1.8.X, ci-après désigné « le système de détection », fourni par la société *THALES SIX GTS FRANCE*, ci-après désignée « le fournisseur », respecte les règles fixées par le décret n° 2015-350 du 27 mars 2015 et est qualifié au niveau élémentaire, sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.

Art. 2 – La présente décision est conditionnée au respect des engagements relatifs au processus de qualification d'un produit pris par le fournisseur au titre de sa demande de qualification.

Art. 3 – La présente décision est valable pour trois ans.

Pour le Premier ministre,
et par délégation,



Fiche 1

Description du produit

Désignation et versions

Le système de détection CYBELS SENSOR qualifié est constitué des composants suivants, développés par *THALES SIX GTS FRANCE* : sonde de détection version 1.8.X, centre de gestion version 1.8.X, centre d'exploitation version 1.8.X.

La version qualifiée des composants est la version 1.8.X, pour X supérieur ou égal à 1.

Le système de détection CYBELS SENSOR est qualifié dans ses modèles 100Mb/s, 1Gb/s, 2Gb/s, 4Gb/s, 6Gb/s et 10Gb/s.

Composants du système

Le système de détection CYBELS SENSOR est composé de :

- la sonde de détection, ci-après désignée « la sonde » permettant l'analyse de flux, l'analyse de fichiers et la remontée d'alerte en cas de détection d'évènements susceptibles d'affecter la sécurité des systèmes d'information ;
- le centre de gestion permettant notamment l'administration des sondes et la consultation des journaux de fonctionnement des sondes ;
- le centre d'exploitation permettant aux analystes de qualifier les évènements de sécurité sur la base des alertes et métadonnées générées par la sonde.

Présentation générale

Le système de détection CYBELS SENSOR est destiné à détecter des activités suspectes ou malveillantes sur un système d'information en analysant les flux réseaux, les fichiers extraits des flux et en générant des alertes le cas échéant. La sonde intègre des signatures qui sont mises en œuvre par un moteur d'analyse de flux et un moteur d'analyse de fichiers.

La sonde offre des fonctions de sécurité et de détection conformes à celles décrites dans la cible de sécurité de la sonde [CDS], elle-même conforme à la cible de sécurité générique élaborée par l'ANSSI [CIBLE_GENERIQUE].

Les fonctionnalités de la sonde lui permettent d'être opérée par un prestataire conforme au référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité [PDIS].

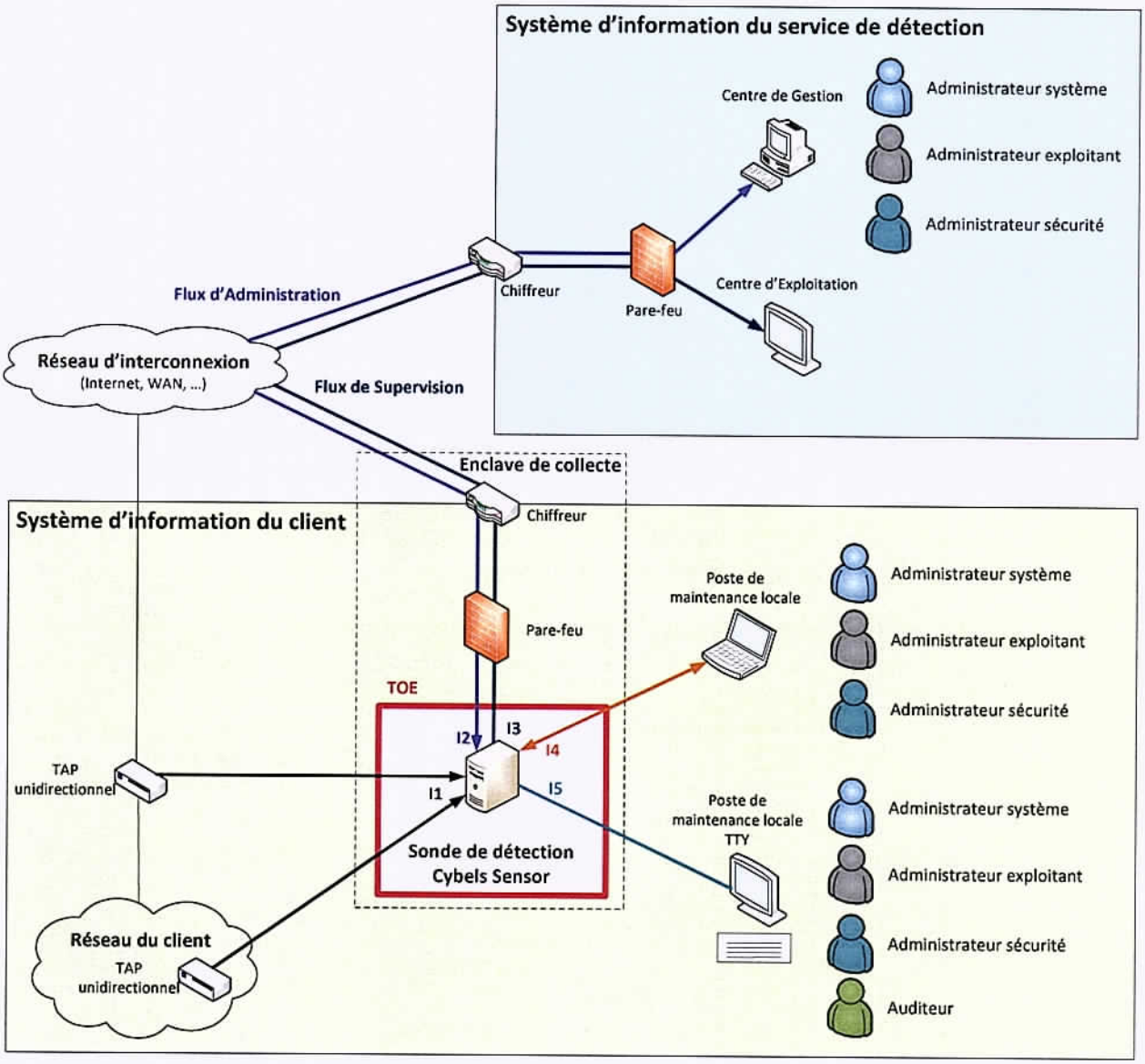


Figure : Environnement d'utilisation du produit

Fiche 2

Conditions et limites de la qualification

Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

Lors de la mise en œuvre du système de détection, l'autorité d'emploi doit s'assurer que :

C1 La sonde est placée en dérivation des flux à analyser et non en coupure.

C2 La dérivation vers la sonde des flux à analyser est réalisée par un TAP qualifié par l'ANSSI au niveau élémentaire.

C3 La sonde est placée au plus près du point de dérivation. Seul un agrégateur de flux respectant les exigences définies dans l'annexe 5 du référentiel [PDIS] peut être déployé entre le TAP et la sonde.

C4 Le réseau sur lequel le système de détection est déployé est en adéquation avec les capacités fonctionnelles du modèle choisi (débit des flux à analyser, capacité de stockage, etc.) et prend en compte la limite L2 (nature des flux à analyser) identifiée ci-dessous.

C5 Les utilisateurs du système de détection sont, selon leur rôle, formés aux composants du système de détection et la documentation de ces composants leur est mise à disposition.

C6 La sonde dispose d'une base de règles de détection à jour conformément au chapitre intitulé « Gestion des incidents » du référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité [PDIS].

C7 La sonde est déployée selon les lois et réglementations en vigueur, notamment vis-à-vis des types d'informations pouvant être contenus dans les flux à analyser (données à caractère personnel, etc.).

C8 Le système d'information du service de détection opérant le système de détection respecte les exigences établies dans le référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité [PDIS].

C9 La sonde est déployée dans une enclave de collecte respectant les exigences établies dans le chapitre intitulé « Enclave de collecte au sein du système d'information du commanditaire » du référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité [PDIS].

C10 Les fonctions d'administration à distance offertes nativement par certains matériels constituant la sonde sont désactivées par défaut, dans la version livrée. Elles ne doivent en aucun cas être réactivées par l'administrateur système de la sonde.

C11 Les composants du système de détection sont hébergés dans des locaux sécurisés dont l'accès est contrôlé et restreint à du personnel de confiance.

C12 Lorsqu'un prestataire de détection supervise les systèmes d'information de plusieurs clients, il met en œuvre un centre de gestion et un centre d'exploitation par client.

Limites

La décision de qualification est valide sous réserve du respect des restrictions énoncées ci-après.

L1. Seules les fonctions de sécurité et de détection identifiées dans la fiche 1 sont couvertes par la présente décision de qualification.

L2. La présente décision de qualification ne couvre pas le décodage et l'analyse des protocoles de type industriel par le système de détection.

L3. Les travaux d'évaluation de l'efficacité et des performances du système en matière de détection ont été réalisés sur le modèle 10Gb/s.

Fiche 3

Base documentaire de la qualification

Cadre réglementaire

[QUAL-PROD-PROCESS]	Processus de qualification d'un produit, version 1.0 du 6 janvier 2017. Disponible sur https://www.ssi.gouv.fr/qualification-processus
[DECRET_QUALIF]	Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. Disponible sur https://www.legifrance.gouv.fr

Documents rédigés par le centre d'évaluation

[RTE]	Rapport technique d'évaluation, Amossys, version 1.14 du 14 décembre 2018.
[REM]	Rapport d'évaluation métier, Amossys, version 1.04 du 8 mars 2019.
[PENTEST]	Tests d'intrusion de l'interface d'administration de la sonde Cybels Sensor, Amossys, version 2.0 du 30 novembre 2018.

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[PDIS]	Prestataires de détection des incidents de sécurité, référentiel d'exigences, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[CIBLE_GENERIQUE]	Sonde réseau de détection des incidents de sécurité – Cible générique. Disponible sur https://www.ssi.gouv.fr

Guides d'utilisation et documentations techniques de l'industriel

[CDS]	Cible de sécurité de Cybels Sensor v.1.8, référence : 63094102-306, version D du 21 juin 2018
[MANUELS]	"Manuel utilisateur logiciel Sonde", référence 63217494-593 "Manuel d'installation de la Sonde", référence 63251906-591

	Centre de Gestion et Centre d'Exploitation : "Manuel utilisateur de l'IHM", référence 63312122-108 Centre de Gestion : "Manuel utilisateur logiciel Centre de Gestion", référence 63308192-593 Centre de Gestion : "Manuel d'installation du Centre de Gestion", référence 63308193-591 Centre d'Exploitation : "Manuel utilisateur logiciel Centre d'Exploitation", référence 63308195-593 Centre d'Exploitation : "Manuel d'installation du Centre d'Exploitation", référence 63308194-591