



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

**Cahier des clauses
techniques particulières
n° 2025-07 du 28 janvier 2025**

Marché public de techniques de l'information et de la communication

Pouvoir adjudicateur contractant :

L'État – Services du Premier ministre
Secrétariat général de la défense et de la sécurité nationale (SGDSN)
51, bd de La Tour-Maubourg - 75700 Paris 07 SP

Service bénéficiaire :

Agence nationale de la sécurité des systèmes d'information (ANSSI)
51, bd de La Tour-Maubourg - 75700 Paris 07 SP

Objet du marché :

Prestations d'assistance à la préparation et à la mise en œuvre d'un exercice majeur de thématique cyber de la sous-direction Opérations – « Exercice HANDSPINNER ».

Table des matières

Article 1 -	Objet du marché.....	3
Article 2 -	Description des prestations attendues	4
2.1	Dimensionnement de l'exercice.....	4
2.1.1	Déroulement prévisionnel.....	4
2.1.2	Localisation	4
2.1.3	Nombre de joueurs.....	4
2.2	Prestations à réaliser	4
2.2.1	Tâche 1 : conseils et élaboration du scénario.....	5
2.2.2	Tâche 2 : développement de la partie technique du scénario.....	6
2.2.3	Tâche 3 : développement de la partie organisationnelle du scénario	7
2.2.4	Tâche 4 : dry-run et exécution de l'exercice	9
2.2.5	Tâche 5 : animation et observation de l'exercice.....	9
2.2.6	Tâche 6 : RETEX de l'exercice	11
Article 3 -	Modalités d'exécution de la prestation.....	12
3.1	Livrables attendus.....	12
3.2	Format des livrables attendus.....	13
3.3	Lieux de réalisation de la prestation et moyens logistiques associés	13
3.4	Interlocuteurs du titulaire.....	13
3.5	Calendrier des prestations et des fournitures	14
3.6	Report de l'exercice	16
3.7	Suivi de la prestation	16
3.8	Critères de vérification et de validation des tâches.....	17
Article 4 -	Propriété des travaux et confidentialité des résultats	17
4.1	Confidentialité des résultats	17
4.2	Propriété des travaux.....	17
Article 5 -	Communication sur l'exercice.....	18

Article 1 - Objet du marché

Créée par le décret n° 2009-834 du 7 juillet 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service à compétence nationale rattaché au secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

L'ANSSI est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Elle a pour mission d'assurer la sécurité des systèmes d'information de l'État et de veiller à celle des opérateurs nationaux d'importance vitale. Elle est également chargée de coordonner les actions de défense des systèmes d'information, de concevoir et de déployer les réseaux sécurisés répondant aux besoins des plus hautes autorités de l'État, ainsi qu'aux besoins interministériels. Elle doit, enfin, créer les conditions d'un environnement de confiance et de sécurité propice au développement de la société de l'information en France et en Europe.

Au sein de l'ANSSI, la sous-direction opérations (SDO) assure la défense des systèmes numériques d'intérêt pour la nation.

Afin de remplir au mieux ses missions, l'ANSSI doit tester régulièrement ses procédures au travers d'entraînements de ses équipes et de son organisation.

Dans le cadre de ses activités d'entraînement, la SDO souhaite réaliser un exercice (ci-après dénommé « exercice *HANDSPINNER* ») à des fins technico-organisationnelles, mobilisant ses fonctions de coordination et de décision ainsi que celles d'un ou plusieurs partenaires ministériels durant dix (10) jours ouvrés.

Pour les besoins de l'exercice, les fonctions de la SDO interviendront relativement à :

- La coordination de l'acquisition et du partage de la connaissance de la cybermenace et des vulnérabilités des systèmes numériques ;
 - La coordination du service de détection mis en œuvre au profit de ses bénéficiaires ;
 - La coordination de la réponse aux incidents de cybersécurité ;
- La coordination de l'ensemble des activités internes de la sous-direction au profit du CERT-FR, et l'échange avec les communautés des CSIRTs françaises et étrangères ;
- La coordination des équipes techniques SDO et interministérielles.

Ainsi, les objectifs de la SDO seront les suivants :

- Tester la capacité de la SDO à coordonner le traitement de la menace, des opérations d'anticipation et de cyber défense ;
- Tester la capacité de SDO à utiliser les fonctions et les prérogatives de cyber défense de ses partenaires de manière proactive et réactive ;
- Tester la capacité de la SDO à prioriser de manière efficiente l'allocation de ses ressources dans un contexte de multi-compromissions de ses bénéficiaires.

Au vu de ces objectifs, l'exercice *HANDSPINNER*, objet du présent marché, devra créer un contexte de menace et d'évènements de cybersécurité ayant un impact sur le maintien de la sécurité publique dans un contexte de perte de confiance dans les systèmes d'information de l'Etat.

Dans ce cadre, la SDO souhaite recourir à une prestation permettant la réalisation de son exercice *HANDSPINNER*. Avec l'aide de l'équipe cyber-entraînement de la SDO et des orientations qui lui seront données, le titulaire devra élaborer un scénario répondant aux objectifs énoncés, proposer des éléments techniques réalistes pour la mise en situation des équipes de la SDO et de ses partenaires. Également, il prendra en charge l'animation nécessaire au rendu réaliste de la situation simulée. Enfin, la réalisation des tâches sous sa responsabilité devra se faire en coordination avec l'équipe interne SDO en charge des compléments de scénario ou des tâches restant à sa charge.

Le présent document constitue le cahier des clauses techniques particulières (dénommé par la suite CCTP), correspondant aux prestations d'entraînement du centre opérationnel ((numéro de référence 79430000-7 – Services de gestion de crise) de la nomenclature CPV).

Article 2 - Description des prestations attendues

2.1 Dimensionnement de l'exercice

2.1.1 Déroulement prévisionnel

L'exercice *HANDSPINNER* proprement dit se déroulera sur dix (10) jours ouvrés consécutifs (J1 à J10) sur une amplitude horaires pouvant être comprise entre 09h00 et 17h00. Les équipes du titulaire devront être disponibles durant la totalité de cette période. Le temps de jeu pourra néanmoins être inférieur aux plages renseignées conformément aux choix de l'équipe du cyber-entraînement durant la phase de préparation de l'exercice (par exemple, 3 heures de jeu lors du J1).

Après publication du dossier de mise en situation, un évènement de cybersécurité déclenche une mobilisation des joueurs de la SDO ainsi que de son ou ses partenaires éventuels.

2.1.2 Localisation

L'exercice *HANDSPINNER* se déroulera principalement dans les locaux de l'ANSSI, situés au 31 quai de Grenelle, 75015 Paris « la Tour Mercure » et au 8, place Jeanne Laurent, 35000 Rennes « Artefact ». Les agents en télétravail devront également être pris en compte.

2.1.3 Nombre de joueurs

L'exercice *HANDSPINNER* décrit dans le présent document impliquera, sous-réserve de modifications et en fonction du scénario retenu, environ 80 joueurs au sein de l'ANSSI et de ses partenaires. Le nombre de joueurs impliqués par le ou les partenaires sera déterminé par eux en amont de la phase de développement du scénario.

2.2 Prestations à réaliser

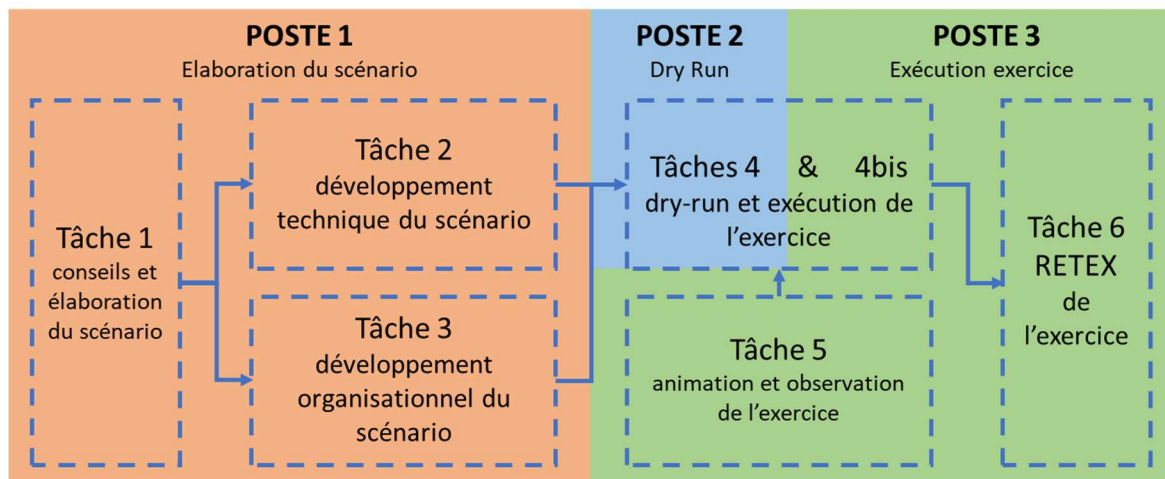
Les prestations du marché sont découpées en trois (3) postes, décomposés en tâches.

Les tâches, au nombre de six (6), sont les suivantes :

- Poste 1 – Elaboration du scénario

- Tâche 1 : conseils et élaboration du scénario
- Tâche 2 : déclinaison de la partie technique du scénario
- Tâche 3 : déclinaison de la partie organisationnelle du scénario
- Poste 2 – Dry Run
 - Tâche 4 : dry-run (exécution de l'exercice à blanc)
- Poste 3 – Exécution de l'exercice
 - Tâche 4bis : exécution de l'exercice
 - Tâche 5 : animation et observation de l'exercice
 - Tâche 6 : RETEX de l'exercice

DECOUPAGE DES ACTIVITES HANDSPINNER 2025



Les deux entités, ANSSI et titulaire, travailleront donc en étroite collaboration tout au long de la préparation et durant l'exécution de l'exercice, en fonction des tâches retenues. L'environnement de travail comprendra un ou deux partenaires de l'ANSSI au sein de l'état. Le responsable du cyber-entraînement de la SDO sera l'interlocuteur principal du titulaire, mais ce dernier pourra être amené à travailler avec l'équipe cyber-entraînement de la SDO, d'autres parties prenantes de l'ANSSI ainsi qu'avec le ou les partenaires pour le développement d'arcs scénaristiques spécifiques.

2.2.1 Tâche 1 : conseils et élaboration du scénario

La tâche 1 a pour objectif l'élaboration du scénario de l'exercice sous la supervision de l'ANSSI, ainsi que toutes les spécifications suffisantes et nécessaires permettant le développement des parties technique (tâche 2) et organisationnelle (tâche 3) de l'exercice. Il comprendra à minima un livrable scénaristique cyber.

En fonction des objectifs définis précédemment (objet du marché), il appartiendra au titulaire d'élaborer un scénario pertinent s'inscrivant dans le contexte de la SDO et de ses partenaires, comprenant des événements de cybersécurité tels que des incidents de sécurité informatique sur les systèmes d'information (SI) de l'écosystème cyber français, des sollicitations de partenaires/bénéficiaires ministériels, le partage de rapport d'analyse de la menace par des prestataires de cybersécurité, etc. Ces éléments viendront générer un important besoin de coordination des joueurs durant toute la durée de l'exercice. L'équipe cyber-entraînement de la SDO de la SDO pourra, en tant que de besoin, orienter le scénario global.

Une *timeline* générale et schématique qui permet une vue d'ensemble et rapide du scénario cyber sur les dix (10) jours ouvrés (2 semaines de 5 jours ouvrés) sera fournie. Cette *timeline* ne comprendra pas l'ensemble détaillé des injections.

Au titre de la prestation, le titulaire rédigera les documents décrivant le scénario de l'exercice et fournira les éléments techniques de mise en situation.

Livrables attendus :

- Le cahier des charges décrira le pilotage du projet de réalisation de l'exercice et l'organisation à mettre en place pour s'assurer de la bonne tenue de l'exercice ;
- Le livrable scénaristique devra être réaliste et fournir des éléments de compréhension pour permettre l'animation du jeu pendant dix (10) jours ouvrés. Ce document servira de base pour la réalisation globale de l'exercice, tant sur le volet technique que sur le volet organisationnel du scénario. Il contiendra l'ensemble des arcs scénaristique ;
- La timeline générale, permettant de synchroniser les arcs scénaristiques dans le temps de l'exercice ;
- Le chemin d'attaque (ou kill chain) ou fil rouge, décrivant les motivations de l'attaquant, les failles ou MOA utilisés ainsi que les « faiblesses » humaines, organisationnelles et/ou techniques exploitées (erreur de manipulation, confiance dans les SI, manque de maturité, vulnérabilités...) pour atteindre les objectifs définis.

2.2.2 Tâche 2 : développement de la partie technique du scénario

Sur la base du scénario global de la tâche 1, le titulaire devra développer les livrables techniques correspondant à l'ensemble des arcs scénaristiques permettant de faire jouer l'intégralité des participants pendant la durée de l'exercice. Le développement de la partie technique de l'exercice devra se faire en parfaite corrélation avec le développement de la partie organisationnelle du scénario (tâche 3).

Plusieurs rapports d'incident détailleront les réponses apportées par un ou plusieurs bénéficiaires/prestataires dans la gestion des incidents scénarisés. Ces rapports devront éclairer les équipes de l'ANSSI sur les actions à réaliser et stimuler le besoin de coordination. Sur validation de l'ANSSI, ces rapports pourront contenir des références à des journaux techniques d'événements, des indicateurs de compromission, des analyses de codes malveillants, etc.

Le développement d'un code « malveillant » permettant l'analyse de la menace et la détection devra être réalisé. Le code devra être inactif et inoffensif, et devra pouvoir être détecté par les outils de surveillance. Les principes et les fonctionnalités de ce code devront être décrits dans le livrable scénaristique. Ce code peut se baser sur des développements déjà existant (sur étagère) et concaténés pour apporter une richesse et une complexité lors de l'analyse par les participants de l'exercice.

La timeline technique devra inclure :

- La description détaillée, étape par étape (causes, interdépendances et conséquences), de l'attaque du ou des systèmes d'information, schéma à l'appui, ainsi que la documentation associée à l'ensemble des tactiques, techniques et procédures (TTP) employées ;
- La description d'un chemin d'attaque imaginé à partir de l'état de l'art, que l'équipe du cyber-entraînement de la SDO pourra orienter. Le titulaire sera chargé de rédiger la documentation associée à l'ensemble des tactiques, techniques et procédures (TTP) employées ;
- Les supports techniques contribuant à l'élaboration d'informations de contexte (rapports simulés d'éditeurs d'antivirus, fiches descriptives de vulnérabilité, rapports d'étonnements, rapports d'analyse de la menace, etc.).

Il est à noter qu'en l'absence de mobilisation d'une partie des équipes techniques de l'ANSSI côté joueurs, les éléments techniques serviront à alimenter et contextualiser le travail de coordination et de décision des joueurs sur le volet organisationnel.

Livrables attendus :

- Code « malveillant » (code exécutable ou détectable)
- Description du code « malveillant » développé
- Rapports d'incidents (5 rapports de CTI, 5 rapports d'incidents)
- Timeline technique

2.2.3 Tâche 3 : développement de la partie organisationnelle du scénario

Sur la base du scénario global de la tâche 1, le titulaire devra développer les livrables organisationnels correspondant à l'ensemble des arcs scénaristiques permettant de faire jouer l'intégralité des participants pendant la durée de l'exercice. Le développement de la partie organisationnelle de l'exercice devra se faire en parfaite corrélation avec le développement de la partie technique du scénario (tâche 2).

Un chronogramme des événements successifs majeurs et mineurs sera proposé et devra entraîner une réaction de la part des équipes de la SDO dans la compréhension de la situation, une mise en perspective et la proposition de mesures de traitement. À cette fin, le chronogramme du titulaire sera organisé avec les catégories et sous-catégories suivantes : événement, incident, injection (selon la norme ISO 22398). Le chronogramme présentera à la fois les événements de cybersécurité qui constituent le fil conducteur organisationnel du scénario de crise ainsi que les événements annexes qui seront créés autour de ce fil conducteur.

L'ensemble des événements ou stimuli seront présentés de manière chronologique. Les données ou faits passés nécessaires au traitement de l'évènement de cybersécurité seront décrits de manière précise. Par exemple, des revues et dossiers de presse quotidiens, des synthèses de messages d'informations/désinformations des réseaux sociaux, des informations provenant d'éditeurs, des tentatives ou des actes avérés visant des systèmes critiques nationaux dans un secteur stratégique, mais également tout contenu technique utile à la suite des investigations ou analyses techniques (rapports de « *Cyber Threat Intelligence* » (CTI), caractéristiques d'une vulnérabilité, détails sur le mode opératoire d'attaque d'un système d'information (SI), etc.). Le dossier de mise en situation (DMSI) exposera un mode opératoire d'attaque existant et fournira des éléments permettant une analyse de la menace par les équipes SDO. La situation au démarrage de l'exercice devra permettre une mobilisation des fonctions de décision et de coordination de la SDO et comprendra toutes données nécessaires à la compréhension des événements.

Les éléments présents dans le chronogramme ainsi que les contenus associés, seront intégrés sur la plateforme d'animation en source ouverte *OpenBAS*¹, permettant de diffuser les événements clefs sous forme d'envois de courrier électronique. Il sera donc demandé au titulaire de préparer les événements d'animation dans un format compatible avec cet outil, et de se former à la maîtrise d'*OpenBAS*.

Tous les documents permettant la mise en situation et le jeu du scénario (articles, documents simulant tel ou tel acteur du scénario, messages de réseaux sociaux) devront être réalisés par le titulaire. A titre d'exemple, le nombre minimum de contenus attendus peut être estimé comme suit : 15 comptes rendus d'échanges fictifs avec des bénéficiaires nationaux, 15 à 20 sollicitations de la part de partenaires institutionnels, entreprises ou entités demandant l'aide ou le conseil de l'ANSSI sur des incidents connexes ou isolés (chacune de ces injections engendrera une réaction plus ou moins importante des joueurs).

Plate-forme OpenBAS d'envois d'injections

Comme précisé précédemment, la plate-forme en source ouverte *OpenBAS* d'envoi d'injections vers les joueurs sera utilisée. Une instance dédiée à l'exercice sera mise à disposition par l'ANSSI et gérée par le titulaire. Les éléments de configuration de la plateforme ainsi que les scénarios et stimuli seront documentés dans *OpenBAS* et également remis à l'ANSSI dans un format réutilisable.

Livrables attendus :

- Un dossier de mise en situation (DMSI) : le dossier de mise en situation décrira la situation telle qu'elle se présente au début de l'exercice et les événements ayant mené à ce contexte.
- Timeline organisationnelle
- Production informationnelle médiatique et publique (articles de presse, informations CERT internationaux, réseaux sociaux) associée pour chaque jour d'exercice
- Chronogramme de l'exercice
- Stimuli au format *OpenBAS*

¹ Les éléments techniques sont disponibles sur internet à l'adresse [OpenBAS Documentation](#)

2.2.4 Tâche 4 : dry-run et exécution de l'exercice

Il s'agit de réaliser les phases d'animation de l'exercice nécessaires à la mise en œuvre du scénario avec l'aide de l'équipe cyber-entraînement de la SDO.

Le titulaire devra assurer la mobilisation de ses équipes durant toute la durée de la phase d'exécution de l'exercice. Il lui appartient de définir l'organisation de ce temps de présence.

Le titulaire devra être en mesure d'effectuer un dry run de l'ensemble du scénario global, au plus tard trois semaines avant le lancement effectif de l'exercice, afin d'anticiper les éventuels ajustements et correctifs à réaliser par le titulaire. A cette fin, il devra être testé l'envoi des injections depuis la plate-forme OpenBAS.

L'équipe cyber-entraînement de la SDO assistera au dry run aux côtés du titulaire, afin de vérifier la cohérence globale du scénario et pourront également réagir à certaines injections techniques.

Hébergement des moyens

Les moyens devront être accessibles sur Internet, à l'ensemble de l'équipe d'animation (ANSSI et titulaire confondus). Il est demandé au titulaire de mettre ses outils à disposition qui seront dédiés à l'exercice, et qui devra être détruit à l'issue de l'exercice. Une copie sera fournie à l'ANSSI au préalable. L'ensemble de ces outils devra être disponible au moins un mois avant le début de l'exercice et testés pendant le dry run.

Livrables attendus :

- Dry run de l'ensemble du scénario technique et organisationnel, avec les animateurs et observateurs (répétition à blanc)
- Rapport des ajustements priorisés à apportés au chronogramme et stimuli
- Exécution de l'exercice

2.2.5 Tâche 5 : animation et observation de l'exercice

L'animation de l'exercice *HANDSPINNER* sera assurée par le titulaire, assisté par l'équipe cyber-entraînement de la SDO et du partenaire.

L'équipe d'animation du titulaire est en charge de jouer le scénario conformément au chronogramme et à la *timeline* définis lors de la phase de préparation de l'exercice. Elle ajuste les événements d'animation (ici appelés injections ou stimuli) au fur et à mesure (rythme, rajout ou modification d'injections) en fonction des aléas du jeu, des réponses et sollicitations de l'ANSSI pendant le jeu. Elle est également le point de contact pour clarifier des événements d'animation au cours du jeu. Elle fixe les limites du jeu en cas d'écart au scénario et veille à leur respect.

Organisation de l'équipe d'animation

L'équipe d'animation sera composée comme suit :

La direction de l'animation (maître du jeu)

La direction de l'animation veillera à la cohérence générale du déroulement de l'exercice. Elle oriente les actions d'animation ainsi que d'éventuels ajustements ou actions à mener sur le plan scénaristique. Elle sera composée de plusieurs agents de l'ANSSI et un représentant du titulaire.

L'équipe d'animateurs

Les animateurs sont les acteurs du scénario, ils endossent le rôle des différents protagonistes présents dans le chronogramme et mènent les actions d'animation. Ils sont également capables d'improviser un rôle en cas de besoin.

La répartition des rôles d'animation se fera en collaboration avec l'équipe cyber-entraînement de la SDO de la SDO durant la phase de préparation de l'exercice. En fonction du scénario établi, il est attendu que le titulaire mobilise des profils techniques en mesure d'endosser le rôle de victimes réalisant une réponse à incident.

Dans le cas où un ou plusieurs partenaires seraient impliqués dans l'exercice auprès de l'ANSSI, ceux-ci joueront leur propre rôle. Toutefois, en fonction des besoins au cours de l'exercice, le titulaire pourra être sollicité pour simuler des réactions ou sollicitations de ces partenaires.

L'équipe d'observateurs

Les observateurs sont les acteurs clés du RETEX, ils connaissent le scénario et observent les réactions des joueurs et les interactions avec les autres joueurs en fonction des stimuli qu'ils reçoivent pendant l'exercice. Ils doivent également alerter les animateurs pour remonter tout fait anormal ou risque sur le bon déroulement de l'exercice. Ils seront répartis entre le titulaire et des agents de l'ANSSI en fonction des besoins d'en connaître. Les observateurs, ainsi que les animateurs, contribueront au RETEX de l'exercice.

Localisation des équipes d'animation et d'observation

L'équipe d'animation sera répartie entre les locaux du titulaire, les locaux de l'ANSSI et les locaux du ou des partenaires, en fonction des contraintes d'exercice identifiées au cours de la préparation.

Moyens de l'équipe d'animation

Modes de communication interne à l'équipe d'animation

Afin de faciliter la gestion de l'animation, l'équipe devra travailler sur des outils collaboratifs. Il sera demandé au titulaire de mettre à disposition :

- Une ou plusieurs adresses emails dédiées à l'animation de l'exercice : le nom de domaine et les adresses seront convenus ultérieurement avec la SDO ;
- Un espace collaboratif sur lequel pourront être déposés des documents, accessible par l'ensemble des parties prenantes à la préparation de l'exercice.

Les animateurs mobilisés par le titulaire devront être joignables par téléphone et visioconférence sur le temps d'exécution de l'exercice.

Livrables attendus :

- Liste et organisation de l'équipe d'animateurs et observateurs
- Outils et kits d'animation, incluant à minima le DMSI, le chronogramme de l'exercice, la timeline générale, les grilles d'observations, les stimuli clés par entité à observer en priorité, une fiche de prise en main de l'outil de communication entre animateurs et observateurs, un annuaire de l'exercice et des animateurs et observateurs, les adresses mails utilisées lors de l'exercice
- Briefing des animateurs et observateurs sur le déroulement et le scénario de l'exercice

2.2.6 Tâche 6 : RETEX de l'exercice

RETEX sur le déroulement de l'exercice

Un retour d'expérience (RETEX) sera réalisé à la suite de l'exercice. Celui-ci fera l'objet d'une réunion en présence des agents de l'ANSSI et éventuellement du ou des partenaires dans les heures ou jours suivant la fin de l'exercice.

Les documents (timeline, schéma et description de l'ensemble du scénario technique) devront être rendus à l'équipe cyber-entraînement de la SDO (cf. article 3.4) dans un délai d'une semaine suivant la fin de l'exercice.

RETEX sur la prestation

Le RETEX sur la prestation se tiendra entre le titulaire et l'équipe cyber-entraînement de la SDO afin d'identifier les axes d'amélioration de la prestation.

Livrables attendus :

- Retour d'expérience sur le déroulement de l'exercice détaillé (format word)
- Retour d'expérience sur le déroulement de l'exercice synthétique (format powerpoint)
- Retour d'expérience sur la prestation synthétique (format libre)

Article 3 - Modalités d'exécution de la prestation

3.1 Livrables attendus

Tâche 1 Conseils et élaboration du scénario
<ul style="list-style-type: none">○ Cahier des charges décrira le pilotage du projet de réalisation de l'exercice et l'organisation à mettre en place pour s'assurer de la bonne tenue de l'exercice ;○ Livrable scénaristique devra être réaliste et fournir des éléments de compréhension pour permettre l'animation du jeu pendant deux (2) semaines ouvrées ; tant sur le volet technique que sur le volet organisationnel du scénario. Il contiendra l'ensemble des arcs scénaristique ;○ Timeline générale, permettant de synchroniser les arcs scénaristiques dans le temps de l'exercice ;○ Chemin d'attaque (ou kill chain) ou fil rouge, décrivant les motivations de l'attaquant, les failles ou MOA utilisés ainsi que les « faiblesses » humaines exploitées (erreur de manipulation, confiance dans les SI, manque de maturité...) pour atteindre les objectifs définis.
Tâche 2 Développement technique
<ul style="list-style-type: none">○ Code malveillant (code exécutable ou détectable)○ Description de la charge active○ Rapports d'incidents (5 rapports de CTI, 5 rapports d'incidents)○ Timeline technique
Tâche 3 Développement organisationnel
<ul style="list-style-type: none">○ Un dossier de mise en situation (DMSI) : le dossier de mise en situation décrira la situation telle qu'elle se présente au début de l'exercice et les événements ayant mené à ce contexte.○ Chronogramme de l'exercice○ Timeline organisationnelle○ Productions informationnelles médiatique et publique○ Stimuli au format OpenBAS
Tâche 4 Dry run et exercice
<ul style="list-style-type: none">○ Dry Run de l'ensemble du scénario technique et organisationnel, avec les animateurs et observateurs (répétition à blanc)○ Rapport des ajustements prioritaires à apporter au chronogramme et stimuli○ Exécution de l'exercice

Tâche 5 Animation et Observation
<ul style="list-style-type: none"> ○ Liste et organisation de l'équipe d'animateurs et observateurs ○ Outils et kits d'animation, incluant à minima le DMSI, le chronogramme de l'exercice, la timeline générale, les grilles d'observations, les stimuli clés par entité à observer en priorité, une fiche de prise en main de l'outil de communication entre animateurs et observateurs, un annuaire de l'exercice et des animateurs et observateurs, les adresses mails utilisées lors de l'exercice ○ Briefing des animateurs et observateurs sur le déroulement et le scénario de l'exercice
Tâche 6 RETEX de l'exercice
<ul style="list-style-type: none"> ○ Retour d'expérience détaillé sur le déroulement de l'exercice (format word) ○ Retour d'expérience synthétique sur le déroulement de l'exercice (format powerpoint) ○ Retour d'expérience sur la prestation synthétique (format libre)

3.2 Format des livrables attendus

Au titre du marché, le titulaire fournira les livrables documentaires au format électronique dans un format réutilisable de type *WORD*, *EXCEL*, *POWERPOINT* ou équivalent.

Les documents réalisés devront faire apparaître la mention suivante « Exercice – Exercice – Exercice » utilisée par l'ensemble des acteurs.

Le titulaire est garant de la qualité, de la cohérence des livrables et du respect de leur échéance de livraison. Le responsable du cyber-entraînement de la SDO est responsable de la validation, ou non, de ces livrables.

3.3 Lieux de réalisation de la prestation et moyens logistiques associés

Les réunions de préparation se tiendront à distance, sauf décision contraire du responsable du cyber-entraînement de la SDO. Le cas échéant, elles se tiendront dans les locaux de l'ANSSI, 31 quai de Grenelle, 75015 Paris « la Tour Mercure » et au 8, place Jeanne Laurent, 35000, Rennes « Artefact » ainsi que dans les locaux du ou des partenaires de l'ANSSI.

Le titulaire exécutera la prestation d'animation de l'exercice dans les locaux de l'ANSSI ou ses locaux.

3.4 Interlocuteurs du titulaire

Les prestations seront pilotées principalement par le représentant du titulaire à la notification du marché en liaison avec le responsable du cyber-entraînement de la SDO, désigné comme représentant technique et point de contact principal par le pouvoir adjudicateur.

En cas de réunion ayant trait aux aspects techniques du scénario de l'exercice et sur demande expresse de l'ANSSI, le titulaire devra être en capacité de mobiliser les profils techniques compétents.

Dans tous les autres cas où les membres de l'équipe du cyber-entraînement de la SDO l'estiment nécessaire, ceux-ci pourront être mise en relation directe avec l'équipe technique du titulaire.

3.5 Calendrier des prestations et des fournitures

La date précise de démarrage de l'exercice sera communiquée au titulaire dès la réunion de lancement du marché (T₁), au plus tard trois (3) mois avant la date fixée. Cette réunion de lancement fera l'objet d'un compte-rendu de la part du titulaire et soumis à validation par le représentant technique du pouvoir adjudicateur.

La phase de préparation de l'exercice se tiendra entre la date de notification et le début de l'exercice. Le calendrier suivant est proposé à titre indicatif et n'a pas de valeur contractuelle.

Les délais sont donnés en semaines calendaires.

Les dix (10) jours ouvrés prévisionnels d'exécution de l'exercice vont de la semaine 40 à la semaine 41 de l'année 2025 (du 29 septembre au 10 octobre 2025), sous réserve de modification par l'ANSSI.

Le calendrier de réalisation des prestations sera celui indiqué par le titulaire dans l'échéancier mentionné dans l'annexe à l'acte d'engagement – description de la solution technique retenue ».

A titre indicatif, le planning ci-dessous donne une vision calendaire du planning de la prestation attendue, intégrant une période de report d'exercice sous conditions.

Calendrier 2025

Calendrier 2026

Mars			Avril			Mai			Juin			Juillet			Août			Septembre			Octobre			Novembre			Décembre			Janvier			Février			Mars				
1	S		1	M		1	J		1	D		1	M		1	V		1	L		1	M		1	S		1	L		1	J		1	D		1	D			
2	D		2	M		2	V		2	L		2	M		2	S		2	M		2	J		2	D		2	M		2	V		2	L		2	L			
3	L		3	J		3	S		Phase de développement									3	Revue fin de développement	3	V		3	L		3	M		3	S		3	M		3	M				
4	M		4	V		4	D		4	M		4	V		4	L		4	S		Exercice			4	M		4	J		4	D		4	M		4	M			
5	M		5	S		5	L		5	J		5	S		5	M		5	V		Exercice			5	M		5	V		5	L		5	J		5	J			
6	J		6	D		6	M		6	V		6	D		Revue bi-mensuelle			6	S		6	L		6	J		6	S		6	M		6	V		6	V			
7	V		7	L		7	M		7	S		7	L		Revue bi-mensuelle			7	D		7	M		7	V		7	D		7	M		7	S		7	S			
8	S		8	M		8	J		8	D		8	M		8	V		8	L		8	M		8	S		8	L		8	J		8	D		8	D			
9	D		Kick-off			9	V		9	L		Revue bi-mensuelle			9	S		9	M		9	J		9	D		9	M		9	V		9	L		9	L			
10	L		10	J		10	S		10	M		Revue bi-mensuelle			10	D		DRY RUN			10	V		10	L		10	M		10	S		10	M		10	M			
11	M		11	V		11	D		11	J		Revue bi-mensuelle			11	L		11	J		Période de report exercice			11	S		11	J		11	D		11	M		11	M			
12	M		12	S		12	L		12	J		12	S		12	M		12	V		Période de report exercice			12	D		12	V		12	L		12	J		12	J			
13	J		13	D		Revue bi-mensuelle			13	V		13	D		13	M		13	S		13	L		13	J		13	S		13	M		13	V		13	V			
14	V		14	L		Revue bi-mensuelle			14	S		14	L		14	J		14	D		14	M		14	V		14	D		14	M		14	S		14	S			
15	S		15	M		15	J		15	D		15	M		15	V		15	L		15	M		15	S		15	L		15	J		15	D		15	D			
16	D		16	M		16	V		16	L		16	M		16	S		16	M		16	J		16	D		16	M		16	V		16	L		16	L			
17	L		Cadrage & KT			17	S		17	M		17	J		17	D		17	M		17	V		17	L		17	M		17	S		17	M		17	M			
18	M		18	S		18	D		18	M		18	V		18	L		18	J		18	S		18	M		18	J		18	D		18	M		18	M			
19	M		19	L		19	J		19	S		19	S		19	M		Ajustements et préparation			19	D		19	M		19	V		19	L		19	J		19	J			
20	J		20	D		20	M		20	V		20	D		Revue bi-mensuelle			20	S		Ajustements et préparation			20	L		20	J		20	S		20	M		20	V			
21	V		21	L		21	M		21	S		21	L		21	J		21	D		21	M		21	V		21	D		21	M		21	S		21	S			
22	S		22	M		22	J		22	D		Revue bi-mensuelle			22	V		22	L		RETEX			22	S		22	L		22	J		22	D		22	D			
23	D		23	M		23	V		23	L		23	M		23	S		23	M		23	J		23	D		23	M		23	V		23	L		23	L			
24	L		24	J		24	S		24	M		24	J		24	D		24	M		24	V		24	L		24	M		24	S		24	M		24	M			
25	M		25	V		25	D		Revue bi-mensuelle			25	V		25	L		25	J		25	S		25	M		25	J		25	D		25	M		25	M			
26	M		26	S		26	L		26	J		26	S		26	M		26	V		26	D		26	M		26	V		26	L		26	J		26	J			
27	J		27	D		27	M		Revue bi-mensuelle			27	V		27	D		27	M		27	S		27	L		27	J		27	S		27	M		27	V			
28	V		28	L		Revue bi-mensuelle			28	S		28	L		28	J		28	D		28	M		28	V		28	D		28	M		28	S		28	S			
29	S		29	M		29	J		29	D		29	M		29	V		29	L		Exercice			29	M		29	S		29	L		29	J				29	D	
30	D		30	M		30	V		30	L		30	M		30	S		30	M		30	J		30	D		30	M		30	V					30	L			
31	L					31	S					31	J		31	D					31	V					31	M		31	S					31	M			

3.6 Report de l'exercice

Dans la limite du 31 janvier 2026, l'exercice *HANDSPINNER* pourra faire l'objet d'un report à une date ultérieure dans les cas suivants :

- En cas de contrainte opérationnelle majeure empêchant l'ANSSI de libérer suffisamment d'agents pour participer à l'exercice ;
- En cas d'évènement extraordinaire faisant obstacle à la bonne exécution de l'exercice, et après décision du sous-directeur Opérations.

Le cas échéant, le titulaire en serait informé dans les plus brefs délais, et la date de report lui serait communiquée par la suite.

3.7 Suivi de la prestation

Sous réserve d'ajustements, l'ANSSI souhaite, au minimum, prévoir les réunions de gestion de l'exercice suivantes :

- 1 réunion de kick-off : réunion initiale de planification pour définir le travail attendu et les objectifs d'entraînement
- 1 à 2 réunions de cadrage et de transfert de connaissance : réunion de présentation des métiers et organisation de la SDO et partenaires
- Des réunions de suivi bimensuelles ou hebdomadaires (selon les besoins)
- 1 réunion de revue et validation des livrables de chacune des tâches
- 1 à 2 réunions de préparation à l'animation et l'observation : préparer le déroulement de l'animation et la répartition des tâches entre les différentes parties prenantes
- 1 réunion de dry run : réunion de dry-run globale pour s'assurer la cohérence et du bon enchaînement des injects, et valider les livrables finaux (dont le dossier de mise en situation, les injects et le chronogramme), 3 semaines avant le début de l'exercice
- 1 réunion de revue et de validation des ajustements pour finaliser la préparation de l'exercice avant exécution
- 1 réunion de revue du RETEX et clôture de la prestation

Au besoin, des réunions supplémentaires pourront être planifiées sur décision du responsable cyber-entraînement de la SDO ou sur demande du titulaire.

Pour le suivi de réalisation et le pilotage de l'exercice, il incombera au titulaire de réaliser un compte-rendu de chaque réunion tenue avec le titulaire et l'ANSSI.

Il incombera au titulaire d'informer l'équipe cyber-entraînement de la SDO de toute difficulté qui l'empêcherait d'honorer les échéances fixées.

Les réunions se tiendront à distance ou bien dans les locaux de l'ANSSI.

3.8 Critères de vérification et de validation des tâches

Les opérations de vérification nécessaires à la réception des prestations porteront sur leur qualité technique et documentaire.

Les opérations de surveillance et de vérification seront réalisées par le représentant technique du pouvoir adjudicateur et consignées dans un procès-verbal de constatation des opérations de vérification mentionnant, s'il y a lieu, les réserves du titulaire. Il sera ensuite transmis au représentant légal du pouvoir adjudicateur.

Quels que soient les résultats des vérifications, les frais qu'elles entraînent sont à la charge du pouvoir adjudicateur pour les opérations qui, conformément aux dispositions du marché, doivent être exécutées dans ses propres locaux. Ils sont à la charge du titulaire dans les autres cas.

Le délai maximum imparti au pouvoir adjudicateur pour procéder aux opérations de vérification d'un livrable du marché est d'une semaine calendaire à compter de sa date de livraison ou de son exécution.

Si les opérations de vérification sont négatives, le représentant technique du pouvoir adjudicateur prendra une décision d'ajournement assortie d'un délai de correction maximum d'une semaine calendaire au titulaire pour parfaire les prestations ; il est rappelé que ce délai ne justifie pas lui-même l'octroi d'une prolongation du délai contractuel d'exécution des prestations.

À l'issue de la livraison du livrable corrigé, le représentant technique du pouvoir adjudicateur dispose de nouveau d'un délai maximum d'une semaine calendaire pour reprendre les opérations de vérification.

En cas de nouvel échec, soit la même procédure sera reconduite, soit le représentant légal du pouvoir adjudicateur prononcera directement le rejet des prestations.

Article 4 - Propriété des travaux et confidentialité des résultats

4.1 Confidentialité des résultats

Pour l'élaboration du scénario, le titulaire ne pourra utiliser aucune donnée classifiée mais pourra s'appuyer sur toute source de nature ouverte et publique.

Toutes les informations auxquelles le titulaire pourrait avoir accès et provenant de l'ANSSI ou d'autres parties prenantes devront rester confidentielles et ne pourront être utilisées dans le cadre d'autres marchés ou être diffusées vers l'extérieur, sauf décision contraire et expresse du pouvoir adjudicateur.

4.2 Propriété des travaux

Il sera fait application de l'article 35 du CCAG-TIC relatif au « transfert de propriété » et de l'article 46 du CCAG-TIC pour le « régime des résultats ». Le titulaire cède, à titre exclusif, l'intégralité des droits ou titres de toute nature afférents aux résultats, permettant au pouvoir adjudicateur de les exploiter librement, y compris à des fins commerciales.

Ces droits sont cédés par le titulaire pour la totalité de la durée de protection légale des droits d'auteur ou de leurs ayants-droits.

La cession de ces droits est applicable dans le monde entier.

Les conditions financières de la cession sont comprises dans le montant prévu au marché.

Les droits de propriété intellectuelle des études, documents et supports produits en exécution des prestations seront cédés au pouvoir adjudicateur à l'occasion de l'admission des prestations du marché.

Tous les documents que les divers intervenants auront remis au titulaire devront être transmis au pouvoir adjudicateur à l'occasion de l'admission des prestations et ne pourront être diffusés à une tierce partie sans l'accord préalable écrit de l'ANSSI.

De même, les documents remis par le représentant technique du pouvoir adjudicateur au titulaire, ne devront pas être communiqués à toute personne étrangère à l'équipe chargée du projet, sauf décision contraire du pouvoir adjudicateur.

Enfin, le serveur dédié virtuel devra être détruit à l'issue de l'exercice par le titulaire.

Article 5 - Communication sur l'exercice

Toute communication liée à la prestation telle que décrite dans le présent document devra être validée par le service communication de l'ANSSI.