Parcours de cybersécurité

—

Cahier des charges

Eléments de contexte

Contexte

Dans le cadre du **volet cybersécurité de France Relance**, l'ANSSI propose aux structures publiques éligibles une offre de services appelée **Parcours de sécurité**.

Les Parcours de cybersécurité répondent aux besoins de mise à niveau du socle de sécurité des structures publiques. Ils se basent sur un cadre de services packagés définis par l'ANSSI, modulables afin d'adapter la démarche à chaque bénéficiaire : quatre parcours de maturité croissante ont été construits pour couvrir l'ensemble des bonnes pratiques à travers 120 mesures SSI.

Objet de l'accompagnement

Dans un premier temps de pré-diagnostic, l'ANSSI a effectué une première évaluation des enjeux et besoins de sécurisation du SI la structure bénéficiaire. Ces travaux ont permis de définir le contenu du **pack initial du Parcours de cybersécurité** qui sera suivi. Ce pack initial doit permettre de dresser un état des lieux complet des besoins de sécurisation SI et de définir une feuille de route, qui sera mise en œuvre dans un second temps sur la base de packs relais dont le contenu restera à définir.

L'objet de la prestation est la réalisation des différents travaux compris dans le pack initial tel que défini conjointement avec l'ANSSI.

Règles de partage des livrables

Les modalités de travail suivantes sont impératives :

- Les livrables sont à réaliser avec la suite MS Office ou toute solution compatible. Les supports de restitution sont à fournir dans ce format ainsi qu'au format PDF ;
- Les documents doivent faire l'objet d'échanges via un conteneur Zed! chiffré avec mot de passe.

Introduction

Ce document contient :

- Les travaux à réaliser dans le cadre du pack initial
- Les hypothèses de dimensionnement (nombre de réunions, …)
- Un planning indicatif
- La liste des documents fournis par l'ANSSI au prestataire terrain et au bénéficiaire en amont de la démarche
- L'estimation des charges nécessaires pour réaliser les travaux (pour le prestataire terrain et pour le bénéficiaire)

En PJ vous trouverez, mutualisés dans un même document :

- Le guide du prestataire terrain
- Le modèle du support de restitution au RSSI/DSI

Ces documents sont à joindre au cahier des charges afin de permettre au prestataire de mieux saisir les attentes de l'ANSSI concernant les travaux à réaliser.

ÉLÉMENTS DE STRUCTURE

Situé à l'est de l'Auvergne, le syndicat mixte du parc naturel régional Livradois-Forez s'étend sur trois départements : le Puy-de-Dôme, la Haute-Loire et la Loire. Aujourd'hui peuplé de plus de 103 000 habitants, il regroupe 163 communes. Territoire sans clôture, le Parc Livradois-Forez s'étend sur 300 000 hectares. C'est un des parcs naturels régionaux les plus étendu de France.

Véritable outil au service du territoire, le Parc a mis en œuvre des opérations de mutualisation avec différents acteurs institutionnels et partenaires du Livradois-Forez :

- SI Maison du Parc : 120 postes, VPN, cluster Hyper-V, 1 tenant O365 ,sauvegarde Veeam + serveur VmWare OVH.
- La maison du Tourisme : 9 sites, 5 postes informatiques au siège de la Maison du Parc, 30 sur les sites déportés, 1 tenant O365
- Cinéparc, Passeurs de mots, SFLF : infrastructure commune avec le PNR Livradois-Forez
- Mutualisation de serveurs hébergés Parcs naturels régionaux Auvergne Rhone-Alpes, cluster Proxmox (OVH)

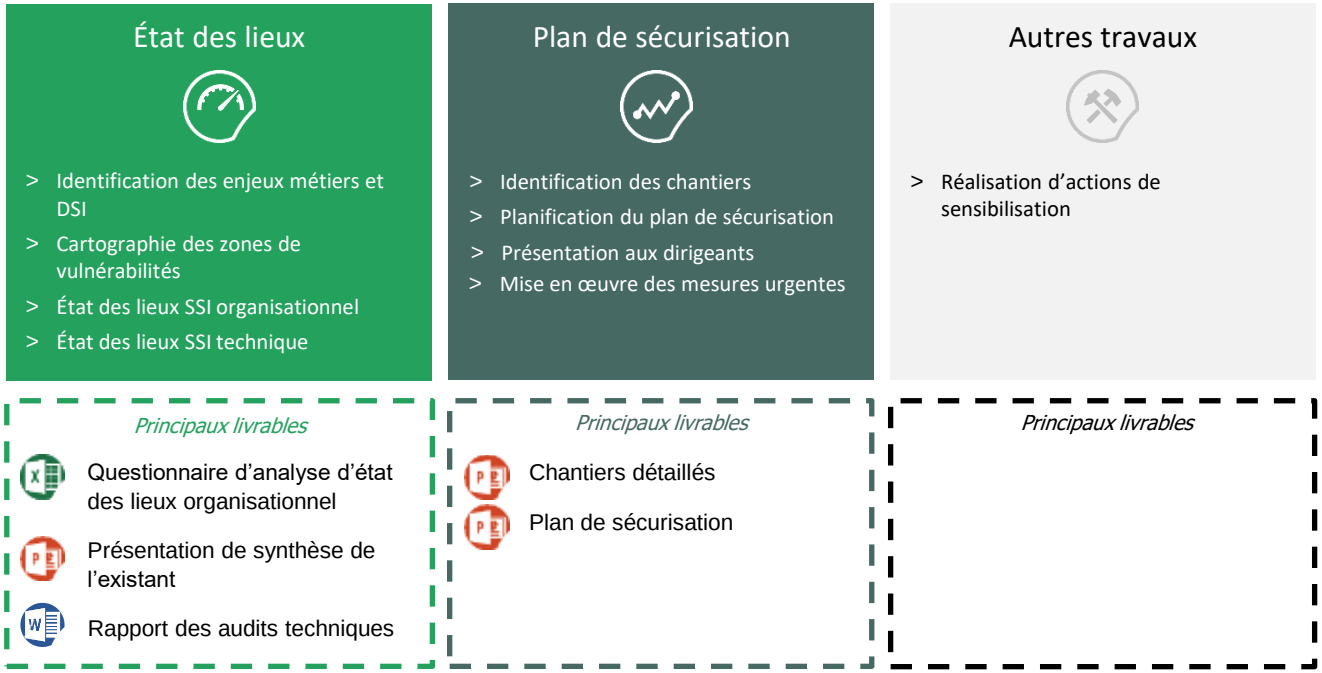
Fort d'un **parc machine de pas loin de 200 postes**, **une trentaine de serveurs virtualisés, dont 70 % exposés sur internet** et diverses applications métiers en mode SaaS ou On-Permise, le syndicat mixte du Parc et ses partenaires sont pleinement conscients des risques accrus liés aux cyber-attaques et souhaitent mettre à profit leur expérience de travail en commun pour améliorer la sécurité des systèmes d'informations.

Principales hypothèses retenues lors du cadrage du pack initial du parcours de cybersécurité

Hypothèses retenus ayant conduit à adapter la démarche type et son dimensionnement :

- Aucune

Démarche du diagnostic et de la formalisation du plan de sécurisation



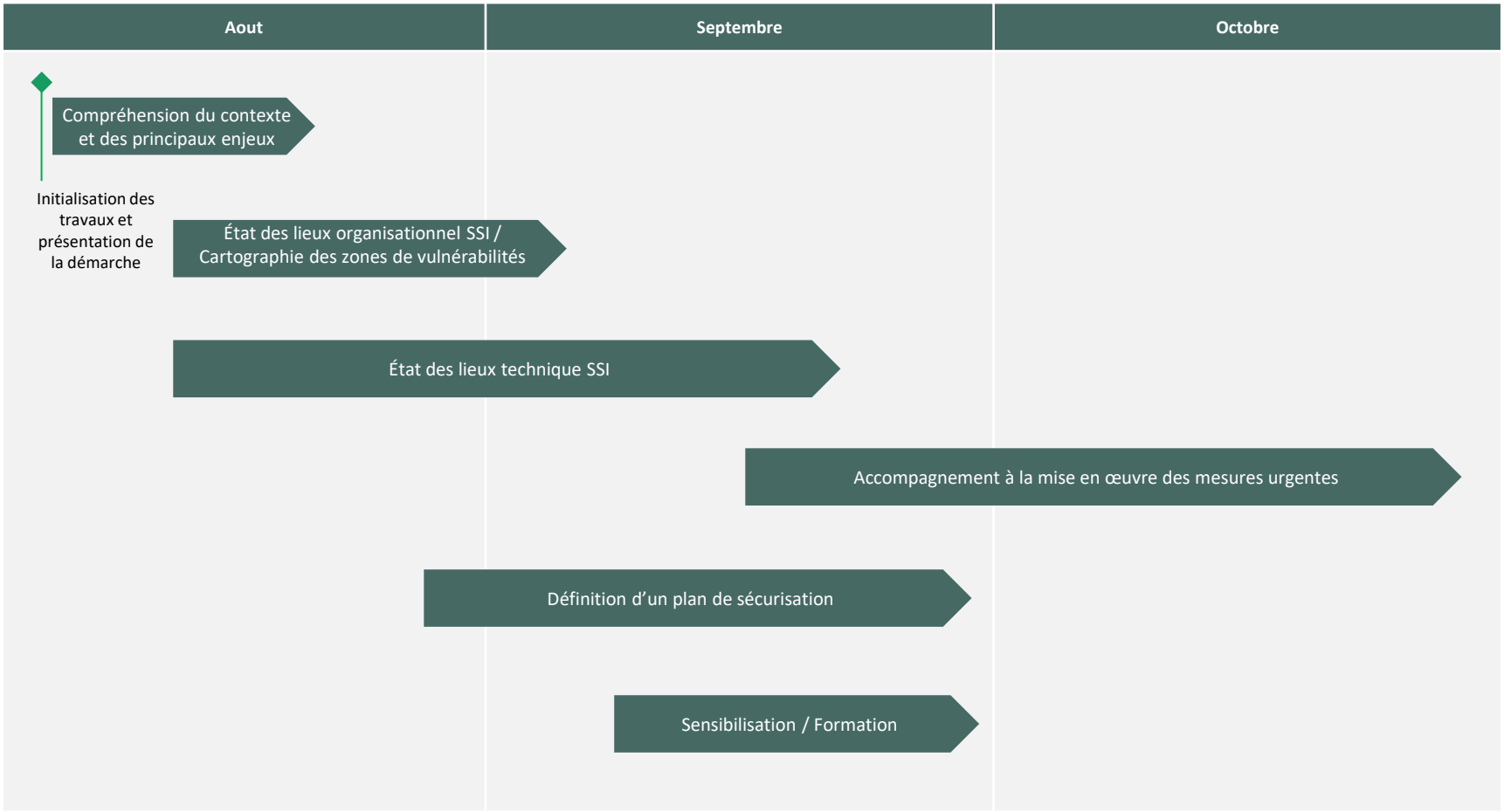
UN ÉTAT DES LIEUX GÉNÉRAL …

L'état des lieux est réalisé sur l'ensemble des mesures de sécurité, quel que soit le parcours cible du bénéficiaire, afin de pouvoir établir un **benchmark** entre toutes les entités.

… MAIS UN PLAN DE SÉCURISATION CIBLÉ

Le plan de sécurisation est quant à lui **adossé au parcours cible du bénéficiaire**, afin de définir des objectifs de cybersécurité qui soient à la fois **adaptés, raisonnables et atteignables**.

Planning estimatif du pack initial



Compréhension du contexte et des principaux enjeux

Objectifs

- Présenter le parcours cible
- Collecter la documentation existante
- Identifier et rencontrer les interlocuteurs métiers et SI
- Identifier les enjeux métiers et DSI

Livrables

- Questionnaire d'analyse de l'existant

Hypothèses

- 1 réunion de lancement
- 2 réunions de présentation du contexte et de compréhension des enjeux (1 réunion métier – 1 réunion DSI)

Activités principales

- **Initialisation des travaux et présentation de la démarche**
  - Présentation des objectifs, du planning et des livrables de la démarche suivie
  - Focus sur le parcours cible retenu et sur son contenu
  - Présentation par le bénéficiaire du contexte et collecte de la documentation existante pour analyse : organigrammes, référentiels, cartographies, schémas d'architecture, plans d'actions, rapport d'audits et de pentests, rapports d'incidents, rapport de la Threat Intelligence, PSSI, échelles de sécurité, plan de sécurisation de la DSI…
  - Identification des interlocuteurs pertinents à rencontrer et planification des entretiens pour la mise en œuvre de la démarche

- **Compréhension du contexte et des principaux enjeux**
  - En s'appuyant sur les travaux déjà réalisés lors de prestations précédentes :
    - Identification des principales activités métier du bénéficiaire, des infrastructures SI applicatives et techniques critiques pour l'activité du bénéficiaire ainsi que des évolutions métiers/évolution des pratiques à venir ayant un impact sur le SI
    - Echanges sur le plan de sécurisation de la DSI et identification des principales évolutions liées au SI du bénéficiaire prévues (Cloud, Agile, API, télétravail externalisation…)
    - Détermination des attentes des interlocuteurs métiers et SI vis-à-vis de la cyber sécurité
    - Identification des besoins de sécurité macroscopiques et détermination des principaux évènements redoutés et des impacts associés

Ressources industrialisées fournies au prestataire terrain afin de réaliser la démarche :

- **Initialisation** : Support Powerpoint d'initialisation complété
- **Compréhension du contexte et des principaux enjeux** : Support Powerpoint d'animation type de la réunion métier ; support Powerpoint d'animation type de la réunion DSI ; Guidelines de préparation et d'animation des réunions

État des lieux

Objectifs

- Faire un état des lieux du niveau de sécurité du bénéficiaire
- Produire une synthèse de l'existant (missions, besoins de sécurité, sources de risques, niveau de maturité)

Livrables

- Questionnaire d'analyse d'état des lieux organisationnel
- Rapport des audits techniques

Hypothèses

- 2 réunions pour l'état des lieux organisationnel
- 8 jours dédiés à l'état des lieux technique

Activités principales

- **État des lieux organisationnel SSI**
  - Réalisation d'un bilan de maturité organisationnel et technique déclaratif sur la base d'un questionnaire d'analyse
- **État des lieux technique SSI**
  - Accompagnement à la mise en œuvre par le bénéficiaire des outils d'audit de l'ANSSI (SILENE, et ADS)
  - Réalisation de travaux de scans de vulnérabilité (internes et externes), de tests d'intrusion, de revues de configuration, de revue d'architecture et de revue des processus d'exploitation du SI
  - Formalisation d'un rapport
  - *Les périmètres pressentis devant faire l'objet de l'état des lieux technique sont les suivants :*

- *Firewall externe : revue des règles (flux dangereux, non-utilisés)*
- *Test d'intrusion : site web exposés sur internet*
- *Revue de configuration et test d'intrusion de la brique VPN*
- *Revue de configuration sur office 365*
- *Revue de configuration et pentest sur un poste de travail*
- *Active Directory*
- *Revue de configuration des politiques de sauvegardes et résilience du SI*
- *Préconisation d'ouverture d'un second cluster*

Ressources industrialisées fournies au prestataire terrain afin de réaliser la démarche :

- **État des lieux organisationnel SSI :** Questionnaire type et grille de notation (Excel) ; guidelines de préparation et d'animation des réunions
- **État des lieux technique SSI :** Guidelines

Plan de sécurisation SSI - Construction

Objectifs

- Identifier et prioriser les actions/chantiers à mettre en œuvre
- Définir un plan de sécurisation à l'horizon 2022 pour compléter le parcours

Livrables

- Cartographie du SI et de ses zones de vulnérabilités
- Chantiers détaillés
- Plan de sécurisation

Hypothèses

- 1 réunion de construction et validation de priorisation des actions/chantiers SSI
- 1 réunion de construction et de validation du plan de sécurisation

Activités principales

- **Cartographie des zones de vulnérabilités**
  - Cartographie macroscopique du SI du bénéficiaire et mise en évidence de ses principales zones de vulnérabilité
- **Synthèse de l'analyse de l'existant et détermination et analyse des actions/chantiers composant le plan de sécurisation SSI**
  - En fonction des constats réalisés lors de l'état des lieux et du parcours cible identifié pour le bénéficiaire, identification des actions/chantiers à mettre en œuvre et caractérisation de la typologie (Gouvernance, poste de travail, infrastructure, applications, serveurs/Datacenters, conformité), de la complexité, des prérequis/adhérences, des acteurs impliqués
  - Priorisation des actions/chantiers (actions immédiates, court terme, moyen terme), incluant les priorités en terme réglementaire et en évaluant notamment pour chaque chantier/action la charge de réalisation et de l'apport en termes de réduction du risque (ratio coût/efficacité)
  - Eventuels arbitrages et validation de de la priorisation
- **Planification du plan de sécurisation SSI**
  - Construction d'un plan de sécurisation à horizon 2022, consolidant les actions/chantiers par paliers et les positionnant dans le temps
  - Identification des mesures urgentes faisant l'objet d'un accompagnement à la mise en œuvre dans la suite des travaux

Ressources industrialisées fournies au prestataire terrain afin de réaliser la démarche :

- **Cartographie des zones de vulnérabilités :** Exemple Powerpoint de cartographie ; guidelines de formalisation de la cartographie
- **Synthèse de l'analyse de l'existant et détermination et analyse des actions/chantiers composant le plan de sécurisation, Planification du plan de sécurisation SSI :** Fichier Excel de construction de la feuille de route ; guidelines de préparation et d'animation des réunions

Plan de sécurisation SSI - Restitution

Objectifs

- Présenter une synthèse de l'existant (missions, besoins de sécurité, sources de risques, niveau de maturité, …) et du plan de sécurisation

Livrables

- Support de restitution
- Support de présentation aux dirigeants

Hypothèses

- 1 réunion de présentation
- 1 réunion de sensibilisation/restitution aux dirigeants

Activités principales

- **Restitution de l'état des lieux et du plan de sécurisation**
  - Présentation des missions principales du bénéficiaire, de leurs principaux besoins de sécurité et des principaux événements redoutés associés
  - Présentation des principaux scénarios stratégiques de risques du bénéficiaire, de la cartographie macroscopique de son SI ainsi que de son écosystème et de leurs vulnérabilités
  - Synthèse de l'analyse du niveau de maturité (états des lieux organisationnels et techniques) et comparaison aux autres organisations tirée du benchmark de l'ANSSI
  - Restitution et validation du plan de sécurisation sécurité
- **Restitution / Sensibilisation SSI aux dirigeants**
  - Présentation des menaces visant le bénéficiaire et d'attaques réelles ayant eu lieu
  - Présentation des principaux enjeux de l'entité
  - Présentation de la synthèse managériale de l'état des lieux et d'un benchmark
  - Présentation du plan de sécurisation
  - Présentation des bonnes pratiques à mettre en œuvre par les équipes dirigeantes et par l'ensemble des agents

Ressources industrialisées fournies au prestataire terrain afin de réaliser la démarche :

- **Restitution de l'état des lieux et du plan de sécurisation :** Support Powerpoint de restitution type ; guidelines de préparation et d'animation de la restitution
- **Restitution / Sensibilisation SSI aux dirigeants :** Support Powerpoint de restitution type ; guidelines de préparation et d'animation de la restitution

Plan de sécurisation SSI – Mise en œuvre des mesures urgentes

Objectifs

- Apporter l'expertise nécessaire à la mise en œuvre des mesures jugées urgentes suite à l'état des lieux et la définition du plan de sécurisation

Hypothèses

- 2 jours dédiés à la mise en œuvre des mesures urgentes

Activités principales

- **Accompagnement à la mise en œuvre des mesures urgentes**
  - Accompagnement des équipes du bénéficiaire à la mise en place des actions rapides (correction de configuration, fermeture de services inutiles, protocoles obsolètes, etc.) permettant de corriger les vulnérabilités (systèmes exposés, configuration de la messagerie, de l'AD par exemple) identifiées lors de l'état des lieux

Ressources industrialisées fournies au prestataire terrain afin de réaliser la démarche :

- **N/A**

Sensibilisation

Objectifs

- Réaliser des actions de sensibilisation et de formation des agents du bénéficiaire
- Accompagner la définition de la stratégie de sensibilisation du bénéficiaire

Livrables

Hypothèses

- 1 réunion de sensib. des admins du SI
- 1 réunion de sensib. des développeurs
- 1 réunion de sensibilisation des agents des services RH
- 1 réunion de formation du référent SI

Activités principales

- **Sensibilisation SSI des administrateurs du SI**
  - Présentation des menaces visant le bénéficiaire, de chemins d'attaque réels et des bonnes pratiques à mettre en œuvre par les équipes d'administration du SI
- **Sensibilisation SSI des développeurs**
  - Présentation des menaces visant le bénéficiaire liées aux développements, de chemins d'attaque réels et des bonnes pratiques à mettre en œuvre dan le cadre des développements
- **Sensibilisation SSI des agents services RH**
  - Présentation des menaces visant le bénéficiaire et d'attaques réelles ayant eu lieu et des bonnes pratiques à mettre en œuvre par les équipes RH
- **Formation SSI du référent SI**
  - Présentation des notions et concepts clés liés à la SSI

Ressources industrialisées fournies au prestataire terrain afin de réaliser la démarche :

- **Sensibilisation SSI des administrateurs du SI, des agents biomédicaux, des développeurs, des agents des services RH, des agents du service achats, des agents de l'organisation :** Support Powerpoint de sensibilisation type ; guidelines de préparation et d'animation de la présentation
- **Formation SSI du référent SI : S**upport Powerpoint de formation type ; guidelines de préparation et d'animation de la présentation

Modalités de travail

Format des livrables

/ Les livrables sont à réaliser avec la suite MS Office ou toute solution compatible. Les supports de restitution sont à fournir dans ce format ainsi qu'au format PDF

Modalités de communication

/ Utilisation d'un conteneur Zed! chiffré avec mot de passe

Modalités de pilotage

/ Des réunions téléphoniques pourront être organisées si besoin

Pilotage des travaux par le prestataire accompagnateur

Objectifs

- Accompagner le bénéficiaire dans la mise en œuvre du pack initial et des éventuels packs relais suivants

Hypothèses

- 1 réunion d'échange avant la restitution avec le prestataire terrain
- 1 réunion d'échange sur les travaux menés et restant à mener avec le bénéficiaire

Activités principales

- **Au lancement du pack initial**
  - Présentation à la fois au prestataire terrain et au bénéficiaire des hypothèses de cadrage des travaux à réaliser et des charges associées
- **Pendant les travaux**
  - Traitement des sollicitations du bénéficiaire en cas de problématique liée à la qualité des travaux
  - Traitement des sollicitations du prestataire terrain en cas de questions liées à la démarche ou de glissement envisagé dans les charges et le planning par rapport aux hypothèses initiales
  - Dans les 2 cas, échanges avec le prestataire terrain et le bénéficiaire et enfin organisation si nécessaire d'une réunion tri partite avec, si nécessaire, un représentant de l'ANSSI
  - Echange avec le prestataire terrain pour vérifier la cohérence des travaux avec le plan de sécurisation définie par l'ANSSI
- **Restitution des travaux**
  - Participations aux réunions de restitution prévues dans le cadre de la démarche
- **Après les travaux**
  - Echange avec le bénéficiaire pour vérifier sa satisfaction et déterminer ses attentes dans le cadre des packs relais

Ressources industrialisées fournies au prestataire terrain afin de réaliser la démarche :

- **Pilotage des travaux :** Outillage Excel de pilotage des prestations ; guidelines d'utilisation de l'outillage

Estimation des charges nécessaires au prestataire terrain à la réalisation des travaux

Travaux réalisés	Charges estimées (en j/h)
Contexte, enjeux, état des lieux organisationnel et plan de sécurisation	16
Etat des lieux technique	8
Sensibilisation	4
Mise en œuvre des mesures urgentes	2
Total	30

Estimation des charges nécessaires au bénéficiaire à la réalisation des travaux d'état des lieux et de définition du plan de sécurisation

Interlocuteurs	Charges estimées (en j/h)
Métiers	0,5
DSI	2
Equipe SSI	3,5
Dirigeants	0,5
Total	6,5