



**PREMIER  
MINISTRE**

*Liberté  
Égalité  
Fraternité*

**Secrétariat général de la défense  
et de la sécurité nationale**

Agence nationale de la sécurité des  
systèmes d'information

**Le Directeur général**

Paris, le 20/04/2026  
N° 2777/ANSSI/SDE/NP

## **DECISION DE QUALIFICATION D'UN PRODUIT**

**SECURITY CENTER SYNERGIS<sup>MC</sup>  
SECURITY CENTER 5.12.2 (GESTIONNAIRE D'ACCES - GAC)  
SYNERGIS<sup>MC</sup> CLOUD LINK 3.1.2 (UNITE DE TRAITEMENT LOCAL - UTL)**

**GENETEC EUROPE  
SIRET N° 484024724**

**4-8 RUE DARU  
75008 PARIS  
FRANCE**

Pièces constitutives de la décision de qualification :

**Fiche 1** : Base documentaire de la qualification

**Fiche 2** : Versions du produit concernées par la qualification

**Fiche 3** : Conditions et limites de la qualification

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

- 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 1<sup>er</sup> ;
- VU le décret du 4 janvier 2023 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. STRUBEL (Vincent) ;
- VU le processus de qualification d'un produit, version en vigueur ;
- VU le rapport de certification ANSSI-CSPN-2025/05 du 27/05/2025 ;
- VU le dossier de demande de qualification déposé par GENETEC EUROPE.

DÉCIDE :

- Art. 1<sup>er</sup> – Le produit « SECURITY CENTER SYNERGIS<sup>MC</sup> » ainsi composé :
- SECURITY CENTER 5.12.2 (GESTIONNAIRE D'ACCES - GAC)
  - SYNERGIS<sup>MC</sup> CLOUD LINK 3.1.2 (UNITE DE TRAITEMENT LOCAL - UTL)
- ci-après désigné « le produit », fourni par GENETEC EUROPE, ci-après désigné « le fournisseur », respecte les règles fixées par les décrets 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 annexe.
- Art. 2 – Le maintien de cette décision est conditionné au respect par le fournisseur des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.
- Art. 3 – La présente décision est valable trois ans.

 Vincent Strubel

## Fiche 1

Base documentaire de la qualification

### Références

#### Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, note n° 274/ANSSI/SDE du 12 janvier 2017, version en vigueur. Disponible sur <a href="https://www.ssi.gouv.fr/qualification-processus">https://www.ssi.gouv.fr/qualification-processus</a>
[RGS]	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
[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
[ANSSI_CONTRÔLE_ACCES]	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection version 2.1, octobre 2023

#### Documents rédigés par le centre d'évaluation

[CRYPTO]	Analysis of Cryptographic Mechanisms Genetec Synergis <sup>MC</sup> CSPN 2024, référence GNT2_CRY, version 1.2, 6 mai 2025
[RTE]	Rapport Technique d'Evaluation CSPN Genetec Synergis <sup>MC</sup> CSPN 2024, référence GNT2_CSPN_RTE_FR_1.4, version 1.4, 12 mai 2025

[CERTIF]	Certificat ANSSI-CSPN-2025/05 du 27/05/2025
----------	---

#### Guides d'utilisation et documentations techniques de l'industriel

[GUIDE_INSTALL]	<ul style="list-style-type: none"><li>• Security Center Installation and Upgrade Guide, version 5.12.2.0, juillet 2024</li></ul>
[GUIDE_UTIL]	<ul style="list-style-type: none"><li>• Security Center Administrator Guide, version 5.12, avril 2024</li><li>• Security Center User Guide, version 5.12, juillet 2024</li><li>• Security Center Hardening Guide, version 5.12, avril 2024</li><li>• Configurer Genetec Security Center et le Synergis<sup>MC</sup> Cloud Link pour conformité ANSSI CSPN, version 1.3</li></ul>
[CDS]	<ul style="list-style-type: none"><li>• Cible de sécurité CSPN Security Center Synergis<sup>MC</sup>, version 1.5, mai 2025</li></ul>

## Fiche 2

Versions du produit concernées par la qualification et l'agrément

	UTL <sup>1</sup>	GAC <sup>2</sup>
Matériel	carte iMX8	serveur Windows
Logiciel	3.1.2	5.12.2

---

<sup>1</sup> Unité de Traitement Local

<sup>2</sup> Gestionnaires d'Accès

### Fiche 3

Conditions et limites de la qualification et de l'agrément
--

#### **Condition(s)**

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

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

- C1. L'installation du produit est faite selon le guide « Configurer Genetec Security Center et le Synergis<sup>MC</sup> Cloud Link pour conformité ANSSI CSPN », qui détaille divers aspects de la sécurisation et de la configuration opérationnelle.
- C2. Le système est installé et configuré par un prestataire de confiance agréé par le développeur. Les éléments critiques (UTLs, serveur GAC) sont placés dans des zones sûres (protégées en accès physique) et les modules de porte sont placés à l'intérieur du local protégé.
- C3. Les consignes de sécurité indiquées dans les guides d'administration [GUIDE\_INSTALL] et utilisateurs [GUIDE\_UTIL] sont mises en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout au long de son cycle de vie.
- C4. Les objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans les cibles de sécurité [CDS] sont strictement respectés.
- C5. Tous les utilisateurs sont formés et entraînés à l'usage des produits SECURITY CENTER SYNERGIS<sup>MC</sup> selon les besoins opérationnels.
- C6. Les administrateurs sont informés de la politique de sécurité du système d'information, et doivent contrôler que les règles de filtrage et de chiffrement qui sont implémentées sont conformes avec la politique de sécurité.
- C7. Le système est maintenu en condition opérationnelle (MCO) et en condition de sécurité (MCS) tout au long de son cycle de vie par l'application régulière des mises à jour, contrôles et mesures de sécurité nécessaires.

#### **Limite(s)**

- L1. Seules les fonctions identifiées dans le rapport [RTE] sont couvertes par la présente décision de qualification.