Rapport de la Réglementation
PDRIS

Prestataires de Détection des Incidents de Sécurité
Prestataires de Réponse aux Incidents de Sécurité

Verion 1 du 28 mars 2019

Mis en vigueur le 21 décembre 2017

I. Objectif du PRIS

PRIS qualifié mène des actions de remédiation rapides pour
- limiter les conséquences
- prévenir des incidents de sécurité graves

Le servie de rsponse aux incidents de sécurité est composé de plusieurs activités distinctes:
- définir une méthode de réponse aux incidents de sécurité adaptée au contexte
- rechercher, collecter et analyser les éléments issus du système d'information
- identifier le mode opératoire et l'objectif de l'attaquant
- qualifier l'étendue de la compromission
- aider à évaluer les risques et les impacts associés
- préconiser des mesures de remédiation

II. Objectif du PDIS

le service de détection des incidents de sécurité est composé de trois activités distinctes:
- la gestion des incidents: identifier,qualifier, stocker et capitaliser des incidents
- la gestion des évènements: recueillir et stocker des évènements
- la gestion des notifications: informer le commanditaire et stocker des notifications.

III. Processus de Prestation

- Détecter des vulnérabilités et des incidents de sécurité
- Qualifier les incidents
- Mettre en place des actions de remédiation contre les incidents de sécurité

IV. Différence entre PDIS et PRIS

- ➔ PRIS traite les activités de réactions et de remédiations aux incidents de sécurité hors périmètre du service de PDIS.
- ➔ PDIS traite les 3 activités: la gestion des incidents, la gestion des évènements et la gestion des notifications.

V.Qualification de Prestation de PDIS

Pour un prestataire, il faut respecter les exigences pour obtenir la qualification.

VI. Gestion des incidents de PDIS

- établir une liste des incidents redoutés et des impacts et conséquences
- prendre en compte les catégories d'incidents redoutés

- élaborer et mettre en œuvre une stratégie d’analyse
- définir et formaliser les règles de classification des incidents
- créer les règles de détection
- élaborer et mettre en œuvre la politique de remarquage des règles de détection
- élaborer et tenir à jour la liste de l’ensemble des règles de détection
- transmettre au minimum une fois par mois un bulletin d’état des règles de détection
- protéger le bulletin d’état des règles de détection
- implémenter dans les outils techniques d’analyse l’ensembe des règles de détection identifiées
- ajouter de manière autonome les règles de détection
- avertir le commanditaire et détailler les raisons de l’échec d’implémentation
- élaborer et tenir à jour la liste des ajouts de règles
- qualifier les incidents de sécurité détectés en vue d’apprécier leur veracité et leur niveau de gravité
- élaborer une échelle de gravité associée aux incidents redoutés
- réaliser des recherches en sources ouvertes à partir d’informations collectées ou des analyses
- utilieser des bases d’informations internes issues de sources ouvertes
- intégrer les résultats de tests de vulnérabilités et d’intrusion
- créer un ticket pour chaque incident de sécurité détectés et le mettre à disposition du commanditaire
- définir le format des tickets d’incidens de sécurité
- disposer d’un outil de gestion des tickets d’incidents de sécurité

VII. Gestion des évènements de PDIS

- élaborer et mettre en œuvre une stratégie de collecte
- identifier pour la stratégie de collecte la liste des sources de collecte, des collecteurs, des évènements à collecter, décrire les méthodes de collecte et identifier les fréquences de collecte
- collecter les évènements en provenance des sources de collecte
- collecter les évènements en provenance des équipements industriels
- journaliser les évènements identifiés
- faire évoluer la capacité de collecte
- avertir le commanditaire et détailler les raisons de l’echec
- exercer un devoir de conseil pour la stratégie de collecte
- sonder chacune des interconnexions du périmètre supervisé
- choisir des sondes qualifiées
- qualifier les équipements de type TAP
- opérer les sondes dédiées aux systèmes d’informations industriels
- élaborer et tenir à jour la liste de l’ensemble de règless de filtrage
- transmettre un bulletin d’état de règles de filtrage
- disposer d’une vision centralisée de l’ensembe des évènements collectés
- indexer l’ensembe des évènements collectés et réaliser des recherches parmi des évènements collectés
- localiser et fournir n’importe quel évènement collecté
- mettre en place un processus de gestion de la capacité de traitement et de stockage des évènements

VIII. Gestion des notifications de PDIS

- disposer de deux canaux d'informations
- disposer de deux moyens de notifications
- élaborer et mettre en œuvre la stratégie de notifications des incidents
- identifier la liste des incidents
- exercer un devoir de conseil pour la stratégie de notifications
- intégrer des notifications spécifiques
- contenir exclusivement le numéro de ticket dans la notification
- centraliser toutes les notifications dans un système de stockage de notifications
- fournir un ticket d'incident et le contexte associé
- mettre en place et tenir à jour un registre centralisé et chronologique
- mettre à disposition de portail web et dispositif de stockage

IX. Les types de PRIS

- la recherche d'indicateurs de compromission ou sabotage
- l'investigation sur périmètre restreint
- l'investigation sur large périmètre

X. Les activités de PRIS

- pilotage technique
- analyse réseau
- analyse système
- analyse des codes malveillants

XI. Les étapes exigées de PRIS

- qualification préalable d'aptitude à la réalisation de la prestation
- établissement d'une convention
- compréhension d'une situation et de l'environnement
- élaboration de la posture initiale
- préparation de la prestation
- exécution de la prestation
- restitutions
- élaboration du rapport d'analyse
- clôture de la prestation
- cas des enquêtes judiciaires