	National Defence Défense Nationale		Retour à la liste des DED

DATA ITEM DESCRIPTION - DESCRIPTION DE DONNÉES

1. TITLE – TITRE	2. IDENTIFICATION NUMBER - NUMÉRO D'IDENTIFICATION
PLAN DE SURVEILLANCE CONTINUE	**DED 3.10.9**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

Le plan de surveillance continue a pour objet de détailler les processus, les procédures et les outils de détection et d'analyse pour une surveillance continue. Les activités de surveillance continue vont de la surveillance en temps réel (p. ex. détection des intrusions, analyse automatisée des journaux) à la surveillance à long terme (p. ex. évaluation de la vulnérabilité et des risques, vérification de la sécurité, etc.), qui est normalement effectuée hors ligne.
La préparation au confinement, à l'éradication et au rétablissement, ainsi que les activités post-incident doivent être couvertes dans le plan d'intervention en cas d'incident, LDEC 3.10.10.

4. APPROVAL DATE DATE D'APPROBATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE PREMIÈRE RESPONSABILITÉ (BPR)	6. GIDEP APPLICABLE APPLICABLE AU GIDEP
ÀD	Autorité technique (AT) de l'OSAN	S.O.

7. APPLICATION / INTERRELATIONSHIP – APPLICATION / INTERDÉPENDANCE

Consulter la LDEC 3.10.9 et le paragraphe 3.10.9 de l'EDT.
Cette DED énonce les instructions relatives au format et au contenu des données produites dans le contexte des tâches énoncées dans l'EDT pour le fonctionnement et l'entretien du Système d'alerte du Nord.

8. ORIGINATOR – AUTEUR	9. APPLICABLE FORMS – FORMULES PERTINENTES
AT OSAN	AUCUNE.

10. PREPARATION INSTRUCTIONS – INSTRUCTIONS SUR LA PRÉSENTATION DES DONNÉES

10.1 Document source

10.1.1 EDT de F et E du SAN section 3, paragraphe 3.10.9.
10.1.2 Processus d'assurance de la cybermission basé sur les risques.
10.1.3 U.S. National Institute of Standards (NIST) SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (doi: SP 800-137).

10.2 Contenu et format

10.2.1 Le plan de surveillance continue doit être préparé et livré selon le format de L'Entrepreneur.

10.2.2. L'Entrepreneur doit établir et mettre en œuvre un plan de surveillance continue à l'intention du Bureau du Système d'alerte du Nord. Le plan doit documenter au minimum ce qui suit :

a. Les énoncés de criticité de la mission à surveiller dans le cadre de la stratégie de surveillance continue de la sécurité.
b. Les circonstances, par exemple avant ou après les opérations militaires, déclenchées par le renseignement sur les menaces ou la détection d'anomalies, et les fréquences, par exemple annuelles, pour la surveillance et l'évaluation continue de la sécurité, doivent être établies.
c. Les activités de surveillance à mener doivent être établies et associées aux circonstances ou aux fréquences. Cela comprend les activités en temps réel (p. ex. détection des intrusions, analyse automatisée des journaux) et les activités hors ligne (p. ex. évaluation de la vulnérabilité et des risques, vérification de la sécurité, etc.).
d. Un plan comprenant les ressources, les outils, les conditions (circonstances et fréquences), les événements de cybersécurité surveillés et la documentation nécessaire à chaque activité de surveillance requise doivent être établis.

e. Lorsqu'ils sont déterminés ou détectés, les événements de sécurité doivent être analysés, catégorisés (incidents, vulnérabilités, menaces ou événements sans effets indésirables), signalés et documentés :
   i. Les incidents doivent donner lieu à une intervention en cas d'incident.
   ii. Les menaces et les vulnérabilités sans correctifs disponibles doivent voir leurs risques évalués.
   iii. La matrice de vulnérabilité et les rapports sur les menaces doivent être mis à jour.
   iv. Des stratégies d'atténuation doivent être proposées pour les risques relevés.
   v. Des décisions relatives aux risques (accepter, éviter, transférer ou atténuer) doivent être prises.

f. Une évaluation continue des risques doit être effectuée dans le cadre de la surveillance continue, y compris ce qui suit :
   i. Détermination, planification et réalisation d'activités d'essai cybernétique.
   ii. Mise à jour des énoncés de criticité de la mission, au besoin et chaque fois que des dépendances de mission changent et/ou que de nouveaux systèmes sont ajoutés.
   iii. Mise à jour de la description des biens.
   iv. Mise à jour de l'identification des vecteurs d'attaque.
   v. Mise à jour des menaces et vulnérabilités.
   vi. Mise à jour des risques.
   vii. Proposition de mesures d'atténuation.
   viii. Analyse des risques et des décisions.
   ix. Mise à jour des documents sur la sécurité.

10.2.3. Une matrice de références croisées doit être fournie dans ce document, laquelle montrera que les éléments énumérés ci-dessus sont couverts dans le document ou d'autres documents référencés.

10.2.4. La catégorisation de sécurité du plan de surveillance livrable continue doit être effectuée lors de la création du document, car le plan de surveillance continue, ou certaines de ses parties, pourraient être protégés. L'étiquetage et le marquage de sécurité, ainsi que la manipulation, l'entreposage et la transmission du plan de surveillance continue doivent être mis en œuvre conformément aux Ordonnances et directives de sécurité de la Défense nationale (ODSDN). Outre le marquage de sécurité, qui est placé dans l'en-tête et le pied de page de chaque page, un ensemble d'énoncés informatifs sera imprimé sur la couverture, ou la première page du document et, dans certains cas, également sur la page verso (au verso de la page de titre ou de la couverture) selon les besoins.

10.2.5. Il incombera à L'Entrepreneur de mener la gestion des changements, tel que décrit ci-dessous :
a. Le plan des principes de base de la cybersécurité doit comprendre une section sommaire de l'historique des modifications, qui renferme ce qui suit :
   i. Un identifiant clair et unique de la version/révision pour chaque soumission ou nouvelle soumission du plan des principes de base de la cybersécurité.
   ii. Une identification claire des révisions ou des modifications apportées au document par rapport à sa soumission précédente.
   iii. Le bien-fondé des révisions et des modifications.
b. Toutes les révisions/modifications mentionnées ci-dessus doivent être clairement définies dans le document à l'aide de la fonction de suivi des modifications appropriée du logiciel de traitement de texte utilisé pour produire le document, par exemple, fonction de « Suivi des modifications » dans Microsoft-Word®, barres latérales, etc.

Page 2 de 2
Décembre 2020