# DIAGNOSTIC CYBER-DEFENSE
## Cahier des charges

Le Diagnostic Cyber-Défense se fixe pour objectif de permettre aux PME exerçant des activités liées au secteur de la défense, d'évaluer le niveau de sécurité de leurs systèmes d'information, d'identifier les failles éventuelles, et d'accompagner la mise en œuvre, le cas échéant, d'un plan de remédiation, audité a posteriori.

Il consiste en une prestation d'audit et de conseil, puis, éventuellement d'accompagnement dans la mise en œuvre des recommandations. Il est mené obligatoirement, dans la première phase, par un PASSI référencé par l'ANSSI[1], et principalement selon la méthodologie EBIOS RM (Expression des Besoins et Identification des Objectifs de Sécurité - Risk Management). La seconde phase pourra être réalisée par un PASSI ou un cyber-expert référencé par l'ANSSI et le ministère de l'intérieur via le dispositif cybermalveillance[2].

Le Diagnostic Cyber-Défense s'adresse aux entreprises[3] françaises[4] ayant des activités de défense, et pour lesquelles la Direction Générale de l'Armement (DGA) donne un pré-accord. Les besoins identifiés des entreprises bénéficiaires doivent être :

- L'identification et la compréhension des risques numériques
- La détermination de mesures de sécurité adaptées aux menaces
- La mise en place d'une démarche d'amélioration continue et de suivi

Le Diagnostic Cyber-Défense comporte ainsi 2 phases :

1. Audit : analyse de risque cyber, et rédaction d'un plan de remédiation
2. Accompagnement à la mise en œuvre du plan de remédiation et audit final de vérification suite aux mesures correctives

La phase 2 n'est pas obligatoire : une entreprise peut bénéficier de la phase 1 du Diagnostic Cyber-Défense, et ne pas nécessiter ou ne pas souhaiter mener la phase 2. L'entreprise devra déposer pour chaque phase une nouvelle demande de diagnostic sur la plateforme en ligne dédiée.

Bpifrance se réserve le droit de refuser la demande de prise en charge du diagnostic déposée sur la plateforme en ligne dédiée (par exemple statut « en difficulté », proposition commerciale non conforme, entreprise ne correspondant pas à la cible du dispositif selon Bpifrance ou la DGA.)

## 1. Etendue de la prestation de Diagnostic Cyber-Défense

[1] Agence Nationale de la Sécurité des Systèmes d'Information. Les prestataires habilités à effectuer la première phase du Diagnostic Cyber-Défense sont obligatoirement des PASSI (prestataires d'audit de la sécurité des systèmes d'information) qualifiés et référencées sur le site de l'ANSSI.

[2] Créé par l'ANSSI et le ministère de l'intérieur, Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes d'actes de cybermalveillance. Les prestataires habilités à effectuer la seconde phase du Diagnostic Cyber-Défense peuvent être « cyber-expert » qualifiés et référencés sur le site cybermalveillance.gouv.fr.

[3] Entreprises (PME ou ETI) de moins de 2 000 salariés. Sont exclues du dispositif les entreprises « en difficulté » au sens de la réglementation européenne. Les entreprises candidates sont soumises aux articles 107 et 108 du traité sur le fonctionnement de l'Union Européenne aux aides « de minimis », et sont exclues si elles ont dépassé le plafond maximum des aides de minimis.

[4] Immatriculées en France et ayant une activité économique significative en France

### 1.1. Phase 1 : Analyse de risques et définition d'un plan de remédiation

Cette première phase consiste à déployer la méthode d'analyse de risque de référence EBIOS RM[5].

La première étape se compose ainsi d'ateliers de travail, pouvant aller jusqu'à 5, et dont le contenu est défini par la méthode. Toutefois, le nombre, l'architecture des ateliers et le temps d'exécution (et donc le coût) diffèrent selon la taille, les besoins et la maturité de l'entreprise bénéficiaire.

Elle aboutit sur une série de recommandations et un plan détaillé de mesures de remédiation. Ce plan consiste en la prescription de mesures tant organisationnelles (procédures, formation de personnels, etc.) que techniques (déploiement de matériels ou logiciels) visant à réduire certains risques résiduels. Un chiffrage estimatif des investissements à fournir par l'entreprise devra être produit au titre du plan de remédiation.

La proposition commerciale de l'Expert devra justifier de façon précise le dimensionnement de sa prestation en détaillant le contexte de l'entreprise (taille, besoin, maturité…).

### 1.2. Phase 2 : Accompagnement à la mise en œuvre du plan de remédiation et audit de vérification

#### a. Accompagnement à la mise en œuvre du plan de remédiation

Cette deuxième phase a pour objectif d'accompagner l'entreprise bénéficiaire dans la mise en œuvre du plan de remédiation, issu de la phase 1.

Elle consiste à assister l'entreprise dans l'organisation et le suivi de la réalisation des mesures. L'intervention de l'Expert dans cette phase dépend de la densité du plan de remédiation, et du degré d'autonomie de l'entreprise.

#### b. Audit final de vérification

L'expert effectue à l'issue de la mise en œuvre du plan de remédiation un audit de vérification visant à confirmer que les risques les plus critiques identifiés lors de l'analyse initiale (phase 1) ont été réduits.

Cette phase doit également permettre d'apporter des conseils sur le dispositif d'amélioration continue et de gestion des risques numériques mis en place par l'entreprise bénéficiaire.

## 2. Réalisation de la prestation

### 2.1. Lancement de la prestation

Préalablement au dépôt par l'entreprise d'une demande de Diagnostic Cyber-Défense, l'Expert échange avec cette dernière, lors d'un entretien (téléphonique ou physique) afin de valider la conduite de l'analyse, ses modalités et son adéquation avec le présent Cahier des Charges. À la suite de cet échange, il établit une proposition commerciale conforme au présent Cahier des Charges, rappelant le contexte fonctionnel et technique de l'entreprise bénéficiaire. Cet échange de préqualification n'est pas facturé à l'entreprise.

Lorsque l'entreprise bénéficiaire dispose d'une proposition acceptable, elle effectue sa demande de Diagnostic Cyber-Défense sur le guichet diagcyberdefense.bpifrance.fr. Celle-ci est alors instruite par la DGA et par Bpifrance.

[5] https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/

## 2.2. Modalités de réalisation

L'ensemble des informations collectées dans le cadre du Diagnostic Cyber-Défense proviendra (i) d'échanges en face à face (y compris via des moyens visio-techniques) entre l'Expert Cyber-Défense et les parties prenantes pertinentes de l'entreprise, (ii) d'*a minima* une visite de l'entreprise pour évaluer les mesures de gestion des risques déjà en place, (iii) des ateliers EBIOS RM de la phase 1, (iv) du dispositif mis en place pour suivre le déploiement du plan de remédiation (échanges téléphoniques hebdomadaires, outil à distance…).

Les délais de réalisation de la prestation courent à partir de la validation par Bpifrance de l'éligibilité de l'entreprise, et sont les suivants :

- 4 mois maximum pour la phase 1
- 4 mois maximum pour la phase 2

## 2.3. Livrables

Le Diagnostic Cyber-Défense fera l'objet de plusieurs livrables distincts :

- Phase 1 : les résultats de l'analyse de risques constitués de comptes-rendus des ateliers menés, du rapport d'analyse synthétique intégrant les recommandations et du plan détaillé de remédiation
- Phase 2 : le compte rendu d'exécution (journal de suivi, comptes-rendus des échanges téléphoniques de suivi…) et l'état de réalisation des mesures de remédiation, ainsi que le rapport d'analyse de risques.

L'ensemble de ces livrables seront transmis à la DGA, dans un délai de 10 jours à l'issue de la prestation. Le rapport d'analyse et le plan détaillé de remédiation relèvent du niveau réglementaire « Diffusion Restreinte ». Ils seront marqués comme tel et transmis de manière chiffrée via le logiciel ZED !

Les modalités de cession des droits de propriété intellectuelle portant sur ces livrables devront être envisagées dans le contrat conclu entre l'Expert Cyber-Défense et l'entreprise bénéficiaire.

## 2.4. Tarifs et taux de prise en charge

Les montants maximums de ce Diagnostic Cyber-Défense faisant l'objet d'une prise en charge à 80% s'élèvent à :

- Phase 1 :
  - 8 000 euros HT maximum (variable selon la taille et les besoins de l'entreprise, à justifier précisément dans la proposition commerciale), pour 7 jours de prestation minimum
  - Une bonification de 2000€ HT par site supplémentaire rentrant dans le périmètre du SI à auditer.

  *Pour justifier de sites supplémentaires à auditer, l'entreprise devra fournir un numéro de SIRET par établissement ainsi qu'un argumentaire prouvant l'indépendance en matière de SI pour chacun des sites.*

- Phase 2: 6 000 euros HT maximum (variable selon la densité du plan de remédiation, à justifier précisément dans la proposition commerciale), pour 5 jours de prestation minimum

Dans le respect de ces seuils, Bpifrance prend en charge 80% du coût total du Diagnostic Cyber-Défense ; la quote-part restante est à la charge de l'entreprise bénéficiaire.

# 3. Qualité et déontologie

La réalisation du Diagnostic Cyber-Défense s'appuie également sur des engagements qualitatifs que le dirigeant d'entreprise est en droit d'attendre de la part de l'Expert Cyber-Défense. Ces engagements s'appuient sur 7 principes fondamentaux.

## 3.1. Compétences

- Mettre à disposition toutes les compétences nécessaires à la bonne exécution de la prestation
- Assurer un devoir de conseil auprès du client tout au long de la mission
- Adapter ses honoraires à la mission proposée et au service rendu et ce, de manière réaliste

## 3.2. Confidentialité

- Conclure un engagement de confidentialité avec le client ou prévoir une clause de confidentialité dans le contrat conclu entre l'expert conseil et l'entreprise bénéficiaire
- Ne pas divulguer les informations transmises par le client dans le cadre de la mission

## 3.3. Ethique professionnelle

Vis-à-vis du client :

- Respecter les intérêts économiques du client
- S'engager à des pratiques commerciales loyales
- S'engager dans la réalisation de sa mission jusqu'à sa finalisation
- Travailler en toute transparence avec le client (devis, facturation, conditions générales de vente, frais annexes)

Vis-à-vis des confrères Experts et des consultants en général :

- S'engager à des pratiques saines et loyales aussi bien vis-à-vis des collaborateurs que des concurrents
- Ne pas enfreindre le droit de la propriété intellectuelle et ce, même si cela émanait de la volonté du client
- Ne fournir aucune production non rémunérée ou à un prix irréaliste
- Ne recevoir aucun avantage en dehors de la rémunération définie par le contrat

## 3.4. Conflits d'intérêts

- S'assurer de l'absence de conflit d'intérêts préalablement au démarrage de la mission
- S'assurer de n'avoir aucun intérêt, à quelque titre que ce soit, chez le client
- Informer le client dans les plus brefs délais au cas où la prise de connaissance d'informations serait susceptible de générer des conflits d'intérêts, et plus généralement informer le client de toute survenance de situation qui pourrait interférer sur le bon déroulement de la mission et/ou qui risquerait de compromettre l'exécution objective de celle-ci

## 3.5. Relation client et gestion de projet

- Informer dès que possible le client de tout retard ou incident
- Informer le client d'une mauvaise communication ou d'une incompatibilité avec celui-ci
- Fournir les livrables de la mission dans les conditions fixées au moment de la signature du contrat de prestation
- Adopter un regard critique face à la problématique client
- Lui communiquer toute erreur perçue, ne pas hésiter à remettre le projet en cause
- Signer un avenant au contrat, si une décision approuvée venait à être remise en cause
- Effectuer une mesure de la satisfaction client au cours d'un entretien à la fin de chaque phase de travail
- Fournir des traces écrites de toute information et décision importantes transmises au cours du projet

- Fournir un compte-rendu approuvé par l'ensemble des parties à l'issue de chaque réunion projet

### 3.6. Méthodologie

Rédiger une offre de prestation :

- Rédiger un devis détaillé qui explique la méthode proposée de manière précise
- Communiquer systématiquement les Conditions Générales de Ventes (obligation légale) et commenter les points importants
- Prévoir et commenter les aspects de cession des droits de propriété intellectuelle
- Vérifier si le devis rédigé est conforme avec le besoin exprimé (en interne mais aussi avec le client)

Structurer et suivre l'offre de prestation :

- Adapter ses outils de communication à la mission
- S'assurer de la bonne compréhension du projet par le client
- Faire valider les différentes phases par le client
- S'engager à la conformité des livrables vendus/délivrés
- S'assurer de la perception qualitative de la prestation par le client
- Respecter le planning établi (exception faite si le retard vient du client)

### 3.7. Conformité

- Être à jour du règlement des cotisations sociales et fiscales
- Respecter le code du travail et le droit à la formation
- Disposer des assurances professionnelles
- Fournir à Bpifrance l'ensemble des documents nécessaires à la constitution d'un dossier de connaissance client
- Rapporter au client tout aléa portant atteinte aux éléments qui pourraient avoir été fournis par lui (perte, endommagement, …)