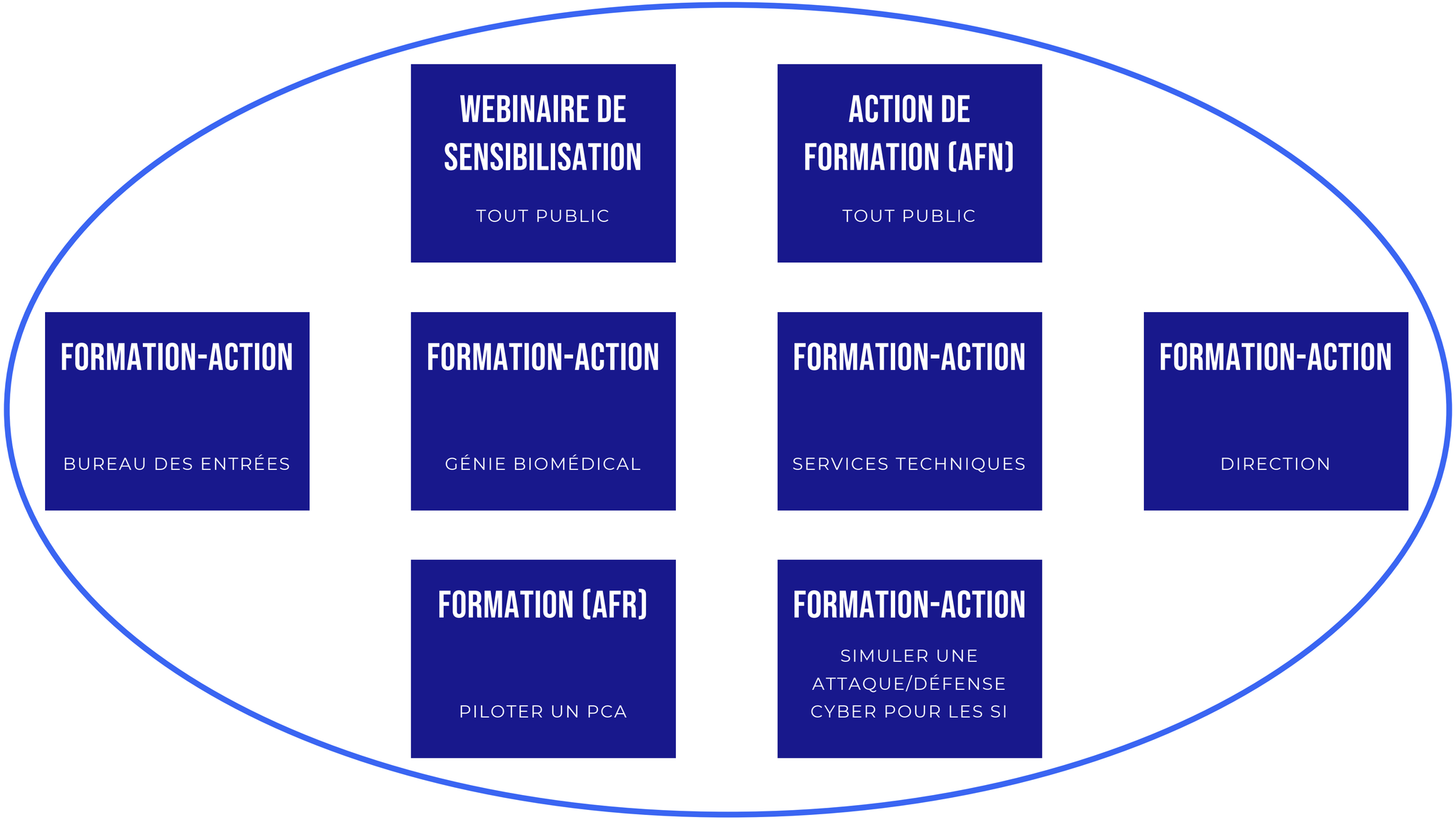
OBJECTIF 1

DISPOSITIF DE L’ANFH

Comprendre le dispositif cyber
de l’ANFH.

15min

DISPOSITIF CYBERDÉFENSE



WEBINAIRE : SE SENSIBILISER À LA CYBERSÉCURITÉ

Si la cybersécurité constitue l'un des enjeux majeurs du numérique, les risques et les bons comportements à adopter face aux cybermenaces sont encore peu connus. Ce séminaire, dont l'objectif est de sensibiliser les participants à la cybersécurité, vous apportera une connaissance de la cybercriminalité, vous permettra de savoir identifier les cybermenaces et les actions malveillantes et d'appréhender les conséquences d'une cyberattaque à travers des récits anecdotiques, des démonstrations et des jeux interactifs.

OBJECTIFS

- ✓ Appréhender la cybercriminalité et ses conséquences pour les établissements de santé
- ✓ Sensibiliser les agents aux risques numériques
- ✓ Connaître les principaux types d'attaques
- ✓ Savoir détecter les menaces liées aux emails malveillants et acquérir les bons réflexes
- ✓ Comprendre les dispositifs *cyberdéfense* de l'ANFH

PROGRAMME

- **La cybercriminalité, ses objectifs et ses conséquences**
  - Les acteurs de la cybercriminalité : les cybercriminels et leurs motivations
  - Les cybermenaces et leurs conséquences sur les établissements de santé
- **Les emails malveillants**
  - Détecter les emails malveillants : les liens douteux et les pièces jointes piégées
  - Les bons réflexes suite à un email malveillant
- **Les mots de passe et l'authentification forte**
  - Les outils pour choisir de bons mots de passe et les retenir
  - L'authentification à deux facteurs
- **Les mises à jour pour se protéger des cyberattaques**
  - Les vulnérabilités des systèmes non mis à jour
  - L'intérêt des mises à jour pour garantir la sécurité des appareils
- **Présentation des dispositifs cyber de l'ANFH**

Renforcement de la cybervigilance : acquérir les bons réflexes

Cette formation a pour but de renforcer les connaissances et la vigilance des agents de la fonction publique hospitalière face aux enjeux de cybersécurité. A travers cette formation, les apprenants seront sensibilisés à la cybervigilance au quotidien dans leur travail, pour être en mesure de détecter les menaces, alerter, et appliquer les premières mesures réflexes en cas de cyberattaque.

La formation alterne des contenus théoriques, des temps d'échanges, des démonstrations et des jeux de mise en situation. Ces derniers permettent d'illustrer, très concrètement, la manière dont un agent pourrait ouvrir accidentellement la porte à une cyberattaque.

Objectifs

N°1 : **Appréhender la cybercriminalité**, ses objectifs, et **les risques inhérents** aux établissements de santé

N°2 : Prendre conscience **du rôle contributeur de chacun** dans la cybersécurité des établissements de santé

N°3 : Être en mesure de **détecter les menaces** les plus courantes et de réagir

N°4 : **Accompagner** l'adoption du numérique au sein des établissements de santé en adoptant **une posture de vigie** et de diffusion des bonnes pratiques

Programme

JOUR 1 :

> Module 0 : Présentation et tour de table

> Module 1 : Appréhender la cybercriminalité :
- Travail de groupe "Dessinons internet"
- Exposé interactif sur les cybercriminels
- Jeu de cartes "Simulation d'une cyberattaque"

> Module 2 : Prendre conscience du rôle de contributeur de chacun :
- Analyse réflexive des pratiques professionnelles
- Exposé interactif sur la cybersécurité

> Module 3 : Être en mesure de détecter les menaces :

Les emails malveillants

- Démonstration de hacking via email malveillant
- Exercice de représentation sur les critères suspects
- Entraînement par atelier pour trouver les emails malveillants
- Exposé interactif sur les pièces jointes.

Les arnaques et fraudes

- Exposé interactif de présentation des diverses fraudes par email et SMS.

Mots de passe et authentification forte

- Démonstration de hacking liées au mot de passe
- Reformulation et synthèse par les apprenants
- Démonstration commentée sur l'utilisation des gestionnaires de mots de passe.

FORMATION : MISE EN SITUATION D'UNE CYBERATTAQUE (bureaux des entrées)

Si la cybersécurité constitue l'un des enjeux majeurs du numérique, les risques et les bons comportements à adopter face aux cyberattaques sont encore peu connus. Cette formation, dont l'objectif est de confronter les participants à une cyber crise, vous apportera des connaissances théoriques sur la notion même de la cyber crise, mais vous permettra également de savoir mesurer les impacts de celle-ci en vous y confrontant, grâce à un exercice de mise en situation réaliste.

OBJECTIFS

Identifier ce qu'est une crise cyber

Connaître les typologies de crises cyber

Identifier les impacts d'une cyberattaque sur les systèmes d'information

Se confronter à une gestion de crise cyber et savoir mettre en place une procédure en mode dégradé

PROGRAMME

- **Qu'est-ce qu'une crise cyber ?**

La définition de la cyber crise
Les typologies de crises cyber

- **Identifier les impacts d'une crise cyber**

Identification des outils SI
Connaître l'impact fonctionnel des cyberattaques sur les outils SI

- **L'exercice de crise cyber**

La reconnaissance d'une situation de crise
La remontée de l'alerte
Définir et mettre en place une procédure en mode dégradé

- **Identification des bonnes pratiques et axes d'amélioration**

FORMATION : MISE EN SITUATION D'UNE CYBERATTAQUE (génie biomédical)

Si la cybersécurité constitue l'un des enjeux majeurs du numérique, les risques et les bons comportements à adopter face aux cyberattaques sont encore peu connus. Cette formation, dont l'objectif est de confronter les participants à une cyber crise, vous apportera des connaissances théoriques sur la notion même de la cyber crise, mais vous permettra également de savoir mesurer les impacts de celle-ci sur le service biomédical, en vous y confrontant, grâce à un exercice de mise en situation réaliste.

OBJECTIFS

Identifier ce qu'est une crise cyber

Connaître le risque de piratage des appareils médicaux

Comprendre les interactions entre le service biomédical et le service de sécurité informatique

Se confronter à une gestion de crise cyber et savoir identifier les risques d'une cyberattaque sur les appareils biomédicaux

PROGRAMME

- **Qu'est-ce qu'une crise cyber ?**

La définition de la crise
La définition de la crise cyber

- **Le risque de piratage des appareils médicaux**

Identification des appareils utilisés quotidiennement
Comprendre l'enjeu de maintenance de ces appareils vulnérables

- **Les interactions entre le service biomédical et le service de sécurité informatique**

La reconnaissance d'une situation de crise
La remontée de l'alerte
L'identification des besoins en situation de crise cyber
Comprendre et identifier les risques générés par une cyberattaque sur les appareils biomédicaux

- **Identification des bonnes pratiques et axes d'amélioration**

FORMATION : MISE EN SITUATION D'UNE CYBERATTAQUE (services techniques)

Si la cybersécurité constitue l'un des enjeux majeurs du numérique, les risques et les bons comportements à adopter face aux cyberattaques sont encore peu connus. Cette formation, dont l'objectif est de confronter les participants à une cyber crise, vous apportera des connaissances théoriques sur la notion même de la cyber crise, mais vous permettra également de savoir mesurer les impacts de celle-ci sur les appareils connectés, en vous y confrontant, grâce à un exercice de mise en situation réaliste.

OBJECTIFS

Identifier ce qu'est une crise cyber

Connaître le risque de piratage des appareils connectés techniques

Comprendre les interactions entre les appareils connectés techniques et le service de sécurité informatique

Se confronter à une gestion de crise informatique et savoir identifier les risques d'une cyberattaque sur les appareils connectés

PROGRAMME

- **Qu'est-ce qu'une crise cyber ?**

La définition de la crise cyber
Les typologies des crises cyber

- **Le risque de piratage des appareils connectés techniques**

Identification des appareils utilisés quotidiennement
Connaître les conséquences d'un dysfonctionnement majeur de ces appareils
Identifier les risques de piratage liés à une cyberattaque

- **Les interactions entre les appareils connectés et le service de sécurité informatique**

La reconnaissance d'une situation de crise
Identifier les actions les plus efficaces à mettre en place pour répondre à une situation de crise cyber
L'identification des besoins et de ses interlocuteurs en situation de crise cyber
Comprendre et identifier les risques générés par une cyberattaque sur les appareils connectés

- **Identification des bonnes pratiques et axes d'amélioration**

FORMATION : MISE EN SITUATION D'UNE CYBERATTAQUE (direction)

Si la cybersécurité constitue l'un des enjeux majeurs du numérique, les risques et les bons comportements à adopter face aux cyberattaques sont encore peu connus. Cette formation, dont l'objectif est de confronter les participants à une cyber crise, vous apportera des connaissances théoriques sur la notion même de la cyber crise, mais vous permettra également de savoir mesurer les impacts fonctionnels de celle-ci, en vous y confrontant, grâce à un exercice de mise en situation réaliste.

OBJECTIFS

Identifier ce qu'est une crise cyber

Identifier les impacts fonctionnels d'une crise cyber sur les différents services

Savoir prioriser les actions en situation de cyberattaque

Se confronter à une gestion de crise cyber et savoir identifier les risques d'une cyberattaque

Réagir en conférence de presse

PROGRAMME

- **Qu'est-ce qu'une crise cyber ?**

La définition de la crise cyber
Les typologies des crises cyber

- **Les impacts d'une crise cyber sur les différents secteurs d'activité**

Identification les acteurs impliqués dans chaque secteur d'activité
Évaluer les connaissances de ces acteurs en crise cyber pour identifier leurs besoins

- **La gestion de crise cyber**

La reconnaissance d'une situation de crise
Identifier et prioriser les actions les plus efficaces à mettre en place pour répondre à une situation de crise cyber
L'identification des besoins et de ses interlocuteurs en situation de crise cyber
Savoir s'exprimer en conférence de presse

- **Identification des bonnes pratiques et axes d'amélioration**

FORMATION : PILOTER UN PLAN DE CONTINUITÉ

Dans la gestion de crise, la continuité d'activité occupe une place centrale. En effet, la priorisation des activités essentielles et l'élaboration d'un plan opérationnel sont primordiales pour parvenir à mettre en œuvre des solutions. Cette formation vous apportera une connaissance approfondie des outils de continuité, de leur articulation ainsi que les clés de compréhension de la stratégie de continuité et de reprise d'activité notamment grâce à de nombreuses activités ludiques et interactives.

OBJECTIFS

Comprendre le contexte et les objectifs d'un Plan de continuité d'Activité (PCA)

Identifier et gérer les risques prioritaires, formaliser les besoins de continuité

Comparer et harmoniser les BIA (Business Impact Analysis)

Définir la stratégie et les outils de continuité d'activité

Rédiger une procédure de continuité d'activité

Spécifier les procédures de gestion et communication de crise

Anticiper la reprise d'activité

PROGRAMME

- **Le contexte et les objectifs du PCA**

La notion de rupture de continuité d'activité
Les enjeux du PCA

- **Le contexte, les objectifs et la comitologie d'un PCA**

Définition des rôles, des responsabilités et de la comitologie d'un PCA
Définition des objectifs et du périmètre
Les ressources documentaires à connaitre

- **La gestion des risques prioritaires**

La cartographie des risques
Le traitement du risque : l'approche par typologies d'impact

- **L'identification et la formalisation des besoins de continuité**

La conduite d'un entretien de BIA
L'inventaire des processus

- **L'identification des activités critiques et la conduite à tenir face à un scénario insoluble**

- **Le besoin d'harmonisation des BIA**

Réaliser un entretien d'harmonisation

- **Définir la stratégie et les outils de la continuité d'activité**

Concevoir une stratégie de continuité d'activité adaptée
Traiter l'absence de solution de continuité

Simuler une attaque/défense pour les services informatiques hospitaliers

Les professionnels des services informatiques sont au coeur de la cybersécurité d'un établissement et seront les premiers sollicités en cas d'attaque. Si beaucoup est déjà fait sur le travail de renforcement de la sécurité des systèmes, il faut également être en mesure de réagir ou d'agir efficacement lorsque les systèmes sont interrompus. A l'instar des entraînements à la sécurité incendie, la sécurité des SI doit aussi appréhender la gestion de crise lorsque le risque survient.

OBJECTIFS

↗ Appréhender les méthodes d'attaques et prévoir les mécanismes de défenses adaptés

↗ Mettre en place les premières actions pour limiter les dégâts

↗ Informer / dialoguer efficacement avec la Direction

↗ Solliciter les bons acteurs extérieurs

↗ Faciliter le fonctionnement de l'établissement en mode dégradé

↗ Spécifier les procédures de gestion de crise et de communication

↗ Assurer et anticiper la reprise

PROGRAMME

JOUR 1 :

▪ **Compréhension des mécanismes d'attaques**

- Reconnaissance
- Découverte de vulnérabilités
- Écriture/Exploit de failles
- Exfiltration
- Couverture des traces
- Répartition travaux pratiques : 70% / 30%

JOUR 2 :

▪ **Simulation réelle**

- Mise en pratique : avec un laboratoire comprenant un Système d'Information virtualise (comprenant des serveurs, site web, système de messagerie, partage de fichiers, imprimantes, routeurs, postes de travail avec des OS reprenant ceux de l'environnement actuel du centre hospitalier...). Le but étant de mettre en pratique en situation « réelle » une phase d'attaque et une phase défense en simultanée permettant d'activer ainsi les différents Protocoles. Division en deux groupes : attaquants & défenseurs, inversement
- Répartition travaux pratiques : 90% / 10%

Se sensibiliser à la cybersécurité - Webinaire

MERCI !

AKYL

Crisalyde | gestion de crise globale

Anfh

Mars 2023