RÉPUBLIQUE FRANÇAISE

DEPARTEMENT
du
VAL D'OISE

ARRONDISSEMENT

D'ARGENTEUIL

COMMUNE
D'ERMONT

Accusé de réception en préfecture
095-219502192-20250205-2025-014-DE
Date de télétransmission : 07/02/2025
Date de réception préfecture : 07/02/2025

EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS DU CONSEIL MUNICIPAL DE LA COMMUNE D'ERMONT

SÉANCE DU 05 FÉVRIER 2025

L'an deux mille vingt-cinq, le cinq du mois de février à 19 H 00

OBJET : ATTRACTIVITE DU TERRITOIRE ET CADRE DE VIE
Approbation de la souscription au lot 4 Interconnexions, Internet, Infrastructures Systèmes, Réseaux et Télécommunications, Sécurité des Systèmes d'Information (marché 2020100) dans le cadre du groupement de commande avec le SIPPEREC

N°2025/014

Le Conseil Municipal dûment convoqué par Monsieur le Maire, le ***29 janvier 2025***, s'est assemblé au lieu ordinaire de ses séances sous la présidence de ***M. Xavier HAQUIN.***

Présents :
M. Xavier HAQUIN, ***Maire***
M. BLANCHARD, M. NACCACHE, Mme MEZIERE, M. LEDEUR, M.RAVIER, Mme CASTRO-FERNANDES, Mme CHESNEAU MUSTAFA, ***Adjoints au Maire***

M. CARON, Mme APARICIO TRAORE, M. ANNOUR, Mme DEHAS, Mme GUEDJ, Mme GUTIERREZ, Mme BENLAHMAR, M. GODARD, M. LAROZE, Mme YAHYA, Mme DE CARLI, Mme LAMBERT, M. KNOBLOCH, Mme CAUZARD, M. HEUSSER, Mme LACOUTURE, Mme BARIL, M. PERROT, M. MELO DELGADO, M. BAY, M. KHINACHE, Mme DAHMANI, ***Conseillers Municipaux***

Absents excusés ayant donné pouvoir :

Mme DUPUY	(pouvoir à M. HAQUIN)
Mme LEMARCHAND	(pouvoir à Mme DEHAS)
Mme SANTA CRUZ BUSTAMANTE	(pouvoir à M. BLANCHARD)
M. KEBABTCHIEFF	(pouvoir à Mme CASTRO FERNANDES)
Mme THYS	(pouvoir à M. GODARD)

Le nombre des Conseillers Municipaux en exercice est de 35 (la condidtion de quorum est de 18 membres présents).

Déposée en Sous-Préfecture le : 07/02/25
Publiée le : 12/02/25

Le Maire,

MAIRIE D'ERMONT 2e Val d'Oise

Les Conseillers présents formant la majorité des membres en exercice, conformément à l'Article L. 2121-15 du Code Général des Collectivités Territoriales, il a été procédé à la nomination d'un secrétaire pris dans le sein du Conseil : ***M. KNOBLOCH*** ayant obtenu la majorité des suffrages, a été désigné pour remplir ces fonctions qu'il a acceptées.

Délais et voies de recours :
Si vous désirez contester la présente décision, vous pouvez saisir le Tribunal Administratif de Cergy –Pontoise compétent d'un recours contentieux dans les deux mois à partir de la notification de la décision attaquée. Vous pouvez également saisir d'un recours gracieux, l'auteur de la décision. Cette démarche prolonge le délai de recours qui doit alors être introduit dans les deux mois suivant la réponse (l'absence de réponse au terme des deux mois valant rejet).

Délibération N° 2025/014

OBJET :
ATTRACTIVITE DU TERRITOIRE ET CADRE DE VIE
Approbation de la l'adhésion au lot 4 Interconnexions, Internet, Infrastructures Systèmes, Réseaux et Télécommunications, Sécurité des Systèmes d'Information (marché 2020100) dans le cadre du groupement de commande avec le SIPPEREC

Sur la proposition du Maire,

VU le Code Général des Collectivités Territoriales, notamment son article L.2121-29 ;

VU le Code de la commande publique ;

VU la délibération n°2019/15 du Conseil municipal du 13 février 2019 relative à l'adhésion à la centrale d'achat « SIPP'n'CO » ;

VU l'avis de la Commission Attractivité du territoire et Cadre de vie du 21 janvier 2025 ;

CONSIDÉRANT l'adhésion de la Commune d'Ermont au SIPPEREC depuis 2005 et à sa centrale d'achat en 2019 ;

CONSIDERANT les missions du lot 4 « Interconnexions, Internet, Infrastructures Systèmes, Réseaux et Télécommunications, Sécurité des Systèmes d'Information » de cette centrale d'achat ;

CONSIDÉRANT que la candidature de la commune d'Ermont a été retenue dans le cadre du parcours sécurité (audit des installations et travaux de mise en conformité et renforcement de la sécurité) de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), autorité nationale en matière de cybersécurité et le versement de subventions pour les deux phases de ce parcours ;

CONSIDÉRANT que l'ANSSI valide le versement de sa subvention pour la phase « audit des installations » par la société Orange Cyberdéfense, principal prestataire du SIPPEREC pour la mise en œuvre du lot 4 de sa centrale d'achat « Interconnexions, Internet, Infrastructures Systèmes, Réseaux et Télécommunications, Sécurité des Systèmes d'Information » ;

CONSIDÉRANT que la souscription à ce marché permettrait à la Commune d'Ermont de bénéficier de services supplémentaires tels que la location de liens fibrés dits « fibre noire », la transition vers la fin des technologies à support cuivré et la résolution des problématiques liées à l'interconnexion réseau et téléphonique,

Après en avoir délibéré,
LE CONSEIL MUNICIPAL

- **APPROUVE** la souscription au lot 4 « Interconnexions, Internet, Infrastructures Systèmes, Réseaux et Télécommunications, Sécurité des Systèmes d'Information » (marché 2020100) dans le cadre du groupement de commande avec le SIPPEREC ;
- **AUTORISE** le Maire à signer tout document y afférent.

MAIRIE D'ERMONT 2 Val d'Oise

Pour extrait conforme,

Le Maire,
Conseiller départemental du Val d'Oise,
Xavier HAQUIN

Orange
Cyberdefense

MAIRIE D'ERMONT 2 Val d'Oise

annexé à
délibération n° 25/014 du 05/02/25
ERMONT, le 07/02/25
Le Maire,

Pack Initial

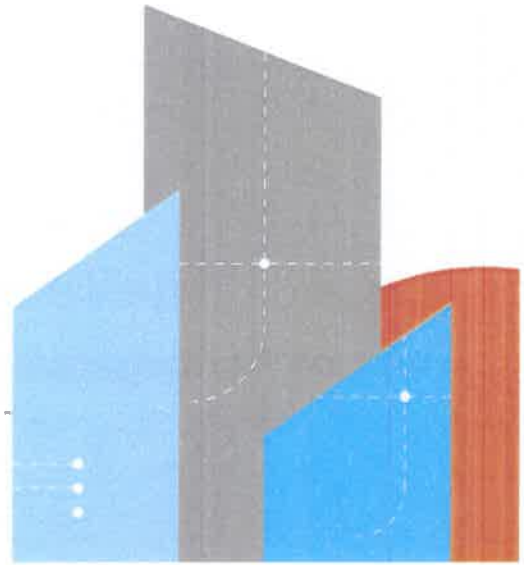
Ville d'Ermont

Proposition technique et commerciale

Marché SIPPEREC - Accord cadre n°2020100
Services de sécurité des infrastructures de communications électroniques

Confidentiel
15 octobre 2024

FRANCE RELANCE



orange™

Cabinet de conseil spécialisé en Gestion des Risques et Sécurité de l'Information, la division Conseil et Audit d'Orange Cyberdefense propose son savoir-faire et son expertise à la ville d'Ermont pour la conduite du pack initial du plan de sécurisation FRANCE RELANCE.

VOS CONTACTS

Romain BOUCHER

Ingénieur Commercial

Mobile : +33 6 38 48 38 86
E-mail : romain.boucher@orange.com

Massyl AIT-MOHAND

Ingénieur Avant-Vente Ethical Hacking

Mobile : +33 6 07 80 33 43
E-mail : massyl.aitmohand@orange.com

Florian GUERIN

Ingénieur commercial

Mobile : +33 6 74 05 63 86
E-mail : florin.guerin@orange.com

Youness BENCHRIFA

Expert cybersécurité

Mobile : +33 6 81 92 25 74
E-mail : youness.benchrifa@orange.com

Sommaire

Orange Cyberdefense, en bref

En tant que leader européen de prestations de services de sécurité, nous vous accompagnons dans le monde entier.

1.072 Milliard CA 2023

+ 11% de Croissance

+ de 3000
experts pluridisciplinaires dédiés à la cyber sécurité

+ 8 500
clients dans le monde, sur tous les secteurs d'activité

Qualifié

PASSI
PDIS
PRIS

Reconnu « **Very Strong** » dans le rapport MSS Competitive Landscape

GlobalData.

+ de 500
sources alimentent en permanence notre base de threat intelligence datalake

Reconnu « **Leader**» dans le rapport 2022 European MSS Wave

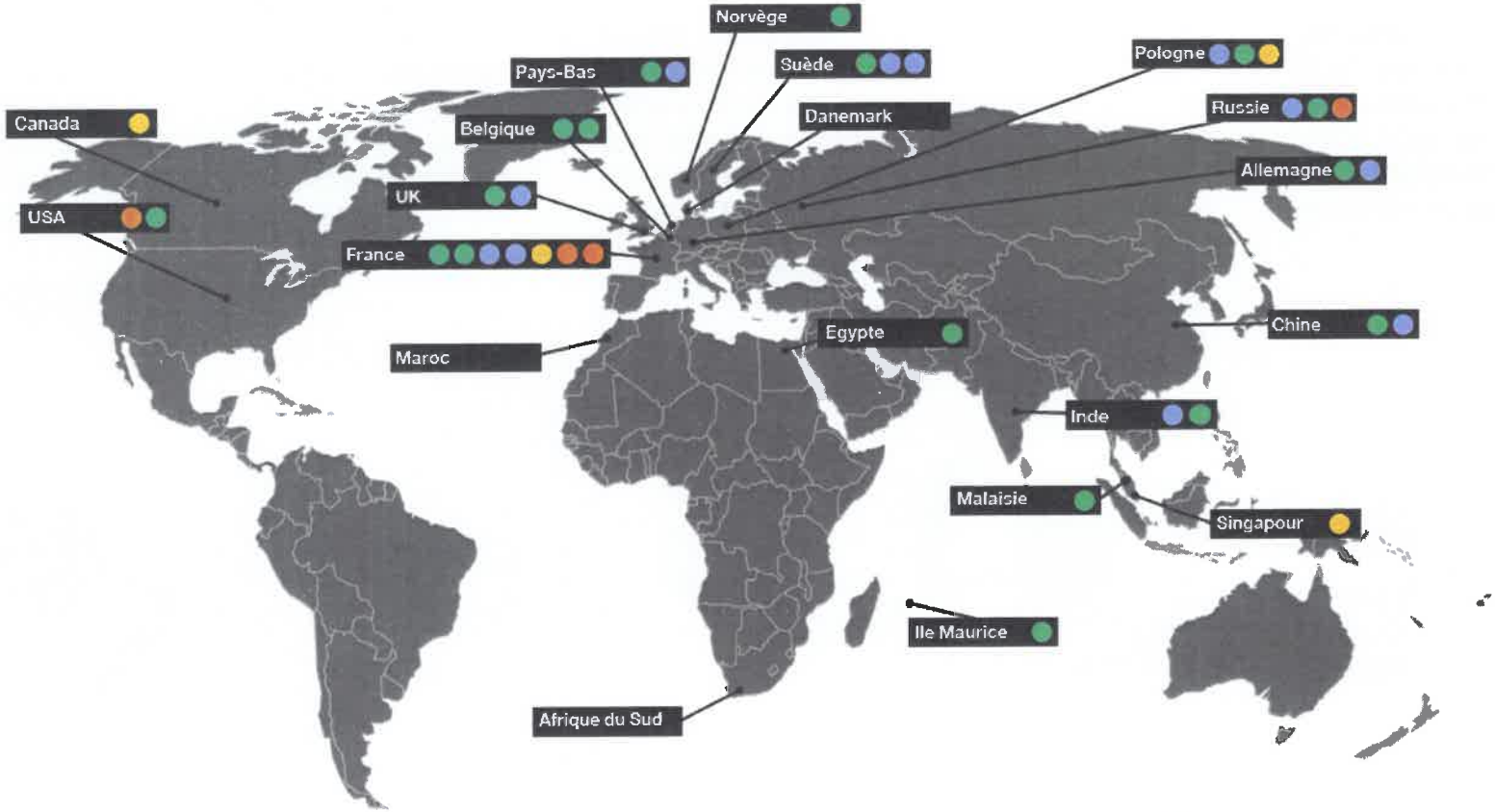
FORRESTER

24/7/365
Capacité de services en « *Follow the Sun* »

Inclus dans 5 guides Gartner des meilleurs acteurs en : Managed Detection and Response, Incident Response and Digital Forensics, OT Security, Threat Intelligence & Managed Security Services

Gartner

Leader européen avec une présence mondiale.



17 SOC répartis dans le monde qui réagissent aux évènements en 24/7/365

11 CyberSOC qui analysent la menace en 24/7/365

4 CERT qui opèrent en continu

4 Scrubbing Centers pour réduire les attaques DDoS

Notre expertise pour vous accompagner en 360

Anticiper

Connaître et anticiper les menaces émergentes, pouvoir les caractériser et anticiper leur évolution.

Identifier

Identifier vos expositions face aux risques, avoir une bonne vision de vos intérêts et priorités. Prévenir, former et sensibiliser.

Protéger

Protéger vos actifs critiques au travers d'un arbitrage sur les choix de solutions techniques et le budget à associer.

Détecter

Surveiller, détecter et analyser les événements de sécurité.

Réagir

Intervenir en cas de crise avérée et réagir à l'incident : le comprendre, le contenir et y remédier.

Orange Cyberdefense

Nos pôles de compétences Conseil & Audit

Audit et Contrôle de conformité

Procède à un état des lieux du niveau de sécurité, évalue la conformité du SI vis-à-vis d'une norme / réglementation, propose un plan d'action priorisé

Gouvernance et pilotage de la cybersécurité

Définit les standards de sécurité, met en place et pilote les SMSI, intègre la sécurité dans les projets IT. Propose la gouvernance du SI et des projets par les risques, accompagne le RSSI

Droit de la cybersécurité et conformité réglementaire

Prend en compte les obligations légales et réglementaires (GDPR, réglementations sectorielles, gestion des traces/preuves, chartes, contrats…)

Conseil technologique en sécurité

Propose des études de cadrage, de choix technologiques, accompagne l'organisation RFP (SIEM, DLP, vulnérabilité assessment, IDS…)

Sécurité du cloud

Accompagne et évalue la sécurité des environnements Cloud sur l'ensemble des modèles IaaS/PaaS/CaaS/FaaS/SaaS, sur les aspects à la fois techniques et organisationnels

Cyber résilience

Cartographie les actifs sensibles. Propose et déploie un dispositif organisationnel, fonctionnel et technique permettant d'assurer la continuité en cas de crise majeure (ex : sinistre, cyberattaque, etc.). Exerce et forme les acteurs.

Formation et sensibilisation

Définit et met en œuvre un cadre de formation à la sécurité ou des mesures de sensibilisation selon une stratégie répondant à vos objectifs.

Sécurité des SI industriels et IoT

Sensibilise à la cybersécurité, audite et matérialise les risques cyber dans le secteur industriel, propose des plans d'action et accompagne à la mise en conformité (LPM).

La recherche et le renseignement sur la menace font partie de notre ADN.

Nos experts surveillent les dernières menaces et vulnérabilités, ce qui vous permet de garder une longueur d'avance sur la menace et de prioriser ce qu'il est essentiel de protéger.






+250
experts dédiés à la l'innovation et à la recherche sur la menace.

20%
du temps de nos auditeurs-pentesteurs est dédié à la recherche.

50
jours d'avance dans la détection des menaces.

+80
publications et articles soutenus lors de conférences cyber l'an dernier.

2500
indicateurs IOC* connus d'aucune autre source alimentent notre base de Threat Intelligence.

30
CVE** nous sont attribués par le MITRE***.

* Indicator Of Compromise, utilisés pour la détection des tentatives d'attaques
** Common Vulnerability Exposure: failles de sécurité découvertes, répertoriées par le MITRE
*** MITRE organisme supervisant la liste des CVE


Sommaire

Contexte, périmètre et objectifs

CONTEXTE

- Conscient de la nécessité de protéger son activité, ses utilisateurs et son image dans un contexte d'évolution des cybermenaces et de renforcement des contraintes réglementaires, vous nous avez sollicité pour vous faire accompagner dans la mise en œuvre du pack initial de l'offre France Relance portée par l'ANSSI.

- Cet accompagnement s'articulera principalement autour de 2 aspects :
  - La réalisation d'un état des lieux de la sécurité de votre SI
  - La formalisation d'un plan de sécurisation incluant la définition d'une stratégie de sensibilisation et l'organisation de sessions de sensibilisation au profit de populations identifiées

PÉRIMÈTRE

- L'accompagnement portera sur l'ensemble votre Système d'Information et vos activités
- Il s'agira de notamment traiter :
  - De l'organisation et de la gouvernance
  - Des outils et de l'architectures
  - Des pratiques de sécurité

OBJECTIFS

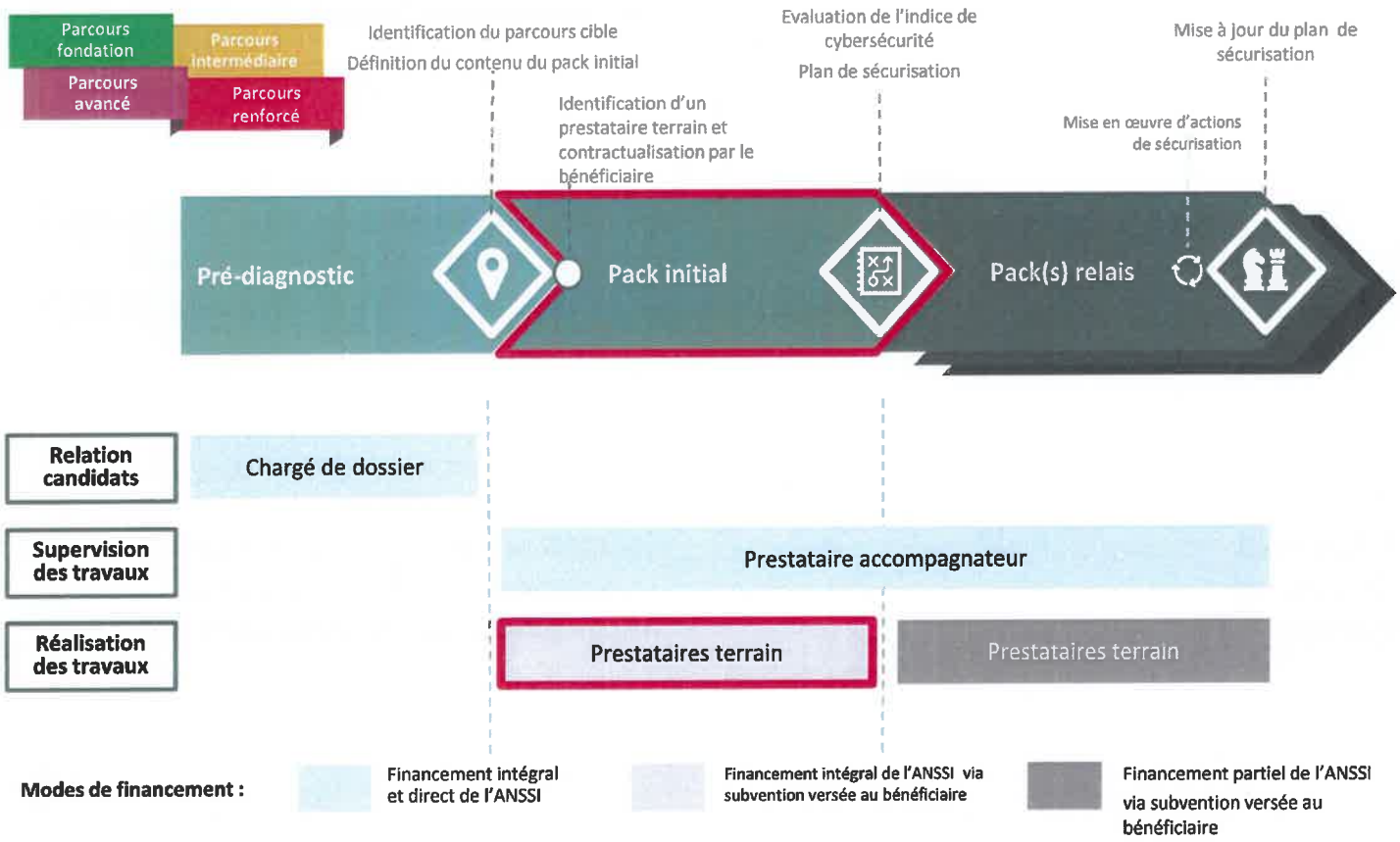
Etat des lieux sécurité

- **Identifier les besoins et enjeux** en matière de sécurité des systèmes d'information, pour déterminer la cible à atteindre
- **Réaliser un état des lieux organisationnel et technique** des pratiques, architectures et solutions de sécurité en place, et mesurer l'écart vis-à-vis de la cible
- **Construire une cartographie des risques** permettant d'identifier ses zones de vulnérabilités

Plan de sécurisation SSI

- **Consolider** les travaux d'analyse de l'existant, déterminer et analyser les chantiers afin de construire le plan de sécurisation du SI
- **Accompagner** la commune d'Ermont dans la mise en œuvre des mesures urgentes identifiées lors de l'état des lieux sécurité
- **Définir** une stratégie de sensibilisation des personnels répondant aux exigences propres à votre contexte

Le dispositif France Relance est structuré en trois phases



La prestation proposée correspond à la partie « Pack Initial » du « Prestataires terrain »

Pourquoi choisir Orange Cyberdefense ?

Une **expertise** et des **savoir-faire reconnus**, par des grandes structures comme par de petites entités

Un **acteur local**, prêt à vous accompagner au quotidien et à être **présent à vos côtés** pour tous les jalons importants

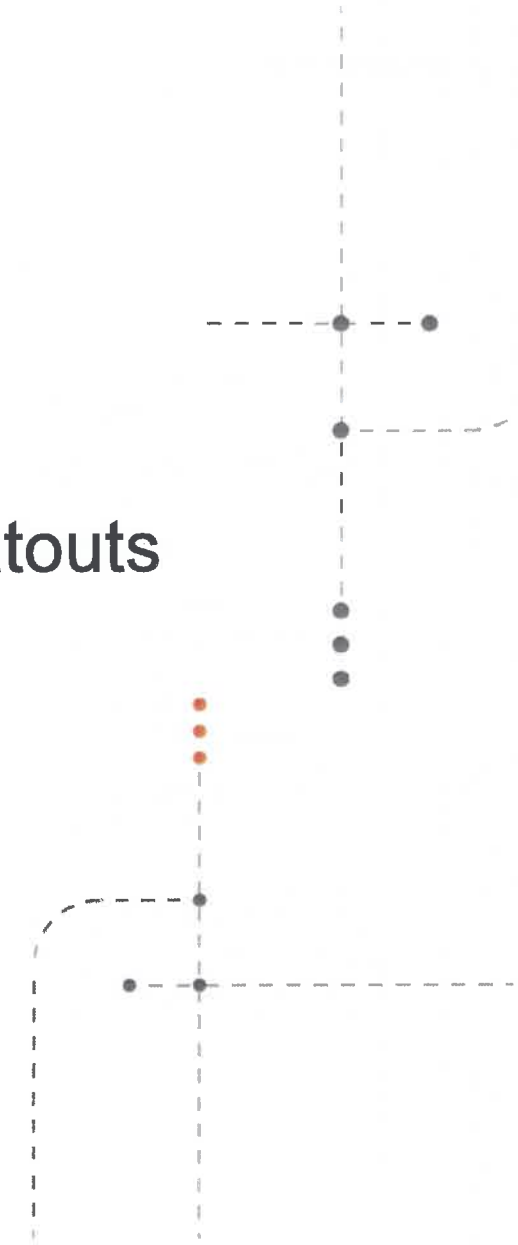
La **force et les ressources d'un grand groupe**, alliés à la **flexibilité d'une petite structure**

Une **démarche bien cadrée**, à la fois **rigoureuse et efficace**

De **nombreuses références de missions similaires** mais aussi **complémentaires**, chez des acteurs de toutes tailles, publics comme privés

Une capacité à **vous accompagner sur ce sujet et au-delà**, sur la **mise en œuvre de vos projets**

Sommaire



Démarche générale

PHASE 1 : Compréhension du contexte et des enjeux	PHASE 2 : Diagnostic organisationnel et technique	PHASE 3 : Construction du plan de sécurisation SSI	PHASE 4 : Restitution	PHASE 5 : Mise en œuvre des mesures	PHASE 6 : Sensibilisation
▪ Réaliser la réunion de lancement ▪ Identifier le contexte et les enjeux métiers	▪ Réaliser un état des lieux organisationnels ▪ Réaliser un état des lieux techniques ▪ Cartographier les zones de vulnérabilités	▪ Consolider les résultats. ▪ Elaborer d'un plan d'actions. ▪ Consolider et planifier les actions	▪ Restituer les conclusions de l'état des lieux à l'équipe projet ▪ Restituer / sensibiliser l'équipe dirigeante aux questions de sécurité	▪ Accompagner à la mise en œuvre des mesures urgentes	▪ Sensibiliser les administrateurs du SI, des agents service RH et des agents du service achats ▪ Rédiger le plan de sensibilisation
PHASE 1 : LIVRABLES	**PHASE 2 : LIVRABLES**	**PHASE 3 : LIVRABLES**	**PHASE 4 : LIVRABLES**	**PHASE 5 : LIVRABLES**	**PHASE 6 : LIVRABLES**
Support d'initialisation Contextes et enjeux de la structure	Rapport d'audit organisationnel et technique Cartographie des zones de vulnérabilités.	Plan d'actions consolidé	Restitution de l'étude	CR d'intervention	Plan de sensibilisation

Détail de la phase 1

Compréhension du contexte et des enjeux

OBJECTIFS

- Lancer le projet et impliquer l'ensemble des acteurs concernés
- Valider les éléments indispensables à l'atteinte des objectifs fixés
- Identifier le contexte et les enjeux métiers principaux du client

DÉMARCHE

- La réunion de lancement réunit les acteurs et permet :
  - De présenter les objectifs, le planning et les livrables
  - D'échanger sur le cadrage de la mission, sa motivation, et ses enjeux
  - D'identifier et de collecter les éléments d'entrée
  - D'identifier les tests techniques à réaliser
  - D'identifier et planifier les entretiens pertinents à réaliser
- A l'issue de cette réunion, Orange Cyberdefense organisera des ateliers de présentation du contexte et de compréhension des enjeux. Au cours de ces points, nous pourrons :
  - Déterminer les besoins sécurité et les principales menaces
  - Identifier les attentes métier vis-à-vis de la cybersécurité
  - Relever les principaux actifs critiques du client (actuels ou à venir)
  - Echanger sur les plans de sécurisation et les évolutions SI et SSI à venir

LIVRABLES

- Support d'initialisation
- Contextes et enjeux de la structure

POINTS D'ATTENTION

- Une réunion de lancement (1h)
- 2 à 3 réunions de présentation du contexte et de compréhension des enjeux (2h)
- La liste des personnes à rencontrer lors des ateliers sera finalisée avec vous durant la réunion de lancement

Détail de la phase 1

Exemples de documents utiles à l'analyse documentaire

Documents utiles pour l'analyse documentaire
▪ Organigramme métier / DSI ▪ Documents de sécurité (politiques, chartes, procédures, etc.) ▪ Cartographie physique et logique du réseau ▪ Inventaire et/ou cartographie des applications ▪ Résultats de précédentes analyses de risques IT ▪ Résultats de précédents audits de sécurité ▪ Rapports d'incidents de sécurité ▪ Plan de sauvegarde ▪ Présentation de sensibilisation à la sécurité du SI ▪ Plan de sensibilisation de la DSI ▪ Echelles de sécurité ▪ Et/ou tout autre document jugé pertinent pour le déroulement de la mission

Détail de la phase 2

Etape 1 : Diagnostic organisationnel

OBJECTIFS

- Etude de l'existant organisationnel

DÉMARCHE

- La prise de connaissance de l'existant est réalisée sur la base de réunions de travail, le recueil de la documentation, en se basant sur questionnaire de maturité France Relance
- Entretiens individuels ou groupes de travail (en fonction de votre organisation) pour :
  - Recueillir les informations nécessaires à l'étude (usage de questionnaires)
  - Valider et compléter éventuellement les informations recueillis
  - Identifier les manques et réactualiser la liste des composants à diagnostiquer
- Analyse de la documentation existante (Cf. page précédente)
- Analyse des résultats
  - En fonction des enjeux et des objectifs de sécurité la phase d'entretiens permet de déterminer le différentiel entre le niveau de sécurité cible et celui qui est constaté

LIVRABLES

- Questionnaire complété

POINTS D'ATTENTION

- Orange Cyberdefense s'appuiera sur les modèles de documents fournis par l'ANSSI
- 4 réunions prévues (d'environ 2 heures) pour l'audit organisationnel

Détail de la phase 2

Etape 1 : Etat des lieux organisationnel

- *Utilisation du questionnaire France Relance (240+ questions)*

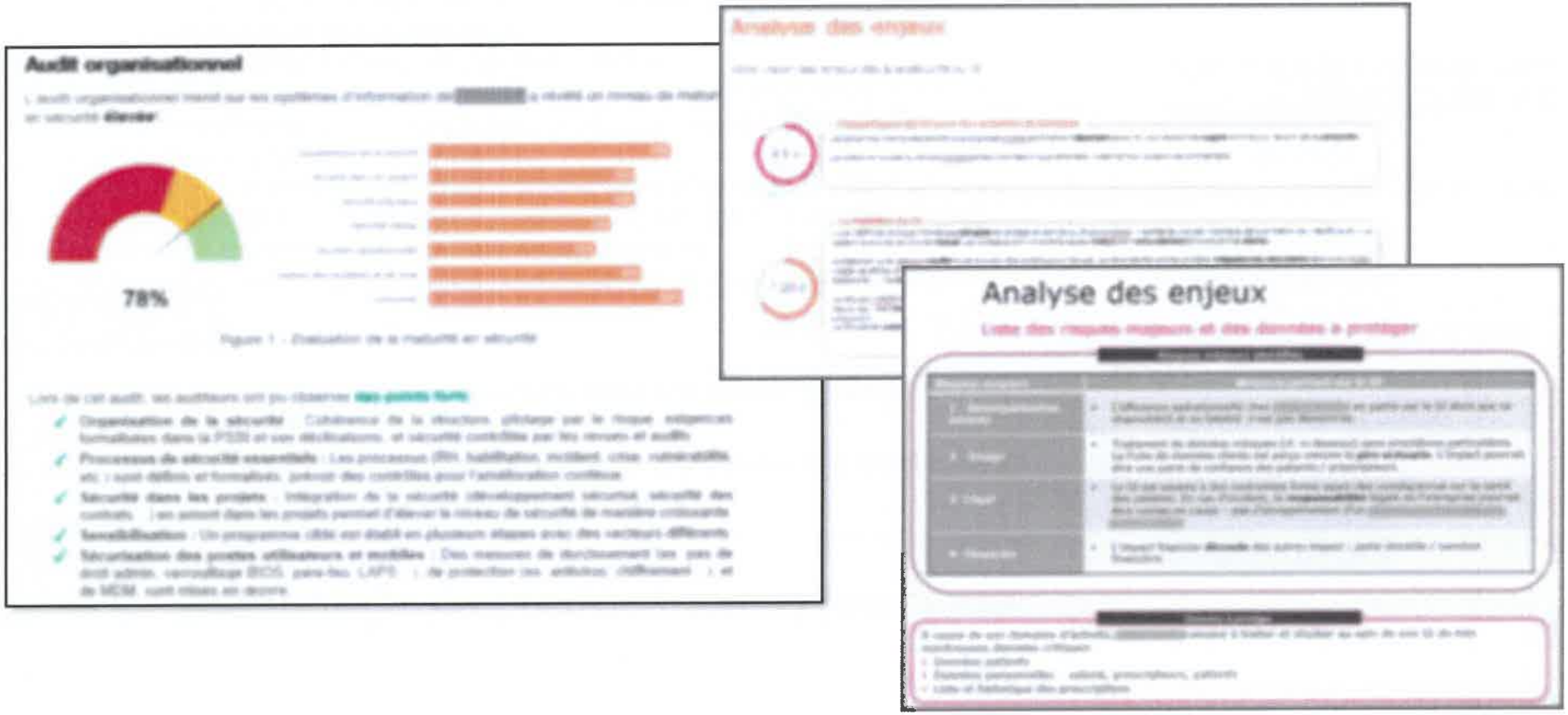
Volet cyber de France Relance : Questionnaire d'analyse d'état des lieux organisationnel

Réf	Catégorie	Question	Coef.	Fondation	Interm. et -	Avancé et -	Renforcé et -	Commentaires amélioration continue	Score actuel	Score après plan d'actions P0/P1	Score après plan d'actions total	Aide à la notation	Commentaire
1	Rôles et les responsabilités en matière de cybersécurité	Qui est le responsable de la Sécurité des Systèmes d'Information au sein de votre organisation ?	4									0 : Personne ne traite le sujet +0,2 : Le DSI est responsable de facto de la SSI +0,6 : Un Référent SSI est nommé +1 : Un RSSI (Responsable SSI) est nommé	
2		A qui est rattaché le RSSI ?	2									0 : Pas de RSSI +0,4 : Le RSSI dispose de moyens et d'appui hiérarchique pour faire appliquer et respecter ses décisions +0,6 : RSSI est rattaché à un niveau hiérarchique proche du niveau décisionnel (e.g. N-1 du DSI)	
3		Quelles sont les ressources en ETP (Equivalent Temps Plein) dédiées à la réalisation des activité de cybersécurité ? *(n'inclut pas les administrateurs des infrastructures)*	4									0 : Ratio de 1ETP SSI pour plus de 2000 agents +0,2 : Ratio de 1ETP SSI pour 2000 agents ou moins +0,4 : Ratio de 1ETP SSI pour 1600 agents ou moins +0,8 : Ratio de 1ETP SSI pour 1200 agents ou moins +1 : Ratio de 1ETP SSI pour 800 agent ou moins	
4		Avez-vous des ressources dédiées à la sécurité opérationnelle ?	4									0 : Aucun ETP n'est totalement dédié à la sécurité opérationnelle 1 : Ratio de 1ETP SSI dédié à la sécurité opérationnelle pour	
5		Avez-vous identifié formellement les processus SSI *(e.g. gestion des incidents, gestion des sauvegardes, gestion des mises à jour, gestion des vulnérabilités, ...)* à mettre en œuvre au sein de votre organisation ? Avez-vous déterminé les compétences, les rôles et responsabilités associés ? Les responsabilités ont-elles été réparties entre les équipes (par exemple au travers d'un RACI) ?	2									0 : Les processus SSI à mettre en œuvre ne sont pas identifiés +0,2 : Les processus SSI sont partiellement identifiés +0,5 : Tous les processus SSI sont identifiés +0,3 : Les rôles, compétences et responsabilités par processus SSI sont identifiés +0,2 : Les responsabilités ont été attribuées au sein des	

Détail de la phase 2

Etape 1 : Etat des lieux organisationnel

Exemple de livrables complémentaires pour la synthèse des enjeux et l'état des lieux organisationnel



Détail de la phase 2

Etape 2 : Diagnostic technique / test d'intrusion

OBJECTIFS

- Fournir un diagnostic complémentaire sur la surface d'exposition aux risques depuis l'interne ou l'extérieur
- Evaluer ce(s) composant(s) supplémentaire(s) dans une optique d'Ethical Hacking

DÉMARCHE

- Les approches techniques choisies seront discutées lors de la réunion d'initialisation :
  - Diagnostic technique sur 5 à 10 adresses IP publiques.
  - Cette prestation permet d'identifier les services disponibles dans des conditions identiques à celles d'un attaquant souhaitant s'introduire dans le réseau du client
  - Diagnostic technique sur un SI interne
    - Le diagnostic a pour but d'évaluer la sécurité interne de l'entreprise
    - L'auditeur explore le réseau local depuis une prise réseau et tente d'accéder aux serveurs, services ou données protégées
    - Périmètres et actions prioritaires :
      - Cloisonnement interne et interconnexions entre réseau Ecole et réseau Mairie
      - Active Directory
      - Tentative d'élévation de privilège et de mouvement latéraux
      - Accès aux serveurs et données critiques

PERIMETRE

- SI de la mairie d'Ermont

LIVRABLES

- Rapport du diagnostic identifiant les failles identifiées

POINTS D'ATTENTION

- Le périmètre et la nature des tests techniques seront affinés lors de la réunion de lancement
- 10 jours sont prévus au diagnostic technique

Détail de la phase 2

Etape 2 : Diagnostic technique / test d'intrusion

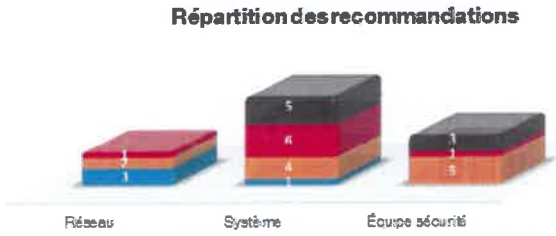
- *Analyse technique : exemple de synthèse*

Points positifs

Points positifs	Commentaires
Points d'accès WIFI : Vérification de l'identité du serveur	Les postes clients sont configurés pour vérifier que les points d'accès XXX et XXX présentent un certificat valide. C'est une configuration conforme aux bonnes pratiques.

Points à améliorer

Points à améliorer	Commentaires
Gestion de l'obsolescence et des mises à jour	De très nombreux éléments non à jour ou même obsolètes ont été identifiés sur le système d'information. De plus un très grand nombre d'entre eux sont impactés par des vulnérabilités critiques publiquement documentées, facilement exploitable et parfois connues pour être exploitées par des malwares.
Gestion des comptes	De nombreux manquement aux bonnes pratiques liées à la gestion des comptes utilisateurs et administrateurs ont pu être notés. Il s'agit entre autre de comptes utilisateurs administrateur de leur poste, des nombreux comptes administrateurs du domaine et plus globalement de comptes avec des mots de passe faibles ou par défauts.
Accès sans restriction à des éléments sensibles	Des interfaces d'administration accessibles sans authentification ou avec des comptes par défaut permettre de prendre le contrôle total des serveurs concernés.



Détail de la phase 2

Etape 2 : Diagnostic technique / test d'intrusion

- *Analyse technique : exemple de détail de vulnérabilité*

Comptes et mots de passe faibles

Critique		
Titre	Comptes et mots de passe faibles	TB- 17
Périmètre	Réseau interne XXX	
Description	Les consoles d'administration des serveurs sont accessibles et possèdent des mots de passe triviaux (faibles ou par défaut).	
Probabilité	Menace / Vulnérabilité / Probabilité d'exploitation	
	Facilité technique d'exploitation — Facilité de découverte	Probable
Impact	Impact technique	Impact global
	Disponibilité, Intégrité, Confidentialité, Preuve	Critique

Recommandations		
Court terme	Responsable	Difficulté
Modifier les mots de passe des comptes et mettre en place un changement systématique des mots de passe par défaut.	Système	

Description

L'utilisation de mots de passe forts est l'une des briques de base dans la sécurisation d'un système d'information.

Cependant cette étape est souvent oubliée, ainsi il est fréquent de trouver des comptes avec des mots de passe triviaux, sans mot de passe ou avec des mots de passe par défaut.

Un mot de passe fort est un mot de passe qui est difficile à retrouver, même à l'aide d'outils automatisés.

La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules.

État constaté

Lors de la réalisation des tests, nous avons constaté les éléments suivants :

Service	Login	Mot de passe	Hôtes
Tomcat	admin	admin	XXXX:8080
Tomcat	tomcat	tomcat	XXXX:8080
Application X	admin	admin	XXXX:8100

Figure 30 - Accès à l'interface d'administration Tomcat

Risques

Le risque principal est qu'un attaquant qui soit en mesure d'obtenir des informations de connexion valides puisse compromettre l'application et le système sous-jacent (ex. : déni de service, falsification des données, compromission d'autres comptes, etc.), voir les scénarios d'intrusion.

Recommandations

À court terme, tous les mots de passe faibles ou par défaut doivent être changés. À moyen terme, il est recommandé de passer en revue l'ensemble des consoles d'administration accessibles afin de limiter les accès aux seules personnes autorisées (cloisonnement réseau par exemple) et de mettre en place une politique de complexité des mots de passe. En général, pour un administrateur le mot de passe doit être au moins de 12 caractères (alphanumériques et spéciaux).

De plus, sur le long terme, il est nécessaire d'utiliser un système d'authentification forte par le biais d'un token RSA ou d'un certificat client. Ce système requiert au moins deux facteurs d'authentification (le mot de passe et le certificat client par exemple) et empêchera les attaques de brute forces permettant en générale de trouver les mots de passe faibles.

Détail de la phase 2

Etape 3 : Cartographie des zones de vulnérabilités

OBJECTIFS

- Fournir une cartographie des zones de vulnérabilités techniques et organisationnelles

DÉMARCHE

- Sur la base des éléments techniques et organisationnels identifiés, Orange Cyberdefense complète et détaille la cartographie des zones de vulnérabilités du Système d'Information du client
- Cette cartographie est soumise au client pour échange et validation

LIVRABLES

- Cartographie des zones de vulnérabilités

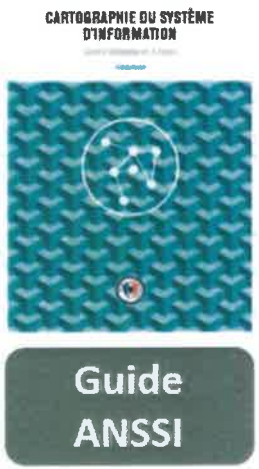
POINTS D'ATTENTION

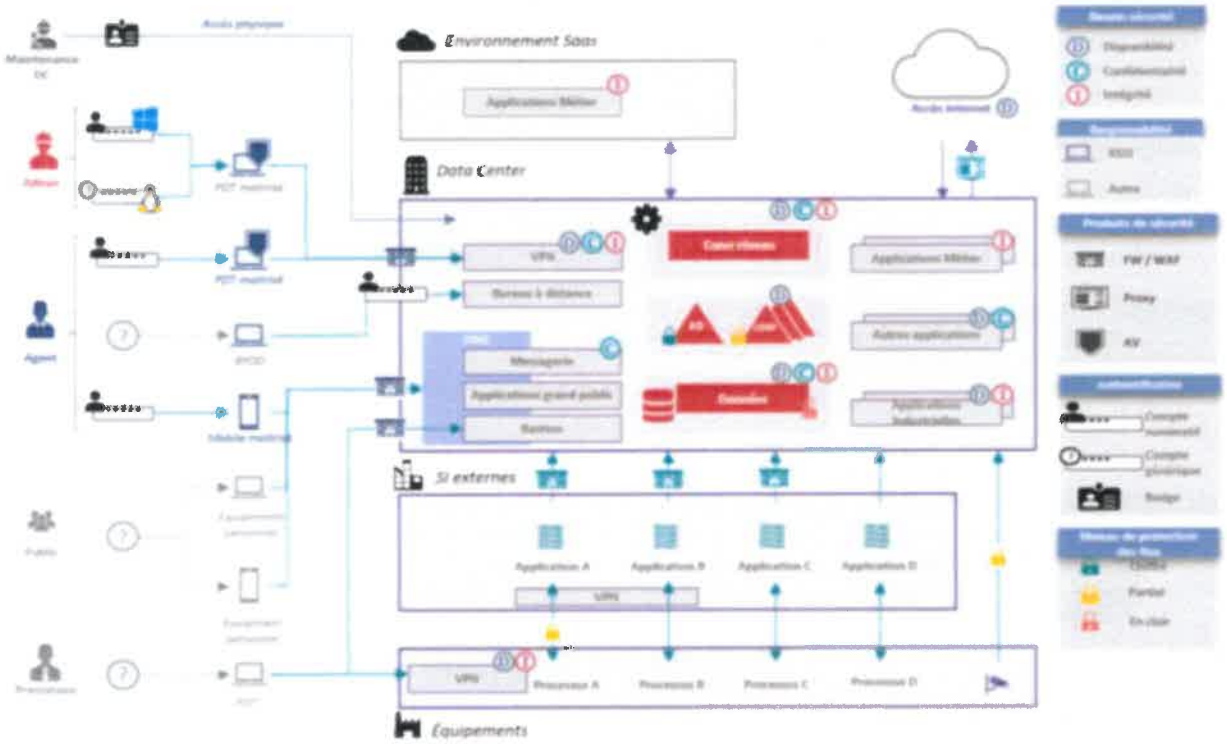
- 1 atelier de validation de la cartographie
- Orange Cyberdefense s'appuiera sur le modèle de cartographie fourni par France Relance

Détail de la phase 3

Etape 3 : Cartographie des zones de vulnérabilités

- *Exemple de cartographie s'appuyant sur le guide de référence de l'ANSSI*





Détail de la phase 3

Définition du plan de sécurisation SSI

OBJECTIFS

- Consolider les résultats
- Intégrer et planifier les actions dans le plan de sécurisation SSI
- Elaborer le plan de sécurisation

LIVRABLES

- Plan de sécurisation

DÉMARCHE

- Elaboration d'un plan de sécurisation :
  - Analyse du niveau de maturité suite aux diagnostics organisationnels et techniques
  - Identification des actions correctives à mettre en œuvre (durée, contraintes techniques/organisationnelles, charges financières, ordonnancement)
  - Identification des « quick wins »
  - Priorisation et planification des chantiers selon leur criticité sur le SI
  - Construction et validation du plan de sécurisation avec la commune d'Ermont

POINTS D'ATTENTION

- 2 à 3 réunions de construction et validation de priorisation des actions/chantiers SSI (2h)
- 1 à 2 réunions de construction et de validation du plan de sécurisation (2h)
- Orange Cyberdefense s'appuiera sur les modèles de documents fournis par le prestataire accompagnateur

Détail de la phase 3

Définition du plan de sécurisation SSI

- *Modèle du plan de sécurisation SSI France Relance*

Volet cyber de France Relance

Réf	Chantier	Rappel de la question	Fondation	Interm. et -	Avancé et -	Renforcé et -	Actions	Priorité	Complexité	Coûts projet		Coûts récurrents	
										Charges (j.h)	Invest. (k€)	Charges (j.h)	Invest. (k€)
1	Rôles et les responsabilités en matière de cybersécurité	Qui est le responsable de la Sécurité des Systèmes d'Information au sein de votre organisation ?						P0	+	90	xx k€	xx j.h.	xx k€
2		A qui est rattaché le RSSI ?						P1	++	40 - 50			
3		Quelles sont les ressources en ETP (Equivalent Temps Plein) dédiées à la réalisation des activité de cybersécurité ? *(n'inclut pas les administrateurs des infrastructures)*						P2	+++	5			
4		Avez-vous des ressources dédiées à la sécurité opérationnelle ?						P3					
5		Avez-vous identifié formellement les processus SSI *(e.g. gestion des incidents, gestion des sauvegardes, gestion des exceptions, gestion des vulnérabilités...)* à mettre en œuvre au sein de votre organisation ? Avez-vous déterminé les compétences, les rôles et responsabilités associés ? Les responsabilités ont-elles été réparties entre les équipes (par exemple au travers d'un RACI) ?											
6		Par quelle moyens la disponibilité des ressources compétentes liées à la SSI est-elle garantie *(e.g. redondance des ressources internes, appel à des prestations...)* ? Y a-t-il des périodes sans compétences SSI au sein de l'organisation (suite à des congés par exemple) ? Des astreintes sont-elles mises en place en heures non ouvrées ?											

Détail de la phase 4

Restitution

OBJECTIFS

- Restituer les conclusions de l'état des lieux à l'équipe projet
- Restituer / sensibiliser l'équipe dirigeante aux questions de sécurité

LIVRABLES

- Restitution de l'étude
- Sensibilisation des dirigeants

DÉMARCHE

- Présentation des résultats à l'équipe projet :
  - Missions principales, besoins de sécurité et évènements redoutés
  - Résultats de l'évaluation des risques.
  - Synthèse de l'analyse du niveau de maturité SSI
  - Restitution et validation du plan de sécurisation SSI
- Présentation des résultats et sensibilisation à la SSI pour l'équipe dirigeante :
  - Synthèse managériale de l'état des lieux organisationnel et technique
  - Menaces sur le SI et cas d'attaques réelles
  - Plan de sécurisation SSI
  - Présentation des bonnes pratiques SSI

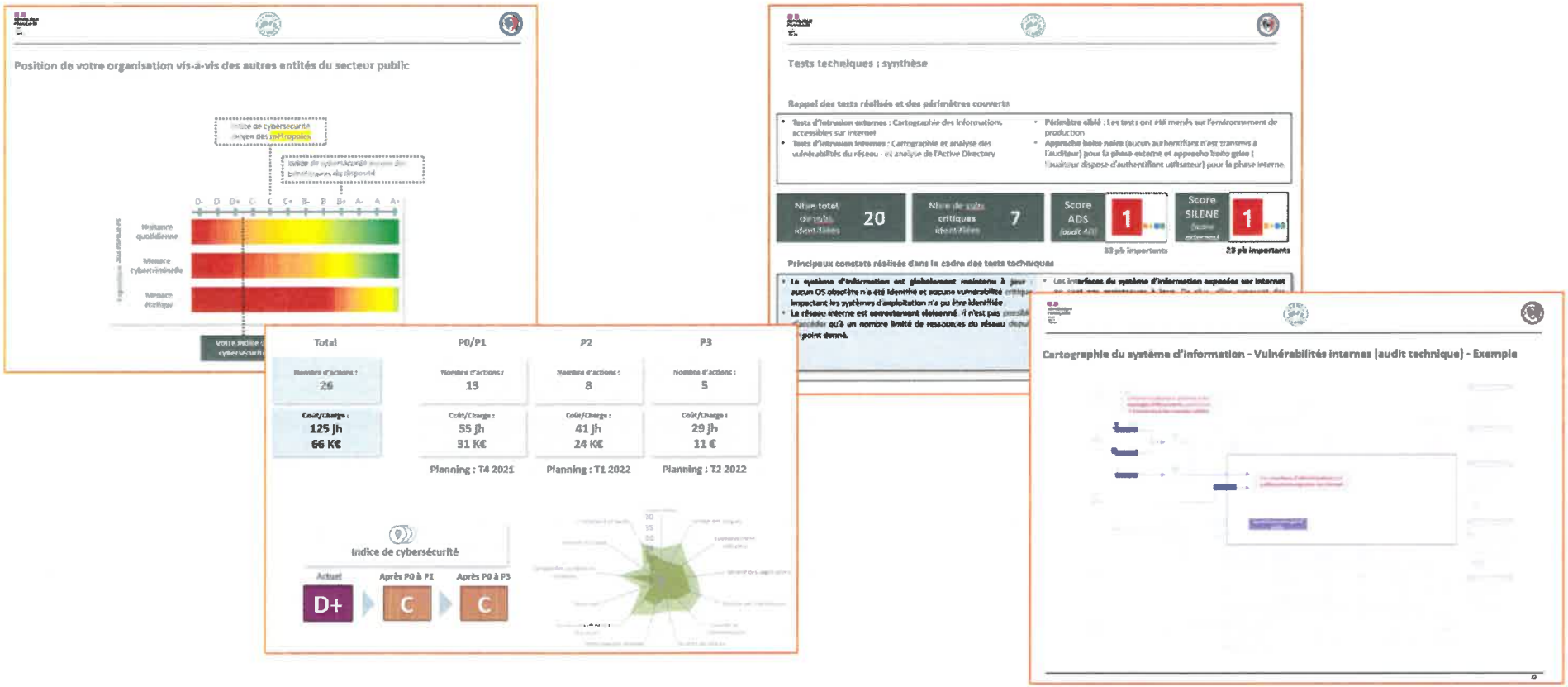
POINTS D'ATTENTION

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

Détail de la phase 4

Restitution

- *Exemple de slides de restitution des travaux menés*



Détail de la phase 5

Mise en œuvre des mesures urgentes

OBJECTIFS

- Accompagner à la mise en œuvre des mesures urgentes

LIVRABLES

- CR d'intervention

DÉMARCHE

- En fonction des chantiers à mettre en œuvre, et sur la base d'un échange avec la commune d'Ermont, Orange Cyberdefense mobilise des experts afin d'accompagner la mise en œuvre des mesures urgentes
- Pour chaque besoin, la commune d'Ermont fait une demande à Orange Cyberdefense qui identifie et mobilise la bonne ressource

POINTS D'ATTENTION

- Chaque besoin sera évalué par OCD pour définir les ressources à mobiliser et de charge nécessaire
- 4 jours sont identifiés pour cette phase

Détail de la phase 6

Sensibilisation

OBJECTIFS

- Réaliser des actions de sensibilisation et de formation des agents

LIVRABLES

- Supports de présentation
- Plan de sensibilisation

DÉMARCHE

- Sur la base des supports fournis par le prestataire accompagnateur, Orange Cyberdefense animera :
  - 1 session de sensibilisation des administrateurs du SI
  - 1 formation de votre référent SSI

POINTS D'ATTENTION

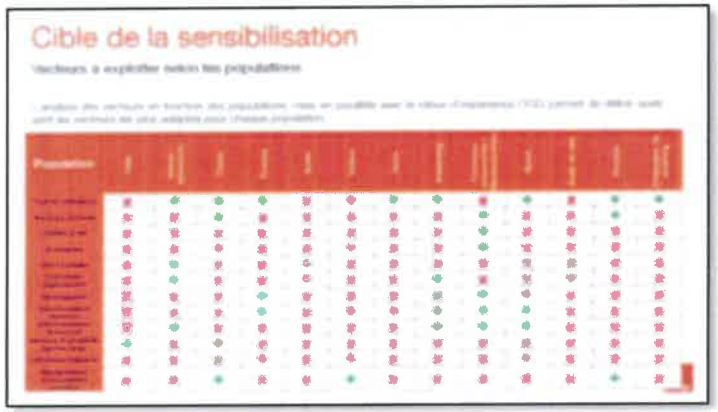
- 1 atelier de sensibilisation des administrateurs du SI
- 1 atelier de formation de votre référent SSI
- Le besoin d'élaboration de la stratégie de sensibilisation n'a pas été retenu par la mairie d'Ermont

Détail de la phase 6

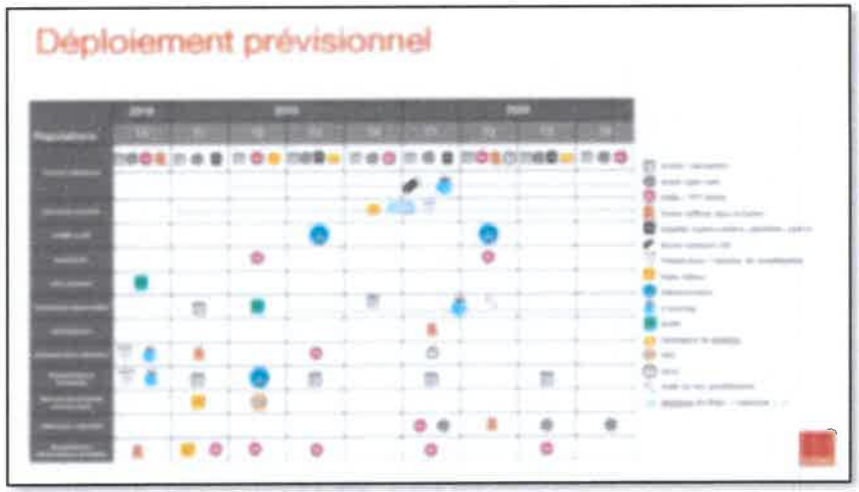
Sensibilisation

Exemple de stratégie de sensibilisation

Identification des thèmes à traiter par rapport aux populations

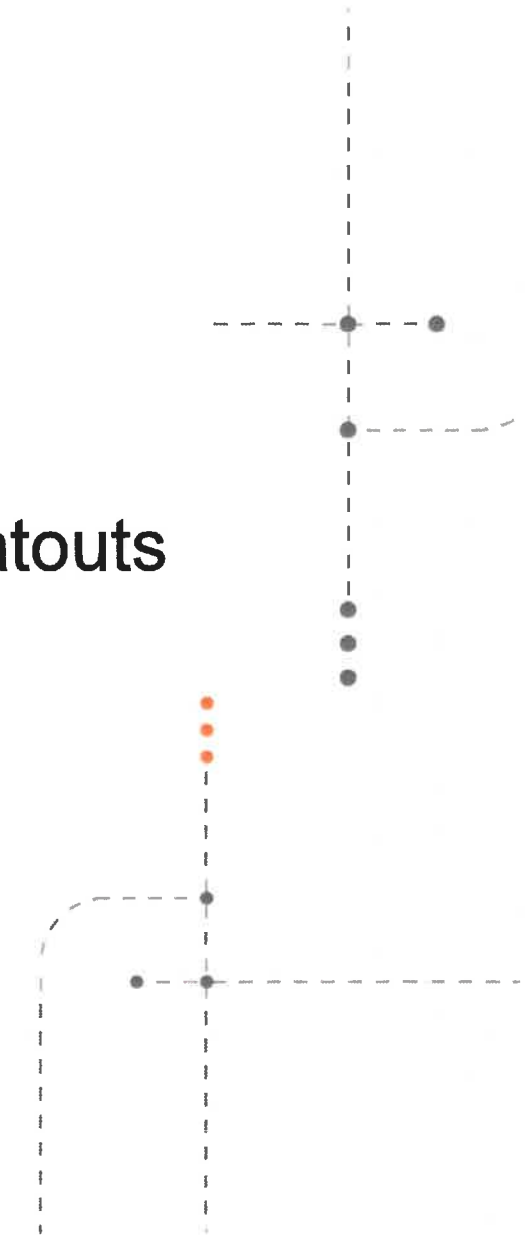


Identification des vecteurs de communications adaptés aux populations



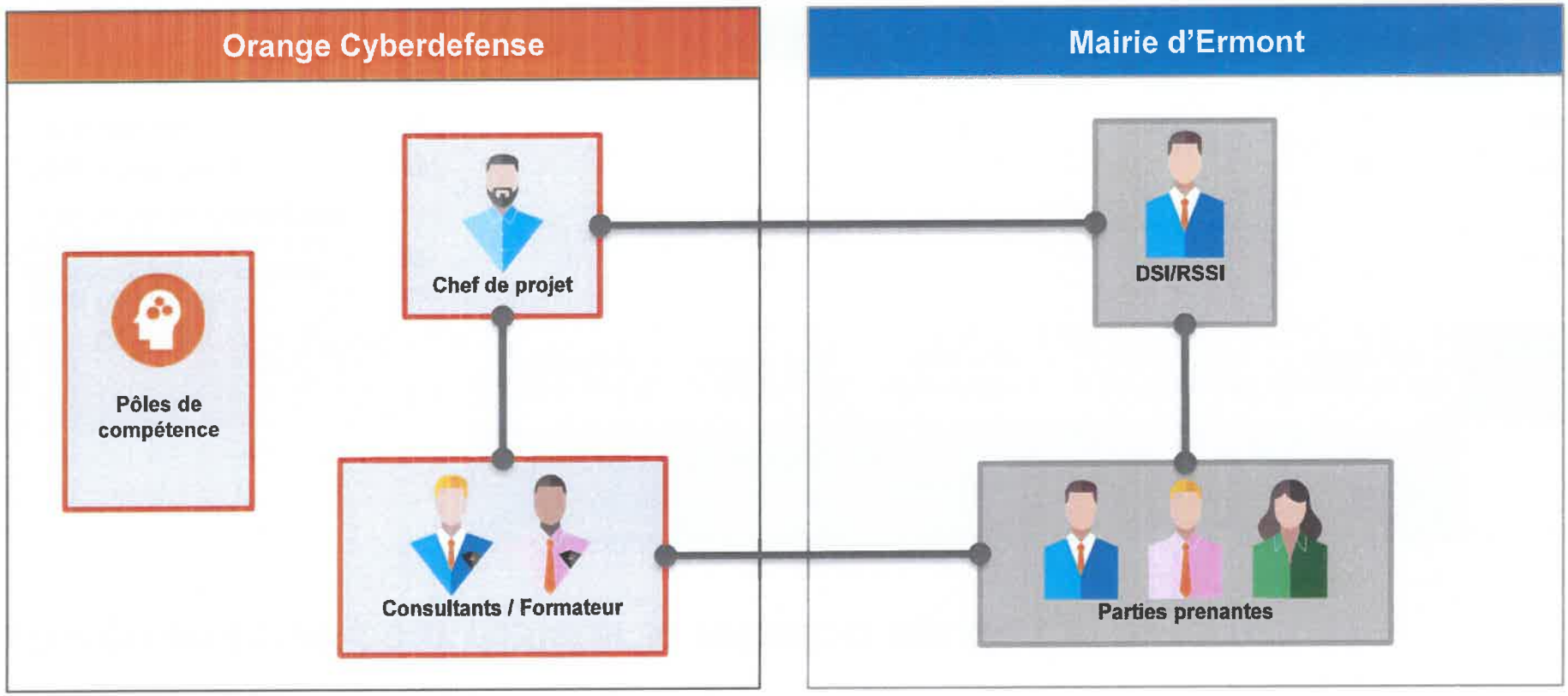
Planification des actions de sensibilisation

Sommaire



Conditions d'intervention

Organisation de la mission



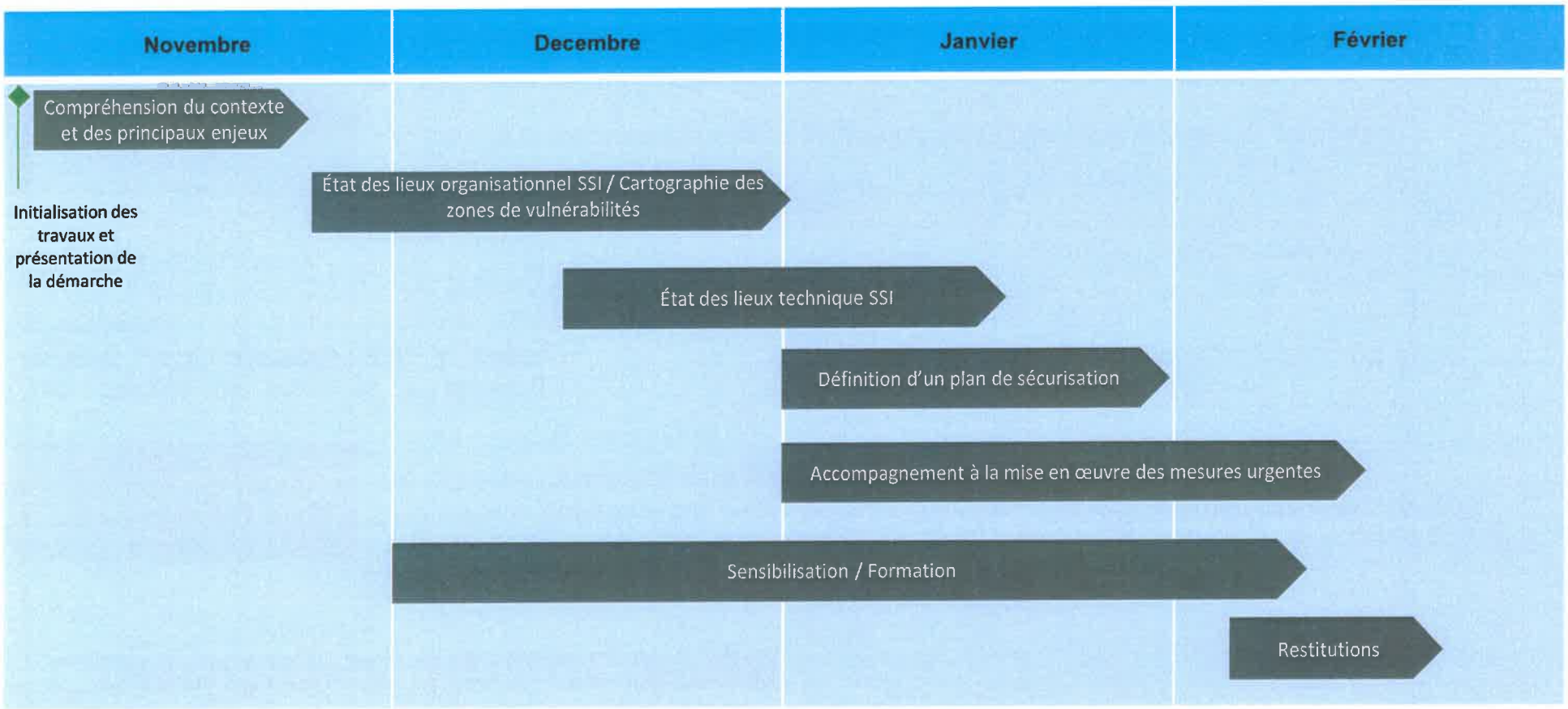
Conditions d'intervention

La charge estimée pour réaliser la mission est de 32 jours

Lot	Activité	TOTAL	Chef de mission & Auditeur organisationnel SI-CONS-TJM-CPE (1143,42 € HT)	Auditeur organisationnel 2 SI-CONS-TJM-CC (827,475 € HT)	Consultant Formateur SERV-TJM-FES (1203,6 € HT)	Consultant Expert technique SI-CONS-TJM-CPE (1143,42 € HT)	Auditeur Technique SI-CSR-TJM-AUS (902,7 € HT)	TOTAUX € HT
1	**Contexte, enjeux et diagnostic organisationnel (cartographie incluse), plan de sécurisation et restitution**	**17**	6	11	-	-	-	15 962,745 €
2	**Diagnostic technique**	**10**	-	-	-	-	10	9 027,000 €
3	**Sensibilisation**	**2**	-	-	2	-	-	2 407,200 €
	Mesures urgentes	**3**	-	-	-	3	-	3 430,260 €
	Total JH	**32**	**6**	**11**	**2**	**3**	**10**	30 827, 205 €

Conditions d'intervention

Planning prévisionnel



Conditions financières

Conditions financières	Pour les taux journaliers des profils indiqués ci-dessus, Orange Cyberdefense utilise les tarifs des UO correspondantes de la grille SIPPEREC

Les charges du projet et le planning indicatif sont présentés aux 2 pages précédentes

Prix HT: 30 827, 20 €
Prix TTC: 36 992,64 €

Frais	Les frais de déplacement en région parisienne sont inclus dans la présente proposition
Conditions de facturation	La facturation se fera en 3 temps : **Facturation à 100% de chaque lot à 100% de leur réalisation.**
Pilotage de la mission	Un point de pilotage bimestriel (30') pourra être organisé avec le client afin de partager sur l'avancement de la prestation.

Conditions d'intervention

Bon pour commande et pour facturation

Bon Pour Commande **Diagnostic et de la formalisation du plan de sécurisation** **30 827,20 € HT** **36 992,64 € TTC**	Date : ..... Nom et Qualité du Signataire : .... Indiquer la mention « bon pour commande et pour facturation » : ..... Signature : Cachet de l'entreprise :

Conditions d'intervention

Lieu de déroulement, validation des livrables

Lieu de déroulement de la mission

- La mission se déroulera dans les locaux d'Orange Cyberdefense (réunions, entretiens, rédaction des livrables, …).
- Pour les travaux identifiés comme devant se dérouler dans les vos locaux (ateliers, présentations, ...), la commune d'Ermont mettra à disposition des consultants d'Orange Cyberdefense un espace de travail pouvant accueillir des personnes équipées d'un ordinateur portable.

Documents et livrables

- Les documents sont échangés avec la commune d'Ermont par messagerie électronique en utilisant des conteneur Zed (demande de l'ANSSI).
- Les livrables seront établis en français, réalisés à partir de la suite MS Office et fournis au format PDF pour les supports de présentation. Chaque étape du projet est close par la remise des livrables et leur validation par le RSSI de la commune d'Ermont.
- Les livrables comprendront un numéro de version.
- Pour chaque étape, Orange Cyberdefense vous propose un délai de relecture de 5 jours ouvrés ce qui permet d'atteindre les objectifs de planning fixés. En l'absence de remarques de votre part au-delà de ce délai de relecture, le livrable est considéré comme validé.

Conditions d'intervention

Nos engagements

Garantir la confidentialité des informations Client

- Notre champ d'intervention recouvre des processus, des données et des informations qui peuvent être hautement sensibles pour nos clients en termes de confidentialité. Nous nous engageons à conserver les documents du Client dans des espaces de stockage protégés et à utiliser uniquement les informations strictement nécessaires à notre mission.
- A la fin de la mission, à votre demande, les données et documents clients seront détruits de manière sécurisée. C'est pour nous la base incontournable d'une relation de confiance avec nos clients.

Réunir la meilleure équipe

- L'une des clés majeures du succès d'un projet de conseil est la composition de l'équipe projet sélectionnée. Les profils proposés ont l'habitude de travailler ensemble et sont choisis pour la complémentarité de leurs compétences. Ils font de la gestion des risques projet leur quotidien. Ils sont tous expérimentés et passionnés par la Sécurité de l'Information.

Tenir parole

- Votre satisfaction n'est pas seulement un indicateur de performance pour notre Tableau de Bord d'entreprise. C'est notre première source de motivation. Notre préoccupation est de livrer à temps, dans les budgets et avec votre satisfaction.

Conseiller efficacement et durablement

- Toutes nos actions et nos préconisations sont élaborées dans un souci permanent de pragmatisme et d'indépendance afin de garantir leur pleine efficacité au sein du SI et de l'organisation du Client.
- Elles sont également conçues pour garantir la pérennité dans le temps de leurs effets bénéfiques sur la sécurité du SI.

Conditions d'intervention

L'engagement de Orange Cyberdefense dans le développement durable

Engagement quotidien de Orange Cyberdefense

- Notre engagement quotidien est le respect des individus et de l'environnement, à la mesure de notre activité
- Nous incitons ainsi notamment nos collaborateurs aux téléréunions et à l'utilisation des transports en commun, à l'usage permanent de papier géré durablement, l'impression lorsqu'elle est nécessaire et le recyclage de conteneurs (toners, eau...)
- Une politique d'économie d'énergie est de plus en place sur l'ensemble de nos équipements informatiques
- Nos bureaux sont équipés de points de collecte pour le papier et nous avons une politique de recyclage sécurisé (destruction des documents papier clients)

Engagements pour cette mission

Pour les préconisations :

- Notre indépendance vis-à-vis de tout fournisseur de matériel ou logiciel garantit des préconisations raisonnées

Pour les réunions et déplacements :

- La tenue de téléconférences ou de web-conférences est privilégiée pour les réunions et entretiens auxquels la présence physique apporte peu de valeur ajoutée
- L'envoi préalable des documents et l'utilisation de vidéoprojecteurs permettent de limiter les impressions

ANNEXE

Références
Exemples de profils types pour cette mission

Chef de mission et auditeur 1

CURRICULUM VITAE

YBE

- 11 années d'expérience.
- Team Leader.
- ISO 27001 Lead Auditor.
- ISO 27005 Risk Management Partitionner.

Consultant en sécurité des systèmes d'information, diplômé d'un master en cryptologie et codage de l'information. Avant de rejoindre Orange Cyberdéfense, il a eu une première expérience de 4 ans en tant que consultant en développement des systèmes critiques.

YBE a un profil pluridisciplinaire qui lui permet travailler sur des sujets aussi bien techniques qu'organisationnelles. Il a participé à des missions d'audit, de conseil en gouvernance de la sécurité et gestion des risques, et des missions techniques de sécurisation de systèmes et de réseaux.

De plus, il a participé à plusieurs missions de sécurisation des environnements hébergés dans le cloud (Azure / O365, AWS).

Domaines de compétences

Compétences fonctionnelles

- Intégration de la sécurité dans les projets.
- Évaluation du niveau de maturité de la sécurité des SI.
- Mise en place d'un SMCA ISO 22301.
- Mise en place d'un SMSI ISO 27001.
- Analyses de risques : EBIOS RM, ISO27005.
- Audit de sécurité ISO27001, guide d'hygiènes ANSSI, SI industriel, plan d'assurance sécurité, France Relance.
- Animation de sessions de sensibilisation et de formation.

Compétences techniques

- Design d'infrastructure/réseau sécurisés.
- Sécurisation des infrastructures Cloud.
- Sécurisation de l'environnement Office 365.
- Sécurisation des systèmes (Windows, Linux, Oracle, autres…).
- Audit de configuration des systèmes.
- Développement logiciel.

Quelques expériences marquantes

- **Réalisation des audits de sécurité et de conformité organisationnelle:**
  - ISO27001, guide d'hygiènes ANSSI, SI industriel, plan d'assurance. sécurité, France Relance.
  - Charge > 40 audits.

- **Pilotage/réalisation d'études en cybersécurité:**
  - Étude de la stratégie d'implémentation et les mesures de sécurité de Zero Trust Network Access.
  - Etude de la sécurité de la conteneurisation
  - Cartographie et élaboration d'un guide de sécurité des relations d'approbations AD.
  - Étude de la sécurité pour la mise en place des réseaux SD-WAN.
  - Élaboration d'un standard de sécurité pour les raccordements des SI.

CONFIDENTIEL

- **Mise en place du processus DevSecOps**
  - Conseil pour la mise en place des outils DevSecOps
  - Cartographie des processus et définition du RACI
  - Validation des procédures DevSecOps.

- **Référent sécurité d'offre d'Orange: Flexible SDWAN Fortinet**

CONFIDENTIEL

- **Implémentation de SMSI pour plusieurs clients**
  - Rédaction PSSI, procédures de sécurité, BCP/DRP

Auditeur 2

CURRICULUM VITAE

BKU

- Consultant confirmé
- 4 années d'expérience
- Certifié ISO27001 Lead Implémenter / ISO 27005 RM

DOMAINES DE COMPÉTENCES

Compétences

- Intégration de la sécurité dans les projets
- SMSI : ISO27001 et 27002
- Continuité d'activité (tests DRP, BIA)
- Gestion de projet
- Sensibilisation à la Cybersécurité
- Suivi plan d'action audit (ISO 27001)
- Homologation RGS
- Analyses de risques : ISO 27005, EBIOS RM
- Gestion des alertes de sécurité (MCAS)

Biriangan est diplômé d'un Master en Systèmes d'Information à l'Université Paris 1 Panthéon-Sorbonne, il est certifié LEAD Implementer ISO 27001 et Risk Manager ISO 27005.
Au cours de ses différentes expériences, Biriangan a participé à différents projets liés à la cybersécurité notamment des projets liés à la cyber-résilience, à de la conformité ISO 27001, à de l'homologation RGS. Il a réalisé ces projets pour de grandes entreprises de différents secteurs notamment le secteur public, de l'automobile et de l'énergie.
Sa dernière mission portait sur l'homologation RGS du parc applicatif d'une direction de l'administration publique.

QUELQUES EXPÉRIENCES MARQUANTES

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

Accompagnement à un projet d'homologation RGS. Réalisation d'homologations sur le parc applicatif de l'administration publique selon la sensibilité de l'application.

ENGIE Home Services

Accompagnement à une campagne BIA sur un périmètre de 10 Directions métiers. Réalisation d'une analyse de risques sur les actifs informatiques identifiés comme sensibles.

Renault Group

Accompagnement à un programme de cyber-résilience. Réalisation d'une démarche de BIA sur un périmètre 14 fonctions métiers et organisation des tests DRP sur le parc applicatif du Groupe

HR Path. Your way to people success

Assistance RSSI sur un projet de certification ISO 27001.
Accompagnement dans la mise en place d'un SMSI (Analyse de risques, rédaction et mise à jour de politiques et procédures de sécurité, sensibilisation à la sécurité, veille cyber, suivi du programme d'audit)

Auditeur technique

CURRICULUM VITAE

GSC

- Pentester confirmé et chef de projet
- 5 ans d'expérience
- OSCP (Offensive Security Certified Professional)
- CRTP (Certified Red Team Professional)

GSC est diplômé de l'École d'Ingénieurs UTT (Université de Technologie de Troyes). Spécialisé dans les Réseaux et les Télécommunications ainsi que la Sécurité des Systèmes et des Communications. Il a rejoint le pôle Ethical Hacking d'Orange Cyberdefense après avoir effectué son stage de fin d'études.

Grâce à ses compétences polyvalentes, GSC intervient aujourd'hui chez OCD en tant que pentester confirmé. Il réalise principalement des tests d'intrusion externe (OSINT, OWASP), interne (Active Directory, Wi-Fi), cloud (Azure, AWS) et mobile (Android).

DOMAINES DE COMPETENCES

Tests d'intrusion

- Réseau interne: cartographie, attaques AD, rebond.
- Infrastructures externes: OSINT, scan de reconnaissance, exploitation de services vulnérables.
- Applications Web et OWASP.
- Environnements Cloud: Azure, AWS
- Mobile: analyse statique et dynamique Android, API mobile.
- Postes de travail: attaques physiques et logiciels.
- Wi-Fi: contournement des protections et des segmentations réseau.
- Audit de configuration: benchmark CIS.

Chefferie de projet

- Qualification : compréhension du besoin auprès des commanditaires et des métiers, estimation de la charge associée, définition du périmètre et initialisation d'audit ;
- Pilotage de missions et suivi d'audits ;
- Restitution : synthèse managériale et/ou technique, explication et accompagnement aux remédiations.

MISSIONS SIGNIFICATIVES

Tests d'intrusion internes

- Réalisation de multiples tests d'intrusion interne pour divers clients (secteur publique, industriel, etc.)
- Compromission totale des SI via un simple accès réseau en boite noire
- Audit technique des postes utilisateurs (poste du stagiaire) pour évaluer la robustesse des postes utilisateurs

Tests d'intrusion externes

- Test d'intrusion externe (boîte noire) d'une entreprise de service afin d'identifier l'exposition globale de cette dernière
- Rebond sur le réseau interne par la compromission d'un service web
- Récupération de droits d'administration du domaine interne depuis le réseau externe

Audit WiFi

- Test d'intrusion sur l'infrastructure WiFi d'un grand client de la finance
- Vérification des sécurités mises en place
- Contournement des accès visiteurs afin de compromettre le réseau interne et le SI

Audit mobile

- Analyse statique et dynamique
- Audit des API mobile
- Contournement de durcissement MDM

Formateur

CURRICULUM VITAE

BBO

- Consultant principal
- 20 années d'expérience
- Certifié ISO27K1 Lead Implementor et ISO27K5 Risk manager

BBO a été diplômé de Telecom Sud-Paris en 2004. Avec 20 ans d'expérience dans le conseil dans les secteurs Telecom et bancaire, dont 4 dans le conseil en cybersécurité, il a acquis de nombreuses compétences en assistance technique et en gestion de projet.

BBO a rejoint le pôle Conseil d'Orange Cyberdefense après avoir participé à des missions d'audit, de pilotage de plan de remédiation, et de conseil et sensibilisation à la sécurité dans les développements applicatifs.

Dernièrement, BBO a réalisé des analyses de risque EBIOS, et a accompagné des RSSI dans la mise à jour de leur PSSI, à améliorer la sécurité de postes de travail, et à intégrer des applications métier dans un outil d'IAM.

Domaines de compétences

Compétences techniques

- Audits de sécurité
- Sécurité applicative
- Sécurité des architectures
- Gestion des identités et accès (IAM)
- Sécurité des postes de travail (HIPS, Bitlocker)

Compétences fonctionnelles

- SMSI : ISO 27001 et 27002
- Analyse de risques : ISO 27005, EBIOS v3 et RM
- Plan d'audit et de remédiation
- Droit de la cybersécurité : GDPR
- PMO / Tableaux de bord / Suivi budgétaire
- Coordination d'équipes transverses
- Pilotage de RFP
- Sensibilisation à la sécurité applicative
- Schéma directeur

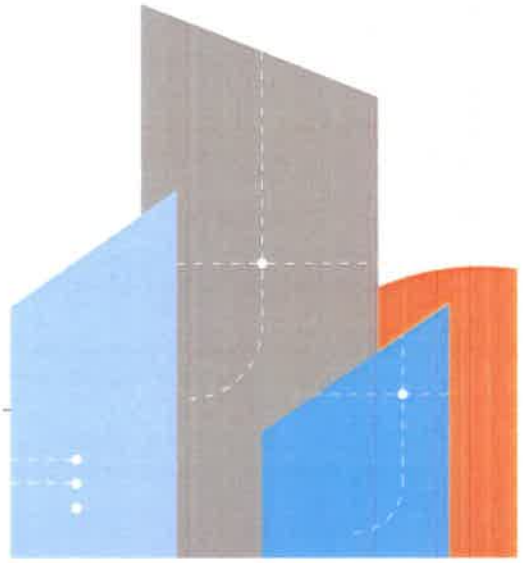
Quelques expériences marquantes

BUFFALO GRILL	RSSI à temps partagé: Définition, mise en œuvre et pilotage d'un schéma directeur à 3 ans, expert sécurité sur les projets, mise en place d'une gouvernance sécurité
STELLANTIS	Référent sécurité sur un programme assurantiel
MINISTÈRE DU TRAVAIL	Analyses de risque EBIOS v3 / EBIOS RM. Accompagnement à l'homologation de sécurité
BNP PARIBAS	IAM: Politiques d'habilitation et recertification, enrôlement d'applications Run sécurité métier: Analyse de demandes d'extractions et dérogation, analyse de risques
LA POSTE	Assistance RSSI: Diagnostic ISO 27002, Rédaction de PSSI, Tableaux de bord stratégique SSI
SOCIETE GENERALE	Sécurisation des applications : Suivi des tests d'intrusion et plans d'action - Assistance renforcée à la correction de failles applicative) - PMO du plan d'audit et remédiation (Suivi budgétaire, Tableaux de bord) - Présentation des risques audit aux métiers - Sensibilisation au développement sécurisé

Orange
Cyberdefense

Merci

https://orangecyberdefense.com/



Accusé de réception en préfecture
095-219502192-20250205-2025-014-DE
Date de télétransmission : 07/02/2025
Date de réception préfecture : 07/02/2025

ANNEXE N°1

SELECTION DES BOUQUETS

Un bouquet représente 20% de la participation fixe, soit le prix par bouquet selon la typologie de votre structure, sachant que ce prix est susceptible d'évoluer en fonction de l'offre de marchés par bouquet conformément à l'article 5.2 de la convention d'adhésion.

Liste des bouquets :

NUMERO DU BOUQUET	NOM DU BOUQUET	ADHESION AU BOUQUET (cocher la case)
1*	PERFORMANCE ENERGETIQUE	☐
2	MOBILITE PROPRE	☐
3	TELEPHONIE FIXE ET MOBILE	☐
4	RESEAUX INTERNET ET INFRASTRUCTURES	☐
5	SOLUTIONS INTELLIGENTES DE SECURITE ET DE SURETE	☐
6	SERVICES NUMERIQUES AUX CITOYENS	☐
7	VALORISATION DE L'INFORMATION GEOGRAPHIQUE	☐
8	PRESTATIONS TECHNIQUES POUR LE PATRIMOINE DE LA VILLE	☐

*l'Adhérent qui n'adhère qu'à ce bouquet et à aucun autre ne paie ni la participation annuelle fixe, ni la participation annuelle additionnelle.

Date :

Pour l'Adhérent