PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 27 JAN. 2025

N° 42/ANSSI/SDE/NP

NOTE

Addendum au référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité (PDIS) version 2.0

Objet : Amendement de certaines exigences du référentiel PDIS version 2.0 dans l'attente de la publication de la nouvelle version.

Références :

1. Décret n°2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de confiance pour les besoins de la sécurité des systèmes d'information.
2. Prestataires de détection des incidents de sécurité – référentiel d'exigence, version 2.0 du 21 décembre 2017.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) qualifie au titre du décret cité en première référence des prestataires de détection des incidents de sécurité (PDIS). La qualification atteste de la conformité des prestataires au référentiel d'exigences en vigueur cité en seconde référence publié en 2017.

Les travaux de mise à jour du référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité initiés en 2022 sont en cours. Dans l'attente de la publication de la nouvelle version du référentiel, la présente note amende certaines exigences du référentiel. Elle permet aux prestataires, après une appréciation des risques, de choisir de se conformer à l'exigence originale telle que définie dans le référentiel cité en seconde référence (option A) ou de se conformer à l'exigence amendée telle que définie ci-dessous (option B).

Les mesures décrites dans la présente note sont transitoires, elles seront rendues caduques à la publication de la nouvelle version du référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité.

Vincent STRUBEL
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél +33.1.71.75.82.78

1. Amendement n°1 : exigence IV.2.3.g (notification)

Option A :

Le prestataire met en œuvre l'exigence IV.2.3.g du référentiel cité en seconde référence.

Rappel de l'exigence

> IV.2.3.g) Les notifications doivent contenir exclusivement les informations suivantes : le numéro du ticket d'incident.
>
> Les notifications ne doivent en aucun cas contenir des informations détaillées sur l'incident de sécurité et notamment sur les évènements collectés ou les règles de détection ayant permis de détecter l'incident de sécurité, la partie du système d'information du commanditaire concernée par l'incident de sécurité ou les impacts de l'incident de sécurité.

Le prestataire est évalué sur cette exigence.

Option B :

Le prestataire ne met pas en œuvre l'exigence IV.2.3.g) et met en œuvre l'exigence suivante :

> g) Les notifications doivent contenir les informations suivantes : le numéro du ticket d'incident et le niveau de criticité de l'incident.
>
> Les notifications peuvent être enrichies par les informations suivantes sous réserve d'accord avec le commanditaire : la date et l'heure de l'incident de sécurité, le périmètre ou système d'information concerné, le type d'incident.
>
> Cet enrichissement est autorisé uniquement si celui-ci n'entraîne pas une dégradation de la sécurité du service conformément à l'appréciation des risques du système d'information supervisé.
>
> Les notifications ne doivent en aucun cas contenir des informations détaillées sur l'incident de sécurité et notamment sur les évènements collectés ou les règles de détection ayant permis de détecter l'incident de sécurité.

Le prestataire est évalué sur cette exigence.

2. Amendement n°2 : exigence IV.3.4.f (audit PASSI qualifié juridiquement indépendant)

Option A :

Le prestataire met en œuvre l'exigence IV.3.4.f) du référentiel cité en seconde référence.

Rappel de l'exigence

> IV.3.4.f) Le programme d'audit doit inclure au minimum un audit qualifié par an, réalisé par un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié. Les prestataires PASSI mandatés doivent être juridiquement indépendants du prestataire.

Le prestataire est évalué sur cette exigence.

Option B :

Le prestataire ne met pas en œuvre l'exigence IV.3.4.f) et met en œuvre l'exigence suivante :

IV.3.4.f) Le programme d'audit doit inclure au minimum un audit qualifié par an, réalisé par un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié.

Le prestataire est évalué sur cette exigence.

3. Amendement n°3 : exigences du chapitre IV.3.7. (Service de détection du service)

Option A :

Le prestataire met en œuvre les exigences du chapitre IV.3.7. intitulé « Service de détection du service » du référentiel cité en seconde référence et est évalué sur ces exigences.

Option B :

Le prestataire ne met pas en œuvre les exigences du chapitre IV.3.7. Service de détection du service et met en œuvre les exigences suivantes :

a) Le prestataire doit mettre en œuvre, pour son propre compte, un service de détection des incidents de sécurité, ci-après dénommé « service de détection du service », portant sur le système d'information du service de détection des incidents de sécurité.

b) Le prestataire doit respecter les exigences des chapitres IV.3.1 et des chapitres IV.3.2 pour le service de détection du service ; la mise en œuvre du service de détection du service ne doit pas dégrader la sécurité du système d'information de détection.

c) Le prestataire doit, sur la base de l'appréciation des risques (voir exigence IV.3.1.a) et de la liste des incidents de sécurité redoutés associée (voir exigence IV.3.1.b), élaborer une stratégie de collecte, une stratégie d'analyse et une stratégie de notification dans le cadre du service de détection du service.

d) Il est recommandé, selon le résultat de l'appréciation des risques et la liste des incidents de sécurité redoutés associée, que le prestataire cloisonne le service de détection du service (séparation des moyens humains, techniques et organisationnels).

e) Le prestataire doit déployer des sources de collecte au profit du service de détection du service. Le choix du type de sources de collecte, leurs positionnements et la manière dont ils sont déployés doivent être cohérents avec l'analyse de risque du prestataire.

f) Il est recommandé que le prestataire mette en place une centralisation et une rétention des données collectées par les sources de collecte au sein d'une zone de confiance dédiée conformément aux exigences de [NT_JOURNAL]. Dans ce cas, il est recommandé que la zone de confiance dédiée mette en œuvre un contrôle d'accès interdisant l'accès aux administrateurs et opérateurs du service de détection des incidents de sécurité respectivement depuis les zones d'administration et d'exploitation.

g) Le prestataire doit élaborer un processus de gestion des incidents de sécurité du service. Ce processus doit prévoir une notification aux commanditaires lors de l'occurrence d'un incident de sécurité sur le service de détection des incidents de sécurité. La notification doit spécifier la nature de l'incident de sécurité et les mesures mises en œuvre par le prestataire pour y répondre.

h) Il est recommandé que le prestataire mette en place un processus de gestion de crise en cas de détection d'un incident de sécurité majeur au sein de son service de détection.

i) Il est recommandé que le prestataire utilise des outils permettant de réaliser une analyse statique ou dynamique de fichiers suspects.

j) Dans le cas où le prestataire utilise des outils d'analyse statique ou dynamique de fichiers suspects faisant appel à des ressources hébergées sur Internet, le prestataire doit réaliser ces opérations hors du système d'information du service de détection des incidents de sécurité.

k) Il est recommandé que le prestataire fasse appel à un prestataire de réponse aux incidents qualifié (PRIS) afin de réaliser l'étude des fichiers suspects par une prestation d'investigation numérique sur périmètre restreint d'analyse de codes malveillants. Dans ce cas, le prestataire de détection des incidents de sécurité s'assurera que la portée de qualification du prestataire de réponse aux incidents inclut ce type de prestation.

Le prestataire est évalué sur ces exigences.

4. Amendement n°4 : exigences du chapitre IV.3.14. (Enclave de consultation au sein du système d'information du commanditaire)

Option A :

Le prestataire met en œuvre les exigences du chapitre IV.3.14. intitulé « Enclave de consultation au sein du système d'information du commanditaire » du référentiel cité en seconde référence et est évalué sur ces exigences.

Option B :

Le prestataire ne met pas en œuvre les exigences du chapitre IV.3.14. Enclave de consultation au sein du système d'information du commanditaire et met en œuvre les exigences suivantes :

a) L'intégralité des dispositifs pouvant accéder à la zone d'échange commanditaire depuis le système d'information interne du commanditaire doit être positionnée au sein d'une ou plusieurs enclaves de consultation au sein de ce système d'information.

b) L'enclave de consultation doit être homologuée au minimum au *Niveau Standard* du guide d'hygiène informatique de l'ANSSI [HYGIENE]. La mise en œuvre de la démarche d'homologation peut être de la responsabilité du commanditaire ou du prestataire.

Remarque : L'entité (prestataire ou commanditaire) en charge de l'homologation doit demander à l'autre entité les éléments de preuve de la mise en œuvre des mesures dont cette dernière a la responsabilité et les porter au dossier d'homologation.

c) Le prestataire doit définir avec le commanditaire dans la convention de service les responsabilités concernant :

- la propriété des dispositifs hébergés dans l'enclave de consultation ;

- l'administration et la mise à jour de ces dispositifs ;

- le responsable (commanditaire ou prestataire) de la démarche d'homologation de l'enclave.

Dans tous les cas, le commanditaire doit avoir la responsabilité de l'administration du dispositif de filtrage entre l'enclave de consultation et le système d'information interne du commanditaire.

d) Il est recommandé que l'entité en charge de l'homologation fasse appel à une prestation qualifiée d'audit de la sécurité des systèmes d'information par un PASSI pour la réalisation de l'audit dans le cadre de l'homologation.

e) Le dispositif intercalé entre une enclave de consultation et le système d'information interne du commanditaire doit assurer le caractère unidirectionnel des flux. Seuls sont acceptés les flux initiés depuis l'enclave de consultation, vers le système.

Le prestataire est évalué sur ces exigences.

5. Amendement n°5 : exigences du chapitre IV.5.1. (Qualité du service)

Option A :

Le prestataire met en œuvre les exigences du chapitre IV.5.1. intitulé « Qualité du service » du référentiel cité en seconde référence et est évalué sur ces exigences.

Option B :

Le prestataire ne met pas en œuvre les exigences du IV.5.1. Qualité du service et met en œuvre les exigences suivantes :

a) Il est recommandé que le prestataire soit certifié [ISO9001] sur le périmètre du service de détection des incidents de sécurité.

b) Le prestataire doit élaborer et mettre en œuvre un processus de capitalisation sur les incidents de sécurité détectés afin d'améliorer continuellement l'efficacité de son service de détection.

c) Le prestataire doit définir avec le commanditaire les indicateurs opérationnels et stratégiques du service de détection des incidents de sécurité. Ils comprennent les indicateurs minimaux spécifiés dans ce chapitre mais ne s'y limitent pas : le prestataire et le commanditaire peuvent convenir d'indicateurs complémentaires, adaptés au contexte de la prestation.

d) Il est recommandé que le prestataire utilise les indicateurs proposés dans [ETSI_ISG_ISI].

e) Le prestataire doit au minimum mettre en place les indicateurs opérationnels d'activité suivants :

- gestion des capacités de détection
    - le nombre d'alertes de sécurité détectées par mois ;
    - le nombre d'incidents avérés suite à une qualification par mois ;
    - le nombre de règles de détection implémentées dans les outils techniques d'analyse ;
    - le nombre de règles de détection créées, modifiées ou retirées par mois en fonction de l'origine de la demande (activité de veille, demande du commanditaire, etc.) ;
    - le classement des 20 règles de détection les plus déclenchées.
- gestion des incidents
    - le nombre de nouveaux tickets d'incidents ouverts par mois ;
    - le nombre de tickets d'incidents de sécurité clos par mois ;
    - le nombre de tickets ouverts cumulé par mois ;
    - la durée minimale, moyenne, maximale entre la création d'un ticket et sa clôture ;
- gestion des évènements

- le taux d'évènements non reconnus et donc non pris en compte par les outils techniques d'analyse ;
- le nombre de collecteurs ;
- le nombre d'évènements collectés par jour et par mois ;
- le nombre d'évènements collectés par collecteur par jour et par mois.

f) Le prestataire doit au minimum mettre en place les indicateurs opérationnels d'efficacité suivants :

- gestion des capacités de détection
  - le délai moyen de mise à jour des règles de détection suite à une demande du commanditaire ;
  - le temps de recherche moyen d'un indicateur de compromission, lors d'une recherche a posteriori, dans le système de stockage, par type d'indicateur de compromission.
- gestion des incidents
  - la durée moyenne des qualifications d'incident.

g) Le prestataire doit au minimum mettre en place les indicateurs stratégiques suivants :

- gestion des incidents
  - l'évolution du temps moyen de traitement des tickets d'incidents, par criticité, par mois ;
  - l'évolution du nombre de tickets d'incidents ouverts cumulé, par criticité, par mois ;
  - le nombre d'incidents avérés par mois pour le périmètre du service de détection du commanditaire.
- gestion des évènements
  - l'évolution du taux de couverture de collecte des journaux des équipements du parc identifiés dans la stratégie de collecte.

h) Le prestataire doit élaborer et tenir à jour un processus de mesure des indicateurs décrivant, pour chacun des indicateurs opérationnels et stratégiques fournis, les méthodes et moyens mis en œuvre par le prestataire pour mesurer l'indicateur.

i) Il est recommandé que le prestataire complète les indicateurs de ce chapitre par les indicateurs opérationnels d'activités suivants :

- gestion de l'infrastructure support du service de détection
  - le taux de remplissage des systèmes de stockage des incidents,
  - la capacité restante des systèmes de stockage des incidents,
  - le taux de disponibilité des dispositifs techniques du service de détection :
    - portail web de la zone d'échange commanditaire ;
    - dépôt relais de l'enclave de collecte ;
    - collecteur de l'enclave de collecte ;
    - système d'envoi des notifications d'incidents ;

        - outils techniques d'analyse.
    - gestion de la sécurité des interconnexions du SI du service de détection
        - le nombre d'échecs d'authentification et authentifications réussies ainsi que la liste détaillée associée concernant :
            - l'accès à la zone d'échanges commanditaire ;
            - l'accès depuis des postes nomades d'exploitation ;
            - l'accès depuis des postes nomades d'administration.
    - gestion des incidents
        - le nombre d'incidents créés selon le niveau de gravité de l'incident.
    - gestion des évènements
        - le nombre de sources de collecte par type d'équipement source ;
        - le nombre d'évènements transmis au système de stockage par jour et par mois ;
        - le taux de remplissage de chaque système de stockage des évènements, y compris les collecteurs dans l'enclave ;
        - la capacité restante de chaque système de stockage des évènements, y compris les collecteurs dans l'enclave ;
        - la capacité de rétention des collecteurs si la communication est impossible (lien réseau coupé par exemple) avec le collecteur supérieur (en volumétrie et en temps).
    - gestion des notifications
        - le nombre de comptes d'accès au portail web créés par mois,
        - le nombre de comptes d'accès au portail web supprimés par mois ;
        - le nombre de comptes autorisés à accéder au portail web et pouvant accéder aux informations du commanditaire.

j) Il est recommandé que le prestataire complète les indicateurs de ce chapitre par les indicateurs opérationnels d'efficacité suivants :
    - gestion des incidents
        - la durée moyenne des qualifications d'incident, par typologie d'incident et selon son niveau de gravité.
    - gestion des évènements
        - la durée minimale, moyenne, maximale entre la génération d'un évènement par la source de collecte et son stockage dans les systèmes de stockage des évènements.
    - gestion des notifications
        - la durée minimale, moyenne, maximale entre la détection d'un évènement de sécurité et la notification d'un incident associé, selon le niveau de gravité de l'incident.

k) Il est recommandé que le prestataire complète les indicateurs de ce chapitre par les indicateurs stratégiques suivants :

- gestion de la sécurité des interconnexions du SI du service de détection
    - l'évolution du nombre d'anomalies et incidents relevés concernant les différents accès externes au SI du service de détection ;
- gestion de l'infrastructure support du service de détection
    - l'évolution par mois du taux de disponibilité des dispositifs techniques du service de détection :
        - portail web de la zone d'échanges commanditaire ;
        - dépôt relais de l'enclave de collecte ;
        - collecteur de l'enclave de collecte ;
        - système d'envoi des notifications d'incidents ;
        - outils techniques d'analyse.

Le prestataire est évalué sur ces exigences.