< Conduire un retour d'expérience d'un exercice de gestion de crise d'origine Cyber >

FICHE MÉTHODOLOGIQUE

< Groupe de travail gestion de crise cyber et entraînement >

Juin 2026

CAMPUS CYBER

SOMMAIRE

Ce document vise à fournir une base solide et un point de départ pour les organisations souhaitant réaliser des retours d’expérience dans le cadre d’un exercice de gestion de crise d’origine cyber, en s'appuyant sur les éléments essentiels pour une approche simple mais efficace.
Il convient de noter qu'il existe plusieurs autres méthodologies qui peuvent être adaptées en fonction du contexte et de la structure spécifiques des organisations. La complexité d’un exercice de crise d’origine cyber peut varier considérablement d'une organisation à l'autre, en fonction de la taille, du secteur d'activité et du niveau de maturité.
Pour les organisations ayant des structures plus complexes ou des besoins spécifiques, des approches plus détaillées ou personnalisées doivent être adoptées.

1| Introduction

1.1 – Fiche méthodologique : Conduire un Retour d'Expérience à la suite d'un exercice de gestion de crise d'origine cyber

Un RETEX, ou retour d'expérience, est un processus d'analyse des événements survenus lors d'une situation, comme un exercice de gestion de crise. Il permet d'identifier les forces et les faiblesses des actions, avec des enseignements pour améliorer les stratégies futures. Réaliser un RETEX après une crise permet d'examiner les pratiques et décisions, assurant une amélioration continue et une meilleure préparation à des situations similaires.
De nombreux documents et ressources sur ce sujet sont disponibles, notamment ceux proposés par l'ANSSI. Pour éviter toute redondance, l'approche adoptée pour la construction de cette fiche consiste à se baser sur ces documents en les complétant par des éléments contextuels et spécifiques à la réalisation d'un RETEX.

Cette présente fiche a été élaborée dans le cadre d'un groupe de travail du Campus cyber, regroupant divers acteurs de la gestion de crise d'origine cyber, présentés ci-dessous :

Organisation		Participants
RENAULT	Groupe Renault	Sebastien BLARD Bruno ESTEVE
Deloitte.	Deloitte Conseil	Sebastien JARDIN Omar EL AHDAB
SNCF	Groupe SNCF	Axel CASTADOT
Almond	Almond	Francesca SERIO
	La Préfecture de Police	Salima TBATOU
Urgence Cyber IledeFrance	Urgence Cyber Ile de France	Fanny RIVAUD
BNP PARIBAS	Groupe BNP Paribas	Viktoriia MIROSHNICHENKO
Schneider Electric	Schneider Electric	Anouk PAULMIER

1.2 – Les Quatre Fondements pour Optimiser le Retour d'Expérience

Chaque exercice a ses objectifs

Un exercice de crise d'origine cyber vise à aiguiser les **réflexes individuels** et la **cohésion** des participants, ainsi qu'à permettre à l'organisateur de mettre en évidence des **risques à couvrir** ou des **projets stratégiques** nécessitant davantage de cyber résilience.

Pour être efficace, même s'il est immersif, un bon exercice n'est pas un jeu ni un audit, mais un **moyen d'entraîner & tester les participants** de manière collective et de renforcer la résilience de l'organisation face aux menaces numériques, de don-ner **des pistes d'amélioration concrètes** à mettre en place avant le prochain exercice.

Par ailleurs, un des bénéfices additionnels d'un exercice est le renforcement de la confiance et de la coordination au sein de l'organisation, l'éntraînement étant tout aussi important que le but à atteindre.

Une méthode structurée

Après un exercice de crise, deux moments sont prévus pour le retour d'expérience : un **à chaud**, immédiatement après l'exercice, permettant **à chaque participant de partager ses apprentissages** et axes d'évolution pendant 20 à 30 minutes, et un **à froid** d'une heure, 3 à 4 semaines après, **où un rapport d'observations est présenté** aux participants après validation auprès de l'organisateur.

Ce dernier retour permet **une analyse factuelle et qualitative** des résultats, mettant en lumière les améliorations mais également les points positifs, pour renforcer la posture de cyber résilience de l'organisation et guider l'organisation sur des projets d'amélioration de sa résilience numérique.

Retour à chaud et à froid

Pour structurer un retour d'expérience après un exercice de crise d'origine cyber, plusieurs outils sont essentiels.

Tout d'abord, les observations faites pendant la séance permettent d'**établir une base factuelle** (triptyque situation-décision-action, et même détection des biais cognitifs pour les organisations les plus matures). Il est crucial de tenir compte du **contexte de l'organisation**, de la **typologie de l'exercice** ainsi que des **risques les plus significatifs**.

Ensuite, la **main courante de l'exercice**, ajustée pour inclure les réactions émotionnelles, contribue à une analyse pertinente.

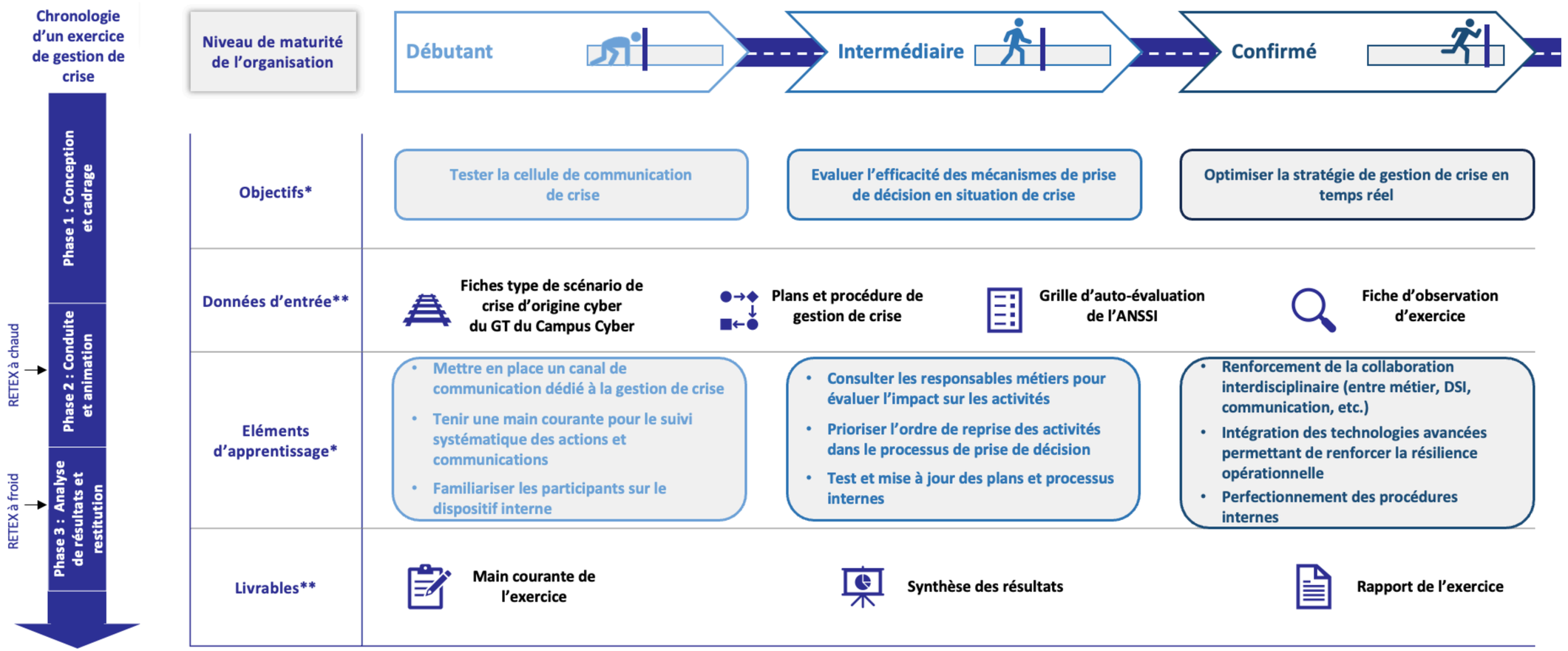
Enfin, **l'expérience personnelle de l'organisateur**, acquise au fil des exercices, est cruciale pour **guider** efficacement les participants et **améliorer** la cyber résilience de l'organisation.

Retour à chaud et à froid

Organiser un exercice de crise d'origine cyber, particulièrement lorsque cela n'est pas encore une évidence, nécessite le **soutien de la direction générale**.
Il est également important de valoriser l'exercice afin de **répondre aux exigences réglementaires**, ainsi qu'aux risques et enjeux opérationnels.

Trouver le bon sponsor ou la bonne justification, comme les impératifs réglementaires, est essentiel. Une fois la logique d'exercices lancée, le processus de dynamique positive et le collectif de crise se mettra en place. A noter qu'il faudra veiller à maintenir le rythme d'exercices et toujours **bien choisir les sujets traités en séance** afin qu'ils reflètent les priorités stratégiques de l'organisation ainsi que les scénarios de risque les plus critiques.
Enfin, le dernier bénéfice de ces exercices est de **renforcer l'engagement des participants** envers le rôle prioritaire à donner à la **réduction du risque numérique.**

1.3 – Stratégie d'entraînement sur long terme : visualisation d'un parcours et des livrables



* Éléments présentés à titre d'exemple, dépendant du contexte de l'organisation
** Liste non exhaustive, comprenant des exemples

2 | Phase de préparation

2.1 – Phase de préparation : Check-List

Constituer l'équipe et planifier les RETEX

- Constituer l'équipe d'observateurs, 1 à 2 par cellule, avec des personnes qui :
  - vont comprendre les enjeux et objectifs de l'exercice
  - pourront avoir un regard "indépendant"
  - seront légitimes par rapport aux thèmes traités
- Identifier la date du RETEX à froid et éventuellement à chaud si différé par rapport à la date de l'exercice
- Lancer les invitations aux RETEX en même temps que les invitations à l'exercice.

Recueillir les éléments

Recueillir les éléments pour compléter la grille d'observation avec les objectifs spécifiques à l'exercice. Voir exemple grille d'observation en annexe.

- Analyser les RETEX des derniers exercices
- Identifier la date du RETEX à froid et éventuellement à chaud si différé par rapport à la date de l'exercice
- S'appuyer sur les objectifs de l'exercice et les organiser par thème. Possibilité d'utiliser la grille fournie en annexe.
- Construire ou mettre à jour la grille d'observations

Organiser un briefing pour les observateurs

Durée : 30 minutes à 1 heure.
Date : quelques jours à une semaine avant l'exercice

- Présenter le scénario et le profil des participants
- Rappeler leur rôle et responsabilités : observer de manière active les aspects qualitatifs et quantitatifs tout en restant en retrait de l'exercice
- Présenter la grille d'observation et expliquer comment la compléter
- Répartir le cas échéant environ une dizaine de points par observateur en fonction de leur légitimité
- Rappeler les éléments de contexte pour identifier les potentiels biais d'exercice
- Prévoir un temps d'appropriation et de questions/réponses, en fonction de la maturité des observateurs.

Anticiper la communication interne autour de l'exercice

- Prévoir de capturer de la matière pour la communication post-exercice (Exemple : photos)

2.2 – Phase de préparation : exemple grille d’observation

La présente fiche méthodologique propose une grille d’observation type divisée en trois niveaux d’expertise : débutant, intermédiaire, et confirmé.
Cette grille évolutive permet de poser des questions adaptées à chaque niveau. Lorsqu’une organisation progresse, elle est incitée à intégrer les questions du niveau supérieur et à ajuster la grille selon son contexte spécifique et ses besoins particuliers.
Les questions associées à la grille suivante sont disponibles dans l’annexe A de cette fiche.

THEME	EVALUER LA CAPACITE A :	Nombre de questions
ANALYSE ET REMONTEE D’ALERTE	Identifier, collecter, trier et escalader les évènements en fonction de leurs impacts	5
ORGANISATION	Identifier et mobiliser les parties prenantes internes et externes, nécessaires à la résolution de la crise	9
PILOTAGE	Conduire le dispositif de gestion de crise de manière efficace (prise de décision pertinente, priorisation des actions, point de situation, main courante, gestion du stress, etc.)	11
COMMUNICATION	Identifier et communiquer efficacement avec les parties prenantes internes et externes	8
CONTINUITE D’ACTIVITE METIER	Connaître les activités impactées et prioriser leurs continuités en mode dégradé en coordination avec les équipes métier	3
CONTINUITE D’ACTIVITE INFORMATIQUE	Organiser la reprise du système d’information (infrastructure et applicatif) sur la base des priorités métier, en considérant le contexte et les impacts de la crise d’origine cyber (investigation, endiguement, début de remédiation, etc.)	6
OBLIGATIONS LEGALES ET CONTRACTUELLES	Connaître et respecter les obligations légales, règlementaires et contractuelles spécifiques au contexte cyber (RGPD, DORA, NIS2, EU CRA, etc.)	3
COORDINATION MULTICELLULE	Coordonner la gestion d’une crise d’origine cyber à périmètre étendu (stratégique, opérationnel, géographique, culturel, plusieurs métiers impactés, etc.)	3

3 | Observation le jour J

– Observation le jour J : les points clés à prendre en compte

Comment observer ?

- Le rôle de l'observateur est crucial dans la conduite du RETEX à chaud et la construction du RETEX à froid. C'est sur la base de ses observations qu'un RETEX pertinent pourra être conçu. Il ne s'agit pas de parler de sentiments mais bien de faits ou de sensations avérées et appuyés sur des faits observés et vécus durant l'exercice.

- L'observateur n'est pas l'animateur, mais dans les exercices réalisés avec une équipe restreinte d'organisation, il peut y avoir un observateur et un animateur. Lorsque l'animateur fait avancer l'exercice, l'observateur analyse les grands thèmes (ex: coordination des participants, connaissances des procédures, qualité des échanges, capacités de la cellule à anticiper et décider, les biais cognitifs exprimés négativement…). Et si l'observateur prend un rôle ponctuel de co-animation, à ce moment-là, l'animateur devient observateur ponctuel.

Les aspects logistiques à prendre en compte

- Lors de l'évaluation d'un exercice de gestion de crise, les aspects logistiques doivent être pris en compte, notamment les dimensions techniques, linguistiques et culturelles, en particulier pour les organisations multinationales.

- De plus, les éléments logistiques de l'évaluation à distance et les outils de collaboration et de visio-conférence sont importants. Les observateurs doivent être capables de capturer les éléments clés de l'évaluation en tenant compte de ces facteurs, et en se basant sur une préparation minutieuse.

La coordination entre observateur et animateur

- Afin que le RETEX soit de qualité, il peut être décidé par l'animateur de laisser un peu plus de temps aux participants pour traiter un sujet, ou alors au contraire de contraindre leur temps. Dans tous les cas, il doit y avoir coordination entre l'animateur et l'observateur afin que les stimuli soient envoyés à la salle d'exercice au moment le plus opportun afin d'observer ce qui est important.

- En complément des éléments d'observation partagés ci-dessus, il faut préciser que l'observation doit couvrir des éléments quantitatifs mais également qualitatifs. C'est ainsi que l'on observera par exemple le temps restant à la salle de crise dans la résolution de tel ou tel incident simulé, mais également le niveau de tension ou de confiance perçue entre les participants (ex: quand la demande de rançon arrive, les comportements peuvent varier d'un participant à l'autre). Le tout devant être consigné dans une main courante d'exercice, une sorte de journal de bord tenu par l'observateur et qui contiendra un maximum ce qui s'est passé durant la séance (voir annexe pour un modèle de main courante)

L'implication de l'observateurs dans l'animation

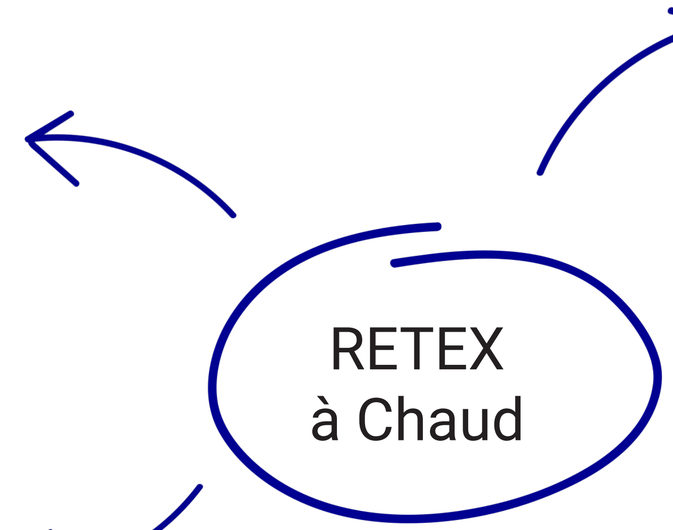
- Lorsque l'observateur devient co-animateur, il est impliqué opérationnellement dans l'animation (appels vers la salle de crise, répondre à des questions des participants, entrer dans la salle pour apporter un certain effet dynamique). Il est donc important de préparer une logistique simple de numéros de téléphones à appeler et de boites e-mails à préparer.

L'ANSSI propose une fiche « rôle de l'observateur », contenant des spécificités relatives au rôle de ce dernier.
Cette fiche est disponible en Annexe B du présent document.

4 | RETEX à Chaud

CAMPUS CYBER

4.1 – Objectifs du RETEX à CHAUD *



Recueillir le ressenti des participants de l'exercice (points positifs, axes d'amélioration…)

Evacuer les éventuelles frustrations causées par l'exercice

Revenir sur l'organisation de l'exercice et sur la préparation des différentes parties prenantes

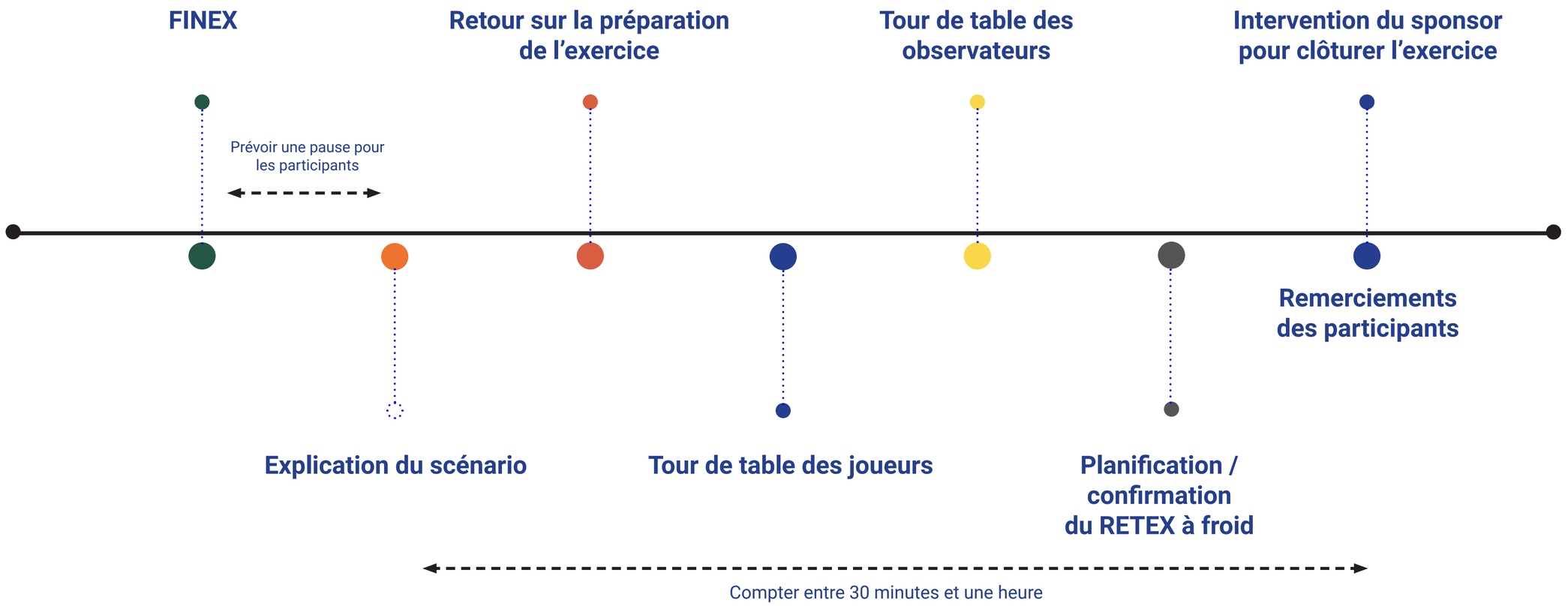
Expliquer le scénario qui vient d'être joué ainsi que le lien avec la menace pour l'organisation

Présenter les points forts observés ainsi que les axes d'amélioration

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.

* Cette diapositive est issue de la source suivante: https://cyber.gouv.fr/sites/default/files/document/ANSSI_JOP_Methodologie_RETEX_Chaud.pdf

4.2 – Déroulement du RETEX à Chaud *

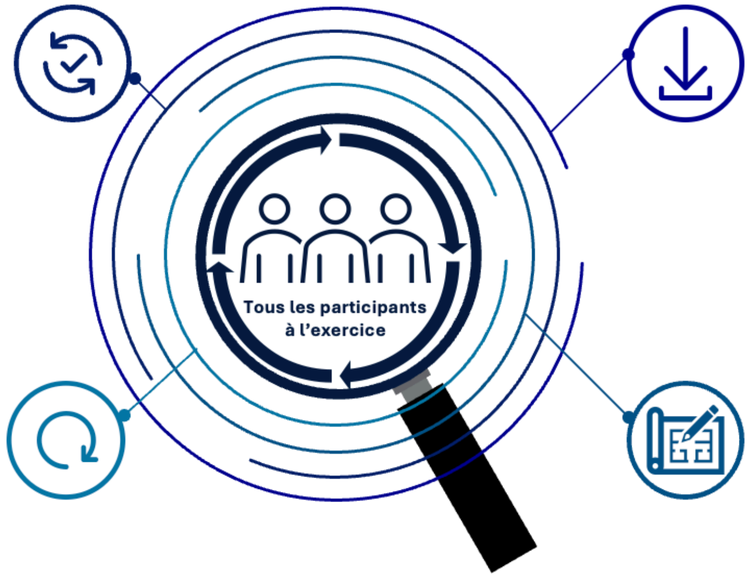


* Cette diapositive est issue de la source suivante : https://cyber.gouv.fr/sites/default/files/document/ANSSI_JOP_Methodologie_RETEX_Chaud.pdf

4.3 – RETEX à Chaud : Activités clés

Rappeler les objectifs de l’exercice et réexpliquer le scénario de l’exercice (schéma d’attaque) pour que tous les participants gardent la même compréhension

Pour maintenir le dynamisme et éviter les effets de répétition ou les biais de restitution, il est essentiel de définir l’ordre à l’avance. Si nécessaire, des représentants des différents rôles et/ou cellules doivent être désignés pour garantir un retour holistique sur l’exercice.



L’animateur est responsable de la collecte des grilles d’observations remplies par les observateurs désignés. Idéalement, il devrait utiliser les points clés et les retours des observateurs comme entrée pour formaliser le RETEX à chaud

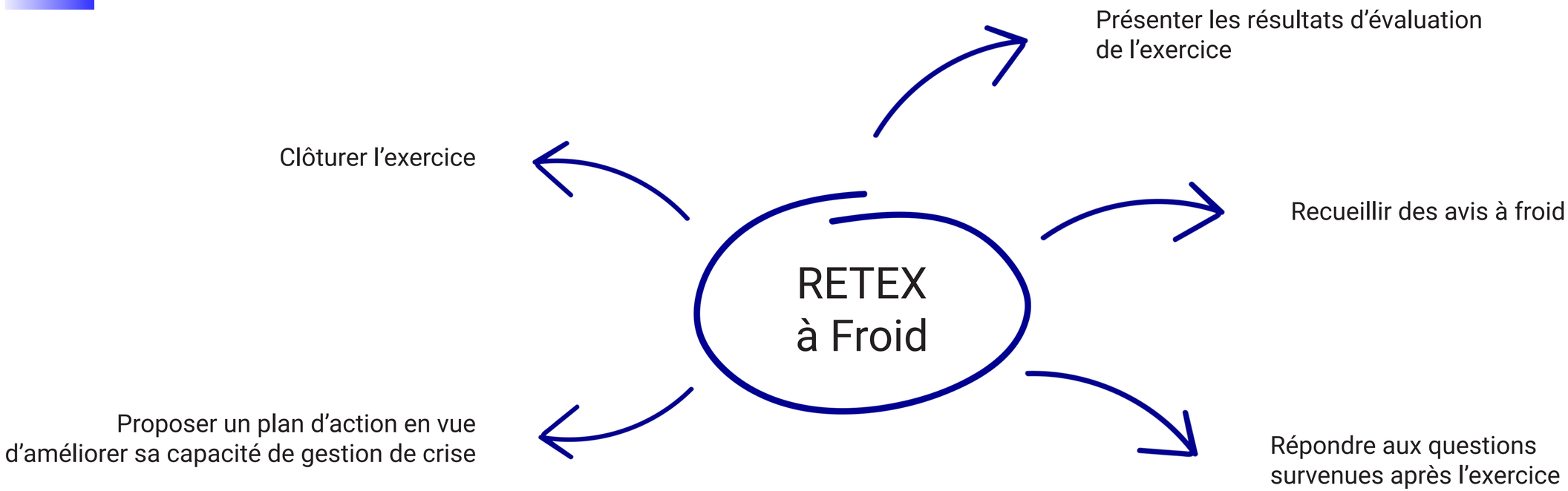
Partager une ébauche de plan d’action incluant les premières recommandations ainsi que les recommandations révisées, qui seront complétées lors du RETEX à froid.

Réaliser un RETEX à chaud à la fin de l’exercice ---> Template Retex à chaud

5 | RETEX à Froid

CAMPUS CYBER

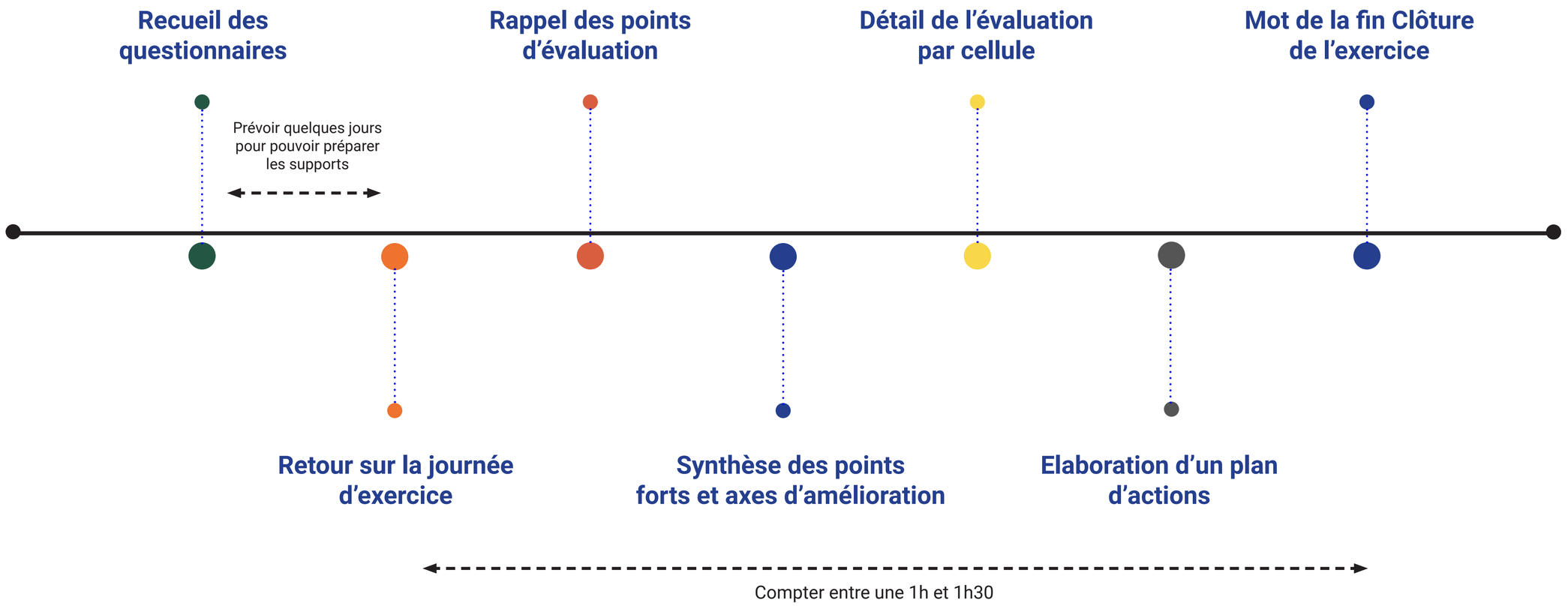
4.3 – RETEX à Chaud : Activités clés



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.

* Cette diapositive est issue de la source suivante : https://cyber.gouv.fr/sites/default/files/document/ANSSI_JOP_Methodologie_RETEX_Froid.pdf

5.2 – Déroulement du RETEX à FROID



Cette diapositive est issue de la source suivante : https://cyber.gouv.fr/sites/default/files/document/ANSSI_JOP_Methodologie_RETEX_Froid.pdf

5.3 – RETEX à FROID : Activités clés

Présenter et organiser les recommandations du plan d’action

(Cette phase s’inscrit dans le temps long du PDCA et ne mobilisera qu’une partie des participants)

Récupérer le feedback des sponsors

Collecter les retours pour identifier les axes d'amélioration concernant la manière dont l'exercice a été réalisé, les scénarios qui ont été mis en œuvre, ainsi que tout autre élément approprié.

Définir et valider un plan d’action

Mettre en place un plan d’actions issu de l’exercice, visant à traiter les sujets clés avant le prochain, afin de suivre la méthodologie PDCA. Établir un planning avec des objectifs atteignables, des jalons précis, et des responsables clairement définis, et garantir un suivi efficace par le biais d’un comité de suivi ou d’une équipe projet.
Faire valider ce plan d’action par le sponsor

Consolider l’ensemble des retours et formaliser le RETEX Global à froid

Celui-ci, autour de la synthèse des axes améliorations, des points forts et des recommandations peut être organisé en trois parties dédiées :
Au rappel du contexte et du périmètre de l’exercice, ainsi que des conventions et objectifs de l’exercice
À l’organisation de l’exercice, au format choisi par rapport aux conventions et aux objectifs, ainsi qu’au rythme de l’animation
À la synthèse des phases de l’exercice (par exemple, phase de réponse, phase de réactions, phase d’investigation, etc.) en s’appuyant sur les objectifs de l’exercice pour pondérer la définition des axes d’améliorations, les recommandations liées et les points forts.

Assurer une communication ciblée des résultats

Communiquer sur l’exercice de crise réalisé et les leçons tirées en fonction du contexte et du public ciblé, en tenant compte des informations partagées. Par exemple :
Public interne (toute l’entreprise) : Informer que l’exercice a eu lieu, en précisant les objectifs globaux, tels que l’amélioration du niveau de maturité et de la posture de cyber-résilience.
Cellules de crise, équipes SSI, SOC, ou toutes autres parties prenantes concernées :
Fournir des détails sur le scénario d’attaques, et le déroulement de l’exercice
Partager les enseignements clés et les actions à entreprendre à haut niveau

Réaliser des RETEX spécifiques

Ne pas hésiter à faire en complément du RETEX Global, des RETEX spécifiques à des situations rencontrées (en rappelant par exemple les réponses données lors du REX à chaud) pour modifier des procédures spécifiques

Fusionner le RETEX à chaud et à froid pour les exercices courts

Sur des exercices courts moins de 2 heures avec souvent un ou deux objectifs, le RETEX à chaud et à froid peuvent être fusionnés s'ils ont lieu dans la journée de l’exercice ou le lendemain matin.

Cette diapositive est issue de la source suivante : https://cyber.gouv.fr/sites/default/files/document/ANSSI_JOP_Methodologie_RETEX_Froid.pdf

6 | Annexes

Annexe A : Grille d'observation – Niveau Débutant (1/3)

THEME	CONSTATS	Observation	NIVEAU D'ATTEINTE DES OBJECTIFS *
ANALYSE ET REMONTEE D'ALERTE	La qualification de l'évènement a été effectuée.		
	Le processus d'alerte permet d'escalader l'information rapidement avec les bons canaux et permet de synthétiser l'information.		
	Le processus de mobilisation de la cellule de crise a été mis en œuvre.		
	Les outils existants pour l'alerte (mail, téléphone, messagerie instantané, outils dédiés, etc…) sont connus et utilisés correctement.		
ORGANISATION	Les rôles clés d'une cellule de crise sont identifiés dès le début de la crise voire en amont : pilote(s), main courante, porte-paroles		
	La composition de la cellule est adéquate pour répondre aux besoins de la situation		
	La cellule de crise sait s'adapter en fonction de l'évolution de la situation		
	Les membres de la cellule sont capables de gérer leur stress pour rester concentrés sur leurs tâches		
	La salle de crise est adaptée dans une telle situation (spacieuse, espaces silencieux, etc.)		
PILOTAGE	La cellule est ouverte avec un point de situation et un tour de table des membres de la cellule		
	Tous les membres de la cellule sont au point de situation et ont eu un temps de parole		
	La tenue de la main courante est structurée, synthétique et accessible à l'ensemble des membres de la cellule		
	Le pilote organise et harmonise la prise de décision		
	Les impacts (métiers, business, informatiques, ect) de la crise sont identifiés		
	Une priorisation des sujets et des actions à entreprendre est réalisée		
COMMUNICATION	Les différents experts (IT, juridiques, Communication,…) sont sollicités pour préparer les éléments de communication		
	En cas de fuite de données, les membres de la cellule de crise intègrent les aspects réglementaire dans la gestion de la communication.		
CONTINUITE D'ACTIVITE METIER	Les parties prenantes internes et externes sont informées des mesures prises pour assurer la continuité		
CONTINUITE D'ACTIVITE INFORMATIQUE	Les membres de la cellule identifient les applications et services indisponibles.		
OBLIGATIONS LEGALES ET CONTRACTUELLES	Les autorités compétentes (CNIL, BCE, ANSSI, ect) sont notifiées dans les délais impartis		
	Les membres de la cellule de crise ont pensé à déposer plainte		
	Les membres de la cellule de crise ont pensé à contacter leur assurance/courtier		

Annexe A : Grille d’observation – Niveau Intermédiaire (2/3)

THEME	CONSTATS	Observation	NIVEAU D’ATTEINTE DES OBJECTIFS *
ANALYSE ET REMONTEE D’ALERTE	Le diagnostic s'appuie sur une matrice de criticité permettant d'ajuster le niveau de mobilisation		
ORGANISATION	La cellule de crise était équipée correctement : ordinateurs, chargeurs, wifi, projecteur, etc.		
	Aucun comportement inapproprié s'est dévoilé (isolement, biais d'autorité, etc.)		
	Des fiches réflexes sont utilisées		
PILOTAGE	Les impacts humains de l'attaque sont évalués par la Cellule de Crise		
	Les points de situation sont fréquents, organisés et pertinents dans la prise de décision		
	La cartographie exhaustive des parties prenantes et leurs attentes est réalisée		
	La cellule de crise dispose d’une stratégie de gestion de crise cyber (détection, réaction, endiguement).		
COMMUNICATION	Les membres de la cellule de crise respectent les fondamentaux de la communication de crise. (FACET : Faits, Actions, Compassion, Engagement, Transparence)		
	La cartographie exhaustive des parties prenantes est réalisée pour une communication adéquate		
	Les canaux de diffusion des messages sont clairement identifiés selon les publics visés		
	Les membres de la cellule travaillent sur une stratégie de communication. Les messages délivrés sont cohérents entre les informations, leur niveau de confidentialité et les publics visés		
	Le processus de rédaction et de validation des messages est opérationnel		
CONTINUITE D’ACTIVITE METIER	Les membres sont en mesure de savoir si les processus critiques ont été maintenus sans interruption majeure		
CONTINUITE D’ACTIVITE INFORMATIQUE	La cellule de crise intègre le volet Forensic IT. Les volets d’investigation et de collecte des preuves sont bien considérés.		

Annexe A : Grille d’observation – Niveau Confirmé (3/3)

THEME	CONSTATS	Observation	NIVEAU D’ATTEINTE DES OBJECTIFS *
ORGANISATION	La documentation de crise est utilisée		
PILOTAGE	La coordination de la cellule de crise est efficace (flexibilité, fluidité, disponibilité, RH)		
COMMUNICATION	L'information circule de manière fluide sans altération des messages entre les différentes cellules de crise, les différents publics et les autorités compétentes		
CONTINUITE D’ACTIVITE METIER	Les plans de continuité sont déclenchés de manière proactive ou réactive selon les besoins de la situation.		
	Les membres de la cellule classent les applications et services indisponibles par ordre de priorité de remise en service en s’appuyant sur le RTO (délais de reprise) renseigné pour chaque actif dans la « Liste des Applications » du PRI (plan de reprise informatique).		
	La cellule établi l’ordre technique de rétablissement en s’appuyant sur le tableau de dépendances applicatives.		
	Les membres de la cellule ont bien consulté les fiches PRI de chaque application et services à restaurer pour identifier les actions et étapes de reprise.		
	Les membres de la cellule estiment les délais de restauration des applications et services afin de disposer d’un échéancier détaillé de retour à la normale.		
COORDINATION MULTICELLULE	La cellule décisionnelle a intégré les retours de la cellule IT dans sa stratégie de réponse à la crise.		
	La cellule IT a ajusté ses priorités en fonction des instructions de la cellule décisionnelle		
	Les différentes Cellules de Crise communiquent suffisamment entre elles.		

Annexe B : Fiche « Rôle de l'observateur de l'ANSSI »

Cette fiche est accessible
via le lien suivant :

RÉPUBLIQUE FRANÇAISE

Exercice de gestion de crise cyber
Kit simulation

Fiche « Rôle de l'observateur »

Volet Observateur

Cette fiche « rôle de l'observateur » a pour objectif de vous guider dans cette fonction d'observateur de l'exercice.

Cette fonction peut être assurée par un collaborateur de l'entité joueuse. Pour chaque cellule de crise mobilisée, un observateur doit être présent.

L'observateur, qui a connaissance du chronogramme, doit remplir plusieurs missions :

- Il observe le fonctionnement du dispositif de gestion de crise à travers une prise de notes et une grille d'observation qui lui a été remise en amont par le planificateur de l'exercice ;
- Il compare les réactions des joueurs avec les réactions attendues mentionnées dans le chronogramme selon le stimuli ;
- L'observateur est aussi « les yeux et les oreilles » des animateurs si ces derniers sont dans une salle différente des joueurs. Ils appuient alors les animateurs en relayant leurs actions et les difficultés afin que l'équipe d'animation puisse adapter le rythme d'envoi des stimulis.
- L'observateur aura pleinement son rôle à jouer lors des retours d'expérience (RETEX) à chaud et à froid, notamment lors du RETEX à chaud où il pourra observer quelques points forts observés lors de l'exercice.

Il convient de préciser que l'observateur ne doit pas intervenir dans le cours de l'exercice, il n'a aucun rôle actif et doit limiter au maximum les échanges avec les joueurs.

Grille d'observation

La grille d'observation a pour but d'évaluer de manière objective le déroulé de l'exercice. Elle est composée de cinq thématiques :

1. Méthodologie de gestion de crise
2. Organisation de la cellule de crise
3. Prise de décision
4. Réponse métier
5. Compétences de gestion de crise de la cellule

Annexe B : Fiche « Rôle de l'observateur de l'ANSSI »

THEME	Objectifs	Les points forts	Les points d'amélioration	La ou les recommandations associée(s)
ANALYSE ET REMONTEE D'ALERTE				
ORGANISATION				
PILOTAGE				
COMMUNICATION				
CONTINUITE D'ACTIVITE METIER				
CONTINUITE D'ACTIVITE INFORMATIQUE				
COORDINATION MULTICELLULE				

CAMPUS
CYBER

POUR EN SAVOIR PLUS : WIKI.CAMPUSCYBER.FR
MAIL : COMMUNAUTES@CAMPUSCYBER.FR / 5 - 7 RUE BELLINI 92800, PUTEAUX

FICHE méthodologique - RETEX