DÉPARTEMENT DE LOIRE-ATLANTIQUE
Arrondissement de Nantes
- - - - - - - -

13, rue des Ajoncs – CS 89409
44194 CLISSON Cedex

EXTRAIT DU REGISTRE DES DÉCISIONS

Année 2022

Décision du 8 juillet 2022

07.2022-07	**INFORMATIQUE** **OBJET : Diagnostic et formalisation du plan de sécurisation du système d'information**

VU l'article L. 5211-10 du Code général des collectivités territoriales,

VU la délibération n°22.02.2022-17 du Conseil communautaire en date du 22 février 2022 portant délégation d'attributions du Conseil Communautaire au Président,

CONSIDERANT que Clisson Sèvre et Maine Agglo participe au plan de Cyber sécurité initié par l'Agence Nationale de Sécurité des Système d'Information (ANSSI) dans le cadre de France Relance,

CONSIDERANT que ce diagnostic est entièrement subventionné,

CONSIDERANT que l'augmentation de nombre d'agents nécessite de vérifier la sécurité des données informatiques,

CONSIDERANT que les nouvelles méthodes de travail, dont le télétravail, imposent de nouvelles contraintes au système d'information,

CONSIDERANT la nécessité de faire appel à un prestataire à même de réaliser un diagnostic de l'existant et de formaliser un plan de sécurisation du système d'information de la CSMA,

CONSIDERANT le devis ci-annexé,

Le Président de la Communauté d'agglomération Clisson Sèvre et Maine Agglo,

D É C I D E

ARTICLE 1 : de signer un devis avec Orange Cyberdefense, sis 54 Place de l'Ellipse 92983 Paris La Défense, pour le diagnostic et formalisation du plan de sécurisation du système d'information pour un montant de 29 476 € HT soit 35 371 € T.T.C.

DIT qu'il sera rendu compte de la présente décision au Conseil communautaire lors de la prochaine séance.

DIT que la présente décision sera adressée à Monsieur le Préfet de Loire-Atlantique.

DIT que la présente décision sera adressée à Madame la Trésorière Communautaire.

« Pour extrait conforme au registre »

Le Président,
Jean-Guy Cornu

AR-Préfecture de Nantes
044-200067635-20220719-2-AU

Acte certifié éxécutoire
Réception par le Préfet : 19-07-2022
Publication le : 19-07-2022

Publication sur le site internet le : 20/07/2022

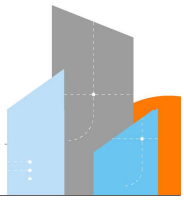
Orange
Cyberdefense

CLISSON SÈVRE&MAINE
l'agglo!

Diagnostic et formalisation du plan de sécurisation

Communauté d'agglomération Clisson, Sèvre & Maine

Proposition technique et commerciale



Confidentiel
1er juillet 2022

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 Communauté d'agglomération Clisson, Sèvre & Maine pour la réalisation d'une démarche de diagnostic et de formalisation du plan de sécurisation FRANCE RELANCE.

VOS CONTACTS

Damien CULO
Consultant cybersécurité
Mobile : +33 6 72 59 03 20
E-mail : damien.culo@orange.com

David GODEFROY
Ingénieur commercial
Mobile : +33 (0) 6 32 26 03 27
E-mail : david.godefroy@orangecybedefense.com

Sommaire

Orange Cyberdefense, en bref

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

768 € millions de CA en 2020

+ de 2 500 experts pluridisciplinaires dédiés à la cyber sécurité

4 000 clients dans le monde, sur tous les secteurs d'activité

Reconnu « Very Strong Performer » MSS
GlobalData.

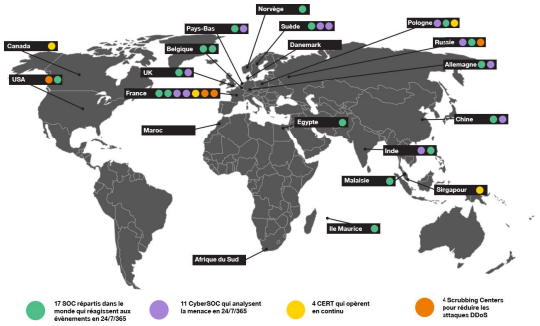
50 milliards d'événements gérés tous les jours par nos CyberSOC

Noté « Strong Performer » MSS
FORRESTER

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

Inclus dans le guide du marché Gartner des meilleurs acteurs en détection et gestion de la menace
Gartner

Leader européen avec une présence mondiale.



17 SOC répartis dans le monde qui réagissent aux événements 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 (CDPR, 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 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.

35
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

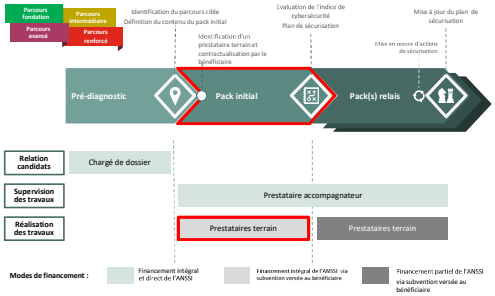
PÉRIMÈTRE

- 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	Plan de sécurisation SSI
Identifier les besoins et enjeux en matière de sécurité des systèmes d'information, pour déterminer la cible à atteindre	**Consolider** les travaux d'analyse de l'existant, déterminer et analyser les chantiers afin de construire le plan de sécurisation du SI
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	**Accompagner** la Communauté d'agglomération Clisson, Sèvre & Maine dans la mise en œuvre des mesures urgentes identifiées lors de l'état des lieux sécurité
Construire une cartographie du SI permettant d'identifier ses zones de vulnérabilités	**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

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

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

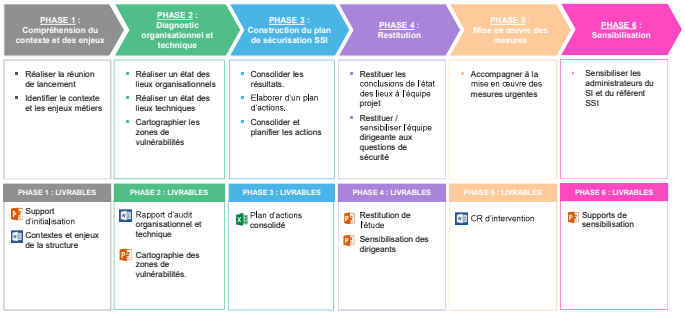
Un **acteur local**, prêt à vous accompagner au quotidien et à être **présent à vos côtés** pour tous les jalons importants

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

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

Sommaire

Démarche générale



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

LIVRABLES

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

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

POINTS D'ATTENTION

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

LIVRABLES

- Compte-rendu des réunions (questionnaires complétés et validés)

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 recueillies
  - 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

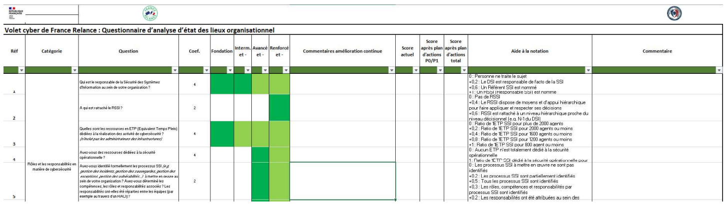
POINTS D'ATTENTION

- Orange Cyberdefense s'appuiera sur les modèles de documents fournis par l'ANSSI
- 3 réunions prévues (d'environ 2,5 heures) pour l'audit organisationnel

Détail de la phase 2

Etape 1 : Etat des lieux organisationnel

- *Utilisation du questionnaire France Relance (238 questions)*



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

LIVRABLES

- Rapport du diagnostic identifiant les failles identifiées

DÉMARCHE

- Les approches techniques choisies seront discutées lors de la réunion d'initialisation :
  - Diagnostic technique sur une adresse IP externe
    - Le diagnostic porte sur une URL ou une adresse IP publique proposée par le client
    - 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
  - Analyse de configuration d'un composant
    - Il s'agit d'auditer la configuration d'un composant interne ou externe afin de vérifier que celui-ci répond aux besoins de sécurité et respecte les standards

POINTS D'ATTENTION

- Le périmètre et la nature des tests techniques seront définis lors de la réunion de lancement
- 10 jours sont prévus au diagnostique technique dans le chiffrage France Relance

Détail de la phase 2

Etape 2 : Diagnostic technique / test d'intrusion

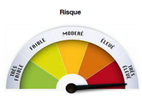
- *Analyse technique : exemple de synthèse*

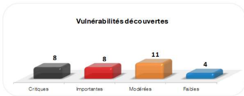
Points positifs

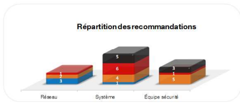
Points positifs	Commentaires
Points d'accès WIFI : Vérification de l'identité du serveur	Les postes clients sont configurés pour vérifier que les points d'accès XXX et XXX présentent un certificat valide. C'est une configuration conforme aux bonnes pratiques.

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		TII- 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		Critique
	Intégrité		
	Confidentialité		
	Preuve		

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	X.X.X.X :8080
Tomcat	tomcat	tomcat	X.X.X.X :8080
Application X	admin	admin	X.X.X.X:8100

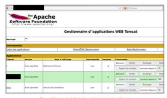


Figure 30 - Accès à l'interface d'administration Tomcat

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

LIVRABLES

- Cartographie des zones de vulnérabilités

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

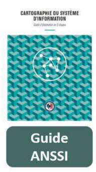
POINTS D'ATTENTION

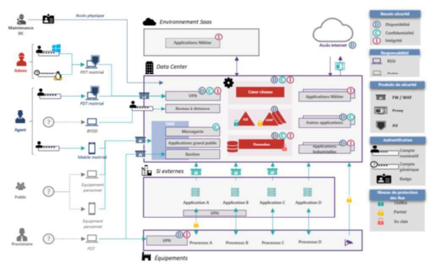
- 1 atelier de validation de la cartographie
- Orange Cyberdefense s'appuiera sur le modèle de cartographie fourni par France Relance

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 Communauté d'agglomération Clisson, Sèvre & Maine

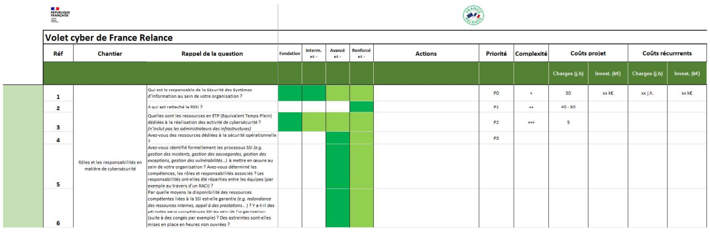
POINTS D'ATTENTION

- 2 réunions de construction et validation de priorisation des actions/chantiers SSI (2h)
- 1 réunion 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*



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

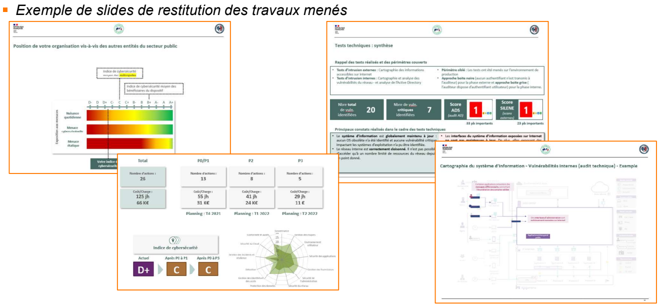
POINTS D'ATTENTION

- 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 Communauté d'agglomération Clisson, Sèvre & Maine, Orange Cyberdefense mobilise des experts afin d'accompagner la mise en œuvre des mesures urgentes
- Pour chaque besoin, la Communauté d'agglomération Clisson, Sèvre & Maine fait une demande à Orange Cyberdefense qui identifie et mobilise la bonne ressource

POINTS D'ATTENTION

- Chaque besoin sera évalué par OCD pour définir la ressources à mobiliser et de charge nécessaire
- 3 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

DÉMARCHE

- Sur la base des supports fournis par le prestataire accompagnateur, Orange Cyberdefense animera :
  - Une session de sensibilisation des administrateurs du SI
  - Une formation de votre référent SSI
- Orange Cyberdefense animera 2 réunions de travail avec l'équipe projet permettant de formaliser un plan de sensibilisation répondant aux exigences et contraintes spécifiques de la Communauté d'agglomération Clisson, Sèvre & Maine :
  - La cible de sensibilisation
  - Les thèmes de sensibilisation ou de formation à adresser selon les populations ciblées
  - Les moyens à utiliser

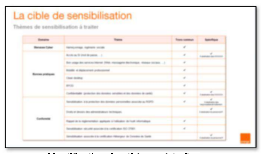
POINTS D'ATTENTION

- 1 réunion de sensibilisation des administrateurs du SI (2h)
- 1 formation de votre référent SSI (1j)

Détail de la phase 6

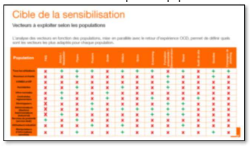
Sensibilisation

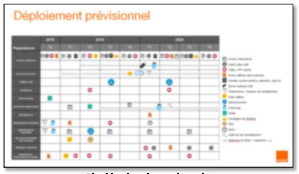
Exemple de stratégie de sensibilisation



Identification des thèmes à traiter par rapport aux populations

Identification des vecteurs de communications adaptés aux populations



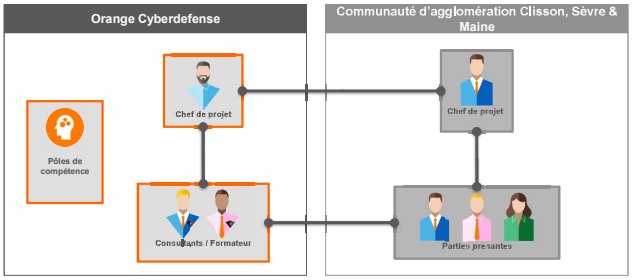


Planification des actions de sensibilisation

Sommaire

Conditions d'intervention

Organisation de la mission



Conditions d'intervention

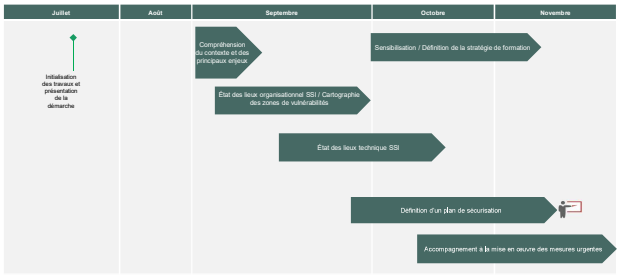
Évaluation des charges pour les étapes du projet

	Chef de projet	Auditeur	Expert technique	Auditeur Technique	Formateur
Phase 1 : Compréhension du contexte et des enjeux	1	2			
Phase 2-1 : Diagnostic organisationnel	2	3			
Phase 2-2 : Diagnostic technique	1			9	
Phase 2-3 : Cartographie		2			
Phase 3 : Construction du plan de sécurisation SSI	2	3			
Phase 4 : Restitution	1	1			
Phase 5 : Mise en œuvre des mesures urgentes			3		
Phase 6 : Sensibilisation	0,5				2
Total pour la mission :	**7,5**	**11**	**3**	**9**	**2**

La charge estimée pour réaliser la mission est de 32,5 jours

Conditions d'intervention

Planning prévisionnel



Conditions d'intervention

Proposition financière

Conditions financières	La prestation réalisée sur un mode forfaitaire vous est proposée pour un montant de : 29 476 € HT / 35 371 € TTC
Frais	Les frais de déplacement et de logistique sont inclus dans la présente proposition
Conditions de facturation	La facturation se fera de la manière suivante ▪ 50% à la commande ▪ 50% au terme de la fourniture au Client des livrables associés
Validité	La présente proposition technique et financière est valable 30 jours à compter de la date d'établissement

Conditions d'intervention

Bon pour commande et pour facturation

Bon Pour Commande

Diagnostic et formalisation du plan de sécurisation

29 476 € HT /
35 371 € TTC

Date : …….. Nom et Qualité du Signataire : ……

……

Indiquer la mention « bon pour commande et pour facturation » :

……..

Prénom / Nom : ……
Titre : ……..

Signature : Cachet de l'entreprise :

☐ Bon pour accord, équivaut à un bon de commande (Le numéro de commande qui sera indiqué sur la facture sera le numéro du présent devis)

☐ Bon pour accord, numéro de commande choisi par le client : _____

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 Communauté d'agglomération Clisson, Sèvre & Maine 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 Communauté d'agglomération Clisson, Sèvre & Maine 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 chef de projet de la Communauté d'agglomération Clisson, Sèvre & Maine.
- 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

Annexes

1. **Curriculum Vitae**
2. Références de missions similaires

Curriculum Vitae

FDA

- Consultant manager
- 20 années d'expérience
- Certifié ISO22301 Lead Auditor
- Certifié ISO27001 Lead Implementor

Depuis 20 ans, FDA intervient sur des projets conjuguant, chez des clients grands comptes, les aspects métier et infrastructure autour de la sécurité, de la continuité d'activité et de la gestion des risques.
FDA a aussi passé 2 ans comme adjoint Responsable plan de continuité dans l'entité en charges des infrastructures informatiques d'une grande banque française.
Imprégné du rôle de facilitateur, il est expert dans l'accompagnement et la gestion des projets de sécurité et dispose d'un talent relationnel certain lui permettant la coordination de l'intégration de la sécurité dans les projets.
FDA accompagne les DSI et les RSSI dans l'évolution de leurs modèles de gouvernance.

Domaines de compétences

Compétences techniques
- Sécurité des infrastructures
- Haute disponibilité / load balancing
- Architectures de secours

Compétences fonctionnelles
- Intégration de la sécurité dans les projets
- SMSI : ISO27001 et 27002
- SMCA : ISO22301
- Assistance RSSI
- Cartographie & Analyses de risques
- Méthodes de conduite de projet
- Gestion de crise.

Quelques expériences marquantes

Assistance RSSI pour la définition et la mise en œuvre de la gouvernance. Définition de la feuille de route sécurité du SI et accompagnement à sa mise en œuvre : sécurité dans les projets, solutions, sensibilisation et pilotage par les indicateurs.

Accompagnement RSSI sur la mise en œuvre et le pilotage du programme de remédiation de la sécurité du SI. En environnement SI Industriel, international sur des problématiques Active Directory, Serveurs, Postes de travail.

Identification, analyse et classification des informations sensibles dans l'entreprise à travers des entretiens avec les métiers et analyse des risques métiers liés aux informations sensibles. Développement de la méthodologie, recueil des informations lors d'entretiens avec les métiers, analyse et synthèse des informations sensibles et des risques associés et recommandations de solutions pour la couverture des risques.

Accompagnement du RSSI et de l'équipe Sécurité SI pour la revue du niveau de couverture de la PSSI et la collecte de preuves. Revue des règles de la PSSI. Collecte et challenge des preuves auprès des équipes opérationnelles. Analyse et synthèse du niveau de couverture et des preuves associées.

Curriculum Vitae

MROU

- Consultante en cybersécurité
- Diplôme d'ingénieur en informatique

MRO est diplômée de l'ESIEA – Ecole d'Ingénieurs du Monde Numérique et est titulaire d'un diplôme d'ingénieur spécialisé en cybersécurité et data science.

MRO a rejoint le pôle Conseil & Audit d'Orange Cyberdéfense après avoir effectué son stage de fin d'études de 6 mois chez Wavestone Nantes portant sur l'implémentation de la norme ISO 27001. Parallèlement, elle a participé à des missions de conseil relatives à des accompagnements de mise en conformité ISO 27001 et d'audits de maintenance du SI.

Domaines de compétences

Compétences fonctionnelles :
- SMSI : ISO 27001
- Analyses de risques : EBIOS
- Audit de maintenance du SI

Formation et sensibilisation :
- MOOC de l'ANSSI : SecNumAcadémie

Quelques expériences marquantes

Secteur public
Accompagnement d'une grande métropole à la désimbrication d'un système de management intégré et au renouvellement de la certification ISO 27001 :
Revue des différents documents du SMSI, mise à jour du questionnaire ISO 27001

Secteur hospitalier
Accompagnement d'un groupement hospitalier à l'implémentation de la norme ISO 27001 :
Préparation et participation à la revue de direction, revue et mise à jour du questionnaire ISO 27001, préparation et participation à la restitution de l'audit à blanc

Secteur assurantiel
Réalisation d'un audit de maintenance du SI :

Définition du périmètre et de l'ordre de mission, rédaction de la grille d'audit, entretiens, demande et analyse des documents audités.

Curriculum Vitae

DCU

- Consultant en cybersécurité
- 12 ans en cybersécurité
- Ancien RSSI certifié ISO 27001 Lead Implementor et Risk Manager ISO 27005 & EBIOS 2010

DCU est diplômé d'un master en Cryptographie de l'Université de Limoges. Il a exercé le rôle de RSSI pour une société de conseil et éditeur de logiciel, mais également en tant que RSSI externe pour des industriels, hébergeur, infogéreur et éditeur SaaS en santé.

DCU a rejoint le pôle Conseil & Audit d'Orange Cyberdéfense à la suite d'un poste de responsable de domaine cybersécurité au sein des Chantiers de l'Atlantique. Avant cela, il exerçait le métier de consultant cybersécurité sur des sujets de conseil en gouvernance (schéma directeur cybersécurité, gestion des risques, politiques de sécurité, accompagnement SMSI), d'audits (2700x, HDS, 22301, RGS) et sectorielles (systèmes industriels et sécurité embarqué pour l'avionique).

Domaines de compétences

Gouvernance Cybersécurité
- Stratégies et schémas directeur cybersécurité
- Analyses de risques (EBIOS RM, 27005, MEHARI, PIA)
- PRA et gestion de crise cybersécurité
- Gestion des incidents de sécurité
- Gestion des risques IT
- Politiques de sécurité (PSSI / Plan d'assurance sécurité)

Conseil en Cybersécurité
- Accompagnements à la mise en place de Systèmes de management (27001, HDS)
- Formations en analyse de risques sécurité, 27001 et HDS
- Sensibilisation
- Accompagnement à la Sécurité de systèmes industriels
- Animations d'ateliers thématiques

Audits organisationnels
- Audits de Systèmes de management (27001, HDS, 20000, 22301)
- Audits physique et Datacenter
- Audits sécurité RGPD
- Audits de Sécurité de systèmes industriels
- Audits internes et sur référentiels internes

Référentiel et réglementation cybersécurité (ISO 2700x, HDS, 20000, 22301, II901, IGI 1300, RGS, PSSIE, RGPD)

Quelques expériences marquantes

Secteur Industriel
RSSI : Définition de la stratégie cybersécurité et accompagnement au pilotage de son déploiement. Réalisation d'une analyse de risques initiale, arbitrage avec la Direction pour établir la stratégie, définition du schéma directeur sur 3 ans. Pilotage des équipes DSI, prestataires et de la Direction industriel pour le déploiement du plan d'action. Mise en place des process de gestion des incidents sécurité, gestion des risques, PRA et gestion de crise. Rédaction pour des sensibilisation vidéos et newsletters. Planification des audits techniques. Animation d'ateliers techniques (cloisonnement réseaux, SIEM, durcissement AD, sécurité industriel). Rédaction de guides de bonnes pratiques.

Secteur Editeur Santé
Accompagnement à la mise en œuvre d'un SMSI HD. Audit de cadrage, Définition du plan de mise en conformité. Élaboration des principaux documents du SMSI. Pilotage du plan d'action technique, Préparation du dossier de certification, Planification de l'audit à blanc.

Secteur Hébergeur
Réalisation des audits internes du Systèmes de management intégré (27001, HDS, 20000, 22301), Définition des plans d'audit, Réalisation des audits documentaire et audits sur site. Restitution à la Direction.

Secteur Infogéreur HDS
Coaching d'un chef de projet à la mise en œuvre d'un SMSI HDS, Réalisation de l'audit initial, Définition du plan de mise en conformité. Formation de l'équipe projet HDS et analyse de risques. Accompagnement coaching réguliers pour suivre le pilotage et conseiller sur les difficultés. Mise en place d'ateliers sur des sujets bloquants (Analyse de risques, Indicateurs, politique de sécurité, RGPD, sujets techniques ...)

CURRICULUM VITAE

MDI

- Consultant Senior
- 10 années d'expérience
- Français, anglais

Issu d'un mastère en Informatique et Systèmes d'information à SUPINFO Lyon, MDI dispose de 10 années d'expérience dans le domaine de la sécurité SI et réseaux, en majorité acquises au sein de grands comptes mais aussi de structures moyennes. Les diverses missions réalisées lui ont permis de développer une compétence mixte : maitrise d'œuvre et pilotage opérationnel de chantiers sécurité.

Il intervient en grande partie, sur des missions d'accompagnement à la mise en conformité réglementaire, de gestion d'identités et des accès, d'audits organisationnel, de gestion des réponses à incidents et de gestion de crises.

Domaines de compétences

Audit et contrôles de conformité
- Audit de sécurité et de conformité réglementaires
- Audit de maturité SSI (LPM, HDS, Directive NIS, ISO27001, RGPD)
- Audit de fournisseurs

Sécurité opérationnelle
- Durcissement de systèmes d'exploitation
- Industrialisation de contrôles de sécurité (gestion des accès)
- Mise en œuvre de contrôles périodiques des accès
- Classification et gestion des données sensibles à travers une solution DLP

Assistance à maîtrise d'ouvrage
- Étude de cadrage et accompagnement dans le choix de solutions techniques
- Gestion des identités et des accès (IAM)
- Mise en place d'un SMSI

Conseil organisationnel
- Évaluation de la maturité
- Analyses de risques
- Définition de schéma directeur
- Mise en conformité RGPD
- Élaboration d'un plan de gestion de crise

Quelques expériences marquantes

Secteur Transport	Réalisation d'une étude de cadrage pour l'évaluation du niveau de conformité par rapport au RGPD et élaboration d'une feuille de route de mise en conformité.
Secteur Pharmaceutique	Définition et déploiement du processus de réponse à incidents. Sensibilisation des parties prenantes. Accompagnement à la conformité sur les aspects détection et réponse à incidents. Élaboration et accompagnement à la mise en œuvre de procédures de revues de comptes et de production d'indicateurs dans le cadre d'un projet de mise en conformité par rapport à la LPM. Automatisation des extractions de comptes systèmes.
Secteur Télécommunication	Réalisation de plusieurs projets d'analyses de risques sécurité, d'audits de conformité par rapport au RGPD, d'audits de conformité aux exigences de sécurité des prestataires et d'analyses des clauses contractuelles liées à la sécurité, de contrats.
Secteur Public	RSSI à temps partiel pour la Ville de Saint-Etienne. Mise en œuvre de le feuille de route de sécurité (Patch management, BYOD, Gestion des identités et des accès, préparation à la gestion de crise, etc.).
Secteur Transport	État des lieux des processus existants, élaboration d'une feuille de route, définition de la politique et des règles de gestion des identités et des accès.
Secteur Industriel	État des lieux puis, accompagnement dans l'élaboration d'un plan de gestion de crise (Définition de la stratégie de gestion de crise Cyber et Organisation de la gestion de crise Cyber).

CURRICULUM VITAE

EAS

- Consultant Junior
- 4 années d'expérience

Issu d'un master en cyber sécurité de l'ENI à Nantes, EAS a réalisé son année de master en alternance au sein du SSTRN avant d'être recruté par Orange Cyber Défense.

Désormais rattaché à la Business Unit Conseil et Audit, EAS intervient dans le cadre de missions relatives à la gouvernance sécurité, notamment dans l'accompagnement des clients à la mise en conformité aux normes ISO 27001/27002 et à la sensibilisation aux risques numériques. Il est par ailleurs impliqué sur des missions d'audits techniques

Domaines de compétences

Audit et contrôles de conformité
- Accompagnement sur les exigences de sécurité et de conformité réglementaires
- État des lieux vis-à-vis du RGPD et plan d'action associé
- Élaboration de PIA
- Élaboration de PAS

Sécurité opérationnelle
- Durcissement des systèmes d'exploitation
- Mise en œuvre des contrôles périodiques des accès
- Sécurisation des réseaux
- Scan de vulnérabilité
- Test d'intrusion

Conseil organisationnel
- Évaluation de la maturité du SI
- Analyses de risques
- Mise en conformité RGPD
- Rédaction de processus de gestion des incidents

Formation & Sensibilisation
- Sensibilisation aux techniques de phishing
- Sensibilisation aux techniques de piratage
- Démonstration des techniques de phishing et de piratage

Quelques expériences marquantes

Secteur Télécom	Des contrôles de conformité RGPD Un PIA via l'outil de la CNIL Des analyses de scan de vulnérabilité via Nessus Des tests de vulnérabilité Des analyses et réalisations de PAS Des analyses de risque et recommandations de mesures de sécurité
Secteur agro-alimentaire	Des scans de vulnérabilité et tests d'intrusion. Une évaluation du niveau de maturité Une exposition des risques identifiés Une définition d'un plan d'action Une sensibilisation sur les bonnes pratiques sécurité
Secteur public	Une sensibilisation sur le phishing et le piratage (Démo) Une présentation des moyens de les reconnaitre, les dénoncer et de s'en prémunir Des scans de vulnérabilité et tests d'intrusion. Une évaluation du niveau de maturité Une exposition des risques identifiés Une définition d'un plan d'action

CURRICULUM VITAE

MRO

- Consultante en cybersécurité
- Diplôme d'ingénieur en informatique

MRO est diplômée de l'ESIEA Ecole d'Ingénieurs du Monde Numérique, et est titulaire d'un diplôme d'ingénieur spécialisé en cybersécurité et data science.

MRO a rejoint le pôle Conseil & Audit d'Orange Cyberdéfense après avoir effectué son stage de fin d'études chez Wavestone, portant sur l'implémentation de la norme ISO 27001.

Elle réalise des missions d'audit, de sensibilisation ainsi que des tests d'intrusion.

MRO possède des compétences techniques et fonctionnelles en sécurité des SI.

Domaines de compétences

Formations et sensibilisations :
- Risques liés au phishing
- Techniques de piratage
- Bonnes pratiques

Audits et contrôles de conformité :
- Diagnostics cybersécurité
- SMSI : ISO 27001
- Audits de maintenance du SI

Tests d'intrusions :
- Interne
- Externe

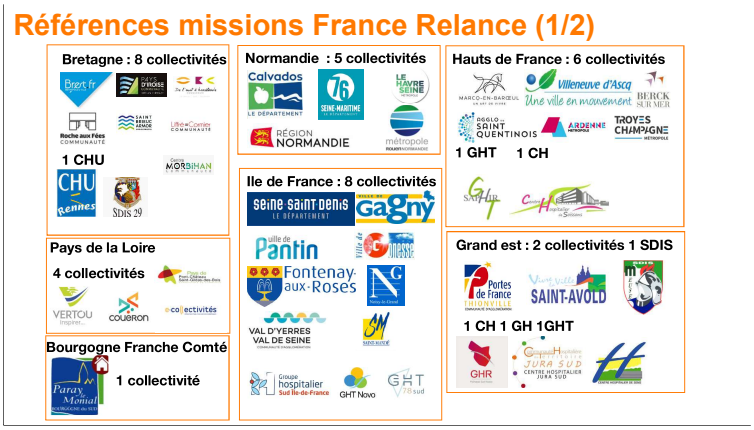
Quelques expériences marquantes

SECTEUR BANCAIRE	Préparation et réalisation d'un exercice de gestion de crise cyber : • État des lieux de l'environnement SI du client, • Élaboration du scénario, • Animation de l'exercice de gestion de crise cyber • Rédaction du rapport détaillé de l'exercice.
SECTEUR INDUSTRIEL	Réalisation de tests d'intrusion internes et externes sur les systèmes d'information.
SECTEUR PUBLIC	Sessions de sensibilisation Réalisation d'état des lieux organisationnels, de plans d'actions dédiés et de sessions de sensibilisation, dans le cadre du plan France Relance dans le but de renforcer la sécurité des systèmes d'information des bénéficiaires
SECTEUR HOSPITALIER	Accompagnement d'un groupement hospitalier à l'implémentation de la norme ISO 27001 : Préparation et participation à la revue de direction, revue et mise à jour du questionnaire ISO 27001, préparation et participation à la restitution de l'audit à blanc

Annexes

1. Curriculum Vitae
2. **Références de missions similaires**

Références missions France Relance (1/2)



Références missions France Relance (2/2)

Orange
Cyberdefense

Merci

https://orangecyberdefense.com/

orange
51 Confidentiel

Le Président,
Jean-Guy Cornu

AR-Préfecture de Nantes

044-200067635-20220719-2-AU

Acte certifié éxécutoire

Réception par le préfet : 19-07-2022

Publication le : 19-07-2022

Publication sur le site internet le : 20/07/2022