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-2023/10

Panorama E2

Version 2022 SP1

Paris, le 29 Septembre 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-2023/10**
Nom du produit **Panorama E2**
Référence/version du produit **Version 2022 SP1**
Catégorie de produit **Autre : SCADA**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Codra Ingénierie Informatique** Immeuble Hélios, 2 rue Christophe Colomb, CS 0851 91300 Massy, France
Développeur **Codra Ingénierie Informatique** Immeuble Hélios, 2 rue Christophe Colomb, CS 0851 91300 Massy, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Gestion des entrées malformées Communications sécurisées Non divulgation des secrets de connexion des utilisateurs gérés par l'*Active Directory* Intégrité des certificats des utilisateurs des interfaces externes OPC-UA Intégrité des certificats des Serveurs de données OPC-UA Accès aux bases de données par Sécurité Intégrée Authentification sécurisée Politique de droits Signature du logiciel Intégrité et confidentialité de la configuration Intégrité 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 « Panorama E2, Version 2022 SP1 » développé par Codra Ingénierie Informatique.

Ce produit est un système SCADA de contrôle et d'acquisition de données, conçu pour être utilisé au sein de réseaux industriels et incluant les deux composants suivants :

- un serveur SCADA, interconnecté avec des équipements de terrain de niveau 1 au sens de la classification CIM (*Computer-Integrated Manufacturing*) et permettant l'acquisition de données terrain et l'envoi de commandes, ainsi que la gestion des alarmes ;
- un client SCADA, permettant notamment de présenter une interface homme-machine (IHM) à l'utilisateur.

Panorama E2 peut également s'interfacer avec d'autres équipements et logiciels tiers de niveaux CIM 2 et 3, en particulier via un serveur OPC-UA avec liaison de type HTTPS.

Panorama E2 est un des éléments de la solution *Panorama Suite*, qui comprend aussi *Panorama COM* (Frontal d'acquisition) et *Panorama Historian*.

La figure ci-dessous explicite l'architecture de déploiement du produit. La cible d'évaluation correspond à la partie grisée.

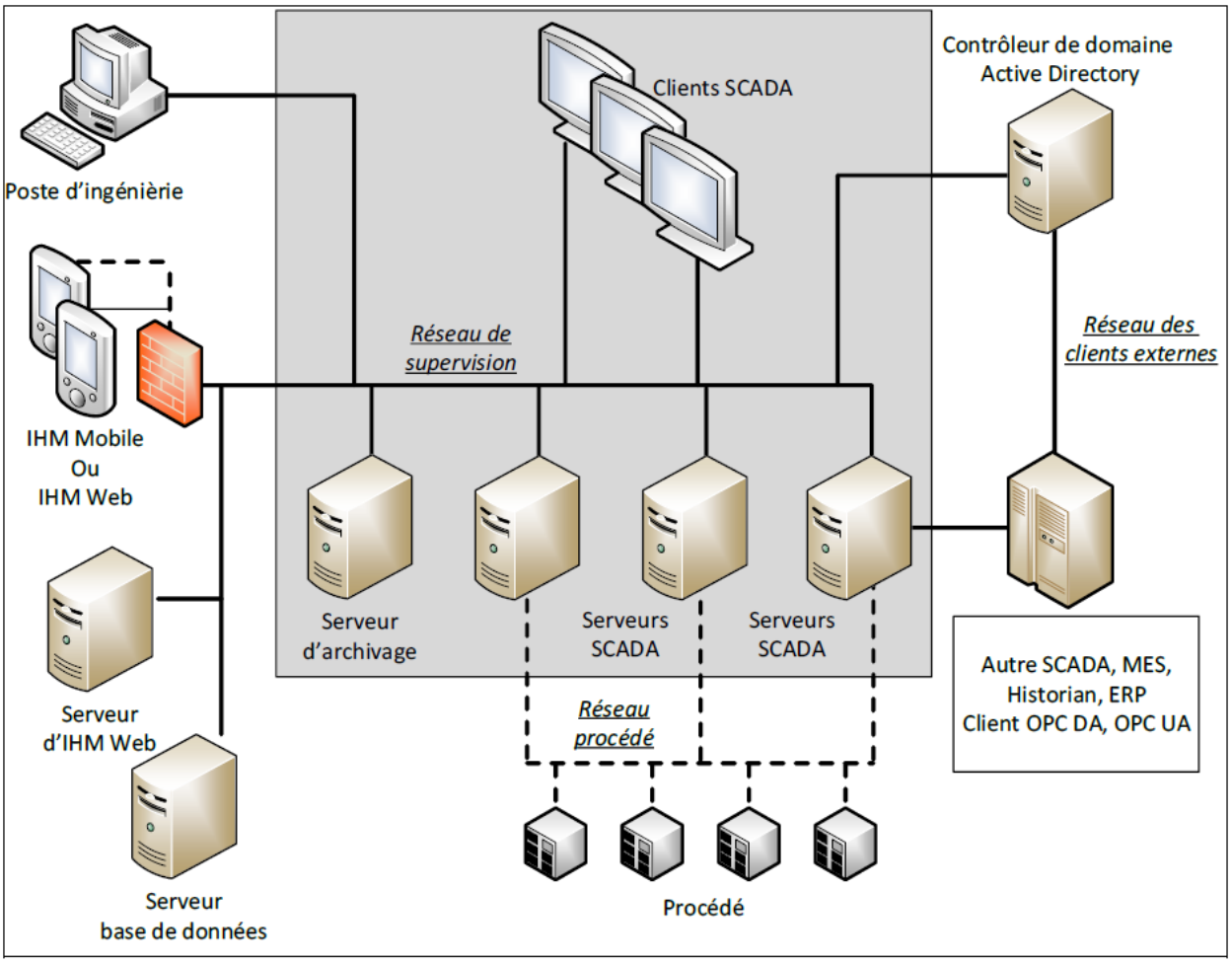


Figure 1 - Architecture de déploiement du produit.

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.

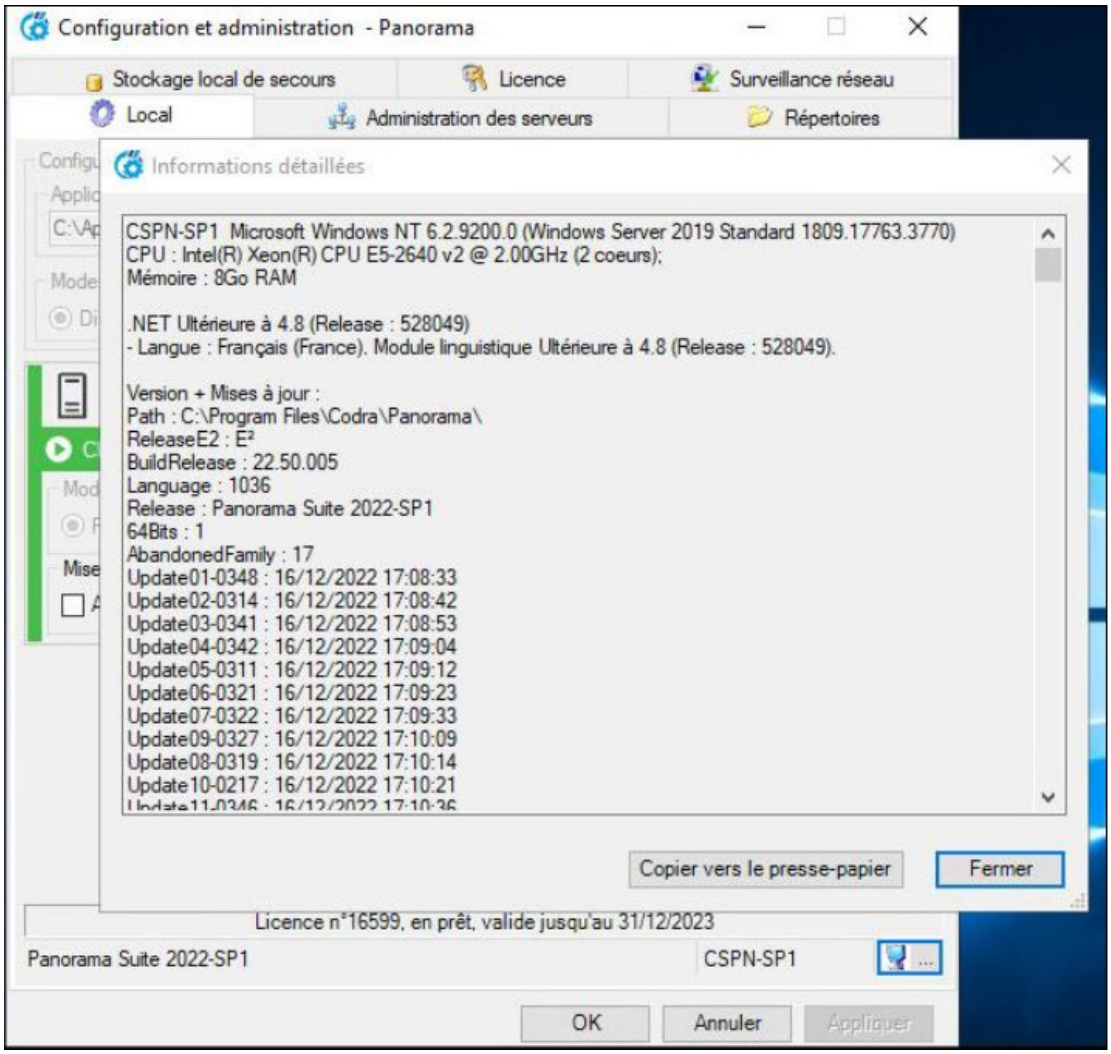
1.2.1 *Catégorie du produit*

☐	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 : SCADA**

1.2.2 *Identification du produit*

Produit	
Nom du produit	Panorama E2
Numéro de la version évaluée	Version 2022 SP1

La version certifiée du produit peut être identifiée de la manière suivante : Sur la machine d'exploitation, lancer le programme « Configuration et administration », aller dans l'onglet « Local » et cliquer sur « informations détaillées » :



1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la gestion des entrées malformées ;
- les communications sécurisées ;
- la protection de la confidentialité des secrets de connexion des utilisateurs gérés par l'*Active Directory* ;
- l'intégrité des certificats des utilisateurs des interfaces externes OPC-UA ;
- l'intégrité des certificats des serveurs de données OPC-UA ;
- l'accès aux bases de données par sécurité Intégrée ;
- l'authentification sécurisée ;
- la politique de droits ;
- la signature du logiciel ;
- l'intégrité et confidentialité de la configuration ;
- l'intégrité des journaux.

1.2.4 *Configuration évaluée*

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

- deux Serveurs SCADA (Windows 10 et Windows Server 2019) ;
- un Client SCADA (Windows 10) ;
- un contrôleur de domaine (Windows Server 2019) ;
- un poste d'ingénierie (Windows 10) ;
- un client SCADA et un Client OPC-UA (Windows 10) ;
- un poste de simulation de procédé (Windows 10) ;
- une machine hébergeant une base de données (SQL Server) et un serveur d'affichage (Windows 10).

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.

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

La solution Panorama E² a été livrée préinstallée sur un ensemble de machines virtuelles pour *VMware ESXi*, et l'installation a été complétée par CODRA en suivant la documentation fournie pour une utilisation sécurisée.

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 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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS]

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

Certains 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

La TOE utilise le générateur d'aléa du système d'exploitation sous-jacent, en source fermée (voir fonctions de sécurité de [CDS]). Il n'est donc pas possible d'en faire une analyse complète au sens de la méthodologie CSPN.

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 « Panorama E2, Version 2022 SP1 » 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 : - Cible de sécurité CSPN PANORAMA Serveur et Client Court-terme, version 5.6, 20 juillet 2023.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN – Panorama E2 – Codra, référence OPPIDA/CESTI/2022/PANORAMA-2022/RTE, version 1.2, 31 juillet 2023
[GUIDES]	Guide d'utilisation, d'administration et d'installation du produit : - Manuel Panorama Suite 2022, version 9.1, 08/04/2022[1]

[1] Ce manuel est accessible aux clients finaux enregistrés sur le site du développeur, ou encore à tout utilisateur final du produit sous forme de pages web accessibles depuis le produit installé.

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.