Autorité de régulation des jeux en ligne
RÉPUBLIQUE FRANÇAISE

RÉFÉRENTIEL TECHNIQUE

ANNEXE I du Règlement relatif à la certification prévue à l'article 23 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne adopté par la décision n° 2014-018 du collège de l'Autorité de régulation des jeux en ligne en date du 17 mars 2014.

Guide méthodologique

Règles essentielles

- Le volet technique de la certification repose sur des exigences de conformité et de sécurité issues du DET et de ses annexes ;
- les exigences de conformité et de sécurité font l'objet de points de contrôle, regroupés dans un référentiel technique de certification ;
- le référentiel technique de certification est constitué du présent guide méthodologique et de deux matrices d'exigences, faisant l'objet de deux documents distincts :
    - la matrice d'exigences de la certification unique à 6 mois du composant frontal,
    - la matrice d'exigences de la certification annuelle ;
- les matrices d'exigences et les points de contrôle associés sont alimentés par :
    - les documents et attestations transmis par l'opérateur,
    - les analyses menées directement par l'organisme certificateur ;

- l'organisme certificateur effectue une mesure unique des différents points de contrôle ;
- l'organisme certificateur dresse, dans le rapport de certification, la liste de l'ensemble des vulnérabilités et non-conformités constatées quel que soit leur niveau de criticité.

- à l'issue de la remise du rapport de certification, l'opérateur réalise, s'il y a lieu, des fiches d'anomalies, reprenant l'ensemble des vulnérabilités et non-conformités soulevées par l'organisme certificateur. Ces fiches sont adressées à l'ARJEL et à l'organisme certificateur dans le délai d'un mois suivant la remise du rapport de certification ;
- les fiches d'anomalies font état, le cas échéant, des mesures correctives proposées par l'opérateur ainsi que de tout désaccord éventuel de l'opérateur avec les conclusions du rapport de l'organisme certificateur ;

- le référentiel technique de certification introduit trois niveaux de criticité des exigences, de la moins critique (1) à la plus critique (3) ;
- chaque exigence est liée, par défaut, à un niveau de criticité ;
- l'organisme certificateur peut moduler le niveau de criticité d'une exigence, à condition de justifier ses critères d'appréciation ;
- le rapport conclut à une certification sans réserve ou avec réserves, si une ou plusieurs exigences du référentiel ne sont pas atteintes ;
- les réserves concernent les exigences non atteintes dont le niveau de criticité est supérieur ou égal à 2 ;

- la certification unique à 6 mois du composant frontal repose sur un socle d'analyses obligatoires ;
- le composant frontal fait l'objet d'une analyse fonctionnelle et technique complète 6 mois après sa date de mise en production ;
- la certification annuelle repose sur un socle d'analyses susceptibles de faire, ou non, l'objet d'une actualisation, partielle ou totale ;
- une analyse non actualisable doit être effectuée dans son intégralité ;
- l'analyse du composant frontal fait l'objet d'une actualisation à chaque certification annuelle ;

- le rapport de certification technique est constitué de la matrice des exigences dûment complétée et des différents livrables et annexes issus des analyses techniques de l'organisme certificateur.

1 Périmètre des certifications

1.1 Certification unique à 6 mois du composant frontal

1.1.1 Périmètre d'intervention technique

Prévue au II de l'article 23 de la loi n°2010-476 du 12 mai 2010, la certification unique à 6 mois porte sur le composant frontal et son infrastructure d'hébergement.

1.1.2 Couverture des exigences

Les exigences concernées sont celles issues du DET et de ses annexes : elles font l'objet des points de contrôle documentés dans le référentiel technique de la certification unique à 6 mois du composant frontal.

1.2 Certification annuelle

1.2.1 Périmètre d'intervention technique

Prévue au III de l'article 23 de la loi n°2010-476 du 12 mai 2010, la certification annuelle porte sur l'infrastructure globale du service de jeu en ligne ainsi que sur les modifications apportées aux logiciels homologués.

Ce périmètre inclut donc également le périmètre de la certification unique à 6 mois du composant frontal (partie 1.1).

1.2.2 Couverture des exigences

Les exigences concernées sont celles issues du DET et de ses annexes : elles font l'objet des points de contrôle documentés dans le référentiel technique de la certification annuelle.

2 Référentiel technique de certification

2.1 Matrice d'exigences

La certification unique à 6 mois du composant frontal et la certification annuelle font l'objet de matrices d'exigences techniques distinctes. Ces matrices d'exigences, tout comme le présent guide méthodologique, sont annexées au règlement de certification.

Chaque matrice regroupe les exigences de conformité et de sécurité issues du DET et de ses annexes. Les exigences font l'objet d'une numérotation et sont classées par thème.

La matrice d'exigences du référentiel de certification doit être complétée par l'organisme certificateur à l'issue de ses analyses. Elle synthétise les résultats obtenus à travers :

- les différentes opérations d'analyses techniques conduites par l'organisme certificateur (audits applicatifs, d'architecture, de configuration ou encore tests d'intrusion interne ou externe) ;

- l'analyse de la documentation remise par l'opérateur ;

- l'intégration des attestations d'absence de modification produites[1], le cas échéant, par l'opérateur. Remarque : cette absence de changement ne doit pas être incompatible avec un maintien en conditions de sécurité (gestion des mises à jour de sécurité, adaptation aux nouvelles attaques par des mesures de durcissement conformes à l'état de l'art, *etc.*).

2.2 Niveau de criticité d'une exigence

Un niveau de criticité, sur une échelle de 1 à 3 (criticité la plus élevée), est affecté à chaque exigence :

- ➔ le niveau de criticité 1 correspond essentiellement aux exigences liées à l'*existence* d'une documentation ou d'une procédure (ex : politique de sécurité, procédure de mise à jour, de durcissement d'un système, *etc.*) ;

- ➔ le niveau de criticité 2 correspond essentiellement aux exigences pour lesquelles une non-conformité a un impact *opérationnel* : défaut d'*application* d'une procédure, défaut de respect des exigences *opérationnelles* de conformité et de sécurité définies par l'ARJEL, ou encore défaut de suivi des règles de bonnes pratiques en sécurité des systèmes d'information ;

- ➔ le niveau de criticité 3 correspond aux exigences dont le non-respect est jugé très critique, le plus souvent en termes de conformité règlementaire ou en termes de sécurité (sur un composant exposé et/ou manipulant des données critiques).

Les niveaux de criticité ne sont pas figés : ils peuvent faire l'objet d'une réévaluation par l'organisme certificateur, après avis d'expert et échange éventuel avec l'opérateur au moment de la mesure du point de contrôle. L'organisme certificateur peut donc moduler le niveau de criticité d'une exigence, selon la nature exacte de la non-conformité identifiée et plus particulièrement de ses éléments de contexte : le cas échéant, il doit indiquer très précisément quels sont ses critères d'appréciation, afin de justifier de tout écart avec le niveau de criticité nominal d'une non-conformité[2].

A l'issue de ces opérations d'analyse, l'attestation de certification produite liste, le cas échéant, les réserves portant sur les non-conformités et vulnérabilités identifiées dont le niveau de criticité est supérieur ou égal à 2.

3 Méthodologie et livrables attendus

3.1 Méthodologie

[1] Attestation certifiant, par exemple, que la cinématique d'enregistrement mise en œuvre par le capteur n'a fait l'objet d'aucune modification depuis la précédente certification.
[2] Par exemple, une vulnérabilité applicative n'aura pas le même niveau de criticité (2, par défaut), selon l'exposition du composant impacté et sa proximité avec les données utilisateurs (cf. annexe I).

L'ensemble des rapports d'audits, documentations et attestations remises, le cas échéant, par l'opérateur permettent d'alimenter le référentiel technique de certification (cf. partie 2.1).

Pour chaque point de contrôle, l'organisme certificateur doit donc compléter la matrice des exigences, en renseignant la conformité de l'exigence évaluée et son niveau « définitif » de criticité (résultant de son analyse et prenant en compte les éléments communiqués par l'opérateur au cours de la réalisation de la mesure, cf. partie 2.2), ainsi que le ou les différents chapitres des rapports démontrant l'analyse effectuée.

Certaines mesures, dont l'analyse ne serait pas issue des rapports d'audits, peuvent être détaillées dans un rapport général intitulé « *Vérification des exigences* ».

Les opérations d'analyse conduites par l'organisme certificateur ne sont pas itératives au cours d'une même certification : l'organisme certificateur doit donc respecter le principe de la mesure unique de chaque point de contrôle. En particulier, les éventuelles modifications apportées par un opérateur, en cours de certification, sur un point déjà évalué ne peuvent pas modifier la constatation initiale qui doit figurer dans le rapport de certification.

, l'organisme certificateur énumère, le cas échéant, dans la synthèse du rapport, les réserves relatives aux vulnérabilités ou non-conformités découvertes lors de ses travaux. Seules les réserves de niveau 2 et 3 seront mentionnées.

Les vulnérabilités et non-conformités constatées font, indépendamment de leur niveau de criticité, l'objet d'une énumération exhaustive dans le rapport de synthèse. La liste de ces vulnérabilités et non-conformités est reprise, s'il y a lieu, dans les fiches d'anomalies. Ces fiches d'anomalies ne font pas partie du rapport de certification et doivent être communiquées à l'ARJEL et à l'organisme certificateur dans le délai d'un mois suivant la remise dudit rapport. Elles sont réalisées par l'opérateur, notamment afin qu'il propose des mesures correctives ainsi qu'un échéancier de mise en œuvre. Si l'opérateur souhaite par ailleurs apporter des précisions sur la mise en place éventuelle d'un correctif[3] qui serait postérieure à la mesure de l'organisme certificateur ou, plus généralement, s'il souhaite porter une information de toute nature à la connaissance de l'ARJEL, il peut formuler ses remarques et commentaires à travers ces fiches d'anomalies. Ces fiches d'anomalies peuvent également être l'occasion pour l'opérateur de préciser son éventuel désaccord avec les conclusions apportées par l'organisme certificateur sur certaines non-conformités ou vulnérabilités. Dans ce cas de figure, l'opérateur doit apporter une analyse contradictoire détaillée.

L'ARJEL détermine, en fonction des différents éléments apportés par l'opérateur et de la pertinence ou de la profondeur des analyses conduites par l'organisme certificateur, les éventuelles suites à donner. .

3.2 Certification à 6 mois du frontal

La certification unique à 6 mois du composant frontal, ainsi que la certification annuelle, sont à périmètre technique et couverture des exigences constants (cf. partie 1). Les deux certifications diffèrent néanmoins en termes de niveau d'analyse des opérations de vérification.

Les contrôles effectués lors de la certification unique à 6 mois du composant frontal reposent sur un socle d'analyses obligatoires.

L'audit applicatif du frontal, concentré sur le ou les composants « capteur(s) », est invariablement composé de deux volets :

- ➔ le premier volet correspond à l'analyse fonctionnelle et technique du code du capteur, permettant de présenter le fonctionnement de la vérification et de l'enregistrement des traces au coffre-fort et la mise en œuvre d'une cinématique conforme aux exigences du DET,

[3] Il est évident qu'en cas de vulnérabilité avérée, l'opérateur a intérêt à proposer un correctif dans les plus brefs délais. La mise en place de ce correctif ne saurait néanmoins annuler la non-conformité à l'exigence associée, ou encore en diminuer le niveau de criticité.

notamment en termes de mise en coupure et d'acquittement préalable par le joueur. L'organisme certificateur n'effectue pas l'analyse syntaxique et sémantique des enregistrements XML, mais s'assure que le positionnement du capteur est conforme aux exigences du DET et que l'ensemble des enregistrements sont correctement formés au sens de la norme XML et des schémas XSD publiés par l'ARJEL.

Lors de la certification annuelle, ce volet peut être actualisé si des modifications ont été apportées par l'opérateur. Si aucune modification n'a été effectuée et que l'opérateur déclare une absence totale de modification par le biais d'une attestation, les analyses spécifiques à ce périmètre peuvent être omises à l'occasion de la nouvelle certification : la matrice des points de contrôle peut alors reprendre à l'identique les résultats obtenus lors de la certification antérieure. Les rapports d'analyse pointés sont alors ceux de la certification antérieure, auxquels s'ajoute l'attestation d'absence de modification produite par l'opérateur pour l'année écoulée.

➔ Le second volet est relatif à la sécurité du capteur, mesurée par le biais d'un audit intrusif. Lors de cette analyse, l'organisme certificateur tente, aux travers de tests intrusifs, d'injecter des évènements spécialement formés dans le coffre afin d'en détourner les fonctions d'enregistrement et de sécurité (corruption des enregistrements, injection de faux évènements, prise de contrôle à distance du composant « capteur » ou encore du coffre-fort), ou encore de modifier les informations liées à ses paris ou à la gestion de son compte.

Lors de la certification annuelle, ce volet est non actualisable. Il est intégré à l'audit intrusif plus généralement conduit sur l'ensemble de la plate-forme. Il s'agit donc d'une nouvelle analyse, qui permet notamment de s'adapter – à implémentation constante – aux évolutions de l'état de l'art en sécurité des systèmes d'information et, à chaque itération, de pallier le manque d'exhaustivité intrinsèque aux tests d'intrusion.

La liste complète des autres analyses et donc livrables attendus dans le cadre de la certification unique à 6 mois du composant frontal figure dans l'annexe II.

3.3 Certification annuelle

Les contrôles effectués lors de la certification annuelle reposent sur des analyses dont les résultats peuvent, ou non, faire l'objet d'une actualisation, partielle ou totale. On parle, le cas échéant, d'une analyse actualisable.

Par actualisation, on entend la réitération, partielle ou totale, des contrôles effectués lors d'une certification antérieure sur un périmètre donné. En termes de livrables, il est donc principalement attendu une mise à jour des résultats obtenus[4] et des commentaires assortis, le cas échéant.
Une attestation d'absence de modification produite par l'opérateur (cf. partie 2.1) peut par ailleurs conduire l'organisme certificateur à ne pas effectuer d'analyse sur le périmètre concerné, sous réserve que cette absence de modification ne soit pas incompatible avec un maintien en conditions de sécurité.

Toutes les analyses ne sont pas actualisables et, à plus forte raison, ne peuvent pas être remplacées par une déclaration d'absence de modification par l'opérateur. En particulier, les points de contrôle qui auraient fait l'objet de réserves à l'occasion de la précédente certification doivent, en tout état de cause, faire l'objet d'une nouvelle analyse.

[4] Par exemple, pour un audit de configuration, les résultats de commande/outils, ainsi que les captures d'écran peuvent donc être mis à jour. Un rapport d'audit ne doit donc pas comporter le résultat de la commande « uname –a » de l'année antérieure, ou une capture d'écran dont la date ne correspond pas à la date de la mesure.

En règle générale, les opérations de vérification des points de contrôle liés à la sécurité *opérationnelle* des systèmes d'information sont actualisables mais ne peuvent pas faire l'objet d'une attestation d'absence de modification, dans la mesure où les vulnérabilités et l'état de l'art en sécurité des systèmes d'information sont en constante évolution :

- ➔ en pratique, les tests d'intrusion, internes ou externes, ne peuvent pas faire l'objet d'une actualisation et doivent donc être chaque année totalement réalisés. Il est d'ailleurs fortement recommandé que les auditeurs soient renouvelés à chaque réalisation d'un test d'intrusion et qu'ils n'aient pas accès, dans un premier temps, aux résultats précédents.

- ➔ en revanche, les audits de sécurité (audit technique de configuration, analyse d'architecture, *etc.*) peuvent faire l'objet d'une actualisation sur l'échantillon antérieur, ainsi que d'une nouvelle analyse sur un nouvel échantillon, complémentaire et introduite à des fins d'exhaustivité.

Les livrables suivants sont donc susceptibles de faire l'objet d'une actualisation ou, exceptionnellement, d'une substitution (en cas d'attestation d'absence de modification produite par l'opérateur) :

- ➔ analyse fonctionnelle et technique du capteur : cette analyse est actualisée si et seulement si l'implémentation du capteur a été modifiée ou afin de valider la correction d'anomalies précédemment identifiées.

  Si l'opérateur communique une attestation précisant que le capteur n'a pas été modifié et qu'aucune non-conformité n'a été relevée dans le précédent audit, l'organisme certificateur peut produire l'attestation dans les annexes et ne pas produire de nouvelle analyse du code source du capteur.

  En revanche, les tentatives de contournement du capteur doivent être dans tous les cas revérifiées annuellement, à l'occasion des audits intrusifs portant sur l'ensemble de la plate-forme de jeu (cf. partie 3.2).

  Pour rappel, l'analyse syntaxique et sémantique des évènements XML enregistrés au coffre ainsi que le fonctionnement du mécanisme d'interrogation des interdits de jeux ne sont pas à effectuer ;

- ➔ analyse d'architecture : le schéma réseau (niveau 3), la matrice de flux, les règles de filtrage ainsi que l'analyse des mécanismes d'administration peuvent faire l'objet d'une simple actualisation par l'organisme certificateur ;

- ➔ audit de configuration : l'organisme certificateur peut initialement, s'il le juge nécessaire, échantillonner les composants à auditer par rôle et/ou par criticité.

  Concernant les certifications ultérieures, la base de connaissances construite au gré des analyses doit permettre à l'organisme certificateur de revoir son échantillonnage et de recentrer son audit sur le fonctionnement d'un ou plusieurs composants qui n'auraient pas fait l'objet d'une analyse approfondie à l'occasion d'une précédente certification. Un travail d'actualisation peut donc être effectué sur les analyses de l'échantillon antérieur.

  Il est important que les contrôles relatifs à la sécurité des systèmes soient systématiquement effectués (état des mises à jour, gestion des comptes utilisateurs, gestion des droits, complexité des mots de passe, synchronisation horaire, *etc.*).

La liste complète des autres analyses et donc livrables attendus dans le cadre de la certification annuelle figure dans l'annexe III. Les livrables qui peuvent faire l'objet d'une actualisation sont indiqués en vert.

Annexe I – Exemples d'évaluation de niveau de criticité en fonction d'éléments de contexte.

Point de contrôle	Anomalie constatée	Contexte	Niveau de criticité initial	Niveau de criticité final
E1	Refus d'accès à un composant de la plate-forme	--	3	3
E5	Version non homologuée d'un logiciel de jeu en production	Des évolutions logicielles mineures ont été effectuées sur une version homologuée sans déclaration à l'ARJEL dans les délais prévus, mais sans impact sur la sécurité ou l'expérience de jeu	3	2
E7	Absence de politique de sécurité	Les équipes techniques présentent un défaut de sensibilisation et de compétences en sécurité informatique	1	2
E29	Back-office accessible depuis Internet, sans filtrage de niveau 3 (IP)	Aucune vulnérabilité découverte (mots de passe faibles, défaut d'implémentation du logiciel back-office [injection SQL, LFI/RFI, etc.])	2	2
E29	Backoffice accessible depuis Internet sans filtrage de niveau 3 (IP)	Vulnérabilité découverte (mot de passe trivial)	2	3
E33	Absence de mises à jour	Serveur wiki interne	2	2
E33	Absence de mises à jour	Serveur applicatif accessible depuis Internet, manipulant des données utilisateurs	2	3
E45	Présence d'un XSS ou d'une injection SQL	Serveur accessible depuis Internet	2	3
E59	Absence de synchronisation NTP	Relais-inverse HTTP en entrée	2	2
E59	Absence de synchronisation NTP	Serveur DNS responsable de l'interrogation des interdits de jeu	2	3

Les éléments ci-dessus ne constituent que des exemples fournis à titre d'illustration et en aucun cas un référentiel d'analyse. Seule l'expertise déployée par l'organisme certificateur peut permettre de moduler les niveaux de criticité.
La modification d'un niveau de criticité par l'organisme certificateur n'a bien entendu de sens que lorsque que l'exigence concernée n'est pas atteinte.

Annexe II – Livrables de la certification unique à 6 mois du composant frontal.

Le rapport de la certification à 6 mois se compose, pour chaque agrément, des 6 livrables suivants :

1. synthèse des rapports, avec mention des réserves ;
2. matrice des exigences ;
3. audit intrusif du capteur ;
4. audit de configuration de l'hébergement du frontal ;
5. rapport de vérification du respect des exigences ;
6. annexes techniques.

Synthèse des rapports :

1. présentation du candidat opérateur ;
2. nombres de jour/homme consacrés à chaque point ;
3. dates des différentes prestations ;
4. date de mise en œuvre opérationnelle du frontal ;
5. synthèse stratégique des résultats obtenus par point ;
6. liste des réserves.

Matrice des exigences.

Audit du capteur :

1. synthèse :
    a. synthèse de l'analyse fonctionnelle et technique,
    b. synthèse technique de l'audit intrusif,
    c. synthèse des vulnérabilités, classées par criticité et impact,
    d. synthèse des recommandations, classées par priorité et coût de mise en œuvre;

2. analyse fonctionnelle et technique :
    a. présentation de la solution :
        i. mécanismes d'enregistrement des traces,
        ii. mécanismes de vérification et de filtrage des données,
        iii. mécanismes de sécurité du capteur,
    b. analyse de code des fonctions les plus importantes du capteur ;

3. audit intrusif du capteur : déroulement linéaire de l'audit, avec description explicite de la méthodologie employée pour détecter les vulnérabilités et les exploiter, le cas échéant.

Audit de configuration du frontal et de son infrastructure d'hébergement :

1. synthèse :
    a. synthèse technique de l'audit de configuration,
    b. synthèse des vulnérabilités, classées par criticité et impact,
    c. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;

2. rapport d'audit :
    a. analyse de la stratégie de sécurité (politique de sécurité technique, procédures, …),
    b. analyse de l'architecture technique (matrices de flux, règles du pare-feu, …),
    c. analyse des configurations, aux niveaux système, réseau et applicatif.

Vérification du respect des exigences : rapport regroupant les différentes analyses n'ayant pas été abordées dans les précédents livrables ;

Annexes techniques :

1. attestations, le cas échéant ;
2. documentation opérateur.

Les fiches d'anomalies sont transmises directement par l'opérateur à l'ARJEL ainsi qu'à l'organisme certificateur. Ces fiches d'anomalies doivent reprendre l'intégralité des vulnérabilités et non conformités pointées par l'organisme certificateur (associées au contenu rédigé par l'organisme certificateur) et intégrer les différentes réponses de l'opérateur (cf. partie 3.1). Chaque fiche doit intégrer au minimum les éléments suivants :

- Numéro et détail de l'exigence ;
- Libellé exact de la vulnérabilité ou non-conformité constatée par l'organisme certificateur ;
- Réponse de l'opérateur.

Annexe III – Livrables de la certification annuelle.

Les éléments actualisables sont présentés en vert. Le rapport de la certification annuelle se compose, pour chaque agrément, des 9 livrables suivants,:

1. synthèse des rapports, avec mention des réserves ;
2. matrices des exigences ;
3. tests intrusifs internes et externes de la plate-forme ;
4. audit fonctionnel du capteur ;
5. analyse de l'architecture technique ;
6. audit de configuration des équipements de la plate-forme ;
7. audit des évolutions des différents logiciels de jeu ;
8. vérification du respect des exigences ;
9. annexes techniques.

Synthèse des rapports :

1. présentation du candidat opérateur ;
2. nombres de jour/homme consacrés à chaque point ;
3. dates des différentes prestations ;
4. synthèse stratégique des résultats obtenus par point ;
5. liste des réserves.
6. liste de l'ensemble des vulnérabilités et non-conformités constatées.

Matrice des exigences.

Audit fonctionnel et technique du capteur :

1. synthèse :
    a. synthèse de l'audit fonctionnel et technique,
    b. synthèse technique de l'audit intrusif,
    c. synthèse des non conformités, classées par criticité et impact,
    d. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;

2. analyse fonctionnelle et technique :
    a. présentation de la solution :
        i. mécanismes d'enregistrement des traces,
        ii. mécanismes de vérification et de filtrage des données,
        iii. mécanismes de sécurité du capteur ;
    b. analyse de code des fonctions les plus importantes du capteur.

Tests intrusifs externes et internes de la plate-forme de jeu

1. synthèse technique des tests intrusifs ;
2. synthèse des vulnérabilités, classées par criticité et impact ;
3. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;

4. rapport du test d'intrusion :
    a. analyse de risques techniques synthétique,
    b. déroulement linéaire du test d'intrusion, avec description explicite de la méthodologie employée pour détecter les vulnérabilités et les exploiter, le cas échéant,
    c. déroulement linéaire du test d'intrusion du capteur.

Analyse de l'architecture technique

1. synthèse technique de l'audit d'architecture ;
2. synthèse des vulnérabilités, classées par criticité et impact ;
3. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;
4. rapport d'analyse :
    a. présentation de l'architecture technique,
    b. analyse de l'architecture technique (matrices de flux, règles de filtrage…),
    c. analyse du cloisonnement,
    d. mécanismes d'administration.

Audit de configuration des équipements principaux des plate-formes

1. synthèse technique de l'audit des équipements ;
2. synthèse des vulnérabilités, classées par criticité et impact ;
3. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;
4. rapport d'analyse : analyse des configurations au niveau système, réseau et applicatif.

Audit des évolutions des différents logiciels de jeu

1. synthèse technique de l'analyse ;
2. rapport d'analyse :
    a. liste des différents logiciels de jeux utilisés (clients et serveur),
    b. analyse des changements apportés.

Vérification du respect des exigences : rapport regroupant les différentes analyses n'ayant pas été abordées dans les précédents livrables.

Annexes techniques :

1. attestations éventuelles ;
2. documentations opérateur.

Les fiches d'anomalies sont transmises directement par l'opérateur à l'ARJEL ainsi qu'à l'organisme

certificateur. Ces fiches d'anomalies doivent reprendre l'intégralité des vulnérabilités et non conformités pointées par l'organisme certificateur (associées au contenu rédigé par l'organisme certificateur) et intégrer les différentes réponses de l'opérateur (cf. partie 3.1). Chaque fiche doit intégrer au minimum les éléments suivants :

- Numéro et détail de l'exigence ;
- Libellé exact de la vulnérabilité ou non-conformité constatée par l'organisme certificateur ;
- Réponse de l'opérateur.