

RÉFLEXES CYBER +

Règles d'utilisation

INNOVATION ANSSI

RÉFLEXES CYBER +

RÉFLEXES CYBER + est un outil créé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) afin de **permettre aux entreprises et aux collectivités de vivre une première simulation de crise d'origine cyber.**

RÉFLEXES CYBER + ne s'adresse pas uniquement aux profils « techniques » mais à **l'ensemble des personnes en responsabilité au sein d'une organisation** : ex. COMEX / CODIR / les élu(es) dans le cas d'une collectivité directions métier (opérations, communication, financier, juridique, RH, etc.).

Les objectifs

1. **Sensibiliser** les comités de directions mais aussi les collaborateurs à la nécessité d'agir **de manière préventive pour éviter la survenue des cyberattaques.**
2. **Faire prendre conscience de la nécessité de se préparer** à l'éventualité d'une crise cyber, de l'anticiper, s'organiser et le jour J adopter les bons réflexes !

Le concept

RÉFLEXES CYBER + permet de «vivre» une crise d'origine cyber fictive et en faire ressentir les enjeux.

Pour cela, les participant(e)s vont **simuler la survenue d'une crise d'origine cyber au sein de leur organisation** (entreprise ou collectivité) et avoir la **possibilité de prendre des décisions** (les «cartes action») sans savoir si celles-ci sont des bons mais aussi des mauvais réflexes.

À la fin de la simulation, l'ensemble des participant(e)s découvrent si les actions prises étaient adaptées à la crise et bénéficient d'une évaluation de la réaction de l'équipe.

À l'issue de la simulation, RÉFLEXES CYBER + vous propose des solutions concrètes pour :

- **Renforcer immédiatement la cybersécurité** de votre organisation.
- **Diffuser les bons réflexes** à avoir en cas de crise d'origine cyber au sein de votre organisation et d'autres ressources utiles pour vous organiser pour y faire face.

RÉFLEXES CYBER + existe également en format standard court et ludique (RÉFLEXES CYBER), permettant de tester en autonomie la capacité de votre organisation à réagir à une crise cyber et à en tirer des enseignements.

Préparation amont

Format

RÉFLEXES CYBER + dure entre 2h et 3h environ et est prévu pour être joué par un groupe composé de **4 à 6 participants**.

Afin de maximiser l'impact de **RÉFLEXES CYBER +** au sein de l'organisation, **il est recommandé de convier des personnes en situation de responsabilité au sein de cette organisation.**

En plus des participant(e)s:

- **Une personne est chargée d'animer la simulation :** l'animateur ou l'animatrice qui assure le déroulé de la simulation.
- **Une personne est chargée d'observer la simulation :** l'observateur ou l'observatrice qui prend note des actions et réflexions de joueurs.

Planification

1. **Choisir le scénario de la simulation** adapté à votre besoin : « entreprise » ou « collectivité ».
2. **Identifier et inviter les personnes** qui participeront à la session
3. **Planifier la session** (date, horaire, salle, matériel, café, etc.).
4. **Informez l'ANSSI** de l'organisation de votre simulation **RÉFLEXES CYBER +** sur **MesServicesCyber/Reflexes-cyber**



Variantes possibles

Si le nombre de participant(e)s est insuffisant, des rôles peuvent être retirés ou un participant pour assurer jusqu'à 2 rôles.

Faire participer plus de 6 joueurs : il est possible de constituer de nouveaux groupes. Chaque groupe joue alors de manière simultanée. Une conclusion commune peut être organisée.

Le jour J

Mise en place

1. Installer les **joueurs** autour de la table.
2. Présenter les **objectifs** de la simulation et les règles associées
3. Distribuer les **plateaux de jeu** (1 par participant).
4. Distribuer les **6 cartes rôles à chaque participant(e)**, soit sur la base du hasard, soit en attribuant les rôles.
5. Installer un «**cavalier**» en fonction du rôle endossé par les joueurs.
6. Distribuer les **10 cartes action** associées au rôle de chaque joueur.

À SAVOIR : le minuté précise chaque sous-étape de la session pour permettre à l'animation de se saisir pleinement du scénario et de ses attendus. Il peut être utilisé comme fil-rouge.



Déroulé de la simulation

La session démarre par la lecture de la « mise en situation générale » aux participant(e)s. La mise à disposition d'un support de briefing facilite le lancement de la session.

L'animateur(rice) distribue ensuite aux participant(e)s concerné(e) s les premières cartes évènement afin de lancer le scénario de jeu.

Le scénario est divisé en 3 phases et se déroule sur une durée d'environ 1 heure.

Une carte est distribuée toutes les 2 à 3 minutes environ.

Bilan de la simulation

La session prend fin lorsque toutes les cartes évènement ont été distribuées.

Elle se poursuit par un échange libre entre les participants sur les enseignements à tirer pour l'organisation (RETEX). Cet échange doit d'abord permettre aux joueurs de partager leurs impressions sur l'expérience qu'ils viennent de vivre et de leur apporter un certain recul vis-à-vis des enjeux liés aux cyberattaques.

L'observateur prend ensuite le relais et partage ses observations et partager quelques bonnes pratiques à tenir.

La séquence se termine par une prise de parole de l'animation, qui partage quelques conseils pour passer à l'action.

L'animation du RETEX est facilitée par la mise à disposition d'un support de débriefing.



RÉFLEXES CYBER +

À vous de jouer !



Passer à l'action avec l'ANSSI !

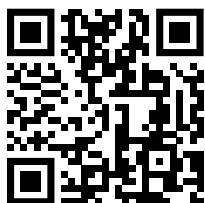
Retrouvez l'ensemble des solutions gratuites proposées par l'État pour accompagner les organisations dans leur montée en maturité cyber sur MesServicesCyber (messervices.cyber.gouv.fr).

Le diagnostic cyberdépart



Demandez à bénéficier du diagnostic cyberdépart sur MesServicesCyber : un 1er diagnostic cyber gratuit, accompagné par un Aidant cyber, réalisé en 1h seulement dans vos locaux ou en visioconférence.

MesServicesCyber



Retrouvez tous les solutions proposées par l'ANSSI et ses partenaires sur MesServicesCyber. Explorez le catalogue, testez votre maturité cyber et prenez votre cyberdépart !





RÉFLEXES CYBER +

Transformez une **menace abstraite**
en une **expérience concrète** de
gestion collective.

Un **outil clé en main** pour sensibiliser,
mobiliser et **préparer vos équipes**
à la **menace cyber.**