DIAGNOSTIC CYBERSÉCURITÉ

Rapport de restitution

Entreprise |
Consultant | CALTHA TECH

Date de restitution | XX/XX/XXXX

1. Rappel du cadre
Approche & étendue de la mission

Contexte	• L'entreprise XXX est en plein développement de son activité et ses équipes grossisses rapidement. Dans ce contexte, elle a souhaité effectuer le diagnostic cybersécurité Bpifrance. • Une grosse partie de l'équipe est mobile, il est donc important de mettre en place de bonnes pratiques dès le départ.	
Objectifs de la mission	• Sensibiliser le comité de direction face à la menace Cyber • Evaluer la vulnérabilité du SI actuel sur 1 site de l'entreprise • Elaborer un plan d'action pour le sécuriser • Se préparer à la gestion d'une crise cyber	

Démarche générale	• Le Diag Cybersécurité s'appuie sur :
	  • Un diagnostic SI basé sur l'analyse des documents disponibles, des entretiens (responsables du SI & prestataires, responsables métiers, utilisateurs…) et des tests complémentaires lorsque c'est pertinent
	  • Une séance de sensibilisation à destination des collaborateurs de l'entreprise
	  • Des ateliers et entretiens d'approfondissement pour élaborer le plan d'action de sécurisation du SI	

Périmètre	• Entreprise XXX	
Livrables	• Grille de maturité sur la sécurité du SI et détail par axe / forces et points d'amélioration • Recommandations et Plan d'actions priorisé de sécurisation du SI • Tableau des macro-actifs et sensibilité / exposition aux risques • Support de sensibilisation des collaborateurs	
Limites éventuelles	• Les consultants respectent la confidentialité des informations et des documents transmis et s'engagent à ne pas les diffuser à de tierces parties. • Les travaux réalisés n'engageront en aucun cas l'implication de Bpifrance dans un éventuel financement ou levée de fonds • Le dimensionnement inclut une visite d'un seul site physique de l'entreprise	Le Diag Action n'inclut pas : • L'élaboration d'un schéma directeur SI • L'identification de besoins fonctionnels non satisfaits • Des tests d'intrusion ou des scans de vulnérabilité • Un audit de durcissement système par système • La restauration du système suite à une cyber attaque • La rédaction d'un Plan de Reprise d'Activité

2. Synthèse du Diagnostic
Principaux constats

Volet technique
- Tous les postes ont des sessions individuelles avec des mises à jour automatiques
- Les accès aux serveurs sont gérés avec des droits par utilisateur
- Tous les utilisateurs sont administrateurs de leur poste de travail

Facteur humain
- Les utilisateurs sont sensibles aux risques
- Prestaire informatique très compétent
- Certaines pratiques peuvent être améliorées (verrouillage systématique du poste de travail, changement des mots de passe, …)

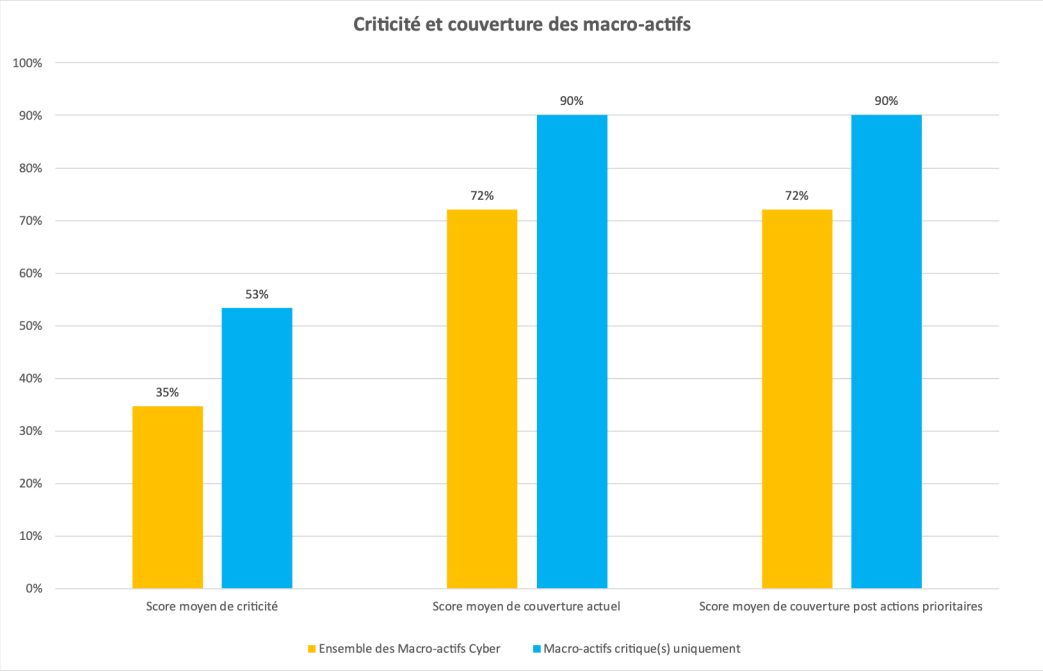
Couverture juridique
- Pas de couverture juridique à l'heure actuelle.

Sécurité physique
- Pas de système d'alarme sur le site
- Local serveur non verrouillé et non adapté
- Portes extérieures frigo non verrouillées
- Sauvegardes déportées entre sites

Process & organisation
- Pas de process de crise
- Process de crise / reprise d'activité en cours de création suite au diagnostic cybersécurité
- Le prestataire informatique peut intervenir rapidement et restaurer le SI en 1/2 journée
- Process entrées / sorties octroi de droits formalisé et suivi par le prestataire

Protection assurantielle *(toujours partielle….)*
- Pas d'assurance

2. Synthèse du Diagnostic
Indicateurs clés



Liste des Macro-actifs critiques identifiés :

1. **Production**

Budget IT estimé (% du CA) : < 1%
Déclaré par le dirigeant – incluant matériel, licences, salaires des internes, prestations externes

Score d'analyse maturité Cyber

39 / 100 - D

Score de projection maturité Cyber
(post actions prioritaires et préconisations)
76 / 100 - B

Actions prioritaires à mener :

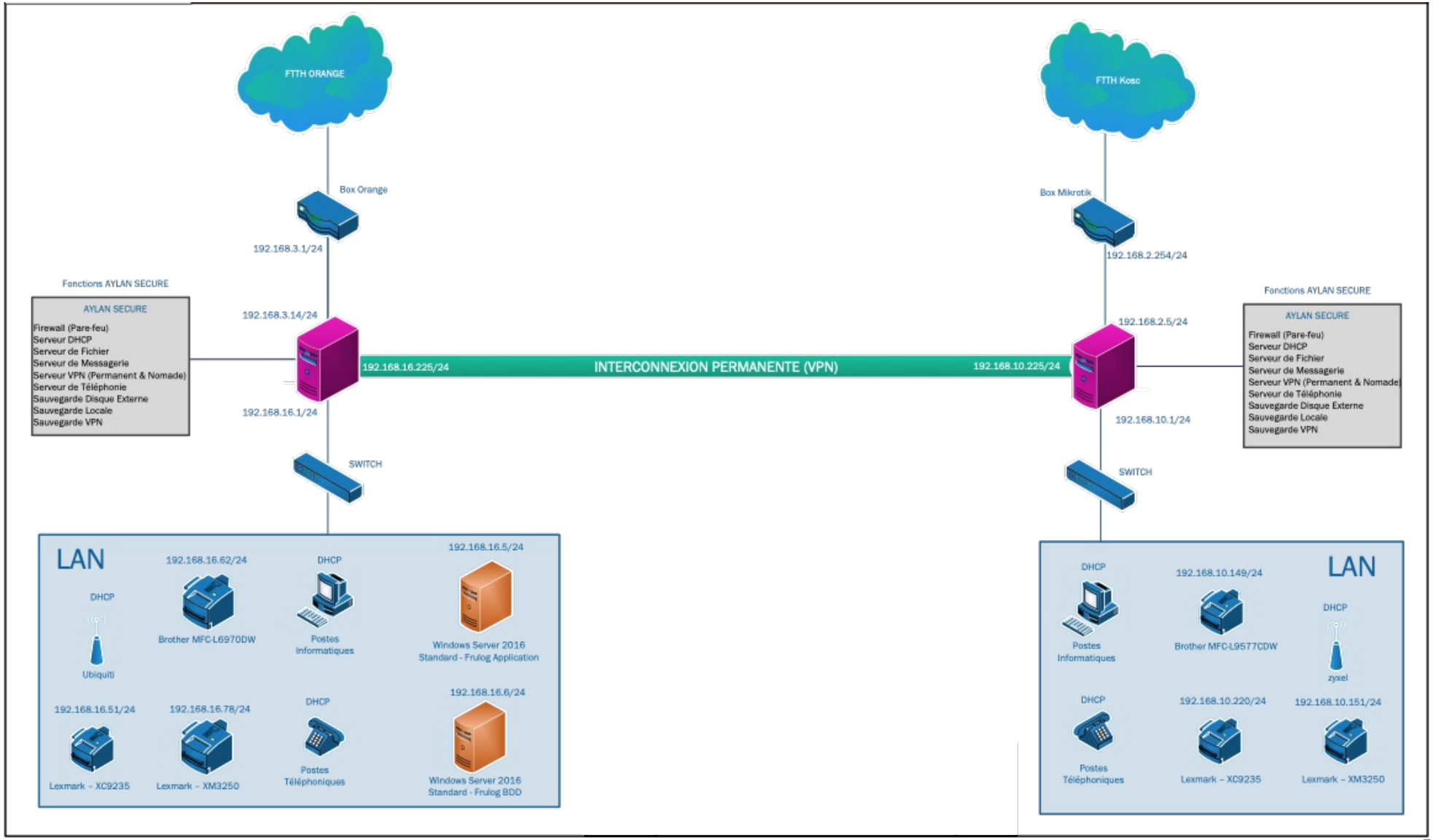
1. **Droits d'accès -** Changement des droits d'accès sur les postes utilisateurs (les utilisateurs ne doivent pas être administrateurs)
2. **Sécuriser l'infrastructure –** Salle serveur à modifier
3. **Sauvegarde -** Effectuer des tests annuels de restauration système
4. **Sécurisation des postes –** Politique de changement de mot de passe, filtre d'écran pour les commerciaux si travail en public (train …)
5. **Gestion des tiers –** Identifier les tiers critiques

3. Cartographie synthétique de l'existant
Sur base des éléments collectés

Cartographie applicative

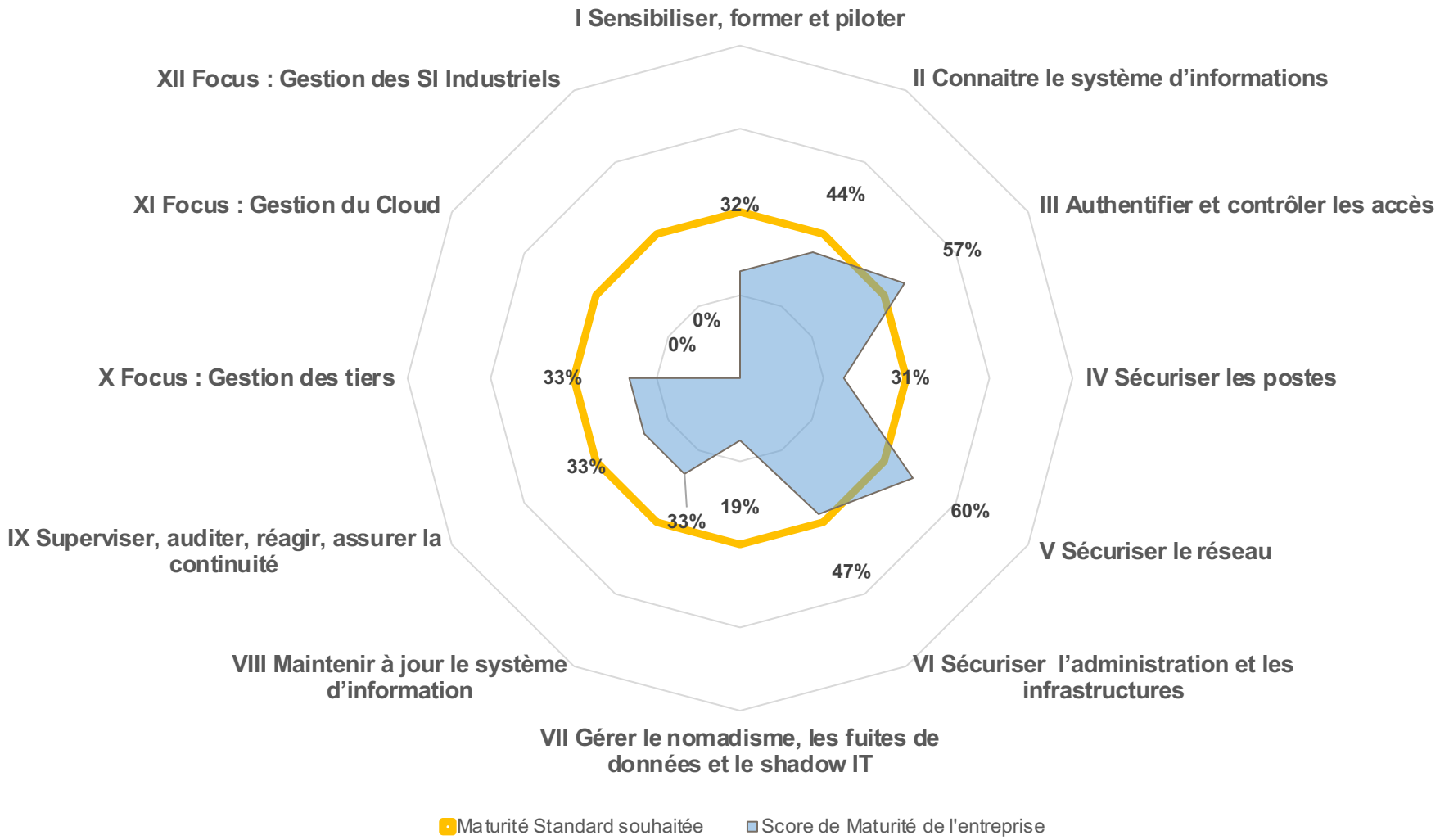
Domaine	Gestion commandes	Finance	Stocks	RH	Communication	Gestion clients/ fournisseurs
Outil(s)	*FRULOG (BC, BL, suivi)*	*EXCEL FRULOG*	*FRULOG*	*SAGE*	*Outlook WhatsApp Teams*	*EXCEL FRULOG*

3. Cartographie synthétique de l'existant
Sur base des éléments collectés



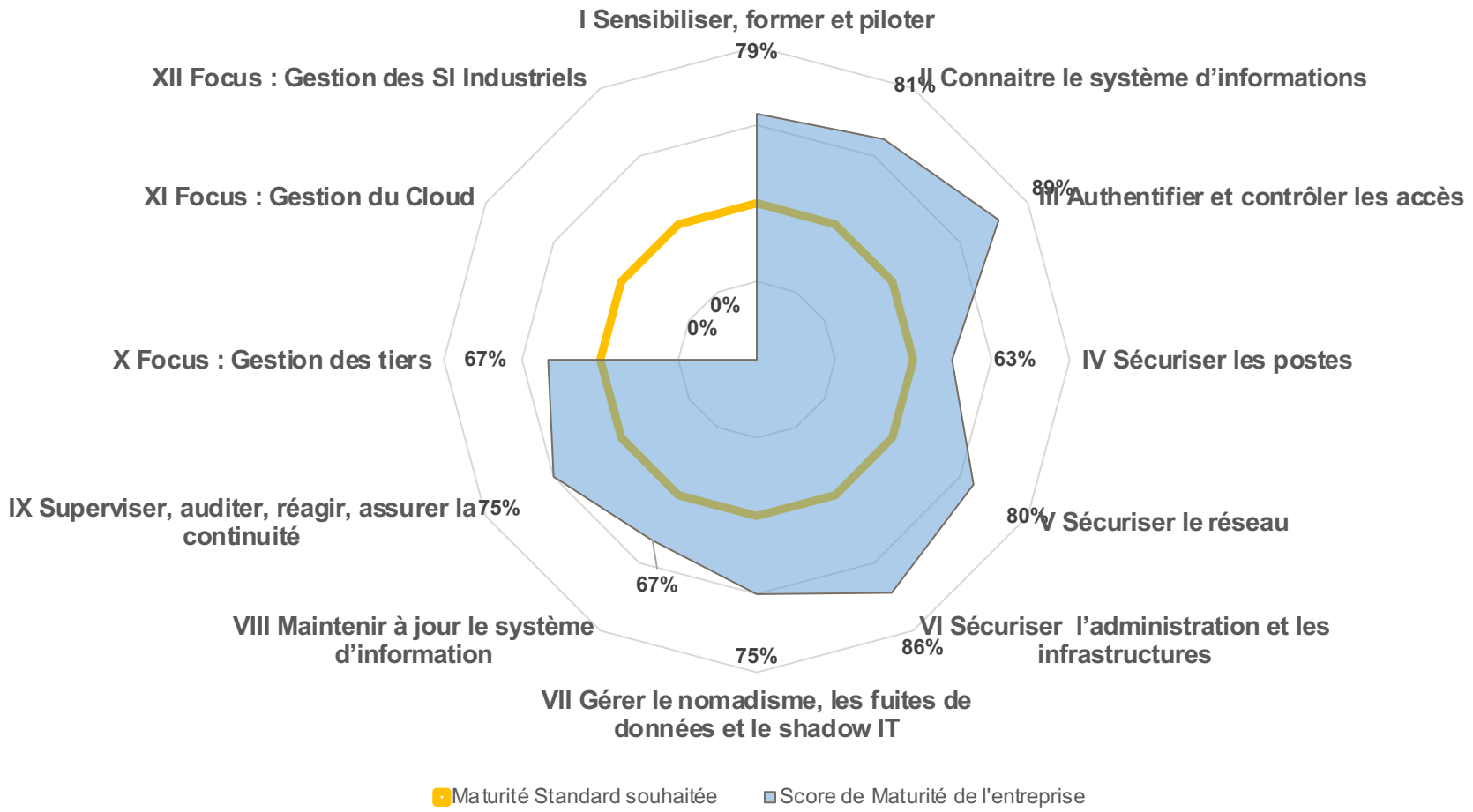
4. Radars de maturité & de projection cyber
Sur base de la grille d'analyse Bpifrance

Radar d'analyse maturité Cyber



4. Radars de maturité & de projection cyber
Sur base de la grille d'analyse Bpifrance

Radar de projection maturité Cyber



4. Radars de maturité & de projection cyber

Niveau de maturité projeté post mise en œuvre du plan d'actions

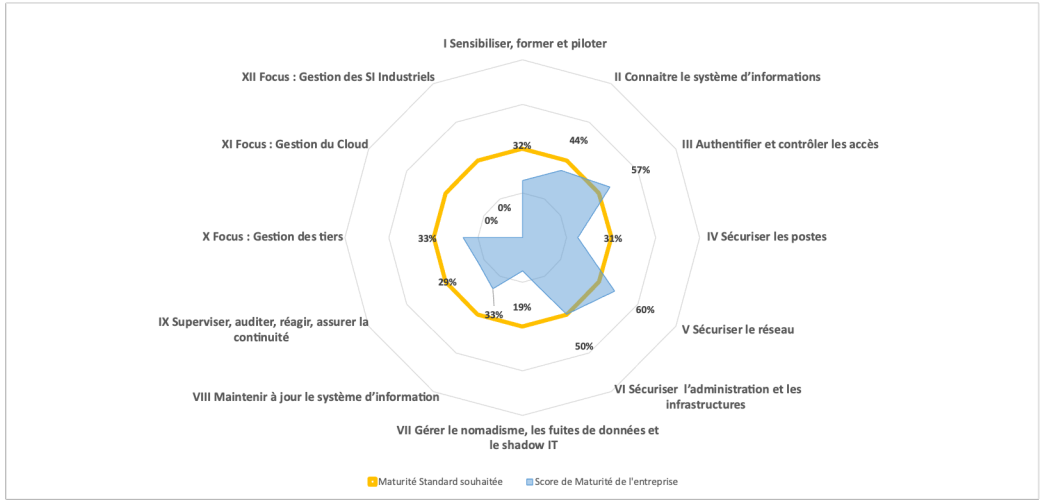
Périmètre choisi :

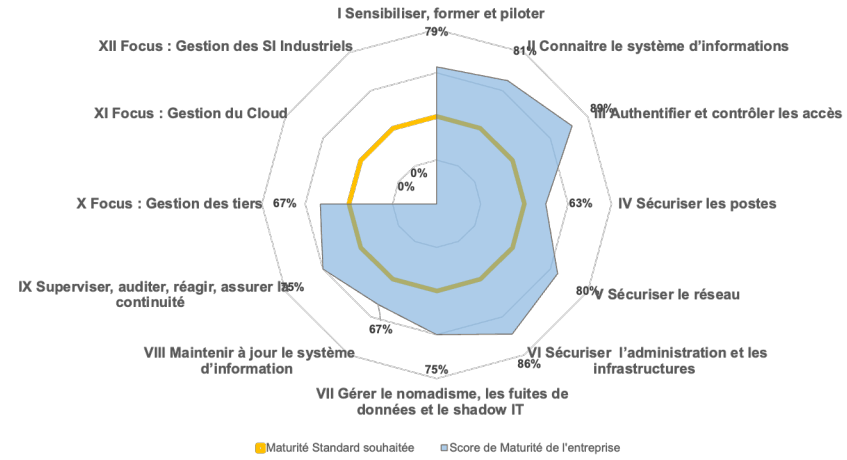
Nombre d'actions :
5

Coût/Charge :
25,5 J-H
<15 k€

Indice de cybersécurité

Actuel	1 an
D	B
38 / 100	76 / 100





5. Détail des constats et recommandations par axe d'analyse

I - Sensibiliser, former et piloter

Constats – Points forts

Niveau de sensibilisation des utilisateurs

- Utilisateurs assez sensibles, certains avez déjà suivi des formations dans des emplois précédents

Rôles et les responsabilités en matière de cybersécurité

- Monsieur X est identifié comme porteur du projet

Constats – Points d'amélioration

Organisation de la sensibilisation des utilisateurs par l'entreprise

- Il est toujours bon d'effectuer un rappel une fois par an ou tous les 2 ans
- Pas de charte informatique

Approche des risques incluant les risques cyber

- Pas d'approche jusqu'au présent diagnostic

Outils et pilotage des indicateurs cyber

- Pas d'outils à l'heure actuelle

Recommandations

- Continuer à sensibiliser les collaborateurs de l'entreprise afin d'ancrer le sujet cyber **surtout en période de recrutement**
- Rédiger une charte informatique

5. Détail des constats et recommandations par axe d'analyse
II – Connaître le Système d'Information

Constats – Points forts

Formalisation de l'architecture du SI
- Schéma complet du SI fourni par le prestataire suite à notre demande

Inventaire des applications
- Un document d'inventaire des applications a été rédigé

Constats - Points d'amélioration

Inventaire des applications
- Il n'existe pas d'inventaire à ce jour

Inventaire des données
- Il n'existe pas d'inventaire à ce jour

Identification des outils et informations sensibles
- Un projet RGPD a été initié et n'a pas été terminé

Recommandations

- Il est nécessaire de se conformer au RGPD
- Etablir un inventaire des données et des outils sensibles

5. Détail des constats et recommandations par axe d'analyse
III – Authentifier et contrôler les accès

Constats – Points forts

Inventaire des utilisateurs et droits
- Chaque utilisateur possède son propre lecteur de stockage sur le serveur et a un accès au lecteur commun.

Compte individuel
- Chaque utilisateur a son propre compte, il n'y a pas de compte générique

Inventaire des utilisateurs et droits
- Le prestataire possède une fiche sur l'organisation des droits afin de configurer les postes de travail facilement

Procédure entrée/sortie/changement de poste
- Le prestaire s'occupe de tout. En sortie le poste est remis en mode usine. Lors d'une nouvelle entrée, un nouveau poste est configuré avec désinstallation des logiciels non nécessaires. Une fiche d'intervention est remise à l'entreprise.

VPN
- **Généralisation de l'utilisation du VPN en dehors de l'entreprise**

Constats - Points d'amélioration

Politique de mot de passe
- Il n'y a aucune politique définissant le changement des mots de passe

Comptes techniques
- Il n'y a pas de compte technique sur les postes de travail, les utilisateurs sont administrateurs de leur poste.
- **Le prestataire se connecte au poste de travail via TeamViewer**

Recommandations

- **TOP 5** : Une mise en place d'une politique de changement de mot de passe est fortement recommandée car il y a une forte utilisation de pc portables.
- Créer des comptes techniques sur les postes des utilisateurs

5. Détail des constats et recommandations par axe d'analyse

IV – Sécuriser les postes

Constats – Points forts

Lutte contre les logiciels malveillants

- L'antivirus ESET Endpoint Antivirus est installé sur tous les postes de travail. Il est configuré pour offrir une protection optimale (fichiers + messagerie) et est mis à jour automatiquement.

Décommissionnement des postes

- Les postes sont rendus au prestataire qui se charge de les remettre en mode usine.

Constats - Points d'amélioration

Sécurisation physique des postes

- Les quelques postes de travail fixes ne sont pas attachés. L'entreprise utilise quasiment que des ordinateurs portables

Lutte contre les logiciels malveillants

- L'antivirus ESET Endpoint antivirus est désactivable par l'utilisateur

Durcissement et chiffrement du poste de travail

- Aucun système de ce type n'est en place, le chiffrement par défaut de Windows est actif

Recommandations

- Il faudrait que l'antivirus ne soit pas désactivable par l'utilisateur
- Le durcissement des ordinateurs portables peut être activé en fonction de la configuration et des usages de celui-ci (si stockage de fichiers confidentiels sur le bureau et non sur le serveur par exemple). Il peut être judicieux de le mettre en place surtout sur les terminaux des dirigeants.

5. Détail des constats et recommandations par axe d'analyse

V – Sécuriser le réseau

Constats – Points forts

Firewall et outils de contrôle
- Le serveur est équipé d'un pare-feu logiciel et d'un antivirus

Messagerie
- L'accès à la messagerie Outlook est sécurisée grâce à l'antivirus

Wifi
- L'entreprise dispose de 3 Wifi sécurisés par clé WPA2 (box Orange + 2 points d'accès)
- L'utilisateur connecté au Wifi peut atteindre uniquement la passerelle, il n'accède pas aux serveurs

Constats - Points d'amélioration

Firewall et outils de contrôle
- Il n'y a pas d'outils de contrôle

Réseau et cloisonnement
- Il n'y a pas de cloisonnement
- Un ordinateur peut être branché en filaire au réseau et accèdera à internet

Accès web
- Accès non redondé et non filtré, nous pouvons faire ce que l'on veut sur internet

Recommandations

- Il est fortement recommandé de créer des Whitelist réseau pour éviter à n'importe quel périphérique de se connecter sur le réseau
- Mettre en place un filtrage des accès web est recommandé mais pas nécessaire au vu de la configuration du site et des usages des utilisateurs
- Vous pouvez également passer à une sécurisation du Wifi plus importante en utilisant le protocole WPA3, mais ce n'est pas une obligation vu l'emplacement isolé du site

5. Détail des constats et recommandations par axe d'analyse

VI – Sécuriser l'administration

Constats – Points forts

Lutte contre les logiciels malveillants
- Antivirus installé sur les serveurs

Sauvegarde des serveurs
- Les données des serveurs sont sauvegardées tous les jours
- Connexion entre entre le site 1 et le site 2
- 1 sauvegarde/semaine de l'image serveur

Constats - Points d'amélioration

Sécurité physique des infrastructures
- Salle serveur inadaptée

Décommissionnement des infrastructures
- Le matériel est rendu tel quel au prestataire

Durcissement du système et chiffrement serveur
- Aucune solution de ce type

Réseau administrateur
- Le prestataire se connecte directement au serveur dans l'entreprise ou via un VPN et utilise un compte un spécifique.

Accès et outils d'administration sur les postes et serveurs
- Les utilisateurs sont administrateurs de leur poste

Accès d'administration à distance
- Le prestataire utilise TeamViewer pour se connecter à distance sur les postes de travail.

Recommandations

- **TOP 5** : changer les droits des utilisateurs sur leur poste de travail afin qu'ils ne soient plus administrateurs
- **TOP 5** : réaménager la salle serveur : peut-être ajouter une cloison comportant une porte pour isoler le chauffe-eau, et déplacer les produits ménagers. Installer une climatisation dans le local.

- Penser à supprimer les données des serveurs avant de les rendre au prestataire

5. Détail des constats et recommandations par axe d'analyse

VII – Gérer le nomadisme, les fuites de données et le *shadow IT*

Constats – Points forts

Nomadisme et télétravail

- Utilisation du VPN OpenVPN pour tous les accès en dehors de l'entreprise

Constats - Points d'amélioration

Nomadisme et télétravail

- Postes de travail non chiffrés
- Accès aux messageries possibles sur tous les smartphones sans contrôle
- **Pas de demande d'identifiant pour se connecter au VPN**

Shadow IT

- Utilisation de certains services en fonction des besoins clients et fournisseurs ou interne, sans risque car sans données confidentielles.

BYOD et smartphone

- Téléphone en configuration classique avec verrouillage systématique, il n'y a pas de notion de sécurisation / contrôle des accès à distance

Lutte contre les fuites de données

- Aucun outil utilisé

Recommandations

- Ne pas autoriser la connexion des smartphones personnels au wifi de l'entreprise
- Eviter les usages personnels des ordinateurs et smartphones professionnels
- La connexion à OpenVPN devrait demander un mot de passe

- **RAPPEL** : la consultation sur un smartphone connecté au wifi de l'entreprise, d'une pièce jointe contenant un logiciel malveillant peut entraîner une propagation de celui-ci sur le réseau et contaminer d'autres postes et le serveur.

5. Détail des constats et recommandations par axe d'analyse

VIII – Maintenir à jour le Système d'Information

Constats – Points forts

Politique de mise à jour des OS

- Les OS des postes de travail sont à jour

Politique de mise à jour des applications

- Les applications sont à jour avec les dernières versions

Constats - Points d'amélioration

Politique de mise à jour des OS

- Pas de politique particulière, les OS sont mis à jour pas les utilisateurs, il n'y a pas de suivi de la part du prestataire

Politique de mise à jour des applications

- Pas de politique particulière, les applications sont mises à jour pas les utilisateurs

Abonnements à des flux d'informations sur les vulnérabilités découvertes

- Pas d'abonnement à des flux d'informations spécifique. L'entreprise n'ayant pas un personnel dédié à l'IT, il est compliqué pour de gérer cette partie

Recommandations

- Etudier la gestion des mises à jour des OS et des applicatifs avec le prestataire pour avoir un suivi

5. Détail des constats et recommandations par axe d'analyse

IX – Superviser, auditer, réagir, assurer la continuité

Constats – Points forts

Supervision et journalisation

- Le serveur de sauvegarde envoie un e-mail d'information au prestataire et à M. XXX lorsque la sauvegarde est terminée.
- Il y a un monitoring du serveur

Politique de sauvegarde

- Données du serveur sauvegardées 2 fois par jour avec sauvegarde croisées entre le site 1 et le site 2.
- Image serveur sauvegardée 1 fois par semaine

Test de restauration

- Test effectué une fois

Constats - Points d'amélioration

SOC

- Pas de SOC et aucun intérêt pour ce type de structure

Audit / Pentesting

- Aucun audit ou pentest n'ont été réalisé à ce jour.

Préparation à la crise et PCA / PRA

- Aucune cellule de crise jusqu'à maintenant et aucun document. Programme initié par le présent document

Recommandations

- **TOP 5** : Tester les sauvegardes et mettre en place des tests annuels de restauration
- Continuer la documentation du PRA et créer un PCA
- Un pentest poussé du système et de l'administration à distance peut être envisagé mais pas obligatoire

5. Détail des constats et recommandations par axe d'analyse

X – Focus : Gestion des tiers

Constats – Points forts

Gestion des paiements et des données fournisseurs

- Contre-appel systématique en cas de doute
- Données financières gérées par M. XXX et le service comptabilité

Constats - Points d'amélioration

Maîtrise des risques liés à l'infogérance et aux prestations SI

- Pas de contrat avec le prestataire

Identification des tiers critiques

- Il n'y a pas d'identification des tiers critiques
- Il n'y a pas de clauses dans les contrats de vente

Recommandations

- Identifier les tiers critiques et établir les contrats nécessaires pour se protéger
- Editer un contrat d'infogérance avec le prestataire afin de déterminer les impacts en cas d'erreur de sa part.

- **Définition** : le tiers est un service que l'entreprise utilise et qui contient des informations sensibles. Si ce service est attaqué, vous pouvez être attaqué à votre tour grâce aux informations que les attaquants auront collectées. Exemple pour l'entreprise XXX : cabinet comptable, SAGE

6. Eléments de préparation à la gestion de crise Cyber

Check list de crise

Avant la crise

- **Anticiper**
  - ❑ Déterminer l'organisation de la cellule de crise et ses outils (cf pages suivantes)
  - ❑ Prévoir une procédure de remontée des incidents Cyber par tous les salariés
  - ❑ Prévoir une procédure de shutdown – mise hors réseau de tout et parties de l'IT / OT / IoT
  - ❑ Formaliser un PRA
- **Communiquer**
  - ❑ Sensibiliser les salariés au risque Cyber, et insister sur la procédure de remontée d'incidents Cyber

Pendant la crise

- **Réagir**
  - ❑ Activer la cellule de crise plutôt trop tôt que trop tard
  - ❑ Procéder aux mises hors réseau de tout ou parties de l'IT / OT / IoT plutôt trop tôt que trop tard
  - ❑ Tenir un registre horodaté des actions conduites / des constats effectués
  - ❑ Veiller à conserver les preuves trouvées (mails, logs…)
  - ❑ Ne jamais payer de rançons (qui vous signalerez comme cible rentable)
  - ❑ Mettre en place des solutions palliatives avec l'aide de vos prestataires et « sachants », suivre le PRA pour un redémarrage progressif et contrôlé post remédiation
- **Communiquer**
  - ❑ Communiquer aux salariés et parties prenantes impactées afin d'éviter qu'ils ne propagent ou contribuent à la crise
  - ❑ Déposer plainte une fois suffisamment d'éléments collectés
  - ❑ Signaler l'incident à cybermalveillance.gouv.fr
  - ❑ Signaler l'incident à la CNIL si des données personnelles ont pu être consultées, modifiées ou détruites par des cybercriminels

Après la crise

- **S'améliorer**
  - ❑ Tirer les leçons de l'incident et les inscrire dans une démarche d'amélioration continue
- **Guérir**
  - ❑ Tenir compte des impacts humains d'une crise en terme de charge de travail, sentiment de vulnérabilité, d'humiliation..
- **Communiquer**
  - ❑ Communiquer aux salariés et parties prenantes la fin d'incident

6. Eléments de préparation à la gestion de crise Cyber

Organisation de la cellule de crise

A maintenir à jour par l'entreprise

Moyens de la Cellule de Crise	Description	Réponse Entreprise	Contact / Accès
Responsable	Coordinateur de la gestion de crise cyber	*XXX*	*xxx@domaine.com* *0123456789*
Suppléant	Remplaçant / Binôme	*Nom du salarié*	*N° téléphone / Adresse mail*
Membres	Participants à la cellule	*Nom du salarié* *Nom du salarié* *Nom du salarié* *…*	*N° téléphone / Adresse mail* *N° téléphone / Adresse mail* *N° téléphone / Adresse mail* *…*
Salle de crise	De préférence physique - attention, les salles virtuelles peuvent être inaccessibles faute de réseau	*Salle de réunion*	*Site 1*
Autorité	Organisme ou personne à qui le responsable Cellule de crise rend compte (Codir, Dirigeant…)	*XXX*	*Modalité de suivi / fréquence*
Sponsor	Porteur responsable du sujet Cyber au sein de la direction (yc hors crise	*XXX*	*xxx@domaine.com* *0123456789*
Moyens IT	Postes utilisés – attention, les postes habituels peuvent être inaccessibles / chiffrés	*Moyens prévus pour la crise*	*Localisation*
Prestataires clés	Prestataires aptes à contrôler / monitorer / restaurer / remédier à la crise	*Prestataire*	*0123456789 (attention la téléphonie fixe peut être compromise)*
Documentation clé	Documentation nécessaire à la cellule de crise : Schéma d'architecture, PRA, inventaires matériel, matrice des droits utilisateurs, logs, contrats	*Schéma d'architecture joint à ce document* *Créer le PRA*	*Les documents de matrice des droits, inventaires matériels et schémas sont chez le prestataire informatique.*
Coordonnées autorités	Coordonnées des autorités à prévenir (yc client sensible, forces de l'ordre, cybermalveillance.gouv.fr, CNIL…)	*Nom de l'interlocuteur*	*Coordonnées*

6. Eléments de préparation à la gestion de crise Cyber
Synthèse des procédures de sécurisation et reprise d'activité

A maintenir à jour par l'entreprise

Thématique	Eléments de gestion de crise	Réponse	Précision / Commentaire
Coupure d'accès / *shutdown*	Existence d'une procédure de mise hors réseaux des actifs	*Oui*	*Affiche en salle serveur et dans les bureaux*
Reprise d'activité	Existence d'un plan de reprise d'activité	*Non*	*Localisation*
	Date de dernière mise à jour	-	
Restauration de sauvegarde *(cf. page suivante)*	Etat le plus récent auquel le système peut être restauré sur base des sauvegardes	*J-1 jour*	*Les données peuvent être restaurées à J-1, en revanche l'image serveur sera restaurable à celle du vendredi de la semaine précédente*
	Actif(s) dont les derniers tests de restaurations sont les plus anciens	*Nom des actifs*	*Cf. dernière colonne du tableau de la page suivante – préciser la date*
	Actifs dont la restauration n'a jamais été testée	*Tous*	*Cf. dernière colonne du tableau de la page suivante – préciser le motif*
	Actifs non sauvegardés	*Disques locaux de chaque poste de travail et téléphones portables*	

6. Eléments de préparation à la gestion de crise Cyber

Inventaires des moyens de restauration

A maintenir à jour par l'entreprise

Objet sauvegardé	Propriétaire métier	Fréquence & Profondeur	Opérateur / Prestataire et coordonnées	SLA restauration	Localisation source	Localisation sauvegarde	Date de dernier test de restauration avec succès
Données du serveur	*DAF*	*Quotidien incrémentale à 12h30 Rétention 30j*	*Prestataire 0123456789*	*1/2 journée*	*SERVEUR site 1 et site 2*	*Disque dur externe sur site 1 et sur site 2*	-
Sauvegarde Image Système	DAF	*Hebdomadaire tous les Samedi 21h*	*Prestataire 0123456789*	*1/2 journée*	Serveur BDD & Application	ImageSystème déposée sur serveur dans le dossier « folder/save] (ensuite sauvegarder sur Disque externe & VPN)	-
Serveur BDD	DAF	Quotidienne à 22h Rétention 14j	*Prestataire 0123456789*	*1/2 journée*	*SERVEUR site 1 et site 2*	Sauvegarde Locale (serveur)	-
Sauvegarde VPN	DAF	00h-04h Rétention 20j	*Prestataire 0123456789*	*1/2 journée*	Serveur site 2	Locale+Disque Externe	-

6. Eléments de préparation à la gestion de crise Cyber

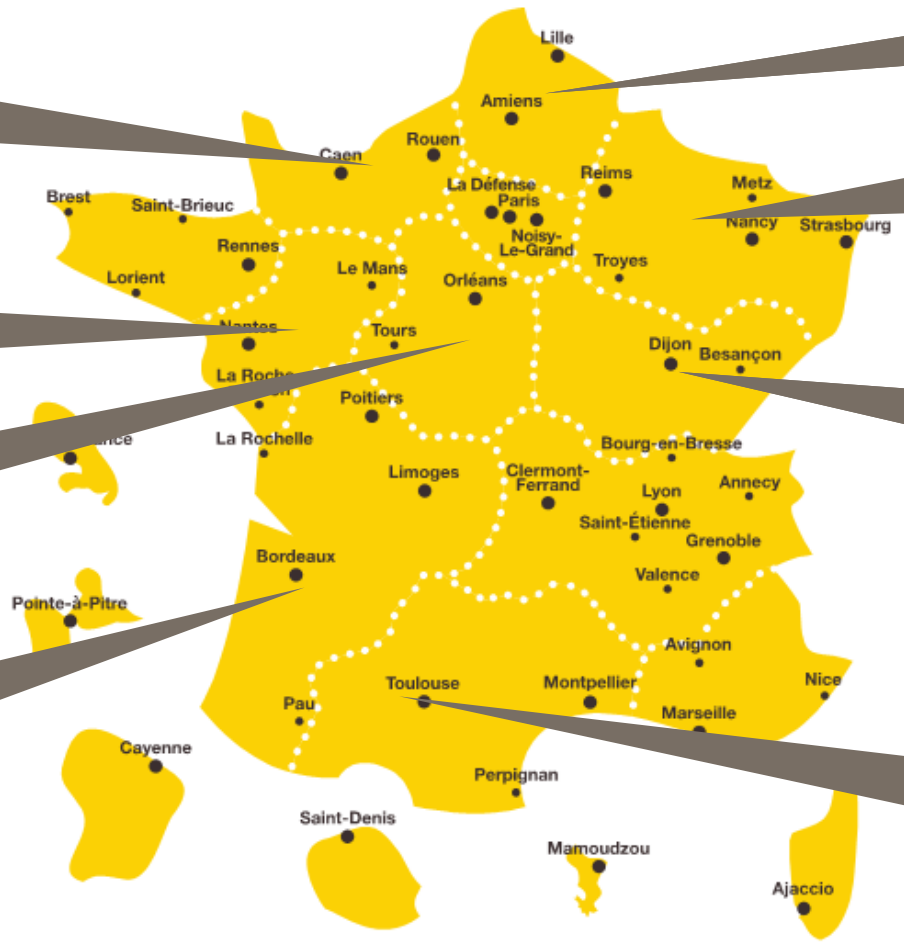
Carte des CSIRT (Computer Security Incident Response Team)

Normandie Cyber
https://adnormandie.fr/besoin/normandie-cyber/

Pays de la Loire Cyber Assistance
https://www.paysdelaloire.fr/economie-et-innovation/entreprise/mon-organisation-subit-une-cyberattaque

CYBE REPONSE
Centre Val de Loire
https://www.cybereponse.fr

Campus régional de Cybersécurité et de Confiance numérique
https://www.campuscyber-na.fr/



CSIRT Hauts de France
http://csirt-hdf.fr/

Grand Est Cybersécurité
https://cybersecurite.grandest.fr/

CSIRT
Bourgogne Franche-Comté
https://www.csirt-bfc.fr/

Cyber'Occ
https://www.cyberocc.com/en-cas-durgence/

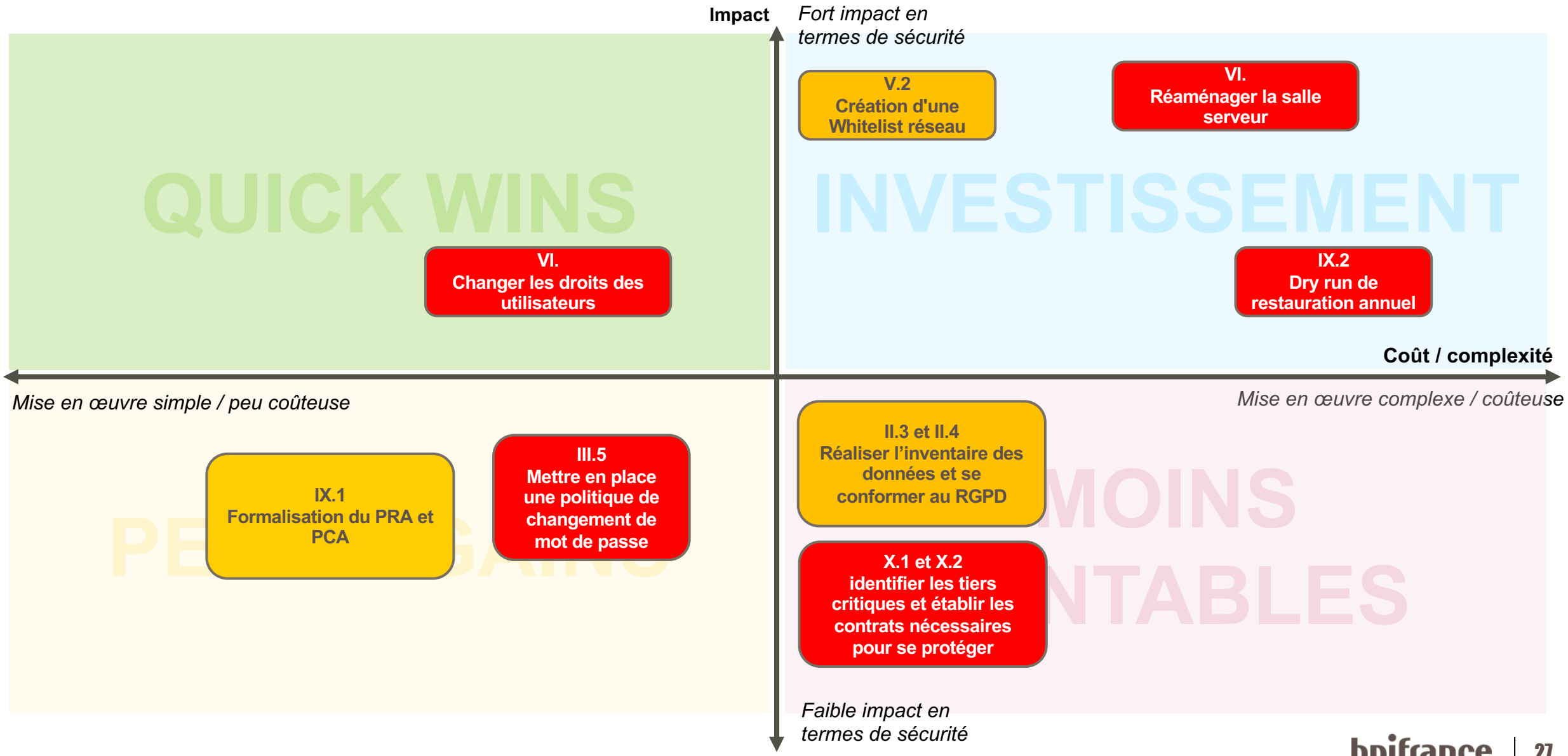
https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux/

7. Elaboration du plan d'action

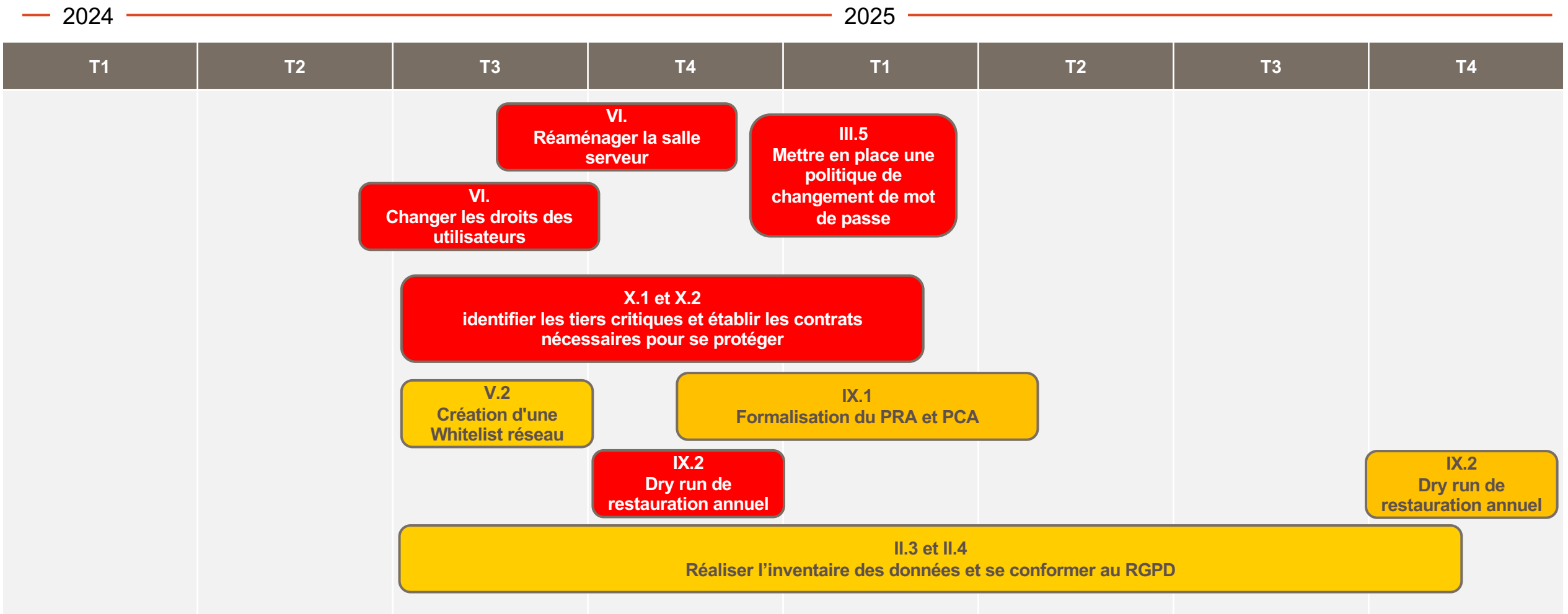
Liste des recommandations

#	Chapitre	Typologie d'action	Détail	A effectuer par	Responsable interne	Priorité	Charge interne Build + Run		Charge externe Build + Run		Proposition de calendrier / lancement
Numéro de l'action	(correspond au chapitre de la grille d'analyse)	Procédure / Action de sensibilisation / Projet à lancer / Mise en œuvre technique / Prestations	Description contextualisée	(nom d'un salarié, prestataire externe)	(salarié validant que l'action a bien été effectuée)	(TOP5 / Haute/Basse)	Build Estimation : JH	Run Estimation : JH / an	Build Estimation : <1k€, 1à10k€, >10k€…	Run Estimation : <1k€, 1à10k€, >10k€ / an	(Date proposée de lancement du chantier -indicatif)
1	III Authentifier et contrôler les accès	Mise en œuvre technique	Mettre en place d'une politique de changement de mot de passe	Prestataire	M. XXX	TOP Prio			1 à 10k€		oct-24
2	VI Sécuriser l'administration et les infrastructures	Mise en œuvre technique	Les utilisateurs ne doivent pas être administrateurs de leur poste de travail. Certains ordinateurs portables n'ont pas de mot de passe session.	Prestataire	M. XXX	TOP Prio			1 à 10k€		juin-24
3	VI Sécuriser l'administration et les infrastructures	Prestation	Repenser la salle serveur en ajoutant une cloison de séparation avec porte entre le chauffe-eau et le serveur, déplacer les produits ménagers et ajouter une climatisation	-	M. XXX	TOP Prio			1 à 10k€		août-24
4	IX Superviser, auditer, réagir, assurer la continuité	Mise en œuvre technique	Tester les sauvegardes et mettre en place des tests annuels de restauration	Prestataire	M. XXX	TOP Prio	1	1	<1k€	<1k€	oct-24
5	X Focus : Gestion des tiers	Procédure	Editer un contrat d'infogérance avec le Prestataire et identifier les tiers critiques	M. XXX	M. XXX	TOP Prio	4				juil-24
6	I Sensibiliser, former et piloter	Procédure	Rédiger une charte informatique	M. XXX	M. XXX	Basse	1				déc-24
7	II Connaitre le système d'informations	Procédure	Rédiger l'inventaire des données et se conformer au RGPD	M. XXX	M. XXX	TOP Prio	15		1 à 10k€		juil-24
8	IV Sécuriser les postes	Mise en œuvre technique	Antivirus non désactivable par l'utilisateur	Prestataire	M. XXX	Basse			1 à 10k€		juin-24
9	V Sécuriser le réseau	Mise en œuvre technique	Création d'une Whitelist réseau	Prestataire	M. XXX	Haute			1 à 10k€		juil-24
10	V Sécuriser le réseau	Mise en œuvre technique	Mettre en place un filtrage des accès web	Prestataire	M. XXX	Basse			<1k€		oct-24
11	VII Gérer le nomadisme, les fuites de données et le shadow IT	Procédure	Ne pas autoriser la connexion des smartphones personnels au wifi	M. XXX	M. XXX	Basse	0,5				août-24
12	VIII Maintenir à jour le système d'information	Procédure	Gestion des mises à jour des OS et des applications	Prestataire	M. XXX	Basse					2024-2025
13	IX Superviser, auditer, réagir, assurer la continuité	Procédure	Continuer la documentation du PRA et créer un PCA	M. XXX	M. XXX	Haute	4				févr-24
14	IX Superviser, auditer, réagir, assurer la continuité	Mise en œuvre technique	Envisager d'effctuer un pentest du système et l'administration à distance	-	M. XXX	Basse			1 à 10k€		2024-2025

7. Elaboration du plan d'action
Analyse Impact / Complexité



7. Elaboration du plan d'action
Proposition de calendrier



Nb : la parallélisation des projets n'est possible que si les ressources projets sont disponibles

08. ANNEXES

8. Annexes
a. Entretiens effectués

Nom	Fonction	Date	Commentaires
M. XXX	DAF	15/04/2024	
Eployé 1	Responsable administration des ventes	15/04/2024	
Eployé 2	Responsable vente et conditionnement	15/04/2024	
Eployé 3	Assistante commerciale à l'administration des ventes	15/04/2024	
Eployé 4	Responsable de centre	15/04/2024	
Eployé 4	Commerciale achat	15/04/2024	
Eployé 5	Commercial export	15/04/2024	
Eployé 6	Assistante commerciale	15/04/2024	

8. Annexes
b. Synthèse des tests complémentaires effectués

Audit messagerie :

Nous avons testé l'adresse e-mail xxx@domaine.com.
Le résultat du test est disponible en consultant le lien suivant : Lien
Saisissez le numéro de rapport suivant xxx dans le champ « Trouvez votre rapport »

ENVOI CONFIDENTIEL : 3/5
Votre fournisseur d'email vous fournit un minimum de confidentialité en utilisant le chiffrement lors de l'envoi et la réception de messages. Toutefois, il ne peut pas assurer l'identité des tiers avec lesquelles il interagit.

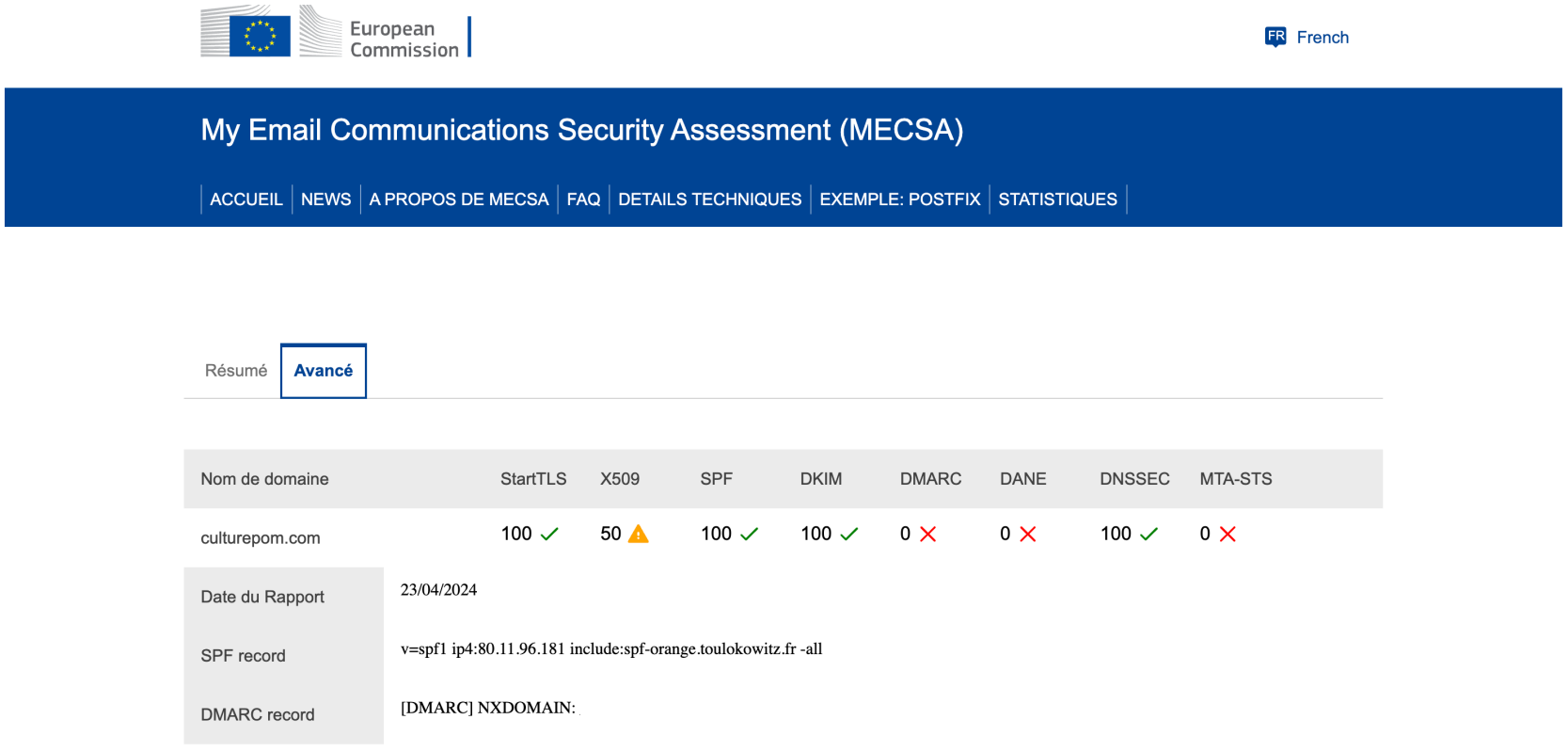
HAMECONNAGE ET USURPATION D'IDENTITE : 4/5
Votre fournisseur d'email bloque les messages provenant de serveurs non légitimes. Il prend également des mesures pour éviter que des serveurs non autorisés envoient des emails à partir de comptes de votre domaine. Grâce à ces actions, il réduit considérablement la probabilité de recevoir (ou de générer) des attaques d'usurpation d'identité et/ou d'hameçonnage.

INTEGRITE DES MESSAGES : 4/5
Votre fournisseur d'email peut identifier les messages qui ont été modifiés ou interceptés durant leur envoi (du MTA de l'expéditeur au MTA du destinataire).

En résumé :
L'entreprise bénéficie d'une très bonne protection de sa messagerie électronique, aussi bien en réception qu'en émission.
Attention, cette protection ne doit pas vous empêcher de rester vigilent.

8. Annexes
b. Synthèse des tests complémentaires effectués

Audit configuration messagerie :



Préconisations:

- Contrôler le certificat X.509
- Ajouter une entrée DMARC dans le DNS du nom de domaine

- Le paramètre DMARC permet aux administrateurs de messagerie d'empêcher les pirates informatiques d'usurper l'identité de leur organisation et de leur domaine.
- Il permet aussi de passer les contrôles de Gmail et Yahoo

Utilisation des messageries par les utilisateurs :

Sur les ordinateurs fixes ou portables, les utilisateurs consultent leurs e-mails via les clients de messagerie Outlook ou Thunderbird. Aucun identifiant n'est demandé à l'ouverture de la messagerie.

Sur les smartphones, les utilisateurs utilisent le client par défaut, sans demande d'identification.

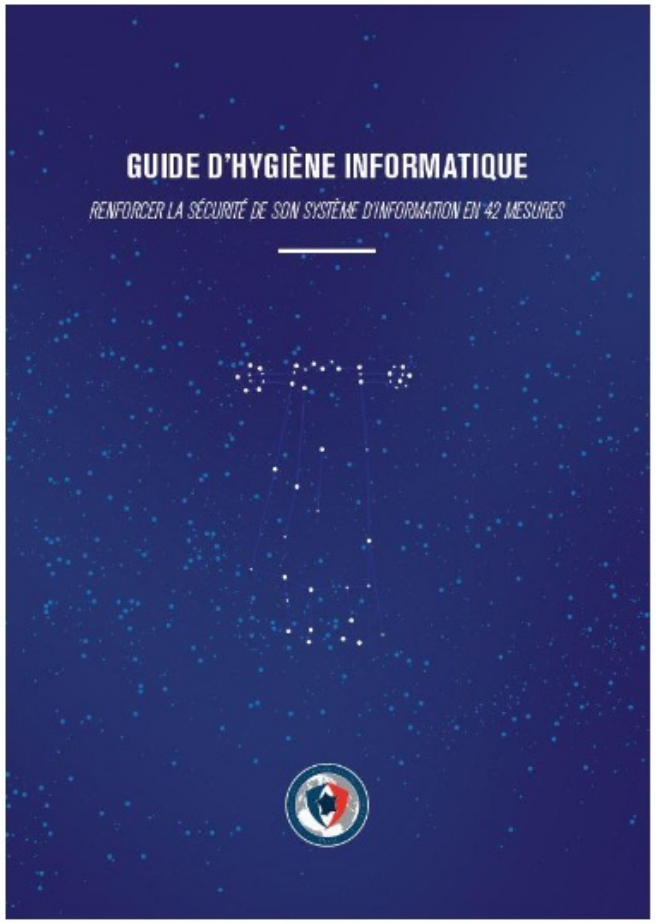
Nous signalons aussi qu'il y a une forte utilisation de la messagerie instantanée WhatsApp pour communiquer directement avec les clients et fournisseurs. Attention si vous envoyez des fichiers contenant des informations sensibles.

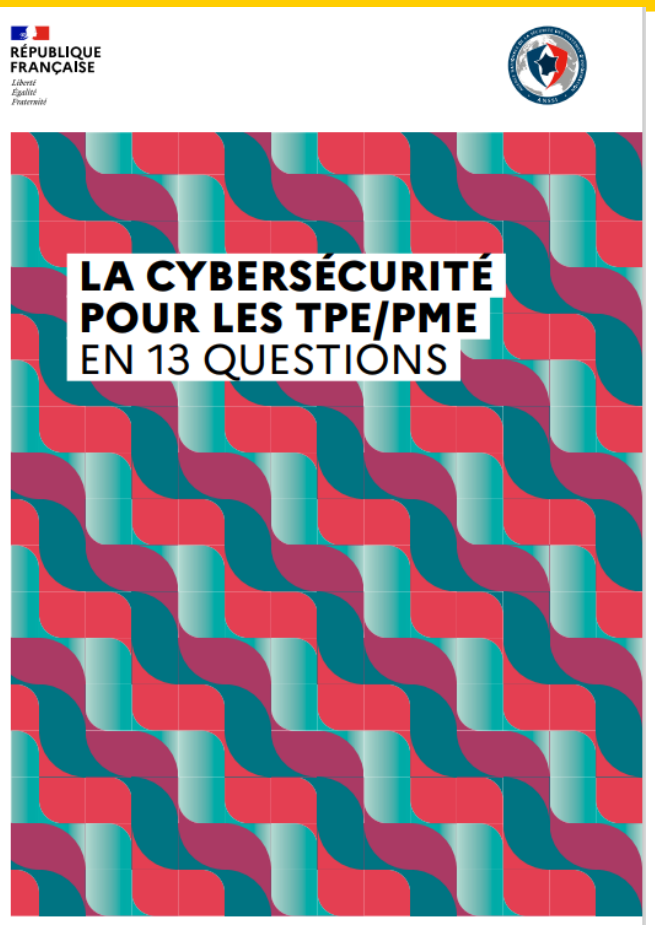
8. Annexes
b. Synthèse des tests complémentaires effectués

Audit DNS :

Le nom de domaine est configuré correctement et bénéficie d'une protection optimale.
Le domaine bénéficie d'une bonne réputation auprès des moteurs de recherche, il n'est pas blacklisté

8. Annexes
c. Guide produit par l'ANSSI





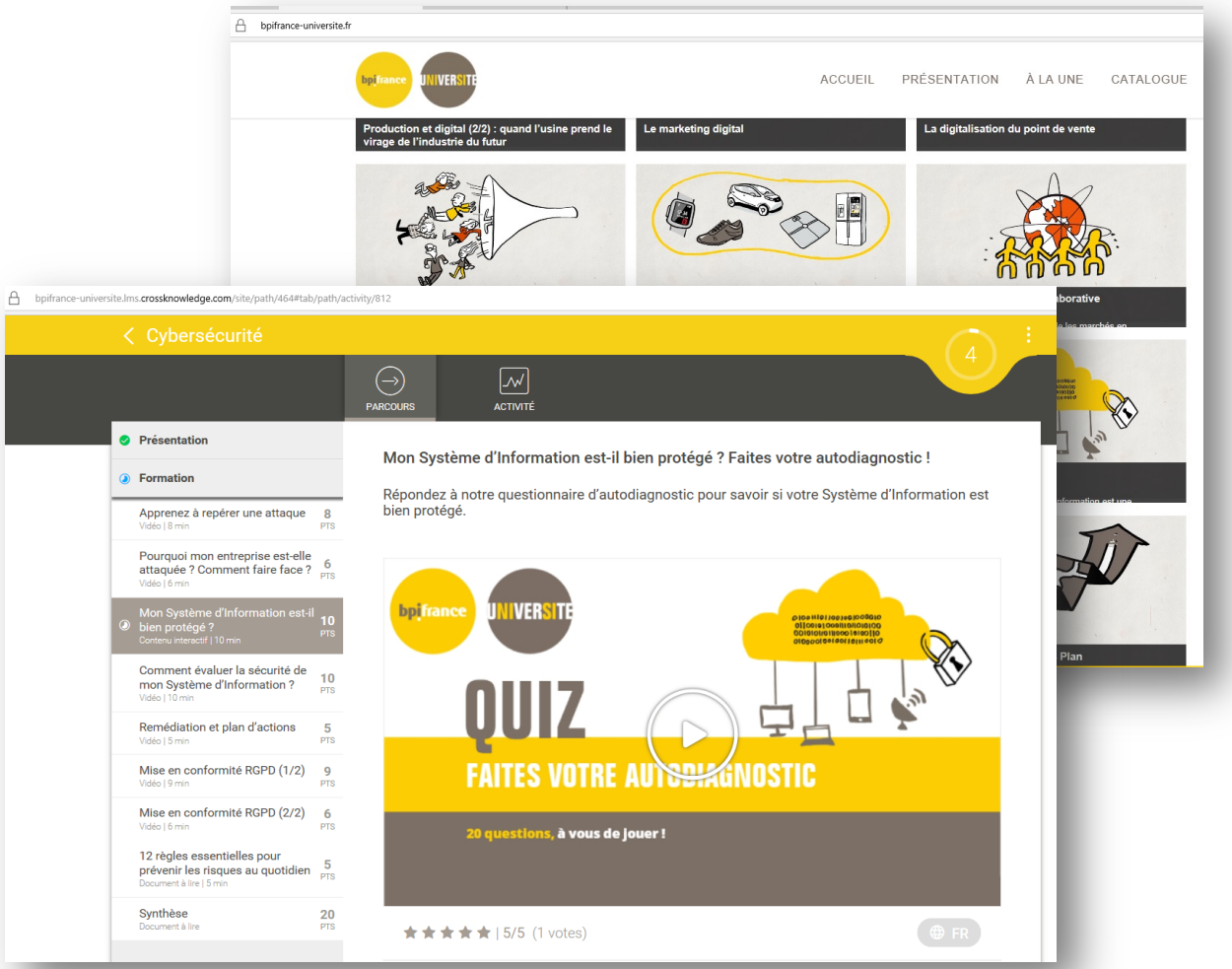
- **Cybersécurité des TPE/PME en 13 question** : https://www.entreprises.gouv.fr/fr/actualites/numerique/la-cybersecurite-pour-tpe-pme-13-questions
- **Guide d'hygiène** : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
- **Vérification de la force d'un mot de passe :** https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

8. Annexes
d. Fiches communication Cyber-malveillance

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition

8. Annexes

e. Module e-learning, autodiagnostic et guide « livre jaune » à l'usage des dirigeants



https://bigmedia.bpifrance.fr/etudes/cybersecurite-un-guide-pratique-a-destination-des-dirigeants

Cybersécurité :
Un guide pratique à destination des dirigeants

SERVIR L'AVENIR