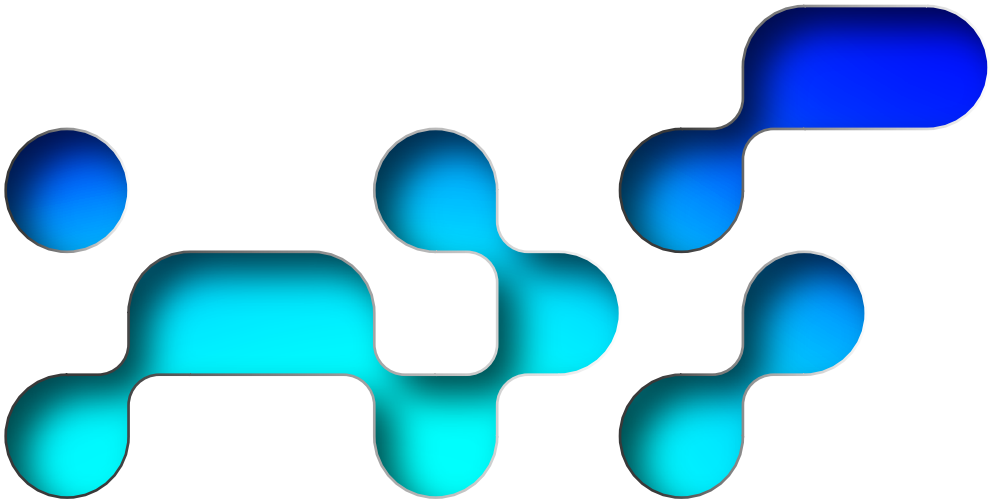
CAMPUS CYBER

FICHE MÉTHODE SENSIBILISATION

GROUPE DE TRAVAIL : GESTION DE CRISE CYBER ET ENTRAINEMENT



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BANQUE DE FRANCE
EUROSYSTÈME

AMRAE
la Maison du risk management

CCA
Club de la Continuité d'Activité

CDSE
CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

CESIN

CLUSIF

EXERCICE DE SENSIBILISATION

Durée de l'exercice ● ○ ○

Ressources nécessaires ● ○ ○

Niveau de maturité ● ○ ○

CONTEXTE

L'exercice de sensibilisation se prépare sur un **modèle court et réutilisable** : il se répète comme un briefing-type afin de sensibiliser de façon descendante les différents publics concernés par la gestion d'une crise d'origine cyber.

La sensibilisation à la gestion de crise cyber porte généralement sur la construction ou l'amélioration du dispositif de crise et réunit les différentes personnes impliquées autour d'une table. La sensibilisation pourra être accompagnée d'une démonstration en live (avec, par ex. un outillage red team – plateforme permettant l'exécution d'outils offensifs) afin de marquer les esprits, en montrant à quel point une crise d'origine cyber peut se propager rapidement.

OBJECTIFS

La sensibilisation est un format idéal pour les organisations peu habituées à mettre en œuvre des exercices de gestion de crise cyber. L'objectif de la sensibilisation est notamment de donner une idée de la **temporalité** de la crise et des **impacts** possibles.

Si les participants doivent **connaître les impacts d'un incident cyber** sur leurs activités, ils ne doivent pas devenir des experts cyber à l'issue de la sensibilisation. Ils ressortent de la sensibilisation avec les **bonnes réactions** à avoir face à une crise, les **bonnes pratiques** ainsi que les **moyens nécessaires** pour assurer leurs missions dans un contexte dégradé voire fortement dégradé.

La sensibilisation s'inscrit comme une **première étape** de la stratégie d'entrainement. Elle est utile avant d'organiser un exercice pour une population à faire monter en maturité.

PUBLIC VISÉ

La sensibilisation peut cibler un public particulier (comité exécutif, comité de direction, cellule décisionnelle/stratégique, etc.) et traiter une problématique bien spécifique (propagation d'un rançongiel, exfiltration de données, campagne de hameçonage, etc.)

Toutes les personnes qui auraient un rôle à jouer dans la réponse à incident ou la gestion de crise, sont ainsi concernées. Par exemple :

- Pour sensibiliser des **utilisateurs** : présenter les bonnes pratiques à respecter, la temporalité et les impacts d'une crise sur les processus et les activités critiques ;
- Pour sensibiliser une **direction** : évoquer la manière d'assurer leur rôle dans un contexte dégradé et partager des exemples ;
- Pour sensibiliser les **équipes IT** : présenter les spécificités d'une crise cyber et de la gestion d'une "panne".

BÉNÉFICES ATTENDUS

- **Améliorer les connaissances des aspects et impacts** d'une crise d'origine cyber et sensibiliser au vocabulaire d'une crise d'origine cyber ;
- **Connaître les différents rôles et responsabilités** de chacun en cas de crise cyber pour avoir les réactions attendues ;
- **Clarifier des zones d'ombre** au niveau du dispositif de crise et mettre en place des processus favorisant la transmission des informations au sein des différentes équipes de l'organisation ;
- **Rencontrer l'écosystème** de crise au sein de l'organisation et renforcer les liens ;
- Travailler sur les **interfaces du dispositif** de crise en place.

EXERCICE DE SENSIBILISATION

COMPÉTENCE / SAVOIR FAIRE À DÉVELOPPER

La sensibilisation vise à développer des compétences multiples :

Les connaissances sur l'organisation de la gestion de crise d'origine cyber :

- Les **impacts** d'une crise et les **objectifs** d'une attaque ;
- Les **risques clés** (IT, business, humains, logistiques, etc.) et les **scénarios d'attaque** possibles.

Les défis que l'organisation peut connaître en cas de crise d'origine cyber :

- **Gestion de la crise** : communications dégradées, continuité de l'activité fluctuante, retour à la normale, temporalité spécifique à une crise cyber, aspects psychologiques de la crise (ex. stress, fatigue, pression, bienveillance), etc. ;
- **Gestion des impacts** : impacts financiers (perte de marché, dévaluation à la bourse, etc.), perte des certifications (licences bancaires, certifications ISO, etc.), perte de confiance et atteinte à l'image de marque, etc. ;
- **Gestion des partenaires :** gestion de l'impact de la crise sur l'écosystème partenaire (régulateurs, prestataires, etc.) dont elle est dépendante , etc. ;
- **Résilience** : prévoir son organisation de crise et s'entraîner, c'est déjà améliorer sa résilience. Il convient de s'appuyer sur les enseignements tirés de la sensibilisation pour améliorer son dispositif de crise.

Continuité d'activité : connaître les solutions de continuité métier et informatique mises en place dans l'organisation, voire identifier celles à mettre en place.

BONNES PRATIQUES

- **Ne pas chercher à faire peur** aux participants ;
- Présenter de manière concrète les **processus existants** dans l'organisation ;
- **Mettre du sens et du concret** : présenter des exemples afin de rendre la présentation plus vivante ;
- Savoir **s'adapter au public visé**, selon les questions qu'il se pose et ce qu'il veut apprendre ou connaître, et selon les différents rôles dans une gestion de crise ;
- Inclure un partage de **retours d'expérience** (même secteur, même type d'organisation, etc.) permet de donner du concret à ce qu'on veut transmettre.

RESSOURCE ET PRÉPARATION NÉCESSAIRES

- Une présentation **visuelle** qui synthétise les différents sujets à aborder - avec une présentation **adaptée aux enjeux de la population visée** dans un contexte de crise ;
- Cette présentation doit être préparée et présentée par **une personne qui comprend les risques** et impacts des incidents cyber et sait les **vulgariser** ;
- En cas d'effectifs nombreux ou de session à distance : prévoir **une deuxième personne** qui répond aux questions.

EXERCICE DE SENSIBILISATION

DURÉE ET JALONS CLÉS

La sensibilisation ne doit pas excéder une demi-journée. En cas de démonstration, il faut l'inclure dans ce temps ; et surtout prévoir un temps d'échange avec les participants pour répondre à leurs questions.

LOGISTIQUE ET OUTILLAGE

- En **présentiel** ou à **distance** ;
- **Outil de questionnaire** ou de quizz en ligne, pour le contenu ou pour récolter un retour d'expérience des participants ;
- **Option** : faire de la sensibilisation innovatrice à l'aide d'un "serious game" pour mieux impliquer les personnes dans l'exercice.

LIMITES ET BIAIS

Si la sensibilisation est préparée en interne :

Attention à suffisamment adapter la sensibilisation au niveau des populations visées et à **ne pas être trop technique** ou à vouloir **aller trop dans le détail** de l'organisation de l'entreprise. Il ne faut pas se positionner uniquement comme le « porteur de processus internes » mais partager son expérience.

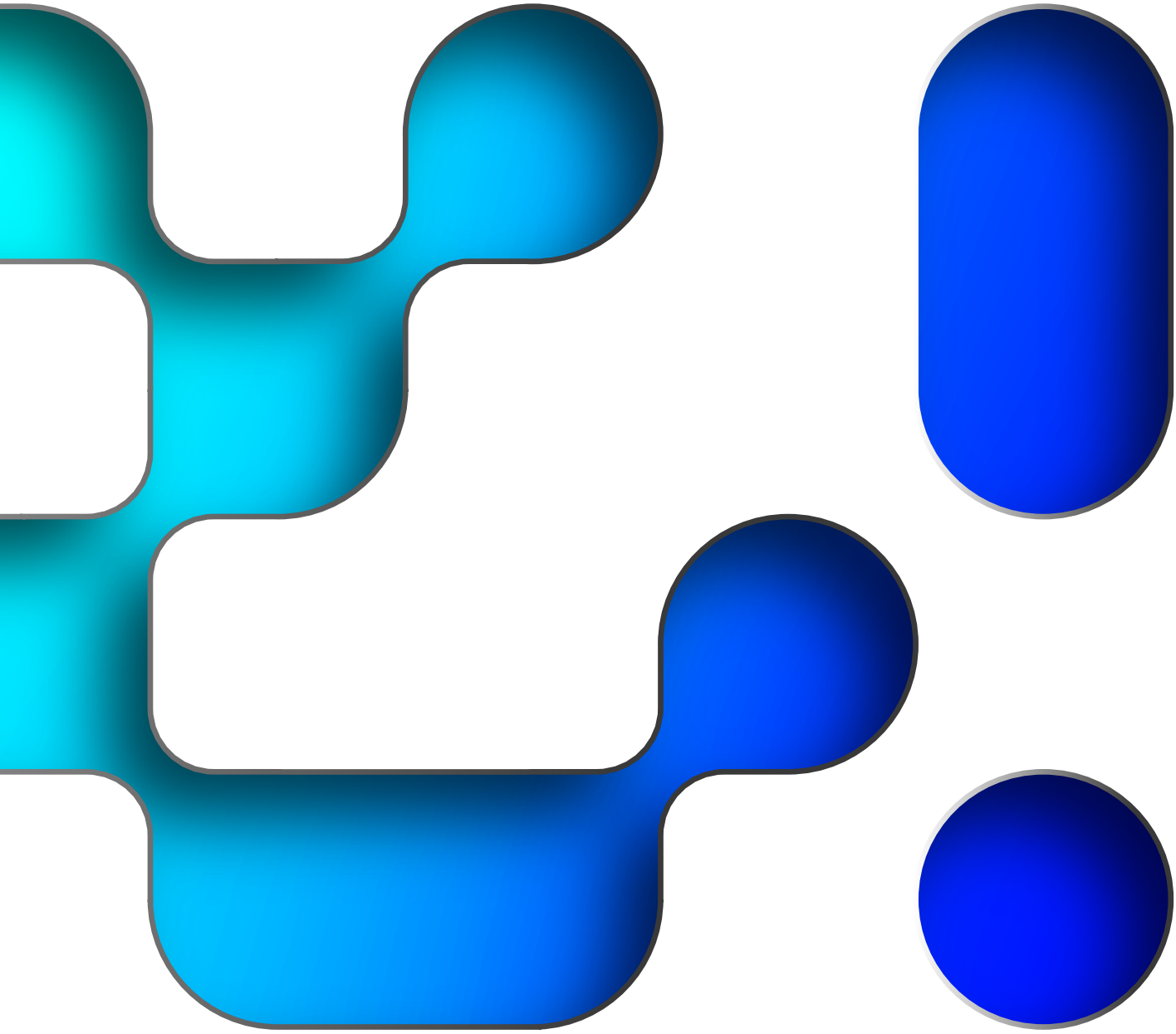
Si la sensibilisation est préparée par une prestation externe :

Un **travail d'ajustement du contenu** pour mieux le contextualiser aux spécificités de l'organisation est nécessaire. Le fait de décentrer la sensibilisation en prestation externe crée un aspect hors des murs qui peut aussi remettre en cause la légitimité du formateur.

DIFFICULTÉS À ANTICIPER

- Comme pour toutes les sessions de sensibilisation, il faut faire attention **au respect du temps de parole** et réserver un temps de questions et d'échanges à la fin. Si la présentation donne lieu à de nombreuses questions, une deuxième session peut éventuellement être proposée ;
- La sensibilisation peut avoir un **aspect redondant ou répétitif** auprès des personnes sensibilisées. Il est important, en fonction des objectifs fixés dans la stratégie d'entrainement, de varier les thématiques de sensibilisation.

Contributeurs : BNP Paribas, ENEDIS, Schneider Electric, SUEZ, Wavestone



CAMPUS CYBER
5 - 7 RUE BELLINI
92800
PUTEAUX

https://campuscyber.fr/