PREMIÈRE
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 02 DEC 2022
N°2535/ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT
AU NIVEAU ELEMENTAIRE

SYSTEME DE DETECTION QE-SECURE en version 2.1.X
100 MB/S, 500MB/S, 1 GB/S, 4 GB/S ET 10 GB/S
composé de :
SONDE DE DETECTION QE-SECURE VERSION 2.1.X
MANAGER QE-SECURE VERSION 2.1.X

ALLENTIS

RCS 533 336 848

140 bis, rue de Rennes
75006 PARIS
France

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit.

Fiche 2 : Conditions et limites de la qualification.

Fiche 3 : Base documentaire 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 nationale ;

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 1er ;

Vu le décret du 27 mars 2014 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Vu le processus de qualification d'un produit ;

Vu la demande de qualification du système QE-SECURE déposée le 24 mai 2019,

Décide :

Art. 1er – Le système de détection des évènements susceptibles d'affecter la sécurité des systèmes d'information portant le nom QE-SECURE en version 2.1.X (X supérieur ou égal à 20), et constitué des composants SONDE DE DETECTION QE-SECURE en version 2.1.X et MANAGER QE-SECURE en version 2.1.X, ci-après désigné « le système de détection », fourni par la société ALLENTIS, ci-après désignée « le fournisseur », respecte les règles fixées par le décret n° 2015-350 du 27 mars 2015 et est qualifiée au niveau élémentaire sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.

Art. 2 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.

Art. 3 – La présente décision est valable jusqu'au 2 juin 2025.

Fiche 1

Description du produit.

Désignation et versions

Le produit qualifié est la solution logicielle et matérielle « QE-SECURE » en version 2.1.X fournie par l'entreprise ALLENTIS. Cette qualification couvre la sonde de détection QE-SECURE 2.1.X et le manager QE-SECURE 2.1.X.

La version qualifiée des composants est la version 2.1.X, pour X supérieur ou égal à 20.

Le système de détection QE-SECURE est qualifié dans les modèles 100Mbps, 500Mbps, 1Gbps, 4Gbps, et 10Gbps.

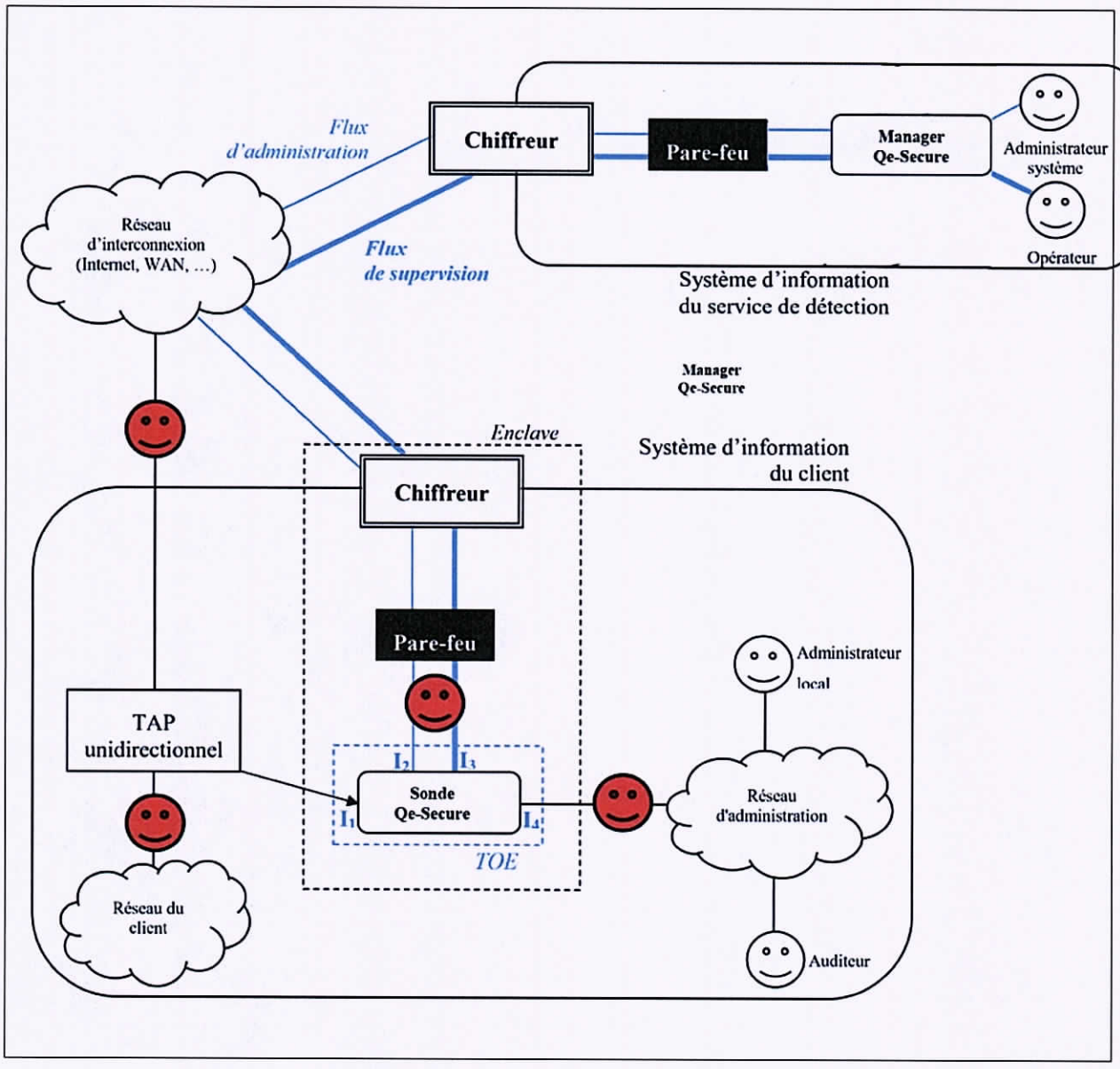

Figure 1. Cas d'usage classique du produit

Présentation générale

La solution QE-SECURE est destinée à aider à détecter des activités suspectes ou malveillantes sur le plan de la sécurité du système d'information. Elle analyse des flux de données circulant sur des réseaux physiques et génère des alertes en cas de détection d'évènements pouvant menacer la sécurité du système d'information.

La sonde offre des fonctions de sécurité et de détection conformes à celles décrites dans la cible de sécurité de la sonde [CDS], elle-même conforme à la cible de sécurité générique élaborée par l'ANSSI [Cible_Générique].

Les fonctionnalités de la sonde lui permettent d'être opérée par un prestataire conforme au référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité [PDIS].

Fiche 2

Conditions et limites de la qualification.

Conditions

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 La sonde est placée en dérivation des flux à analyser et non en coupure.

C2 La dérivation vers la sonde des flux à analyser est réalisée par un TAP qualifié par l'ANSSI au niveau élémentaire.

C3 La sonde est placée au plus près du point de dérivation. Seul un agrégateur de flux respectant les exigences définies dans l'annexe 5 du référentiel [PDIS] peut être déployé entre le TAP et la sonde.

C4 Le réseau sur lequel le système de détection est déployé est en adéquation avec les capacités fonctionnelles du modèle choisi (débit des flux à analyser, capacité de stockage, etc.) et prend en compte la limite L2 (nature des flux à analyser) identifiée ci-dessous.

C5 Les utilisateurs du système de détection sont, selon leur rôle, formés aux composants du système de détection, et la documentation de ces composants est mise à leur disposition.

C6 La sonde dispose d'une base de règles de détection à jour conformément au chapitre intitulé « Gestion des incidents » du référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité [PDIS].

C7 La sonde est déployée selon les lois et réglementations en vigueur, notamment vis-à-vis des types d'informations pouvant être contenus dans les flux à analyser (données à caractère personnel, etc.).

C8 Le système d'information du service de détection opérant le système de détection respecte les exigences établies dans le référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité [PDIS].

C9 La sonde est déployée dans une enclave de collecte respectant les exigences établies dans le chapitre intitulé « Enclave de collecte au sein du système d'information du commanditaire » du référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité [PDIS].

C10 Les fonctions d'administration à distance offertes nativement par certains matériels constituant la sonde sont désactivées par défaut, dans la version livrée. Elles ne doivent en aucun cas être réactivées par l'administrateur système de la sonde.

C11 Les composants du système de détection sont hébergés dans des locaux sécurisés dont l'accès est contrôlé et restreint à du personnel de confiance.

C12 Lorsqu'un prestataire de détection supervise les systèmes d'information de plusieurs clients, il met en œuvre un Manager QE-SECURE par client nécessitant un manager.

Limites

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

L1. Seules les fonctions de sécurité et de détection identifiées dans la fiche 1 sont couvertes par la présente décision de qualification.

L2. La présente décision de qualification ne couvre pas le décodage et l'analyse des protocoles de type industriel par le système de détection.

Fiche 3

Base documentaire de la qualification

Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, note n° 274/ANSSI/SDE du 12 janvier 2017, référence QUAL-PROD-PROCESS, version en vigueur. Disponible sur https://www.ssi.gouv.fr/qualification-processus
[LPM]	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 nationale. Disponible sur https://www.legifrance.fr

Documents rédigés par le centre d'évaluation

[RTE]	Rapport technique Solution Qe-Secure Référence : ALL20210625 ; Version : 2.0 ; Date : 25 juin 2021. Analyse des mécanismes cryptographiques Référence : CRY20210623 ; Version : 1.1.
[REM]	Rapport d'évaluation métier, LEXFO, référence ALL20220207, version 2.0 du 31 août 2022
[CONFIG]	Rapport technique de configuration, LEXFO, référence ALL20200724, version 1 du 24 juillet 2020
[ORGA]	Rapport d'évaluation des processus métier de suivi de développement d'une sonde de détection, LEXFO, référence ALL20220530, version 1.0 du 30 mai 2022.

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[CERTIF]	Rapport de certification, référence ANSSI-CSPN-2021/23, du 11/10/2021
[PDIS]	Prestataires de détection des incidents de sécurité, référentiel d'exigences, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[CIBLE_GENERIQUE]	Sonde réseau de détection des incidents de sécurité – Cible générique. Disponible sur https://www.ssi.gouv.fr

Guides d'utilisation et documentations techniques de l'industriel

[CDS]	Qe-Secure Sonde réseau de détection des incidents de sécurité Version, v1.7
[Manuels]	Qe-Secure – Guide utilisateur, version 2.1 Référence : DOC-QESEC-FR-V12