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

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

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

VI. Gestion des incidents

- 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