RÉPUBLIQUE FRANÇAISE

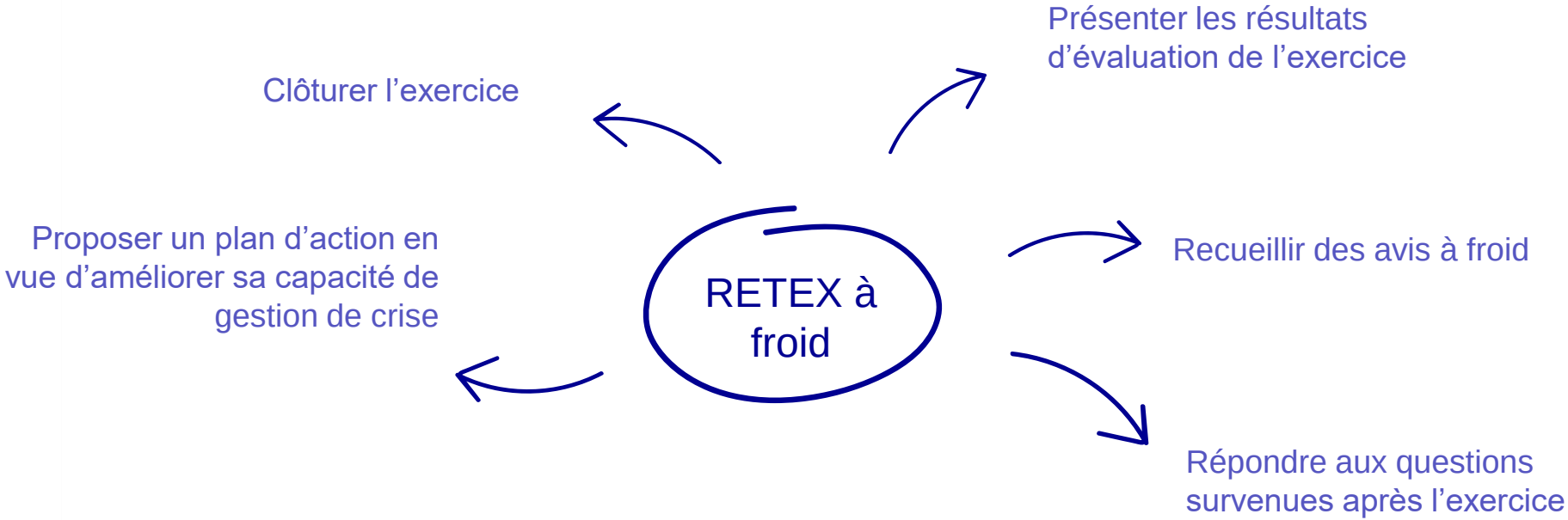
Liberté
Égalité
Fraternité

EXERCICE DE CRISE CYBER JOP 2024

Méthodologie de RETEX à Froid

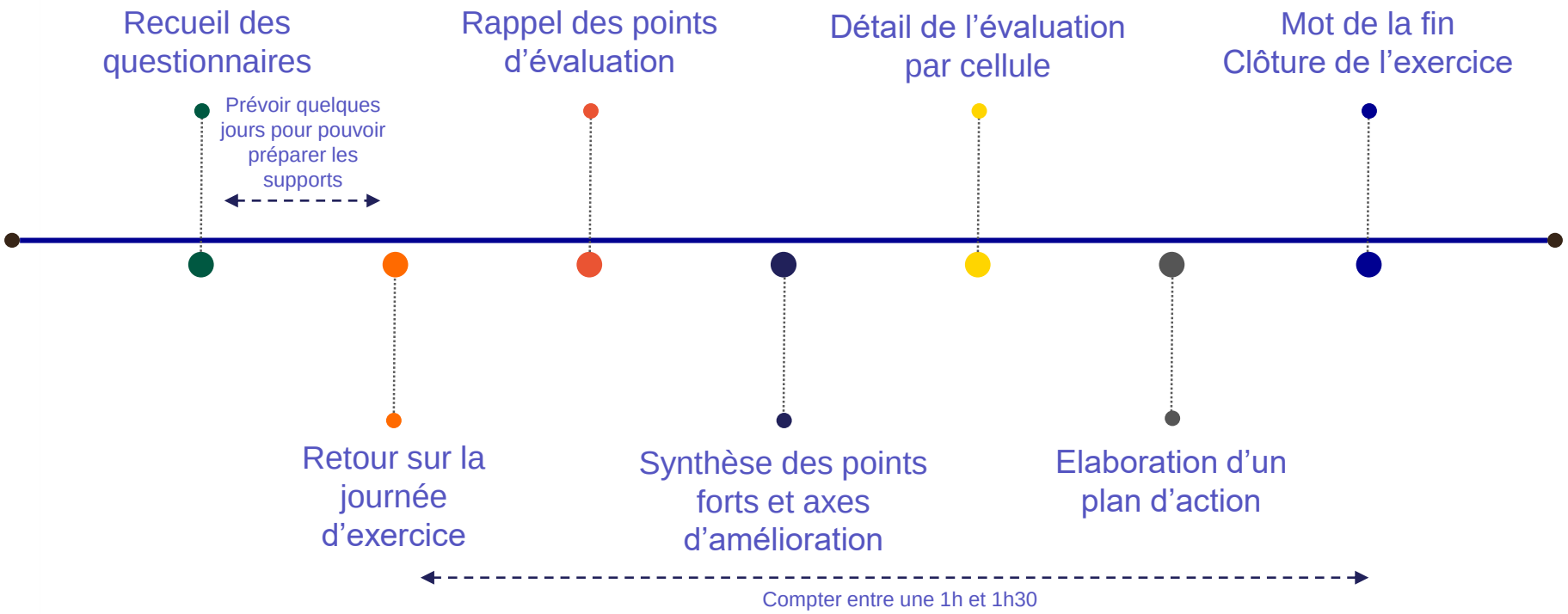
SOMMAIRE

1. OBJECTIFS DU RETEX À FROID



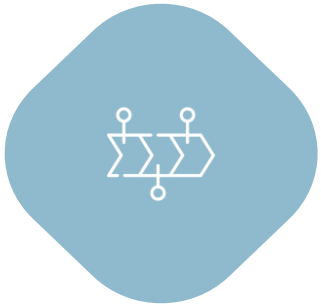
RETEX : Un RETEX est un acronyme pour "retour d'expérience". Il s'agit d'une analyse rétrospective d'une situation, d'un événement ou d'un projet afin d'identifier les points forts et les points faibles, les réussites et les échecs, et de tirer des enseignements pour améliorer les pratiques futures.

2. DÉROULEMENT DU RETEX À FROID



3. RETOUR SUR LA JOURNÉE D'EXERCICE

Afin de permettre une évaluation la plus complète possible, il est important de rappeler aux participants comment s'est déroulé la journée d'exercice sans évoquer uniquement l'exercice mais aussi les éléments annexes (briefing, scénario, équipes, RETEX à chaud, etc.).



→ Rappel du déroulement de la journée d'exercice

→ Rappel du scenario de l'exercice

→ Rappel des différentes équipes

→ Rappel des points forts et axes d'amélioration vus au RETEX à chaud

4. RAPPEL DES POINTS D'ÉVALUATION (NIVEAU 1)

Niveau	Thème d'analyse	Référence au guide ANSSI	Intégration dans le scénario final	
			Stimuli proposés	*Attendus de la part des opérateurs / joueurs*
Niveau 1	Ouverture de crise	**8 - Activer son dispositif de crise cyber**	• Remontées d'alertes cyber par des utilisateurs de l'opérateur (dysfonctionnements, pannes, etc.)	• Appui sur la documentation de crise • Appui sur les critères d'activation de crise cyber pour déclencher le processus d'alerte et informer les fonctions décisionnelles de l'organisation • Déclenchement de la crise • Armement des cellules de crise • Revue des systèmes de détection d'incidents (« SIEM/SOC ») • Mobilisation des équipes
	Pilotage de crise	**9 - Piloter son dispositif de crise**	• Demande de visibilité sur les évènements et la crise	• Suivi via main courante • Suivi des mesures conservatoires et de remédiation
	Capacité à impliquer / prévoir d'impliquer un acteur PRIS	**8 - Activer son dispositif de crise cyber** **11 - Activer ses réseaux de soutien**	• Rattrapage : Demande du management de réaliser des investigations	• Identification des experts à impliquer • Activation le cas échéant d'une assurance cyber • Lancement d'investigations • Recherche des vecteurs potentiels d'infection
	Alerte managériale	**8 - Activer son dispositif de crise cyber**	• Demande du management d'obtenir des informations sur l'état de la crise	• Revue des modalités d'escalade de l'alerte vers la direction générale (synthèse, informations, arbitrages)
	Capacité de communication	**12 - Communiquer efficacement**	• Pression médiatique et de la part des organisateurs • Demande des fonctions de communication pour avertir les utilisateurs et collaborateurs	• Capacité à établir (en amont si possible) une stratégie de communication • Capacité à communiquer
	Alerte aux autorités de référence	**11 - Activer ses réseaux de soutien**	• Réception de la demande d'une autorité de tutelle / pouvoirs publics d'obtention d'informations	• Anticipation des déclarations obligatoires
	Réfléchir à des modalités de reprise informatique (palliatifs et/ou sauvegardes**)**	**14 - Mettre en place un mode de fonctionnement dégradé pour les métiers impactés** **16 - Préparer et industrialiser la reconstruction**	• Pression des utilisateurs et du management à relancer les services	• Appui sur le PCA / PRA • Préparation d'une stratégie de reconstruction • Checklist de reconstruction

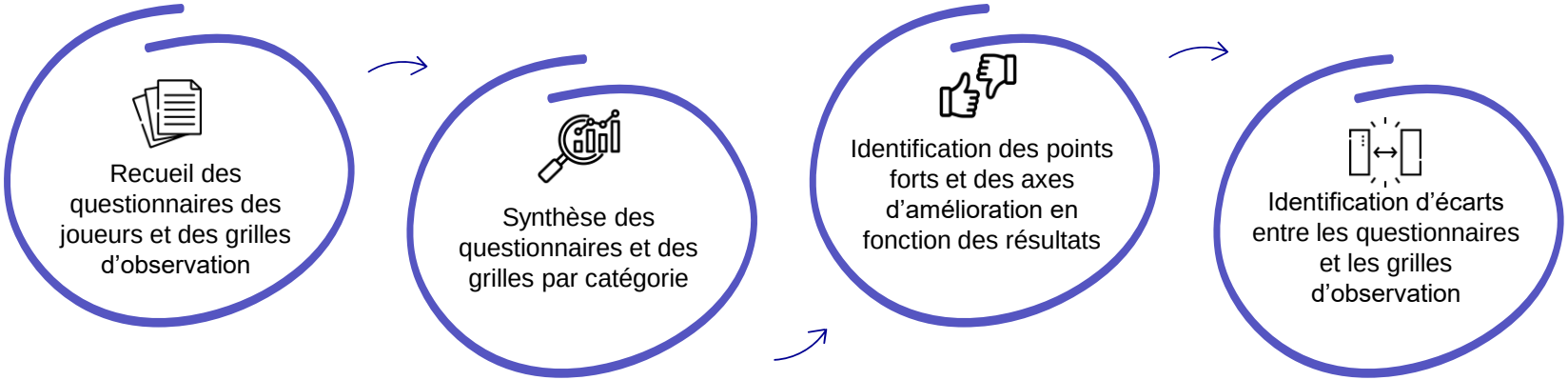
4. RAPPEL DES POINTS D'ÉVALUATION (NIVEAU 2)

Niveau	Thème d'analyse	Référence au guide ANSSI	Intégration dans le scénario final	
			Stimuli proposés	*Attendus de la part des opérateurs / joueurs*
Niveau 2	***Cf. niveau 1*** Cartographie des systèmes impactés	**9 - Piloter son dispositif de crise**	• Demande d'état du SI	• Capacité à s'appuyer sur une cartographie du SI • Capacité à s'appuyer sur une cartographie des actifs sensibles
	Impliquer un acteur PRIS	**11 - Activer ses réseaux de soutien**	• Demande du management de réaliser des investigations • Réaliser un point de situation incluant la liste des actions constatées et réalisées à destination d'un prestataire PRIS	• Contractualisation avec un acteur PRIS • Capacité à préparer l'intervention du partenaire
	Cartographie des impacts	**13 - Conduire l'investigation numérique**	• Demande de l'étendue des impacts, des points d'entrée • Demande des principales actions de l'attaquant	• Identification du périmètre de compromission • Recherche des vecteurs potentiels d'infection • Documentation des actions de l'attaquant
	Plan d'actions d'endiguement	**13 - Conduire l'investigation numérique**	• Demande des opérationnels d'un plan d'action de défense et d'endiguement	• Comprendre l'étendue et le chemin de la compromission • Prioriser les actions de remédiation par un plan de défense
	Maitrise des tiers	**12 - Communiquer efficacement**	• Demande d'un ou plusieurs tiers concernant la compromission de leur données / accès et/ou métiers	• Rassurer ses parties prenantes • Dresser et schématiser le périmètre de la compromission
	Restauration de sauvegarde / continuité métier	**14 - Mettre en place un mode de fonctionnement dégradé pour les métiers impactés**	• Nécessité d'avoir accès aux sauvegardes • Nécessité d'assurer les fonctions essentielles liées aux JO (assurer les épreuves, assurer la sécurité des athlètes et des spectateurs, assurer la couverture médiatique de l'évènement, etc.)	• Définir et soutenir les modes d'utilisation des solutions de contournement • Communiquer en interne sur les solutions de contournement choisies
	Communiquer vers les autorités de tutelle	**11 - Activer ses réseaux de soutien**	• Demande de déclaration auprès des autorités compétentes (*Stimuli balais uniquement*)	• Déclarer son incident auprès des autorités compétentes (ANSSI, CNIL, autorités judiciaires) • Dépôt de plainte

4. RAPPEL DES POINTS D'ÉVALUATION (NIVEAU 3)

Niveau	Thème d'analyse	Référence au guide ANSSI	Intégration dans le scénario final	
			Stimuli proposés	*Attendus de la part des opérateurs / joueurs*
Niveau 3	Formaliser un plan d'action reconstruction	**16 - Préparer et industrialiser la reconstruction**	• Demande de stratégie opérationnelle de reconstruction • Processus de restauration des sauvegardes • Demande de calendrier prévisionnel de réouverture des services (avec un arbitrage coût à proposer)	• Construire une stratégie de reconstruction • Stratégie de restauration des données par des sauvegardes saines • Dresser un calendrier prévisionnel réaliste pour la réouverture des applications métiers
	Interactions en multi-cellules (cellules stratégiques / opérationnelle, multisite	**10 - Soutenir ses équipes de gestion de crise**	• Demande de point de situation inter-cellules par la DG • Demande d'identification des obligations auprès des partenaires, clients et fournisseurs qui ne pourront pas être respectées • Prévoir le roulement des équipes, anticiper l'augmentation du nombre d'heures des collaborateurs concernés, effectuer le suivi RH des prestataires mobilisés, etc.	• Bien dissocier la cellule stratégique, la cellule opérationnelle et la cellule de communication • Création « d'équipes-projet » afin de répartir les sujets • Qualité d'échange des informations entre chaque cellule • Mobilisation des équipes juridiques • Support RH à prévoir
	Investigation	**13 - Conduire l'investigation numérique**	• Cf. Cartographie des impacts (niveau 2)	• Poursuivre la stratégie d'investigation (en lien avec le PRIS) • Organiser la suite des investigations sur l'étendue des compromissions
	Plan d'amélioration de sécurité numérique	**15 - Durcir et remédier** **18 - Tirer les leçons de la crise**	• Orienter les participants vers la révision des pratiques d'administration et de gestion du SI • Orienter les participants vers une réflexion autour de leur gestion des sauvegardes • Orienter les participants vers l'adaptation du PCA/PRA • Orienter les participants vers une meilleure surveillance du SI	• Protéger le SI de nouvelles attaques • Reprendre le contrôle des systèmes et durcir pour empêcher de nouvelles compromissions • Commencer à construire un plan d'actions d'amélioration du niveau de sécurité SI • Réflexion autour de la surveillance des systèmes

5. SYNTHÈSE DES POINTS FORTS ET AXES D'AMÉLIORATION



6. DÉTAIL DE L'ÉVALUATION

Présenter les résultats de l'évaluation sous la forme d'un tableau avec les mêmes catégories que sur les questionnaires et les grilles d'observation.

Dissocier les résultats à la fois par rôle et par cellule pour présenter des éléments les plus détaillés possibles.

Pour chaque catégorie et chaque cellule, indiquer le score obtenu ainsi que les points forts et axes d'amélioration possibles par catégorie.

Réaliser la présentation d'une manière peu formelle, permettant ainsi aux participants d'intervenir en cas d'incompréhension ou de désaccord.

6. DÉTAIL DE L'ÉVALUATION : EXEMPLE

Evaluation de la cellule de crise décisionnelle
Point de vue joueur

Thème	Score	Points forts	Points à améliorer
Exercice et ingénierie d'exercice			
Gouvernance et interactions entre équipes mobilisées			
Processus et outillage			
Communication de crise et relations externes			
Détection et réponse à incidents			
Continuité d'activité et reconstruction			

7. ÉLABORER UN PLAN D'ACTION

01	Extraire les axes d'amélioration depuis l'évaluation
02	Réfléchir à chaque axe d'amélioration et trouver des éléments correctifs
03	Discuter avec les participants d'un délai pour la mise en place des mesures
04	Formaliser ce plan d'action sur un document transmis à tous après le RETEX

8. MODE D ’EMPLOI DANS LE CADRE DU PROJET D’EXERCICES MASSIFIÉS JOP 2024

01

Recueillir les questionnaires de RETEX à froid de tous les participants ainsi que les grilles d’observation

02

Rassembler l’ensemble de ces résultats dans le document Excel de RETEX global

03

Reporter les données du RETEX global dans le support de présentation de RETEX à froid

04

Compléter le support de présentation du RETEX à froid pendant sa réalisation avec un maximum d’éléments supplémentaires évoqués pendant le RETEX

05

Transmettre à l’ANSSI votre Excel de RETEX global ainsi que votre support de présentation du RETEX à froid complété pour permettre une analyse globalisée des exercices réalisés

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

BON RETEX !