PREMIÈRE MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2023/07

CYBELS Sensor

Version 2.0.5

Paris, le 21 Juillet 2023

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification	**ANSSI-CSPN-2023/07**
Nom du produit	**CYBELS Sensor**
Référence/version du produit	**Version 2.0.5**
Catégorie de produit	**Détection d'intrusions**
Critère d'évaluation et version	**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire	**THALES SIX GTS France** 4 avenue des Louvresses 92622 Gennevilliers Cedex, France
Développeur	**THALES SIX GTS France** 4 avenue des Louvresses 92622 Gennevilliers Cedex, France
Centre d'évaluation	**AMOSSYS** 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées	Chiffrement du système de fichiers Identification, authentification et contrôle d'accès Mise à jour des logiciels Mise à jour de règles de détection Journalisation du fonctionnement Protection des flux Cloisonnement Remontée des journaux de fonctionnement
Fonctions de sécurité non évaluées	Sans objet
Restriction(s) d'usage	Non

PREFACE

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « CYBELS Sensor, Version 2.0.5 » développé par THALES SIX GTS France.

Ce produit est une sonde de détection des incidents de sécurité, conçue pour analyser le trafic de la couche 2 à la couche 7 du modèle OSI et y repérer des activités suspectes ou malveillantes, sur la base de signatures. Ces signatures sont exploitées par le moteur de détection d'intrusion ainsi que par le moteur d'analyse statique de fichiers du produit, afin de générer des évènements de sécurité.

Sur la base des flux analysés, la sonde de détection CYBELS Sensor génère des alertes (correspondant à des évènements de sécurité), des métadonnées relatives au trafic surveillé, des fichiers extraits du trafic surveillé et des journaux de fonctionnement.

La sonde de détection CYBELS Sensor s'intègre dans le système de détection CYBELS Sensor, qui permet une surveillance globale de la sécurité et intègre les composants suivants :

- la sonde de détection CYBELS Sensor elle-même, assurant le rôle de source de collecte d'évènements dans le cadre d'un déploiement PDIS[1] et déployée au sein d'une enclave de collecte ;
- le Centre de Gestion (CG), assurant les fonctions d'administration distante des sondes et de consultation des journaux d'évènements ;
- le Centre d'Exploitation (CE), permettant aux analystes de qualifier les évènements de sécurité sur la base des alertes et métadonnées générées par la sonde.

La figure ci-dessous explicite l'architecture globale du système de détection CYBELS Sensor.

[1] Prestataires de Détection d'Incidents de Sécurité.

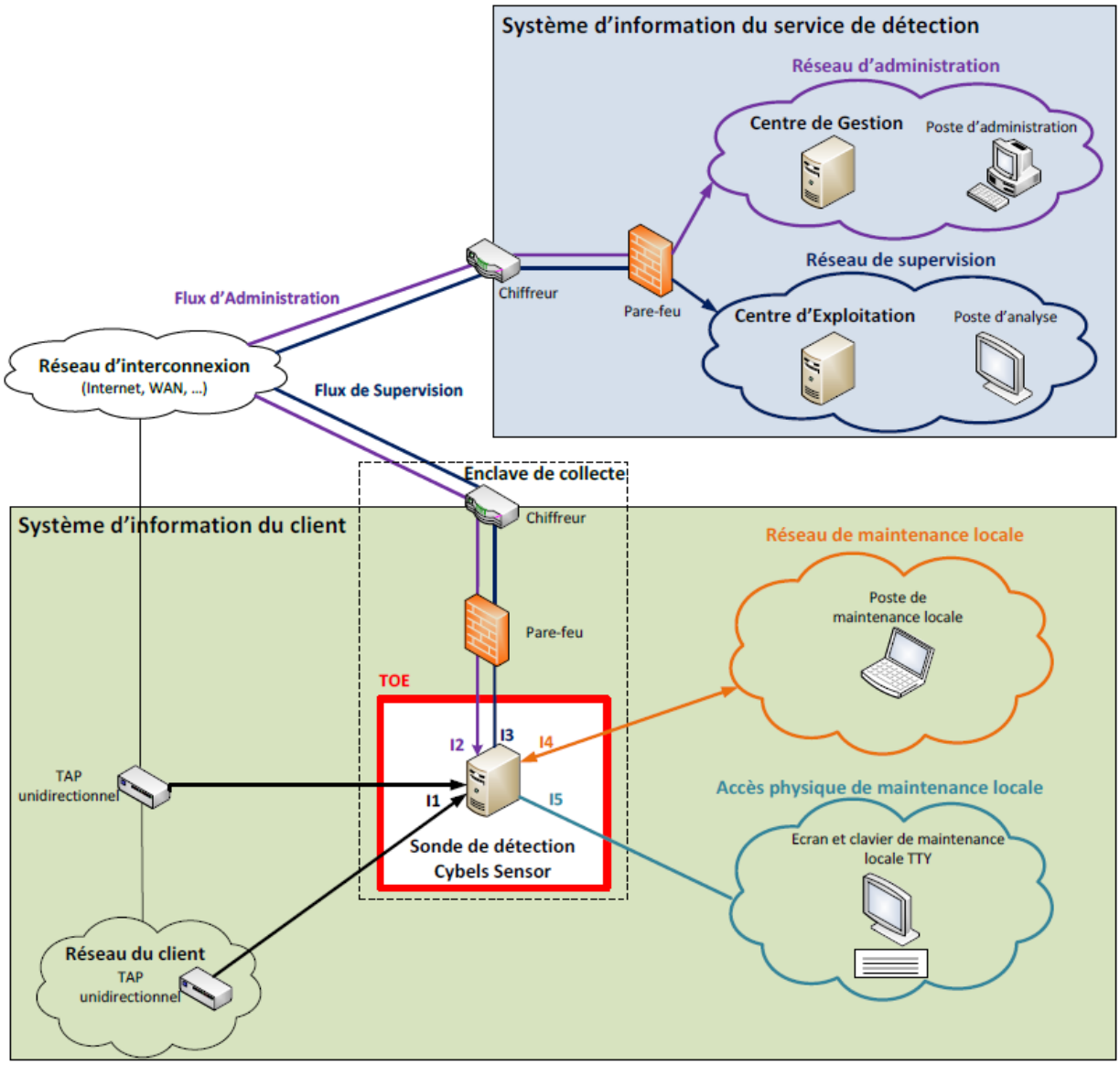


Figure 1 – Architecture globale du système de détection CYBELS Sensor.

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 *Catégorie du produit*

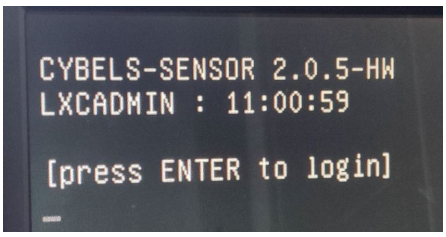
☒	**1**	**détection d'intrusions**
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☐	6	identification, authentification et contrôle d'accès
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	CYBELS Sensor
Numéro de la version évaluée	Version 2.0.5

La version certifiée du produit peut être identifiée de la manière suivante :

- via le prompt d'authentification à la console (TTY) :



- via la commande suivante, lancée via une connexion à distance sur l'interface de maintenance (ethML) ou l'interface de gestion (via le centre de gestion) :

```
CybelsSENSOR|administrateur:adminsys>$ get_version.sh
CYBELS-SENSOR version: 2.0.5-HW
```

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- le chiffrement du système de fichiers ;
- l'identification, l'authentification et le contrôle d'accès ;
- la mise à jour des logiciels ;
- la mise à jour de règles de détection ;
- la journalisation du fonctionnement ;
- la protection des flux ;
- le cloisonnement ;
- la remontée des journaux de fonctionnement.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond au logiciel de la sonde CYBELS Sensor et ses interfaces.

La plateforme d'évaluation est constituée des éléments suivants :

- la sonde de production ;
- un ordinateur portable servant à la fois de Centre de Gestion (CG) et de Centre d'Exploitation (CE) ;
- une machine virtuelle Kali Linux ;
- une seconde sonde en mode *debug* (avec accès root au socle).

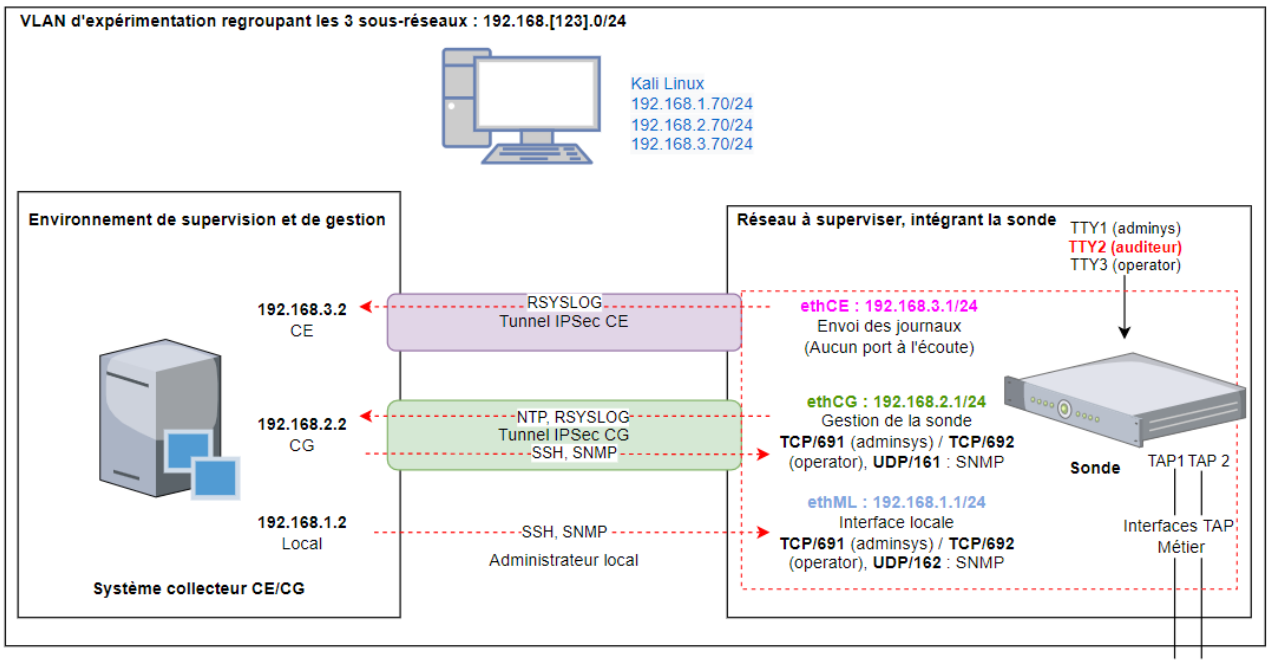


Figure 2 – Plateforme d'évaluation.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-05].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

L'installation du produit évalué se déroule en trois étapes principales :

- mise à jour de la plateforme (serveur Dell, BIOS et TOE) ;
- configuration de la TOE ;
- contrôle du fonctionnement de la TOE.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source :

- des scripts permettant d'organiser et de contrôler les actions utilisateur ;
- des scripts opérationnels CYBELS liés aux opérations d'administration et configuration du produit ;
- de l'implémentation des mécanismes cryptographiques du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur familier.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « CYBELS Sensor, Version 2.0.5 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - CYBELS SENSOR - Sonde de détection des incidents de sécurité – Cible de sécurité, référence SYS_CSPN-63094102-306_CDS-2.0.5_O_REV-K, version -K, 12 juin 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - CYBELS SENSOR - Sonde de détection des incidents de sécurité – Cible de sécurité, référence SYS_CSPN-69346741-306_CDS-2.0.5-cspn-_O_REV-K, 29 juin 2023.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN – Produit CYBELS Sensor – version 2.0.5, référence CSPN-RTE-TARAMA-DR-1.02, version 1.02, 4 juillet 2023.
[ANA_CRY]	Rapport technique d'évaluation des mécanismes cryptographiques : - Expertise des mécanismes cryptographiques - Produit CYBELS Sensor – version 2.0.5, CSPN-CRY-TARAMA-DR-1.01, version 1.01, 16 juin 2023.
[GUIDES]	Guides d'utilisation du produit : - Guide d'utilisateur : SYS_63094601BA-591_User-Manual-2.0.5_O_REV-F - Complément au guide d'utilisateur : SYS_63094601BA-179_User-Manual-Additionnal-Content-2.0.5_O_REV-C

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 4.0, 3 mars 2022. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[NOTE-05]	Note d'application - Méthodologie pour l'évaluation des sondes réseau sur base Linux de détection d'intrusion en vue d'une certification de sécurité de premier niveau pour une qualification selon le décret 2015/350, référence ANSSI-CSPN-NOTE-05, version 2.0, 28 juin 2020.