Le prestataire interviendra au sein du programme cybersécurité , et réalisera sa mission en collaboration avec le RSI et l'équipe SHIELD en charge des scans de vulnérabilités.

Il devra travailler en relation avec:

- les équipes DDO en charge de la remédiation (windows, linux, middleware…)

- les équipes CDS et les responsables de programme CARS clients

DDO: Direction des Operations

CDS: Centre des Services

RSI: Responsable de la Sécurité de l'Information

COSUV: Comités de Suivi des Vulnérabilités

Il participera aux points d'équipe hebdomadaires du programme Cybersécurité , aux COSUV (comités de suivi des vulnérabilités), et aux points de suivi spécifiques sur le sujet de la gestion des vulnérabilités.

1.Objectifs de la mission

DRC/SEC recherche un/une consultante pour:

- •Mettre en place le processus de gestion des vulnérabilités entre DDO, CDS et les clients
- •Assurer la gestion du changement avec DDO, CDS, et les clients
- •Documenter le processus mis en place
- •S'assurer du bon passage en RUN des processus (complétion de l'outillage splunk par les équipes, suivi des KPI)
- •Identifier les charges de RUN supplémentaires pour DDO et CDS
- •Etablir des reportings à plusieurs niveaux (opérationnel, client, stratégique…) sur l'avancement de la correction des vulnérabilités
- •Recueillir les besoins d'évolution de l'outillage
- •Mettre à jour la politique de gestion des vulnérabilités pour l'adapter aux processus mis en place si nécessaire

Le processus de gestion des vulnérabilités signifie détecter des vuls, qualifier des vuls et remédier/corréler des vuls. Et aussi établir et maintenir une base de données des vulnérabilités. Après ajouté un patch ou un petit morceau des codes, toujours suivre la gestion des changement avec DDO, CDS et les clients.

2. DESCRIPTION DE LA MISSION

Les fonctions à réaliser ou la description des lots

2.1 La prestation demandée concernera la mission suivante:

Mise en place des processus de gestion des vulnérabilités (*voir plus haut «objectifs de la mission»)*

2.2 Livrables attendus

L’accompagnement devra fournir les livrables suivants :

- Tableaux de bord et reporting
- Supports de présentation et comptes rendus de réunion
- Documentation des processus

Il y a des outils de gestion d’incidents: CR d’incidents, Tableaux de bord, Reporting ou autres fichiers bureautiques.

2.3 Compétences requises

La mission requiert:

- Pilotage et organisation
- Capacité d’analyse et esprit de synthèse
- Aisance relationnelle
- Rigueur
- Attitude dynamique et volontaire
- Connaissances de base sur sur la gestion des vulnérabilités et le patching
- Une connaissance de splunk ou ELK serait un plus

ELK signifie Elastisearch , Logstash et Kibana.

Logstash est un outil de collecte, analyse et stockage des logs. Il est généralement associé avec Elastisearch, Moteur de recherche distribué, et Kibana, Interface de ElasticSearch.