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

# Rapport de certification ANSSI-CSPN-2019/14

# Panorama $E^2$

# Version 7.00

*Paris, le 7 novembre 2019*

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]

SÉCURITÉ CERTIFICATION

# 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-2019/14

*Nom du produit*

## Panorama E$^2$

*Référence/version du produit*

## Panorama E$^2$

**Version 7.00 intégré à Panorama Suite 2017 (build 17.00.011) avec *updates* PS2-1700-01-1086, 03-2128, 05-1024, 06-0348, 07-1082, 08-1054, 09-1052, 13-0348, 14-1051, 17-1037; 18-1157**

*Catégorie de produit*

## Autres (SCADA)

*Critères 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**
**Communication sécurisée**
**Non divulgation des secrets de connexion des utilisateurs gérés par l'*Active Directory***
**Intégrité des certificats des utilisateurs des interfaces OPC-UA**
**Intégrité des secrets de connexion aux Serveurs de données OPC-UA**
**Accès aux bases de données authentifiés par l'*Active Directory***
**Authentification sécurisée**
**Politique de droits**
**Signature du logiciel**
**Intégrité et confidentialité de la configuration**
**Intégrité des journaux**

*Fonction(s) de sécurité non évaluées*

**Sans objet**

*Restriction(s) d'usage*

**Oui (cf. §3.2)**

# Préface

## 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 Premier ministre 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 matières

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est le « Panorama $E^2$, version 7.00 » développé par *CODRA INGENIERIE INFORMATIQUE*.

Conçu pour être déployé au sein de réseaux industriels, Panorama $E^2$ inclut un serveur SCADA pouvant être connecté à des équipements de terrain de niveau 1 au sens de la classification CIM (*Computer-Integrated Manufacturing*). Ce serveur permet l'acquisition de données terrain et l'envoi de commandes, ainsi que la gestion des alarmes.
Panorama $E^2$ inclut également un client SCADA, qui permet notamment de présenter une interface homme-machine (IHM) à l'utilisateur.
Panorama $E^2$ peut enfin être connecté à d'autres équipements de niveaux 2 et 3, en particulier via un serveur OPC-UA avec liaison de type HTTPS.

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

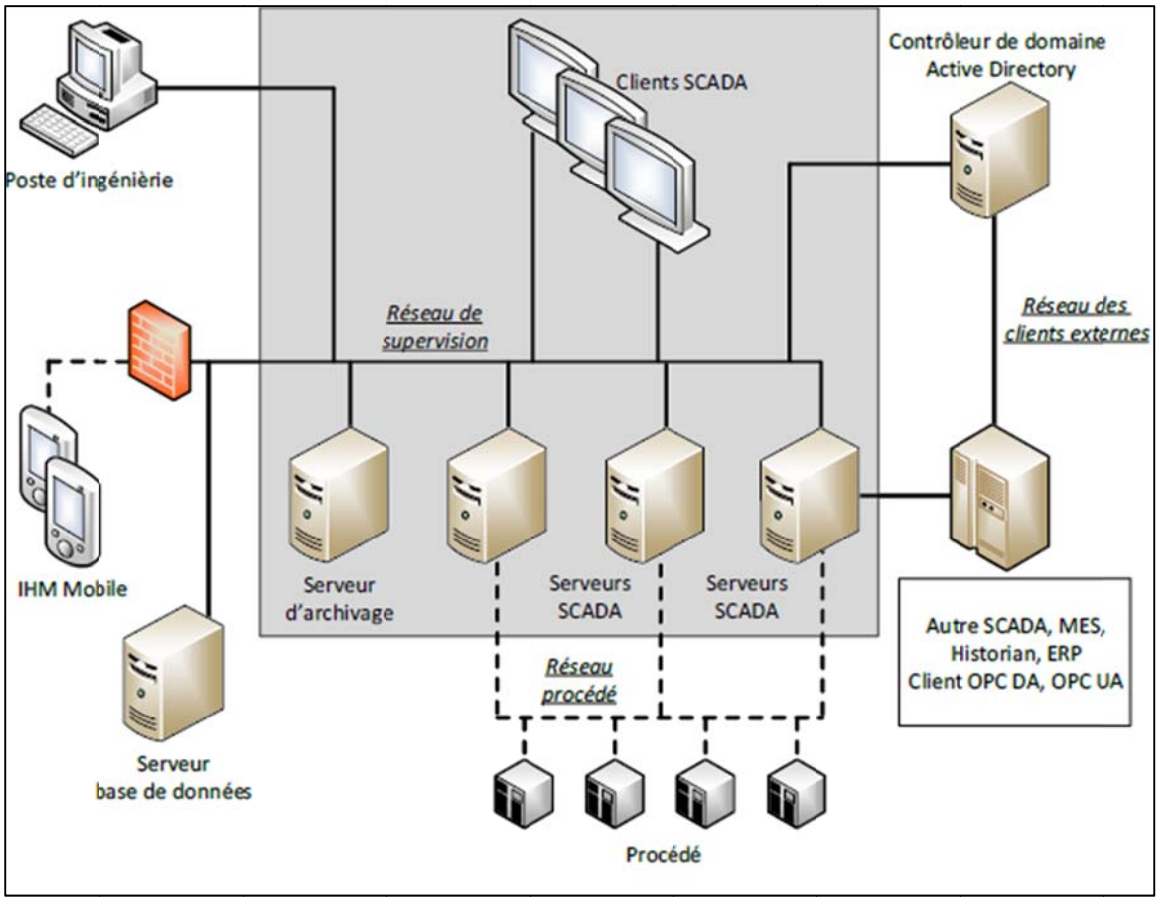


**Figure 1 - Architecture de déploiement du produit.**

## 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

| | |
|---|---|
| Nom du produit | Panorama E$^2$ |
| Numéro de la version évaluée | 7.00 (version complète : Version 7.00 intégré à Panorama Suite 2017 (build 17.00.011) avec updates PS2-1700-01-1086, 03-2128, 05-1024, 06-0348, 07-1082, 08-1054, 09-1052, 13-0348, 14-1051, 17-1037) |

Pour vérifier la version de Panorama E$^2$, se connecter à une des machines sur laquelle est installée Panorama E$^2$ et lancer le programme « configuration et administration ». Dans l'onglet « Local », cliquer sur « informations détaillées », comme indiqué sur la figure ci-après.

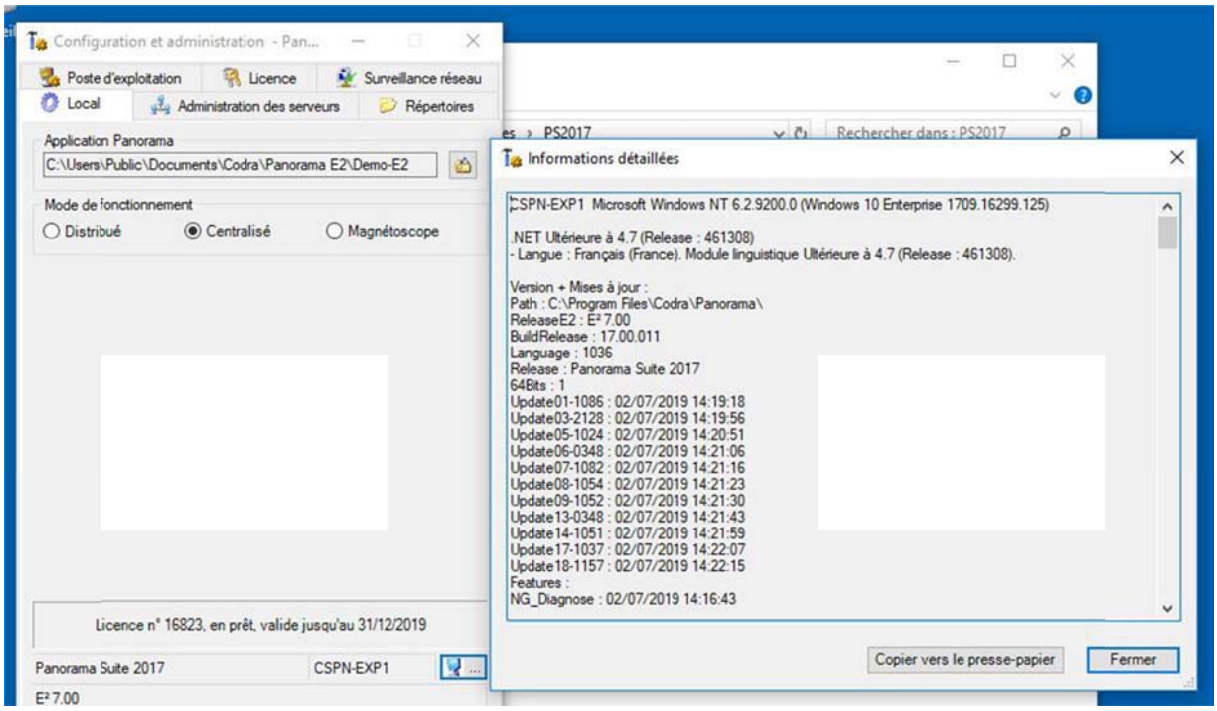


**Figure 2 : Affichage de la version de Panorama E$^2$ et des mises à jour**

### 1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la gestion des entrées malformées ;
- la protection de l'intégrité et de l'authenticité des flux des réseaux de supervision et du réseau de clients externes ;
- la protection de la confidentialité des secrets de connexion des utilisateurs ;
- l'intégrité des certificats des utilisateurs des interfaces OPC-UA ;
- l'intégrité des secrets de connexion aux serveurs de données OPC-UA ;
- l'authentification des accès aux bases de données *via* l'*Active Directory* ;
- l'authentification sécurisée ;
- la gestion des droits d'accès ;
- la signature du logiciel ;
- l'intégrité et la confidentialité de la configuration ;
- l'intégrité des journaux.

### 1.2.4. Configuration évaluée

La plateforme de test était constituée des éléments suivants :

- deux serveurs fonctionnels, sur lesquels le produit Panorama E$^2$ est déployé sur un ensemble de machines virtuelles installées dans un ESXi
  - l'un sous Windows Server 2016 version 10.0.14393
  - l'autre sous Windows 10 entreprise version 10.0.16299

  Ces serveurs sont ceux;
- un contrôleur de domaine *Active Directory* sous Windows Server 2016 version 10.0.14393 ;
- une base de données sous Windows Server 2016 version 10.0.14393 ;
- un poste d'exploitation sous Windows 10 entreprise version 10.0.16299 ;
- un poste d'ingénierie sous Windows 10 entreprise version 10.0.16299 ;
- un client externe sous Windows 10 entreprise version 10.0.16299 ;
- un équipement sur réseau procédé sous Windows 10 entreprise version 10.0.16299.

**Version ESXi :** pour vérifier la version d'ESXi, se connecter sur l'interface graphique web. La version utilisée pour l'évaluation était la version 6.0.0 / 3073146, ainsi que le montre la figure ci-après.

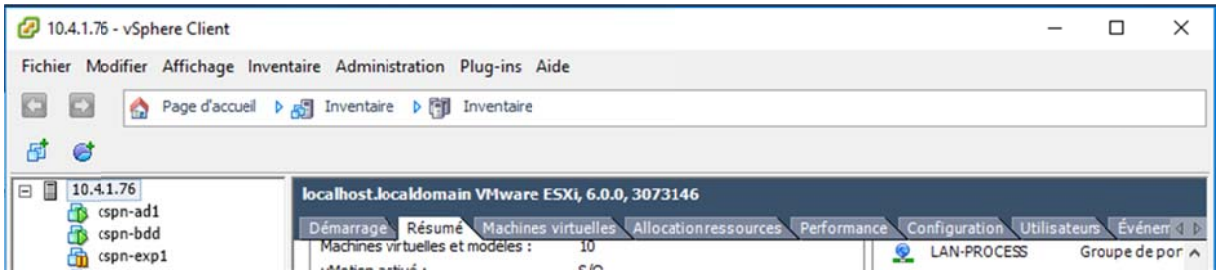


**Figure 3 : Affichage de la version ESXi**

**Version des OS :** pour vérifier les versions d'OS, se connecter aux machines Windows et lancer « Get-WmiObject Win32_OperatingSystem | Select Caption, Version » dans PowerShell. Les versions d'OS utilisées pour l'évaluation sont rappelées au chapitre 1.2.4.

-

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

## 2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

## 2.3. 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 **l**a cible de sécurité [CDS].

### 2.3.1. Installation du produit

#### 2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4. Les installations ont été réalisées par le développeur en suivant les recommandations indiquées au chapitre 3.2

#### 2.3.1.2. Description de l'installation et des non-conformités éventuelles

Sans objet.

#### 2.3.1.3. Durée de l'installation

Sans objet.

#### 2.3.1.4. Notes et remarques diverses

Sans objet.

### 2.3.2. Analyse de la documentation

L'évaluateur a eu accès aux [GUIDES] et au document [ANNEXE_PTF] dans le cadre de cette évaluation.
Les guides du produit permettent d'utiliser le produit sans causer de dégradation accidentelle de la sécurité. Bien que le produit ait été installé par le développeur, l'évaluateur a pu étudier le document [ANNEXE_PTF], utilisé lors de l'installation, et a jugé qu'il permettait d'effectuer une installation sûre du produit.

#### 2.3.3. Revue du code source (facultative)

L'évaluateur a revu le code source de l'intégralité du produit au moyen d'outils automatisés. L'évaluateur a également effectué une revue manuelle des fonctionnalités OPC-UA. Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

#### 2.3.4. Analyse de la conformité des fonctions de sécurité

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

#### 2.3.5. 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.

#### 2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

##### 2.3.6.1. Liste des vulnérabilités connues

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

##### 2.3.6.2. 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.

#### 2.3.7. Accès aux développeurs

Sans objet.

#### 2.3.8. Analyse de la facilité d'emploi

##### 2.3.8.1. Cas où la sécurité est remise en cause

Les risques identifiés lors de l'évaluation entraînent des recommandations et des restrictions d'usage pour l'utilisateur (voir chapitre 3.2).

##### 2.3.8.2. Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

##### 2.3.8.3. Notes et remarques diverses

Sans objet.

### 2.4. Analyse de la résistance des mécanismes cryptographiques

Le produit utilise des fonctions cryptographiques afin de protéger les flux en confidentialité, intégrité et authenticité. Pour cela il se base sur des fonctions de l'OS sous-jacent Windows,

dont le code source n'est pas disponible, ce qui ne permet pas d'effectuer une analyse cryptographique au sens de la méthodologie CSPN.
Pour cette raison, le produit n'a pas fait l'objet d'une analyse des mécanismes cryptographiques au titre de cette évaluation.

## 2.5. Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléas.

# 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 $E^2$, version 7.00 » 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 mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations et restrictions suivantes.

Afin de garantir l'utilisation sécurisée du produit, il est impératif que l'utilisateur suive les mesures suivantes :

- le réseau de supervision, le réseau des clients externes et le réseau procédé doivent être des réseaux séparés ;
- les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis ;
- l'utilisateur doit consulter les bulletins de sécurité [BDS] publiés par le développeur. En particulier, comme indiqué dans le Bulletin de Sécurité Pano/BS-010, il convient de mettre en place une politique de surveillance de l'état d'expiration des certificats et de mise à jour de la liste pour retirer les empreintes des certificats expirés pour OPC-UA et les remplacer par celles des certificats renouvelés.
- l'utilisateur doit suivre les recommandations du document [ANNEXE_PTF] lors de l'installation, et ne pas se contenter de suivre le programme d'installation, car ce dernier ne montre pas explicitement comment effectuer une installation sécurisée.

# Annexe 1. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | *Cible de sécurité CSPN PANORAMA Serveur et client Court-terme*<br>Référence : PANO/CibleCSPN Court-terme ;<br>Version : 3.5 ;<br>Date : *8 octobre 2019.* |
| [RTE] | *Rapport Technique d'Évaluation CSPN – PANORAMA*<br>Référence : OPPIDA/CESTI/PANORAMA/RTE ;<br>Version : 1.1 ;<br>Date : *26 septembre 2019.* |
| [GUIDES] | *Guide technique programmeur, intégré en tant qu'aide en ligne dans le produit.* |
| [ANNEXE_PTF] | *Cible de sécurité CSPN PANORAMA Serveur et Client Court-terme – Annexe Plateforme*<br>Référence : *PANO_CSPN Panorama Plateforme* ;<br>Version : 1.2 ;<br>Date : *26 juin 2019.* |
| [BDS] | *Bulletins de sécurité, publiés à l'adresse* https://codra.net/service/bulletin-securite-informatique |

# Annexe 2. Références 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-01/2.0 du 6 septembre 2018.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018.<br><br>Documents disponibles sur www.ssi.gouv.fr. |
| [RGS] | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr. |