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-2023/20

Stormshield Endpoint Security Evolution

Version 2.4.3

Paris, le 13 Novembre 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-2023/20**
Nom du produit **Stormshield Endpoint Security Evolution**
Référence/version du produit **Version 2.4.3**
Catégorie de produit **Détection d'intrusions**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **STORMSHIELD** 1 place Verrazzano 69009 Lyon, France
Développeur **STORMSHIELD** 1 place Verrazzano 69009 Lyon, France
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées Protection des journaux Protection du logiciel Protection de la configuration Téléchargement de la configuration Transmission des journaux
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 « Stormshield Endpoint Security Evolution, Version 2.4.3 » développé par STORMSHIELD.

C'est une suite logicielle offrant une solution de sécurisation des postes de travail et des serveurs sous Windows : elle permet à une organisation de protéger de manière centralisée l'intégralité de son parc de serveurs, micro-ordinateurs et ordinateurs portables contre les attaques informatiques connues et inconnues, le vol ou la perte de données, les intrusions informatiques et les opérations non autorisées.

L'administrateur configure la politique de sécurité d'un ensemble protégé d'équipements via un système d'administration centralisée, et les changements sont déployés et appliqués automatiquement sur tous les postes de travail via un agent sur le poste de travail qui communique de manière sécurisée avec le système d'administration centralisée.

Le présent certificat porte sur cet agent déployé sur le poste de travail, qui télécharge et applique la politique de sécurité sur le poste, et génère des journaux et alertes qu'il remonte au gestionnaire d'agents situé sur le système d'administration centralisée.

La figure ci-dessous explicite l'architecture du produit.

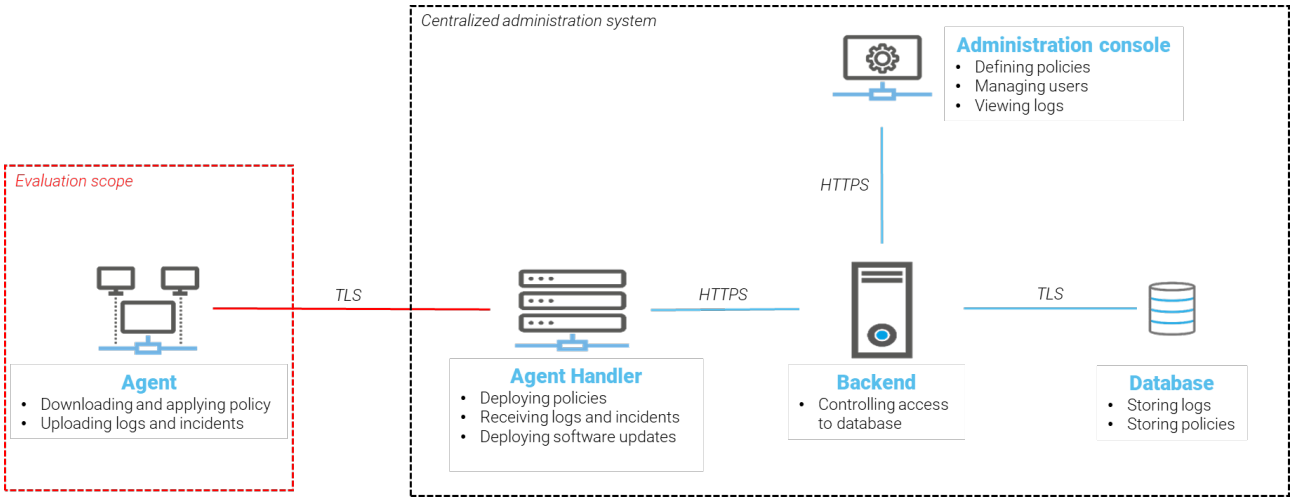

Figure 1 - Architecture Produit.

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	Stormshield Endpoint Security Evolution
Numéro de la version évaluée	Version 2.4.3

La version certifiée du produit peut être identifiée sur l'onglet d'accueil de l'interface graphique du de l'agent :

Figure 2 – Identification de la version certifiée du produit.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la protection des journaux ;
- la protection du logiciel ;
- la protection de la configuration ;
- le téléchargement de la configuration ;
- la transmission des journaux.

1.2.4 *Configuration évaluée*

La configuration évaluée est celle décrite dans [CDS] et correspond à une plateforme d'évaluation constituée des équipements suivants :

- un serveur sous Windows *Server* 2019 hébergeant le centre d'administration centralisée (comprenant lui-même le gestionnaire d'agents, la console d'administration, une base de données et le serveur dorsal) ;
- un poste de travail sous Windows 10 hébergeant l'agent (le produit évalué).

La figure ci-dessous explicite la plateforme de test.

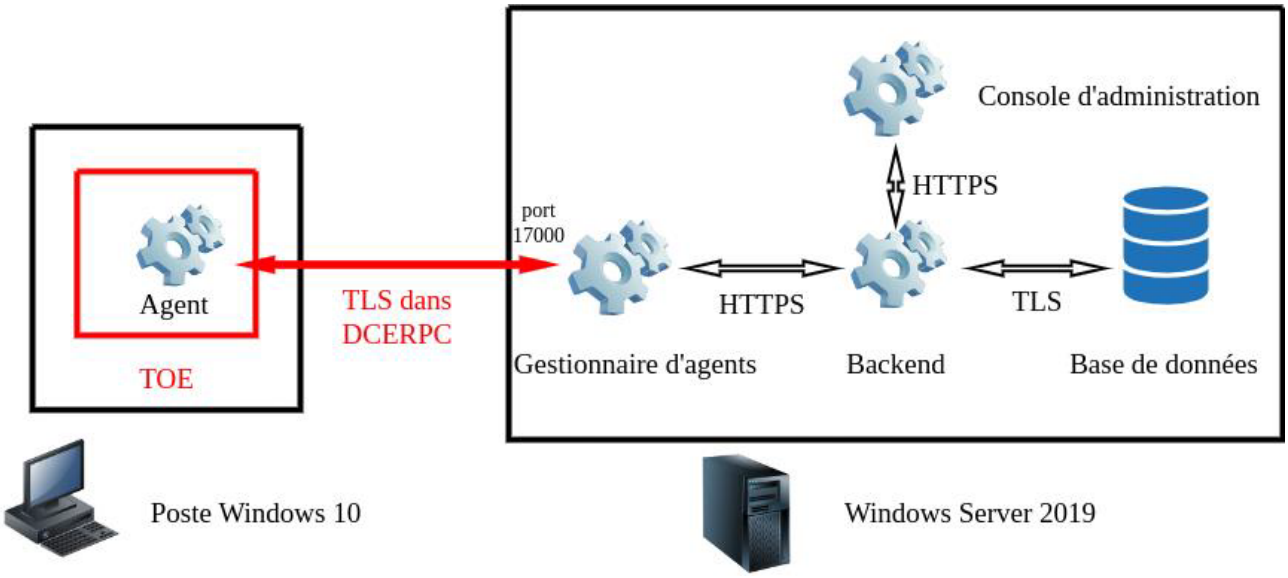

Figure 3 – Plateforme de test.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

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.

Le guide d'installation (voir [GUIDES]) mentionne deux possibilités pour l'installation des composants hors cible d'évaluation : l'installation standard ou bien l'installation de démonstration. C'est cette deuxième option qui a été retenue pour l'évaluation.

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

Le produit évalué et les composants hors cible d'évaluation ont été installés et configurés en suivant les documents [GUIDES].

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)*

Le code source n'a pas fait l'objet d'une revue dans le cadre de cette l'évaluation.

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

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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.

Le produit en lui-même n'offre que très peu d'interactions, toute la configuration est effectuée sur le serveur grâce à la console. Aussi, hors circonstances exceptionnelles, le produit ne requiert pas d'actions de la part de l'utilisateur.

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 [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit ne comporte pas de générateur d'aléa entrant dans le périmètre d'évaluation.

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 « Stormshield Endpoint Security Evolution, Version 2.4.3 » 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 : - *Stormshield Endpoint Security Evolution – CSPN Security Target*, référence KILEMA/ST, version 1.4, 2 octobre 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Stormshield Endpoint Security Evolution – CSPN Security Target*, référence KILEMA/ST, version 1.4, 2 octobre 2023.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN – Produit *Stormshield Endpoint Security Evolution* - version 2.4.3, référence CSPN-RTE-KILEMA-2.02, version 2.02, 9 octobre 2023.
[GUIDES]	Guides d'installation et d'administration du produit[1] : - *Stormshield Endpoint Security Evolution* – Guide d'installation, référence ses-fr-guide_d_installation-v2.3.1, version 2.3, 8 septembre 2022 ; - *Stormshield Endpoint Security Evolution* – Guide d'administration, référence ses-fr-guide_d_administration-v2.4.3, version 2.4.3, 22 juin 2023 ; - *Stormshield Endpoint Security Evolution* – Préconisations SQL Server, référence ses-fr-préconisations_sql_server-v2.3.1, version 2.3, 8 septembre 2022.

[1] Tous les guides du produit sont disponibles publiquement à l'adresse : https://documentation.stormshield.eu/SES/v2/fr/Content/Home.htm.

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.