Kit Observateur - Version 1.0 - 28/05/2025

Clause de non-responsabilité: Les présents documents sont fournis sans garantie d'exactitude ou d'adéquation. Nous déclinons toute responsabilité en cas d'erreurs ou d'omissions. Veuillez consulter un professionnel pour toute vérification ou adaptation nécessaire. Ils sont mis à disposition gratuitement par le canton de Vaud.

Licence: Ce document est mis à disposition selon les termes de la Licence Creative Commons Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 4.0 International. Pour voir une copie de cette licence, visitez http://creativecommons.org/licenses/by-nc-sa/4.0/

CYBER24

TABLEAU D'ORDONNANCEMENT OBSERVATEUR

Fiche destinée à l'observateur

Présentation du contexte

Pendant toute la durée de l'exercice, le scénario et ses différentes phases seront cadencés par l'envoi de SMS, qui joueront un rôle central dans le déroulement des activités. Ces SMS vous indiqueront le début et la fin de chaque phase, ainsi que les instructions nécessaires pour avancer dans le scénario. Toutefois, en cas de problème technique ou si vous ne recevez pas les SMS (un léger délai étant possible), vous pourrez vous référer au tableau d'ordonnancement fourni à la page suivante. Celui-ci détaille les étapes et les délais pour vous permettre de poursuivre l'exercice sans interruption.

Objectif

Pour garantir un déroulement optimal de l'exercice, il est essentiel de respecter les actions indiquées dans les SMS. Votre rôle principal consiste à :

- **Distribuer la documentation :** Avant le début de chaque phase, assurez-vous que chaque participant reçoive les documents nécessaires pour leur mission.
- **Observer et documenter :** Pendant l'exercice, utilisez la grille d'observations pour noter les actions clés, les éventuelles difficultés rencontrées et toute remarque constructive. Ces observations seront cruciales pour le retour d'expérience en fin d'exercice.

Quittance des SMS

Certains SMS nécessiteront une confirmation de réception (quittance). Lorsque cela est demandé, suivez les instructions de réponse spécifiées. Le premier quittancement au début de l'exercice est très important pour nous, afin de garantir que les entités sont prêtes à débuter. **Merci de vous assurer que le responsable de la cellule de crise et vous-même ont bien quittancé le SMS en début de journée.**

En cas de problème

Si vous rencontrez un problème au cours de l'exercice, vous pouvez contacter la direction d'exercice via l'adresse email : cyber24@vd.ch ou utiliser le numéro : 021 338 43 50.

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

Horaire Phase	Durée (min)	ID Phase	Etapes	Heure de distribution SMS	ID SMS	Contenu SMS	Destinataires
08:00-08:10	10	0	**Quittancement présence**	8h00	SMS0.1	[CYBER24] Bonjour, l'exercice CYBER24 de gestion de crise va commencer à 8h10. Vous serez l'observateur. Merci de quittancer votre participation en répondant à ce SMS par "OK" (si possible avant le début de l'exercice).	Observateurs
				8h00	SMS0.2	[CYBER24] Bonjour, l'exercice CYBER24 de gestion de crise va commencer à 8h10. Vous serez la cellule de crise. Merci de quittancer votre participation en répondant à ce SMS par "OK" (si possible avant le début de l'exercice).	Testés
08:10-08:35	25	1	**Appréhension du problème**	8H05	SMS1.1	[CYBER24] La première phase de l'exercice va débuter. Merci de distribuer les documents de la phase 1 "Activation de la cellule de crise" (page 1 à 5) afin que la cellule de crise puisse débuter à 08h10.	Observateurs
				8h10	SMS1.2	[CYBER24] Nous vous signalons qu'une panne informatique est en cours. La quasi-totalité de nos ordinateurs et ressources informatiques sont affectés. Notre système de messagerie est hors service, les services informatiques sont paralysés, et la gestion des éclairages, tant à l'intérieur qu'à l'extérieur, est affectée. Il ne s'agit pas d'un simple dysfonctionnement technique : un message alarmant laissé par des hackers révèle qu'ils semblent avoir pris le contrôle de nos systèmes. Pour plus d'informations merci de lire le rapport de l'informatique.	Testés
				8h25	SMS1.3	[CYBER24] Il vous reste 10 minutes pour compléter la phase 1. Une proposition de solution vous sera distribuée à 08h35.	Testés
08:35-08:40	5		**Solution**	8H35	SMS1.4	[CYBER24] La phase 1 se termine dans 5 minutes. Merci de distribuer la proposition de solution pour la phase 1 (document 1.SOL).	Observateurs
08:40-09:00	20	2.1	**Mesures d'urgences**	8h38	SMS2.1	[CYBER24] La phase 2 de l'exercice va commencer. Veuillez distribuer tous les documents de "Phase 2 – Gestion de crise" et indiquer à la cellule de crise qu'elle a 20 minutes pour compléter la partie 2.1.	Observateurs
				8h40	SMS2.2	[CYBER24] Vous avez 20 minutes pour compléter la partie 2.1.	Testés
09:00-09:25	25	2.2	**Rapport d'orientation**	9h00	SMS2.3	[CYBER24] Veuillez répondre par "oui" à ce message, si la cellule de crise vous a averti qu'elle souhaitait appeler la police. De plus, merci de notifier à la cellule de crise qu'elle peut passer à la partie "2.2.1 - Rapport d'orientation" et qu'elle a 25 minutes à	Observateurs
				09h15	SMS2.4	[CYBER24] Il vous reste 10 minutes pour compléter la phase 2. Une proposition de solution vous sera distribuée à 09h25.	Testés
09:25-09:45	20	2.3	**Solution**	9h25	SMS2.5	[CYBER24] La phase 2 est terminée. Vous pouvez partager le document "2.sol - Gestion de crise - Proposition de Solution".	Observateurs
				9h25	SMS2.6	[CYBER24] Féliciations vous avez complété la phase 2 ! Vous avez maintenant 20 minutes à diposition pour revoir la proposition de solution distribuée et prendre une pause.	Testés
09:45-10:15	30	3.1	**Stratégie de communication**	9h42	SMS3.1	[CYBER24] La phase 3 de l'exercice va commencer et durera 50 minutes au total. Veuillez distribuer tous les documents de "Phase 3 – Communication" et indiquer à la cellule de crise qu'elle a 30 minutes pour compléter la partie 3.1.	Observateurs
				9h48	SMS3.2	[CYBER24] Madame, Monsieur, Je suis Léa Dupraz, journaliste au quotidien romand *Le Quart d'Heure Vaudois* . Nous venons de publier un article sur les cyberattaques en cours (voir document 3.1.5) et souhaiterions obtenir des précisions concernant les mesures concrètes que votre organisation a mises en place pour rétablir la situation. Dans l'éventualité où aucun communiqué officiel ne serait publié rapidement, nous poursuivrons nos investigations afin d'éclairer nos lecteurs sur les implications et le déroulement de cette crise. Dans l'attente de votre réponse, nous vous adressons nos salutations distinguées. Léa Dupraz	Testés
10:15-10:35	20	3.2	**Communiqué de presse**	10h05	SMS3.3	[CYBER24] Il vous reste 10 minutes pour compléter la phase 3.1. Vous pourrez ensuite entamer la rédaction du communiqué de presse jusqu'à 10h35.	Testés
10:35-10:55	20	3.3	**Proposition de solution et pause**	10h35	SMS3.4	[CYBER24] La phase 3 est terminée. Vous pouvez partager le document "3.sol - Communication - Proposition de solution"	Observateurs
				10h35	SMS3.5	[CYBER24] Féliciations vous avez complété la phase 3 ! Vous avez maintenant 20 minutes à diposition pour revoir la proposition de solution distribuée et prendre une pause.	Testés
10:55-11:25	30	4.1	**Vol de données**	10h53	SMS4.1	[CYBER24] La phase 4 va commencer. Merci de distribuer tous les documents de la phase "4 – Vol de données"et indiquer à la cellule de crise qu'elle a 30 minutes pour compléter l'exercice 4.1.6.	Observateurs
				10h55	SMS4.2	[CYBER24] Bonjour, je suis journaliste. Une de mes sources m'indique que les données de votre organisation ont été publiées sur le darknet à la suite de la cyberattaque. On y retrouve de nombreux documents sensibles et confidentiels. Nous préparons un sujet pour le 19h30 de ce soir à la RTS. Je vous invite à me contacter dans les plus bref délais. Avec mes meilleures salutations, Jean S.	Testés
11:25-11:40	15	4.2	**Proposition de solution et pause**	11h25	SMS4.3	[CYBER24] La phase 4 est terminée. Vous pouvez partager le document "4.sol - Vol de données - Proposition de solution".	Observateurs
				11h25	SMS4.4	[CYBER24] Féliciations vous avez complété la phase 4 ! Vous avez maintenant 15 minutes à diposition pour revoir la proposition de solution distribuée et prendre une pause.	Testés
11:40-12:00	20	5.1	**Sortie de crise et Retour d'expérience (RETEX)**	11H37	SMS5.1	[CYBER24] La dernière phase de l'exercice CYBER24 va commencer. Veuillez distribuer les documents "5 – Sortie de crise".	Observateurs
				11H40	SMS5.2	[CYBER24] Après des jours d'efforts acharnés, la situation semble enfin sous contrôle. Les équipes techniques ont rétabli les principales fonctionnalités et sécurisé les systèmes critiques, tandis que les décisions stratégiques prises ont permis de limiter les impacts. Nous entrons en phase de sortie de crise. Vous avez 20 minutes à disposition pour un débriefing à chaud.	Testés
12:00	/	6.1	**FIN et feedback**	12H00	SMS6.1	[CYBER24] L'exercice de gestion de crise CYBER24 est terminé. Merci à toutes les entités participantes pour votre mobilisation et votre engagement. La préparation et les exercices renforcent notre résilience, développent les bons réflexes et améliorent notre capacité à gérer efficacement les crises réelles. Bravo pour votre participation active ! Nous vous invitons à prendre quelques minutes pour nous transmettre votre feedback, essentiel pour continuer à progresser ensemble. Lien vers le formulaire :	Testés
				12H00	SMS6.2	[CYBER24] L'exercice de gestion de crise CYBER24 est terminé. Merci à toutes les entités participantes pour votre mobilisation et votre engagement. La préparation et les exercices renforcent notre résilience, développent les bons réflexes et améliorent notre capacité à gérer efficacement les crises réelles. Bravo pour votre participation active ! Nous vous invitons à prendre quelques minutes pour nous transmettre votre feedback, essentiel pour continuer à progresser ensemble. Lien vers le formulaire :	Observateurs

PHASE 1 – ACTIVATION CELLULE DE CRISE
1.OBS – APPRÉHENSION DU PROBLÈME

Fiche destinée à l'observateur

Durée à disposition

De 8h10 à 8h40

Les exercés disposent de 30 minutes pour lire et compléter les documents de la phase 1.

Rôle de l'observateur

Durant tout l'exercice, la cellule de crise va recevoir diverses informations via SMS et les documents que vous distribuerez. Vous êtes chargé de distribuer les documents appropriés au moment adéquat, et d'observer les actions des participants à l'aide des grilles d'observations fournis pour chaque partie.

Note : Vous recevrez des SMS pour guider l'exercice. En cas de problème technique lié à l'envoi des SMS, merci de vous référer au tableau d'ordonnancement.

Objectif

Dans la phase 1, l'objectif pour les participants est de comprendre la situation actuelle et de remplir le document « 1.1 – Appréhension du problème » avec leurs observations. La définition des mesures d'urgence sera abordée lors de la prochaine étape de l'exercice.

Grille d'observations

Objectif

Cette grille a pour but d'aider à évaluer, pour une partie donnée, les actions et réactions des exercés. Vous devez observer les actions, réflexions, mesures qui ont été faites et/ou prises par les exercés. Il est également possible de noter, sous forme de texte, différentes remarques. Les propositions sont classées par ordre alphabétique sans notion de priorité.

Note : une croix [X] signifie que cela a été effectué ou dit.

Eléments **importants**

- ☐ La cellule de crise est activée. Une personne est désignée pour la diriger.
- ☐ Les exercés ont bien pris connaissance de tous les documents.

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

- ☐ Les exercés ont compris l'importance de la crise.
- ☐ Les exercés ont lu le message de la demande de rançon.
- ☐ Les exercés ont vu, dans la note des pirates informatiques, que ceux-ci sont en possession des données (« for now, your data is secured and safely stored on our server »).
- ☐ Les exercés ont rempli les 2 premières parties de l'appréhension du problème.
- ☐ Les exercés ont identifié la demande de rançon (en bitcoin).
- ☐ Les exercés ont mentionné qu'ils devront, à un moment donné, demander de l'aide externe.

Eléments **non-essentiels mais intéressants**

- ☐ Les exercés demandent à leur département informatique si la situation peut s'empirer ou non.
- ☐ Les exercés ont calculé le montant de la rançon en CHF.
- ☐ Les exercés ont compris que l'attaque pourrait durer longtemps (dans un cas réel).
- ☐ Les exercés ont effectué une recherche sur les potentiels pirates informatiques (RansomCyber24)

Eléments **qui ne devraient pas apparaitre**

- ☐ Les exercés continuent à utiliser le matériel informatique en place.
- ☐ Les exercés pensent qu'il s'agit d'une panne classique et laisse la gestion à la personne en charge de l'informatique.
- ☐ Les exercés ont éteint des ordinateurs.
- ☐ Les exercés pensent payer la rançon en bitcoin afin de sortir de cette crise.

Champ libre pour appréciation et information via texte

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

PHASE 2 – GESTION DE CRISE
2.1.OBS – IDENTIFICATION DES MESURES

Fiche destinée à l'observateur

Durée à disposition

De 8h40 à 9h00

Les exercés disposent de 20 minutes pour lire et compléter la partie 2.1

Présentation du contexte

IMPORTANT : Bien qu'il soit demandé de contacter les services de police dans le cas d'un cyber incident réel, il est crucial de garder en tête qu'il s'agit ici d'un exercice. Vous devrez donc uniquement SIMULER cet appel. Merci de NE JAMAIS contacter le 117 ou toute autre partie prenante au cours de cet exercice.

Cet exercice vise à simuler la gestion d'une situation de crise. La cellule de crise devra identifier des mesures d'urgence, simuler des communications avec les services compétents (comme la police), et définir les priorités d'actions. Votre rôle consiste à observer et évaluer les actions des participants, en utilisant la grille d'observations ci-dessous. Vous ne devez pas intervenir directement dans leurs décisions, mais vous pouvez répondre aux questions factuelles concernant le déroulement de l'exercice ou les procédures.

La cellule de crise devra :

- Dans le document « 2.1.1 – Appréhension du problème suite » compléter
  - « Quelles sont les mesures les plus urgentes ou les plus importantes »
  - « Comment les prioriser »
- Si jugé nécessaire, simuler la réflexion sur un éventuel contact avec la police. Encore une fois, ceci est un exercice, il **NE** faut **PAS** contacter la police.

Si la cellule de crise estime qu'un appel à une entité externe (police ou autre) serait nécessaire dans cet exercice, elle devra vous en informer pour que vous en preniez note.

Une fois cette partie (2.1) terminée, vous pourrez entamer la partie 2.2, principalement centrée sur la rédaction d'un rapport d'orientation.

Objectif

L'objectif pour les participants est d'apprendre à identifier les éléments clés, appelés mesures d'urgence, indispensables à la gestion d'une crise, ainsi qu'à déterminer et organiser les priorités. Il vise également à les familiariser avec les modalités de prise de contact avec les services compétents et à identifier les types d'informations pertinentes à leur transmettre.

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

Grille d'observations

Objectif

Cette grille permet d'évaluer les actions et réactions de la cellule de crise durant la partie 2.1 de l'exercice.

A l'aide de cette grille vous devez identifier les actions, réflexions et les mesures qui ont été mises en œuvre par les participants. Des remarques peuvent être ajoutées sous forme de texte libre. Les propositions sont classées par ordre alphabétique sans notion de priorité.

Note : une croix [X] signifie que cela a été effectué ou dit.

Eléments **importants**

- □ Les exercés ont bien pris connaissance de tous les documents.
- □ La cellule de crise est toujours activée.
- □ Les exercés ont complété les parties « *Quelles sont les mesures les plus urgentes ou les plus importantes* » et « *Comment les prioriser* » du document 2.1.2 – Appréhension du problème suite.
- □ Les exercés ont identifiés des mesures d'urgence correspondant à :
    - Activer leur Plan de Continuité des Activités (PCA) ou tout autre plan existant permettant de gérer une crise. S'assurer qu'ils s'appuient sur des procédures définies au préalable.
    - Appeler la police cantonale pour demander du soutien et le support de la force cantonale d'intervention cybersécurité (CSIRT).
    - Evoquer la nécessité d'évaluer la criticité des systèmes et des données compromises et de l'impact potentiel sur l'organisation et sur les citoyens de l'attaque.
    - Identifier les services les plus critiques (e.g., gestion de l'eau, transport, santé, collecte des déchets) et s'assurer de leur rétablissement en priorité.
    - Mise en place d'un canal de communication au sein de l'équipe de gestion de crise se passant des systèmes informatiques en place.
    - Veiller à ce que tout le monde soit conscient qu'en cas de demande de rançon, aucun paiement ne doit être effectué.
    - Demander aux collaborateurs non-essentiels de s'atteler à des tâches qui n'ont pas de liens avec l'informatique.
    - Lister toutes les actions effectuées afin de tenir un journal d'activités.
- □ Les exercés ont préparé un message à l'attention de la police cantonale. Ce message contient les mots clés ou idées suivant(e)s :
    - Cyberattaque (ou attaque informatique)
    - Demande de rançon
    - RansomCyber24 (le nom du groupe qui attaque)

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

PHASE 2 – GESTION DE CRISE
2.1.OBS – IDENTIFICATION DES MESURES

Eléments **non-essentiels mais intéressants**

- □ Les exercés ont identifiés des mesures d'urgence correspondant à :
  - Déconnecter une partie ou tous les accès (des systèmes, ordinateurs et serveurs) de tous réseaux.
  - S'assurer que les services externes avec lesquels l'organisation collabore n'ont pas été affectés.
  - Installer des pancartes ou des supports d'information visuels sur les portes d'entrée des bureaux (communs ou autres) afin de communiquer des informations sur la situation actuelle.

Eléments **qui ne devraient pas apparaitre**

- □ Les exercés continuent d'utiliser les moyens informatiques de l'organisation.
- □ Les exercés font appels à des services tiers hors : canton, police, EMCC et leur gestionnaire informatique usuel.
- □ Les exercés ne prévoient pas de communication (qu'elle soit interne ou externe).
- □ Les exercés souhaitent gérer la cyberattaque seuls, sans contacter la police cantonale.
- □ Les exercés souhaitent payer la rançon.

Champ libre pour appréciation et information via texte

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

PHASE 2 – GESTION DE CRISE
2.2.OBS – RAPPORT D'ORIENTATION

Fiche destinée à l'observateur

Durée à disposition

De 9h00 à 9h25

Les exercés disposent de 25 minutes pour lire et compléter la partie 2.2

Présentation du contexte

Cette fiche a pour objectif de permettre à l'observateur d'évaluer, pour une partie donnée, les actions et réactions des participants. Elle est destinée à être utilisée dans le cadre du rapport d'orientation (2.2.2).

Cette fiche devrait pouvoir être utilisée par n'importe quel observateur, quel que soit son degré d'expérience ou de formation en gestion de crise. Cette fiche ne doit pas être partagée avec les participants de l'exercice tant que la séquence n'est pas terminée.

Grille d'observations

Objectif

L'observateur doit identifier les actions, réflexions, mesures qui ont été faites et/ou prises par la/les personne(s) participant à l'exercice. Il est également possible de noter, sous forme de texte, différentes remarques. Note : une croix [X] signifie que cela a été effectué ou dit.

Eléments ***importants***

- □ Les exercés ont bien pris connaissance de tous les documents.
- □ La cellule de crise est toujours activée.
- □ La liste des personnes qui doivent être présentes est établie.
- □ L'ordre du jour est distribué aux participants.
- □ Le rapport d'orientation a été préparé en amont avec les points clés à communiquer.
- □ Le rapport est conduit soit :
  - Les participants sont cadrés par la personne en charge de conduire le rapport
  - L'ordre du jour est respecté
- □ Les documents de conduite sont visibles (journal d'événement, mesures en cours)
- □ Un PV est pris lors du rapport et distribué au terme (il s'agit d'un PV décisionnel)
- □ Au terme du rapport, chacun sait ce qui est attendu de lui pour la suite des travaux
- □ La durée du rapport n'excède pas 30 min.

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

*Eléments **non-essentiels mais intéressants***

- ☐ Ordre du jour a été mis à disposition sur les places des participants.
- ☐ Les places sont identifiées.

*Eléments **qui ne devraient pas apparaitre***

- ☐ Les exercés répondent au téléphone durant le rapport.
- ☐ Les exercés quittent le rapport.
- ☐ Présence de personnel non essentiel lors du rapport.
- ☐ Discussion de points trop techniques et opérationnels.

Champ libre pour appréciation et information via texte

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

PHASE 3 – COMMUNICATION
3.1.OBS – STRATÉGIE DE COMMUNICATION

Fiche d'observateur

Durée à disposition

De 9h45 à 10h15

Les exercés disposent de 30 minutes pour lire et compléter la section 3.1

Présentation du contexte

Cette fiche a pour but de permettre à l'observateur d'évaluer la stratégie de communication de la cellule de crise.

La fiche devrait pouvoir être utilisée par n'importe quel observateur, quel que soit son degré d'expérience ou de formation en gestion de crise. Cette fiche ne doit pas être partagée avec les participants de l'exercice tant que la séquence n'est pas terminée.

Grille d'observations

Objectif

L'observateur doit identifier les actions, réflexions, mesures qui ont été faites et/ou prises par la/les personne(s) participant à l'exercice. Il est également possible de noter, sous forme de texte, différentes remarques. Note : une croix [X] signifie que cela a été effectué ou dit.

Eléments **importants**

- □ Une personne chargée de la gestion de la communication est désignée ; ainsi qu'une personne responsable de valider la communication avant envoi.
- □ Le public cible et les parties prenantes clés sont identifiés.
- □ Une stratégie de communication externe est établie. Le plan comprend les destinataires, les moyens de communication, ainsi que la nature des messages à communiquer.
- □ Une stratégie de communication de communication interne est établie. Le plan comprend les destinataires, les moyens de communication, ainsi que la nature des messages à communiquer.
- □ Une ligne de parole est établie.
- □ Les grandes lignes d'un communiqué interne et externe sont définies.
- □ Les sujets importants concernant la cyberattaque sont correctement identifiés par les participants et sont incorporés dans les communications de manière adéquate.
- □ Les messages sont cohérents, clairs et ne contiennent pas d'informations inexactes.

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

PHASE 3 – COMMUNICATION
3.1.OBS – STRATÉGIE DE COMMUNICATION

Eléments **non-essentiels mais intéressants**

- □ Le rapport de situation est mis à jour prenant en compte les attentes et publication de la presse.
- □ Une stratégie de communication préétablie par l'organisation est utilisée.
- □ La liste des destinataires internes est disponible hors moyen informatique.

Eléments **qui ne devraient pas apparaitre**

- □ Une décision de ne pas communiquer vers l'extérieur ou à l'interne.
- □ La communication est incorrecte (par exemple, prend des hypothèses comme des faits).
- □ Divulgation dans les communiqués d'information non vérifiées ou sensibles/nécessaires à l'enquête en cours.

Champ libre pour appréciation et information via texte

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

PHASE 3 - COMMUNICATION
3.2.OBS – COMMUNIQUE DE PRESSE

Fiche d'observateur

Durée à disposition

De 10h15 à 10h35

Les exercés disposent de 20 minutes pour lire et compléter la section 3.2

Présentation de la fiche

Cette fiche a pour but de permettre à l'observateur d'évaluer la stratégie de communication de l'exercice de crise.

La fiche devrait pouvoir être utilisé par n'importe quel observateur, quel que soit son degré d'expérience ou de formation en gestion de crise. Cette fiche ne doit pas être partagée avec les participants de l'exercice tant que la séquence n'est pas terminée.

Grille d'observations

Objectif

L'observateur doit identifier les actions, réflexions, mesures qui ont été faites et/ou prises par la/les personne(s) participant à l'exercice. Il est également possible de noter, sous forme de texte, différentes remarques. Note : une croix [X] signifie que cela a été effectué ou dit.

Eléments **importants**

- ☐ Les participants prennent connaissance du modèle de communiqué de presse (document « 3.2.2 - Document modèle de communiqué de presse pour le public »)
- ☐ Les participants préparent un communiqué de presse :
  - La nature et les impacts de l'attaque, autant pour l'organisation victime que pour ses utilisateurs / usagers, sont expliqués.
  - Les premières actions entreprises par l'organisation sont indiquées.
  - Le ton de la communication se veut rassurante et transparente.

Eléments **non-essentiels mais intéressants**

- ☐ Une analyse des avantages et des inconvénients de communiquer ou de s'abstenir est réalisée.
- ☐ Des conseils de vigilance envers les utilisateurs / usagers sont mis à disposition.

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

Auteurs : CSIRT +EMCC

Eléments **qui ne devraient pas apparaitre**

- ☐ Des promesses de résolution qui ne pourraient pas être tenues
- ☐ La communication est incorrecte (par exemple, prend des hypothèses comme des faits)
- ☐ La communication est anxiogène (suscite la crainte ou la peur chez le destinataire)

Champ libre pour appréciation et information via texte

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

PHASE 4 – VOL DE DONNÉES
4.1.OBS – ANALYSE DES DONNÉES VOLÉES

Fiche destinée à l'observateur

Durée à disposition

De 10h55 à 11h25

Les exercés disposent de 30 minutes pour lire et compléter la section 4.1

Présentation de l'exercice

Les exercés recevront plusieurs documents afin de pouvoir comprendre et évaluer le niveau de risque associé aux documents dérobés. La cellule de crise prendra ensuite le rôle d'un collaborateur chargé de la classification des documents. Plusieurs milliers de documents sont potentiellement à analyser dans le cas d'une attaque réelle ce qui nécessite une bonne organisation et compréhension de la classification. L'aspect communication, bien qu'essentiel en cas de diffusion de données, ne sera pas abordé dans le cadre de cet exercice. Un exemple de communiqué de presse mis à jour sera transmis comme proposition de solution.

Grille d'observations

Objectif(s)

L'observateur doit identifier les actions, réflexions, mesures qui ont été faites et/ou prises par la/les personne(s) participant à l'exercice. Il est également possible de noter, sous forme de texte, différentes remarques. Note : une croix [X] signifie que cela a été effectué ou dit.

Eléments **importants**

- ☐ La cellule de crise a pris en compte le SMS reçu, ainsi que la publication des données sur le darknet.
- ☐ L'organisation ne cède pas à la pression et refuse toujours de payer la rançon.
- ☐ L'organisation prévoit de notifier les autorités compétentes.
- ☐ La cellule de crise utilise sa propre grille de classification si existante ou utilise celle de l'exercice.
- ☐ L'organisation établit la criticité de l'échantillon des données volés sur la fiche 4.1.6.
- ☐ La cellule de crise est consciente qu'elle doit prendre des actions en priorité sur les documents classifiés « Confidentiel Prioritaire » puis « Confidentiel » (selon grille proposée).

Eléments **non-essentiels mais intéressants**

- ☐ La cellule de crise décide d'une action à entreprendre pour chaque document. Dans un cas réel, en raison du volume, il est primordial de se focaliser sur les documents les plus critiques/sensibles.

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.

- □ La cellule de crise a compris que les personnes en charge de classifier les données doivent être rigoureusement choisies et signer un accord de non-divulgation.
- □ Les exercés ont bien pris connaissance de tous les documents.
- □ L'organisation prévoit de communiquer sur le nouveau statut de la situation et la découverte des informations sur le darknet.

Eléments **qui ne devraient pas apparaitre**

- □ La cellule de crise décide de ne pas faire cette analyse de données.
- □ La cellule de crise décide de payer la rançon.
- □ Les personnes en charge de la classification n'utilisent pas la même grille pour la classification des données.

Champ libre pour appréciation et information via texte

Les informations contenues dans ce document sont fournies dans le cadre d'un exercice de gestion de crise cyber. Elles sont fictives et ne doivent en aucun cas être interprétées comme représentant un événement réel ou une situation actuelle.