

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Bureau Qualifications et Agréments

Paris, le
N° 428

01 FEV. 2019
/ANSSI/SDE/PSS/BQA

**DECISION DE QUALIFICATION
D'UN SERVICE**

**SERVICE DE DETECTION DES INCIDENTS
« SOC PDIS : SERVICE DE DETECTION ET DE SUPERVISION DE SECURITE »**

SOGETI FRANCE

RCS 479 942 583

24, rue du Gouverneur général Éboué
92 130 Issy-les-Moulineaux
France

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

Vu la loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, et notamment son article 22 ;

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° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense ;

Vu le code de la défense, notamment ses articles R. 1332-1, R. 1332-2, L. 1332-6-1 et R. 1332-41-1 à R. 1332-41-9 ;

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^{er} ;

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 la décision du 22 octobre 2014 portant délégation de signature (Secrétariat général de la défense et de la sécurité nationale) ;

Vu le *Processus de qualification d'un service*, référence QUAL-SERV-PROCESS, version en vigueur ;

Vu le référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité, version en vigueur ;

Vu le référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité pour les besoins de la sécurité nationale, version en vigueur ;

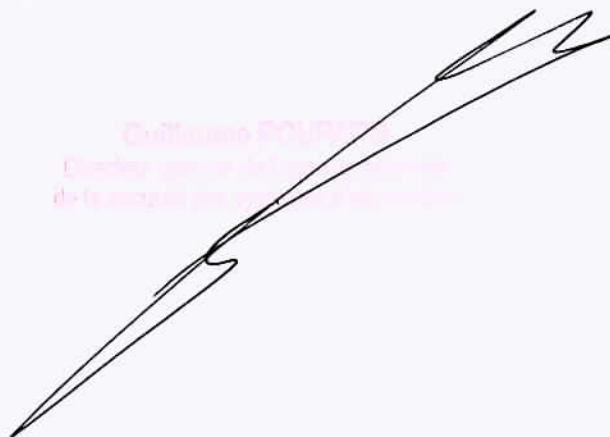
Vu les éléments fournis par *SOGETI FRANCE* dans le dossier de demande de qualification ;

Vu le rapport d'évaluation de la conformité de la société *SOGETI FRANCE* au référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité,

Décide :

- Art. 1 – Le service de détection des incidents de sécurité portant le nom *SOC PDIS : SERVICE DE DETECTION ET DE SUPERVISION DE SECURITE*, ci-après désigné « le service », fourni par la société *SOGETI FRANCE*, ci-après désigné « le fournisseur » respecte les règles du référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité et est qualifié sous réserve du respect des conditions d'utilisation énoncées en annexe.
- Art. 2 – La présente décision est conditionnée au respect des engagements relatifs au *Processus de qualification d'un service* pris par le fournisseur au titre de sa demande de qualification.
- Art. 3 – La présente décision est valable pour une durée de trois ans.

Pour le Premier ministre,
et par délégation,



Guillaume SORRES
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information

Annexe
Conditions d'utilisation du service

La décision de qualification est valide sous la condition énoncée ci-après.

- C1. Il est recommandé que les commanditaires de services de détection qualifiés respectent les recommandations énoncées dans l'annexe 3 du référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité.
- C2. Le prestataire de détection doit opérer un système de détection qualifié conformément aux conditions d'utilisation définies dans la décisions de qualification dudit système, notamment :
- le système de détection doit disposer d'une base de règles de détection à jour et testées avant d'être importées ;
 - le système de détection doit être déployé dans une enclave de collecte respectant les exigences établies dans le référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité ;
 - des solutions de chiffrement et d'authentification *IPSEC* agréées par l'ANSSI au niveau adéquat et utilisées conformément aux conditions de leur agrément doivent être déployées au plus près du système de détection ;
 - lorsqu'un prestataire de détection supervise les systèmes de plusieurs opérateurs d'importance vitale, le centre de gestion et le centre d'exploitation du système de détection doivent être dédiés à un et un seul opérateur d'importance vitale.