Ne pas diffuser aux joueurs

Exercice « REMPAR22 »

Atelier 2 - Outillage

CCA Club de la Continuité d'Activité

ANSSI

CAMPUS CYBER

Sommaire

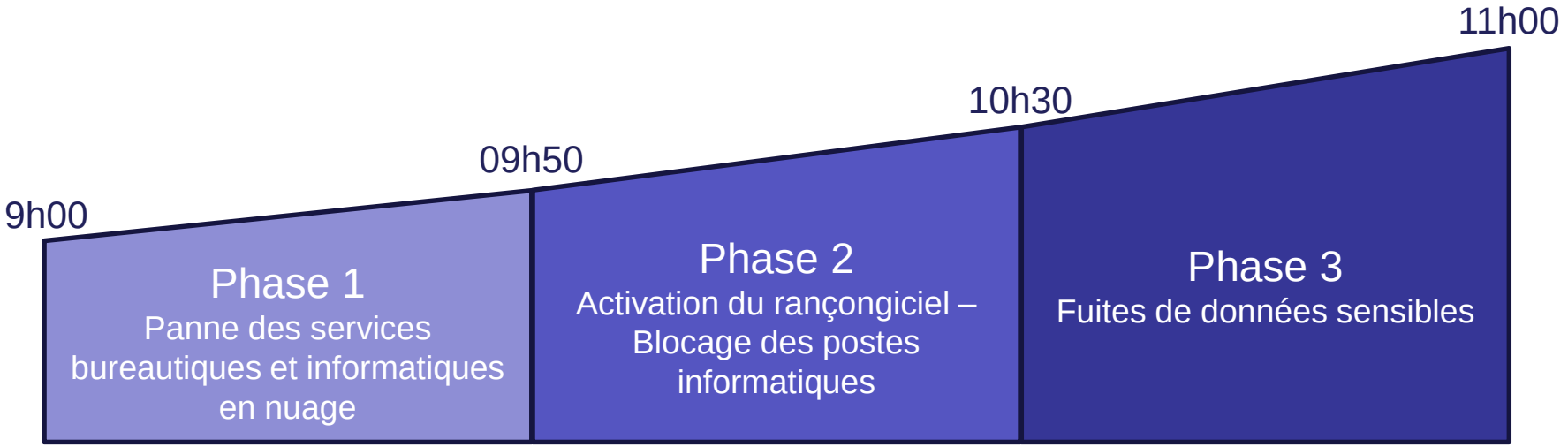
Ne pas diffuser aux joueurs

1. Rappel sur les phases d’exercices
2. Présentation des formats d’exercice et de l’outillage associé
3. Focus sur l’outil OpenEx
4. Questions-réponses

1. RAPPEL SUR LES PHASES D’EXERCICES

Temporalité de la crise

Ne pas diffuser aux joueurs



Suite à la **perte d'infrastructure** d'un fournisseur infonuagique, les **services de bureautique** (messagerie, tableur, traitement de texte, stockage en ligne, etc.) ainsi que plusieurs **applications SaaS** cessent de fonctionner.

Après avoir récolté des données sensibles, l'attaquant utilise les informations récupérées pour **s'introduire sur le réseau interne** et pour **chiffrer des postes de travail et des serveurs** avec un **rançongiciel.**

Pour mettre la pression sur les organisations touchés, **l'attaquant décide de publier certaines données sensibles** récupérées sur les stockages en ligne.

2. PRÉSENTATION DES FORMATS D’EXERCICE ET DE L’OUTILLAGE ASSOCIÉ

Modalités d’exercice et formats possibles

Ne pas diffuser aux joueurs

Selon les objectifs de votre organisation, l’exercice va pouvoir prendre différentes formes:

- **Exercice sur table** (format plus léger, déroulement d’un scénario en mode présentation pour identifier les réactions de chaque partie prenante)
- **Atelier d’anticipation** (afin d’identifier les impacts du scénario sur l’organisation et les possibles évolution de la crise, et pour identifier les actions à prendre sans jouer la gestion de crise)
- **Exercice fonctionnel mono-cellule**
  - Au niveau opérationnel – Equipes SI, SSI, Communication de crise, Métiers, etc.
  - Au niveau décisionnel – Equipe dirigeante
- **Exercice fonctionnel multi-cellules**, combinant la cellule opérationnelle et décisionnelle

Plusieurs moyens d'animer l'exercice

Ne pas diffuser aux joueurs

L'exercice peut être joué de différentes manières, selon la typologie et l'intensité de la crise jouée:

Exercice restreint, peu de joueurs, pas d'injects spécifiques

Exercice ouvert, beaucoup de joueurs et d'injects spécifiques par équipes

Présentation
Permet de dérouler un scénario à l'ensemble des joueurs présents dans une salle, sans inject spécifique à certains joueurs

Animation manuelle
Permet de partager des injects à chaque équipe, en envoyant des courriels aux collaborateurs, qui doivent se coordoner pour consolider la situation et remédier les impacts

Outil d'automatisation
(OpenEx)
Permet de planifier et d'animer l'exercice depuis une plateforme unique, en s'intégrant avec d'autres outils de simulation (PMS, cyberrange, etc.)

Plusieurs moyens d’animer l’exercice

Ne pas diffuser aux joueurs

Type d’exercice	Présentation	Email	OpenEx
Exercice sur table	X		
Atelier anticipation	X	X	
Exercice fonctionnel mono-cellule (opérationnel)		X	X
Exercice fonctionnel mono-cellule (décisionnelle)		X	X
Exercice fonctionnel multi-cellule		X	X

Autres outils pertinents le jour de l'exercice

Ne pas diffuser aux joueurs

Selon le format choisi et les objectifs, d'autres outils pourront être utilisés pendant l'exercice:

- Pour gérer la crise:
  - Cellule de crise (physique ou virtuelle)
  - Main courante et registre de suivi des actions
  - Outils de communication (téléphonie, routeurs, etc.)
- Pour animer les équipes:
  - Générateur de messages de réseaux sociaux (Exemple: Twitter)
  - Plateforme de pression médiatique (disponible via OpenEx)
  - Appel téléphonique

3. FOCUS SUR L’OUTIL OPENEX

Présentation général de l’outil

Ne pas diffuser aux joueurs

GitHub - OpenEx-Platform/openex: Open Exercises Planning Platform

Objectifs

- Professionnalisation de la planification d’exercices / capitalisation
- Automatisation pour rendre « disponible » l’animation
- Facilitation du travail collaboratif
- Visualisation en temps réel de l’état et de l’avancement de l’exercice

Vision

- Un produit libre et ouvert (précisions sur la licence un peu plus loin)
- Résolument orienté « expérience utilisateur »
- Application web
- Automatisation complète afin de se concentrer sur l’animation de l’exercice

Organisation des droits

Ne pas diffuser aux joueurs

Joueur

- Accède à l'univers médiatique
- Accède à la plateforme de challenge

Planificateur

- Peut voir et éditer des joueurs sur les organisations auquel il est assigné
- Peut voir et éditer des les organisations auxquels il est assigné
- Peut voir et éditer des exercices auxquels il est assigné
- Peut voir les documents sur « ses » exercices
- Peut voir les médias disponibles
- Peut voir et éditer les challenges
- Peut voir et éditer les modèles de RETEX

Administrateur

- Idem planificateur
- Voit et contrôle l'ensemble de la plateforme
- Contrôle de la configuration de l'instance
- Peut assigner les droits de planificateur (sur des exercices et des organisations) et d'administration
- Peut supprimer des joueurs, planificateurs et administrateurs

Principaux modules à prendre en compte

Ne pas diffuser aux joueurs

L’outil OpenEx est composé de différents modules, que nous allons explorer ensemble:

- Le module **Exercices**, où la majorité de la planification va se passer ;
- Le module **Joueurs**, qui permet d’ajouter ou de modifier les joueurs ;
- Le module **Documents**, qui rassemble l’ensemble de la documentation utilisée sur les exercices ;
- Le module **Médias**, définissant les différents sites disponibles sur le module de PMS ; et
- Le module **Retour d’expérience**, qui sera utilisé pour le RETEX.

L’onglet Challenges ne sera pas utilisé pendant l’exercice.

Explication de la segmentation logique d'OpenEx

Ne pas diffuser aux joueurs

Les éléments visibles par planificateur :

- Les exercices
- Les organisations
- Les joueurs (par organisation)
- Les documents

Les éléments visibles par tous le monde :

- Les médias **-> Non modifiable, demander à l'animation si besoin de modification**
- Les « tags » **-> Ne pas modifier modifier/supprimer les tags existants**
- Les modèles de retour d'expérience **-> Ne pas travailler dans ce module, plutôt directement dans l'exercice**

Les challenges sont également communs à tous, mais ne seront pas utilisés dans l'exercice.

A. MODULE « EXERCICE »

Le module « Exercice »

Ne pas diffuser aux joueurs

5 onglets disponibles :

- L’aperçu,
- La définition de l’exercice (en terme d’Audiences et de Pression Médiatique)
- Le scénario
- L’animation
- Les résultats

Le module « Exercice » - Onglet Aperçu

Ne pas diffuser aux joueurs

- Donne un aperçu global de l’exercice en terme de nombre de joueurs, de déroulé de configuration
- Permet de décider de pauser un exercice en cours de route
- Permet de lancer une simulation (*dry-run)* vers le planificateur
- Permet de réaliser un contrôle (*comcheck)* pour vérifier que les joueurs reçoivent bien les emails

Consignes:

- Ne pas modifier la date de début d’exercice
- Ne pas modifier l’adresse émettrice
- Se coordonner avec l’équipe centrale avant de pauser l’exercice en cours

Le module « Exercice » - Onglet Définition / Audiences

Ne pas diffuser aux joueurs

- Permet de créer, modifier et supprimer des audiences (groupes de joueurs)

  Les audiences sont les groupes récepteurs d'injects (impossible d'envoyer un inject à un seul joueur)
- Possibilité d'activer ou de désactiver une audience

  Une audience désactivée ne reçoit pas les injects associés.

Consignes:

- Astuce : il est possible de créer une audience lors de la création d'inject également. Impossible en revanche d'ajouter un joueur dans une instance à ce moment, il faut passer par l'onglet Définition / Audience.
- Ne pas désactiver d'audience pré-exercice.

Le module « Exercice » - Onglet Définition / Pression méd.

Ne pas diffuser aux joueurs

- Permet de créer, modifier et supprimer des publications médiatiques
- Voir l'apercu des publications médiatiques, et des médias à un moment donné

Consignes:

- **Une publication médiatique doit être définie en amont de sa publication** via un inject (i.e.: définir un article ne conduit pas à sa disponibilité au départ du jeu, il faut pour cela le publier via un inject).
- **La publication peut être annoncée aux joueurs ou non**.
- Dans l'aperçu, deux vues existent: **une vue planificateur** qui donne la vision complète des publications disponibles ou à venir, et **une vue joueur** qui n'affiche que l'existant.

Le module « Exercice » - Onglet Scénario

Ne pas diffuser aux joueurs

- Permet de créer, modifier et supprimer des stimulis
  - Un stimuli peut être de différents types: mails individuels, mail vers un groupe, pression médiatique, inject « manuel » - par exemple appel téléphonique à réaliser par un animateur.
  - Un stimuli est associé à une ou des audiences, et avoir des pièces jointes.
  - Un stimuli est planifié de manière relative.
  - Un stimuli peut avoir des attendus (élément facultatif et non nécessaire du point de vue de l'animation centrale).

Consignes:

- Ne pas chiffrer les mails par défaut. Si besoin, contacter l'animation centrale (nécessité d'ajouter des clés PGP à vos joueurs).
- Pour une vue par audience de l'exercice, n'hésitez pas à passer par l'onglet animation.
- **Attention à la distinction entre Désactiver et Supprimer!**

Le module « Exercice » - Onglet Animation / Chronologie

Ne pas diffuser aux joueurs

- Permet de voir l'ensemble des stimulis par audience sur l'ensemble de l'exercice
- Permet de réaliser le suivi de l'animation, notamment d'activer/désactiver des stimulis, de les jouer en avance de phase ou de les modifier en cours de route.

Consignes:

- Réaliser une simulation (via onglet Aperçu) avant l'exercice
- Utiliser l'onglet Animation pour suivre l'exercice durant l'animation!
- En cas d'erreur, modifier l'inject et le reprogrammer via l'onglet Chronologie

Le module « Exercice » - Onglet Animation / Mails

Ne pas diffuser aux joueurs

- Permet de suivre les conversations par mail des joueurs durant l’exercice
- Permet d’animer par mail durant l’exercice (création d’injects ou réponse sur l’existant)

Consignes:

- Durant l’atelier animation

Le module « Exercice » - Onglet Animation / Validations

Ne pas diffuser aux joueurs

- Permet de voir ou de valider les attentes des stimulis (notamment pour « compter les points »)

Consignes:

- Durant l’atelier animation

Le module « Exercice » - Onglet Animation / Journal d’exercice

Ne pas diffuser aux joueurs

- Permet de prendre des notes partagées entre organisateurs durant l’exercice

Consignes:

- Durant l’atelier animation

Le module « Exercice » - Onglet Résultats / Statistiques

Ne pas diffuser aux joueurs

- Donne une vue d’ensemble de l’exercice notamment sur:
  - La distribution des stimulis/attendus entre audiences et typologie de stimuli
  - Les données d’exercice au cours de son exécution
  - Les scores par audience ou joueur

Consignes:

- Peut être utilisé durant la planification pour vérifier de la bonne prise en compte d’une audience ou de l’évolution attendue de la crise durant l’exercice

Le module « Exercice » - Onglet Résultats / Retour d’expérience

Ne pas diffuser aux joueurs

- Permet de solliciter les joueurs et planificateur lors d’un RETEX
- Définir des objectifs d’exercice
- Définir un questionnaire partageable vers les joueurs

Consignes:

- Utiliser le modèle fourni par l’animation centrale, et rajouter les questions spécifiques à votre organisation
- Plus de consignes lors de l’atelier RETEX

Le module « Exercice » - Onglet Résultats / Rapports

Ne pas diffuser aux joueurs

- Permet de générer un rapport sur l’exercice

Consignes:

- Plus de consignes lors de l’atelier RETEX

A. MODULE « JOUEURS »

Le module « Joueurs »

Ne pas diffuser aux joueurs

- Permet d’ajouter un joueur sur la plateforme (indépendamment de l’exercice)
- Permet de voir l’ensemble des joueurs sur les organisations autorisées
- Permet de modifier ou de supprimer des joueurs existants

Consignes:

- Lors de la création des joueurs, assigner votre organisation (un joueur sans organisation sera visible de tous).
- Seul les champs Nom, Prénom et Email sont obligatoires.

A. MODULE « ORGANISATION »

Le module « Organisations »

Ne pas diffuser aux joueurs

- Permet de voir et de modifier votre organisation.

Consignes:

- Pas d’utilisation nécessaire.
- Si besoin de créer une organisation supplémentaire, contacter l’équipe centrale pour valider les modalités et créer cette deuxième organisation.

A. MODULE « DOCUMENTS »

Le module « Documents »

Ne pas diffuser aux joueurs

- Voir l’ensemble des documents utilisés sur l’exercice.
- Supprimer les documents existants
- Ajouter des documents.

Consignes:

- L’ajout de document est également possible via le volet Exercice. Pas besoin d’utiliser ce module, sauf pour voir l’ensemble des documents ou supprimer de l’existant.

A. MODULE « MÉDIAS »

Le module « Médias »

Ne pas diffuser aux joueurs

- Permet de voir les médias disponibles sur la plateforme.
- 3 types de médias existants:
  - Les médias classiques (pour des articles de presse en ligne)
  - Les « chaines de télévision » (permettent de diffuser des vidéos)
  - Le « microblogging » (pour des messages courts de type « réseaux sociaux »)

Consignes:

- Impossible de modifier les médias de votre côté.
- Si besoin d’un média spécifique, contacter l’équipe d’animation centrale.

A. MODULE « RETOUR D'EXPERIENCE »

Le module « Retour d’expérience »

Ne pas diffuser aux joueurs

- Propose un modèle de RETEX pour l’exercice

Consignes:

- Ne pas travailler dans ce module, et rajouter les questions spécifiques à l’organisation dans l’onglet dédié de l’exercice (voir atelier RETEX)

4. FAQ

Questions/réponses

Ne pas diffuser aux joueurs

- **Peut-on effectuer l'exercice sans OpenEx ou est-ce un prérequis ?** Il n'y a pas d'obligation à utiliser OpenEx pour organiser l'exercice, mais son utilisation facilite le déroulé de l'exercice en automatisant l'animation. Toutefois, le chronogramme fourni en format Excel permet de gérer l'exercice sans l'outil.

- **Les documents doivent déjà être téléchargés dans l'outil ou ils peuvent être directement être téléchargés depuis notre PC ?** Il est possible d'uploader de téléverser un document dans l'outil. Si vous ne souhaitez pas mettre un document au sein de OpenEx, vous pouvez dans ce cas intégrer dans un stimuli le lien vers l'emplacement du document dans votre SI.

- **Le temps relatif d'une action est -il défini par rapport au début ou par rapport à l'action précédente ?** Le temps relatif est par rapport au T0 de l'exercice et non par rapport à l'action précédente.

- **Y a-t-il une notion de filiation entre les actions. Une action ne pouvant pas s'engager tant que l'action "mère" soit terminée ?** La fonction n'est pas disponible pour le moment mais est bien intégrée dans les besoins de futurs développements. Elle ne sera toutefois pas disponible pour l'exercice.

- **Est-il possible d'envoyer des stimuli à une partie d'une audience ?** Non. Il faut créer une nouvelle audience.

- **Les mails sont-ils réellement envoyés via un client de messagerie ou tout reste en interne d'OPENEX ?** Les emails sont réellement envoyés. OpenEx est connecté à un service SMTP qui permet d'envoyer des mails. Tout est standardisé pour que l'on ne voit pas que les mails proviennent d'OpenEx.

- **Avons-nous un accusé de réception / prise en compte du stimuli par les joueurs ?** Si l'ID de l'inject est conservé dans les échanges mail, ainsi que l'adresse d'envoi du mail, il est possible d'avoir l'historique des échanges et la confirmation que les injects ont été traités.

Questions/réponses

Ne pas diffuser aux joueurs

- **Y a-t-il une possibilité d'import, export Excel ?** L'outil permet d'importer et exporter des exercices. Il est possible d'exporter le scénario, les joueurs, les documents : une archive zip est générée mais un format JSON est utilisé pour faciliter la réinjection. Il sera possible d'exporter, à la fin de l'exercice, le scénario (stimulis, scénarios, …), les audiences, le RETEX, … Cela permettra de réinjecter sur une instance interne, par exemple. La fonction d'export au format Excel n'est pas disponible pour le moment mais est bien intégrée dans les besoins de futurs développements.

- **Si nous envisageons un exercice d'envergure avec beaucoup de participants est-il possible de faire un import de masse la première fois d'une base de joueur (ex : export LDAP) ?** Pas possible à ce jour. La fonctionnalité n'est pas encore disponible.

- **Peut-on exporter l'environnement après exercice vers une instance OpenEx en interne ?** Une fois l'exercice fini, il est possible d'exporter l'exercice (scénarios, documents, les audiences et les joueurs) et importer ensuite le fichier .ZIP qui va créer un second exercice en mode import et disponible en interne.