Anfh Association nationale pour la formation permanente du personnel hospitalier

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 webinaire, 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.

PUBLIC VISÉ :
Tout public

ORGANISÉ PAR :
CRISALYDE

NOMBRE DE PARTICIPANTS :
60 participants

DURÉE :
2 heures

PRÉREQUIS :
Aucun prérequis pour cette sensibilisation

CONTACT :
Pour s'inscrire

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

MODALITÉS PÉDAGOGIQUES

Exposés participatifs

Quizz et jeux interactifs

Démonstrations de *hacking*

Questionnaire d'évaluation et de satisfaction du webinaire

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**

Anfh Association nationale pour la formation permanente du personnel hospitalier

OFFRE POUR LES ACTIONS DE FORMATION NATIONALES

Renforcement de la cybervigilance : acquérir les bons réflexes

Public Visé
Tout agent de la Fonction Publique Hospitalière (FPH)

Organisé par
CRISALYDE

Nombre de participants
8 à 16 participants

Durée
1 journée

En savoir plus
www.anfh.fr

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

Modalités pédagogiques

Tours de tables

Travail de groupe

Exposés interactifs

Jeu de cartes

Analyse réflexive

Démonstration de hacking

Entrainements par atelier

Cas concrets

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.

Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

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.

PUBLIC VISÉ :
Equipes de direction

ORGANISÉ PAR :
CRISALYDE

NOMBRE DE PARTICIPANTS :
Entre 6 et 12 participants

DURÉE :
1 journée (7heures)

PRÉREQUIS :
Aucun prérequis pour cette formation

CONTACT :

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

MODALITÉS PÉDAGOGIQUES

Exposés participatifs

Quizz, jeux et ateliers interactifs

Travaux de simulation en groupe, utilisation de scénarii pédagogiques favorisant l'analyse de pratiques et la simulation, visant à comprendre le fonctionnement, les enjeux et conséquences d'une cyberattaque

Phases de debrief régulières

Support de retour d'expérience du formateur

Questionnaire d'évaluation et de satisfaction de la formation

Supports "Pour aller plus loin"

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**

Votre texte ici 1

Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

Formation-action : mise en situation cyberattaque (direction)

Le rôle de la direction de l'établissement dans la gestion de la cybersécurité est central. En effet il lui incombe de piloter les équipes et les moyens mis en œuvre afin d'assurer la sécurité informatique de l'établissement qui dépend d'elle. A cette fin il lui faudra définir un ensemble de règles et de protocoles afin de construire et utiliser une chaine décisionnelle efficace. C'est également elle qui validera les plans d'actions et de réponse sur incident de l'ensemble de ses équipes.

En période de crise elle aura également le rôle crucial de communiquer en interne et en externe et de piloter la crise en priorisant, organisant et contrôlant les efforts de chacun afin de maintenir les activités et de revenir le plus vite a un état normal de fonctionnement.

PUBLIC VISÉ :
↗ Tout agent de la FPH travaillant aux services de direction

ORGANISÉ PAR :
↗ Déméter Santé

NOMBRE DE PARTICIPANTS :
↗ 8 à 16 participants

DURÉE :
↗ 1 jours

PRÉREQUIS :
↗ Aucun

CONTACT :

OBJECTIFS

↗ "Comprendre à quoi sert la SSI dans un établissement de santé (protection des données, réputation de l'établissement, continuité des soins)."

↗ "Communiquer efficacement avec le SSI"

↗ "Repérer les acteurs"

↗ "Mettre en place une chaîne décisionnelle efficace"

↗"Connaître les prérogatives de chaque secteur d'activité"

↗"Déployer un plan d'action prédéfini"

↗"Mettre en place un plan de de communication adapté en interne et en externe"

MODALITÉS PÉDAGOGIQUES

↗ Expression guidée par questionnement.

↗ Travail en sous groupes

↗ Apports didactiques et conceptuels.

↗ Echanges

↗Etude de cas, analyse de situations

↗Démonstration, exercices

↗Analyse, démarche réflexive autour du vécu et des situations de travail

PROGRAMME

Comprendre à quoi sert la SSI dans un établissement de santé et plus particulièrement dans son service

- Quelle est aujourd'hui l'état de la menace cyber ?
- Les principes de base de la SSI.
- La direction le centre de planification de la politique SSI.

Communiquer efficacement avec le SSI

- Maitriser le vocabulaire et les lignes directrices de la cybersécurité.
- Les types de cyberattaques et leurs impacts.
- Connaitre les bases de sons SI.
- Méthode de communication.
- Quelques aides à la communication.
- Debriefing et mise en commun.

Repérer les acteurs, mettre en place une chaîne décisionnelle efficace

- Les acteurs qui interviennent sur le SI.
- Les processus de décision et de contrôlent en période normales.
- Les processus de décision et de contrôlent en périodes de crises.
- Mise pratique avec test du processus décisionnel pour une situation normale et une situation de crise.
- Debriefing et retour d'expérience sur le processus décisionnel.

Connaître les prérogatives de chaque secteur d'activité

- Définir les rôles et les responsabilités de chacun vis-à-vis du SI et de ses équipements
- Déployer un plan d'action prédéfini
- Phase 1 : Alerter, mobiliser, endiguer
- Phase 2 : Maintenir la confiance et comprendre l'attaque :
- Phase 3 : Relancer les activité métier et durcir les SI.
- Phase 4 : Tirer les leçons de la crise.
- Mise en situation pratique.
- Debriefing partage d'expérience.

Mettre en place un plan de de communication adapté en interne et en externe

- Connaitre les parties prenantes.
- Mettre aux points les procédures de communications.
- Exemple de communication au cours de chaque phase du plan d'action.
- Mise en pratique rédaction.
- Debriefing partage d'expérience

Anfh Association nationale pour la formation permanente du personnel hospitalier

Projet Cybersécurité

Pilotage d'un plan de continuité des activités

Face au risque d'interruption d'activité provoquée par des cyberattaques, la mise en œuvre d'un Plan de Continuité des Activités (PCA) est primordiale pour les établissements de santé. L'ensemble des mesures à mettre en oeuvre, selon les divers scénarii de crises et la durée de la crise, doit être déployé rapidement afin de maintenir l'organisation des soins et l'accueil des patients. Ce Plan de Continuité des Activités doit également prévoir la mise en place de l'activité en mode dégradé et anticiper la reprise à la normale des activités.

PUBLIC VISÉ :
- RSSI
- Consultants en sécurité de l'information

ORGANISÉ PAR :
- Ascent Formation

NOMBRE DE PARTICIPANTS :
- Jusqu'à 20 participants

DURÉE :
- 2 jours (14 heures)

PRÉREQUIS :
- Avoir des connaissances générales en sécurité des systèmes d'information

CONTACT :

OBJECTIFS

- Savoir construire et déployer un PCA
- Reconnaître les enjeux et avantages d'un PCA
- Démontrer les étapes essentielles à la mise en œuvre d'un PCA

MODALITÉS PÉDAGOGIQUES

- Distanciel
- Présentiel
- Cas pratiques
- Mises en situation

PROGRAMME

JOUR 1 :

▪ **Élaborer un Plan de continuité d'activité**

- Principe et scenarios d'approches
- Mise en place SMCA
- Gestion de crise
- SMCA et amélioration continue
- Travaux pratiques : Analyser des cas d'étude et de prendre des décisions sur base d'énoncé pratique

JOUR 2 :

▪ **Comprendre et anticiper les risques du facteur humain et techniques**

- Identification des risques
- Évènements redoutes (par domaine)
- Plan d'action
- Évaluation des risques résiduels, et acceptation ou remédiation

Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

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.

PUBLIC VISÉ :
Personnel d'un même domaine d'activités et personne(s) de la direction des services informatiques en charge de l'applicatif du domaine

ORGANISÉ PAR :
CRISALYDE

NOMBRE DE PARTICIPANTS :
Entre 6 et 12 participants

DURÉE :
2 journée en présentiel (14heures)

PRÉREQUIS :
Aucun prérequis pour cette formation

CONTACT :

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

MODALITÉS PÉDAGOGIQUES

Exposés participatifs

Quizz d'évaluation des connaissances

Jeux et ateliers interactifs en sous-groupe

Des phases de debrief régulières

Questionnaire d'évaluation et de satisfaction de la formation

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

Anfh Association nationale pour la formation permanente du personnel hospitalier

Projet cybersécurité

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.

PUBLIC VISÉ :
- Professionnel des SI
- Équipe SSI
- Administrateur

ORGANISÉ PAR :
- Ascent Formation

NOMBRE DE PARTICIPANTS :
- Jusqu'à 20 participants

DURÉE :
- 2 jours (14 heures)

PRÉREQUIS :
- Maîtrise de l'environnement informatique

CONTACT :

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

MODALITÉS PÉDAGOGIQUES

- Présentiel
- Distanciel
- Cas pratiques
- Mise en pratiques

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%

Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

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.

PUBLIC VISÉ :
Tout agent des bureaux des entrées/admissions

ORGANISÉ PAR :
CRISALYDE

NOMBRE DE PARTICIPANTS :
Entre 6 et 12 participants

DURÉE :
1 journée (7 heures)

PRÉREQUIS :
Aucun prérequis pour cette formation

CONTACT :

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**

MODALITÉS PÉDAGOGIQUES

Exposés participatifs

Quizz, jeux et ateliers interactifs

Travaux de simulation en groupe : utilisation de scénarii pédagogiques favorisant l'analyse de pratiques et la simulation, visant à comprendre le fonctionnement, les enjeux et conséquences d'une cyberattaque

Phases de debrief régulières

Support de retour d'expérience du formateur

Questionnaire d'évaluation et de satisfaction de la formation

Supports "Pour aller plus loin"

Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

Formation-action : mise en situation cyberattaque (bureaux des entrées)

L'écosystème du secteur de la santé évolue considérablement avec le développement de nouveaux outils numériques, leur lot d'avantages et de risques numériques. Ces risques numériques ne sont plus aujourd'hui à prendre à la légère, s'il y a 10 ans une panne informatique pouvait engendrer des désagréments passagers, elle peut aujourd'hui mettre à l'arrêt des services complets et impacter la continuité des soins.

Le bureau des entrées qui est en charge de l'admission et de la saisie des premières informations patient joue donc un rôle important au sein du flux de données du SI. La maitrise des modes dégradés et la continuité des activités sont vitales.

PUBLIC VISÉ :
↗ Tout agent de la FPH travaillant au bureau des entrée.

ORGANISÉ PAR :
↗ Déméter Santé

NOMBRE DE PARTICIPANTS :
↗ 8 à 16 participants

DURÉE :
↗ 1 jours

PRÉREQUIS :
↗ Aucun

CONTACT :

OBJECTIFS

↗ " Comprendre à quoi sert la SSI dans un établissement de santé (protection des données, réputation de l'établissement, continuité des soins)."

↗ " Lister les outils SI utilisés dans son service "

↗ " Reconnaître une situation de cyberattaque"

↗ " Concevoir l'activité du service sans ces outils"

↗" Etablir quels documents papier, supports, outils, peuvent pallier l'absence de système SI opérationnel"

↗" Définir une procédure d'activité en mode dégradé spécifique à son service/pôle. "

MODALITÉS PÉDAGOGIQUES

↗ Expression guidée par questionnement.

↗ Travail en sous groupes

↗ Apports didactiques et conceptuels.

↗ Echanges

↗Etude de cas, analyse de situations

↗Démonstration, exercices

↗Analyse, démarche réflexive autour du vécu et des situations de travail

PROGRAMME

Comprendre à quoi sert la SSI dans un établissement de santé et plus particulièrement dans son service

- Quelle est aujourd'hui l'état de la menace cyber ?
- Les principes de base de la SSI.
- L'importance du BDE dans la sécurité des parcours patients.

Lister les outils SI utilisés dans son service et les risques associés à chaque outil qui dysfonctionnerait

- Comprendre le rôle et le fonctionnement de chaque outil utilisé au sein de son service.
- Connaître et visualiser facilement l'écosystème des outils SI de son service.
- Debriefing sur les résultats des travaux en sous-groupe et synthèse collective.

Concevoir l'activité du service sans ces outils

Etablir quels documents papier, supports, outils, peuvent pallier l'absence de système SI.

- Mesurer les impacts d'un dysfonctionnement total ou partiel du SI sur l'activité de son service en projetant des méthodes de travail sans ces outils.
- Formaliser le fonctionnement possible de son service en l'absence total ou partielle du SI
- Debriefing sur les résultats des travaux en sous-groupe et synthèse collective

Reconnaître une situation de cyberattaque

- Quels environnements techniques pour quel type de menaces.
- Reconnaitre les cyberattaques les plus courantes.

Définir une procédure d'activité en mode dégradé spécifique à son service/pôle

- Le mode dégradé.
- Le mode dégradé installation.
- Le mode dégradé dans la durée.
- Quitter le mode dégradé.
- L'après mode dégradé
- Simulation de mise en œuvre du mode dégradé
- Debriefing sur les simulations et mise en place d'un plan d'actions pour la mise en place du mode dégradé

Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

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.

PUBLIC VISÉ :
Ingénieurs et techniciens des services biomédicaux

ORGANISÉ PAR :
CRISALYDE

NOMBRE DE PARTICIPANTS :
Entre 6 et 12 participants

DURÉE :
1 journée (7 heures)

PRÉREQUIS :
Aucun prérequis pour cette formation

CONTACT :

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

MODALITÉS PÉDAGOGIQUES

Exposés participatifs

Quizz, jeux et ateliers interactifs

Travaux de simulation en groupe : utilisation de scénarii pédagogiques favorisant l'analyse de pratiques et la simulation, visant à comprendre le fonctionnement, les enjeux et conséquences d'une cyberattaque

Phases de debrief régulières

Support de retour d'expérience du formateur

Questionnaire d'évaluation et de satisfaction de la formation

Supports "Pour aller plus loin"

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**

Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

Formation-action : mise en situation cyberattaque (génie biomédical)

L'écosystème du secteur de la santé évolue considérablement avec le développement de nouveaux outils numériques, leur lot d'avantages et de risques numériques. Ces risques numériques ne sont plus aujourd'hui à prendre à la légère, s'il y a 10 ans une panne informatique pouvait engendrer des désagréments passagers, elle peut aujourd'hui mettre à l'arrêt des services complets et impacter la continuité des soins.
Les services Biomédicaux gèrent une grande quantité de données confidentielles ainsi que des équipements et des services indispensables à la continuité des soins. A ce titre la protection des données, la réactivité et la reprise sur incident sont des critères qui doivent sans cesse être challengés et améliorés. La réalité d'une cyberattaque impose des évolutions dans les pratiques.

PUBLIC VISÉ :
↗ Tout agent de la FPH travaillant aux services Biomédicaux

ORGANISÉ PAR :
↗ Déméter Santé

NOMBRE DE PARTICIPANTS :
↗ 8 à 16 participants

DURÉE :
↗ 1 jour

PRÉREQUIS :
↗ Aucun

CONTACT :

OBJECTIFS

↗ " Comprendre à quoi sert la SSI dans un établissement de santé"

↗ "Comprendre les interactions entre le service biomédical et le service sécurité informatique"

↗ "Connaître le risque de piratage des appareils médicaux"

↗ "Communiquer efficacement avec le SSI"

↗"Savoir être vigilant lors de la maintenance des appareils médicaux "

↗"Définir un protocole de mise au rebus des disques durs contenant des données de santé"

↗"Etablir des protocoles d'action en cas de cyberattaque. "

MODALITÉS PÉDAGOGIQUES

↗ Expression guidée par questionnement.

↗ Travail en sous groupes

↗ Apports didactiques et conceptuels.

↗ Echanges

↗Etude de cas, analyse de situations

↗Démonstration, exercices

↗Analyse, démarche réflexive autour du vécu et des situations de travail

PROGRAMME

Comprendre à quoi sert la SSI dans un établissement de santé et plus particulièrement dans son service

- Quelle est aujourd'hui l'état de la menace cyber ?
- Les principes de base de la SSI.
- L'intégration des personnels biomédicaux dans la SSI.

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

- Des appareil connectés et donc vulnérables.
- Les bonnes pratiques pour la connexion d'équipement de santé.

Connaître le risque de piratage des appareils médicaux.

- Les attaques sur les appareils médicaux.
- Savoir évaluer les risques pour un appareil ou une situation donnée.

Communiquer efficacement avec le SSI

- Communiquer avec la SSI pour maintenir la sécurité
- Quelle communication en période de crise
- Communiquer sur les évolutions des matériels et les remontées utilisateurs
- Bien communiquer la méthode CNV
- Mise en situation au travers d'un cas pratique
- Debriefing sur les résultats de la simulation et synthèse des différent éléments.

Savoir être vigilant lors de la maintenance des appareils médicaux

- Les étapes de la maintenance.
- Effacer et mettre au rebut un disque dur de manière sécurisé

Etablir des protocoles d'action en cas de cyberattaque

- Quels environnements techniques pour quel type de menaces
- Co-Construction d'un protocole d'action contre les menaces vues ci-dessus
- Mise en commun des plans d'actions et réflexion autour de leur construction et fonctionnement
- Mise en application d'un plan d'action sur équipement réel, si disponibilité, accord et validation de l'équipe SSI de l'établissement. Sinon mise en situation sur un scénario fournis par le formateur.
- Debriefing sur le plan d'action avec la SSI et le formateur si simulation sur équipements réel .

Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

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.

PUBLIC VISÉ :
Personnel des services techniques

ORGANISÉ PAR :
CRISALYDE

NOMBRE DE PARTICIPANTS :
Entre 6 et 12 Participants

DURÉE :
1 journée (7 heures)

PRÉREQUIS :
Aucun prérequis pour cette formation

CONTACT :

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

MODALITÉS PÉDAGOGIQUES

Exposés participatifs

Quizz, jeux et ateliers interactifs

Travaux de simulation en groupe : utilisation de scénarii pédagogiques favorisant l'analyse de pratiques et la simulation, visant à comprendre le fonctionnement, les enjeux et conséquences d'une cyberattaque

Phases de debrief régulières

Support de retour d'expérience du formateur

Questionnaire d'évaluation et de satisfaction de la formation

Supports "Pour aller plus loin"

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**

Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

Formation-action : mise en situation cyberattaque (services techniques)

L'écosystème du secteur de la santé évolue considérablement avec le développement de nouveaux outils numériques, leur lot d'avantages et de risques numériques. Ces risques numériques ne sont plus aujourd'hui à prendre à la légère, s'il y a 10 ans une panne informatique pouvait engendrer des désagréments passagers, elle peut aujourd'hui mettre à l'arrêt des services complets et impacter la continuité des soins.
Le service technique gère un grand nombre d'appareils et de systèmes connectés ayant des fonctions de support et de sécurité. Il est donc indispensable que ce service soit capable de mettre en place une politique de sécurisation de ses appareils connectés. Les appareils support étant également plus répandus et plus nombreux il est important de mettre en place une politique de gestion des risques et de réponse sur incident.

PUBLIC VISÉ :
↗ Tout agent de la FPH travaillant aux services techniques

ORGANISÉ PAR :
↗ Déméter Santé

NOMBRE DE PARTICIPANTS :
↗ 8 à 16 participants

DURÉE :
↗ 1 jours

PRÉREQUIS :
↗ Aucun

CONTACT :

OBJECTIFS

↗ " Comprendre à quoi sert la SSI dans un établissement de santé (protection des données, réputation de l'établissement, continuité des soins)."

↗ " Comprendre les interactions entre les différents appareils connectés et le service sécurité informatique. "

↗ " Connaître le risque de piratage des appareils. "

↗ " Être confronté à des scénarii d'attaque mettant en cause ces appareils connectés. "

↗" Apprendre à réagir efficacement en cas de cyberattaque. "

MODALITÉS PÉDAGOGIQUES

↗ Expression guidée par questionnement.

↗ Travail en sous groupes

↗ Apports didactiques et conceptuels.

↗ Echanges

↗Etude de cas, analyse de situations

↗Démonstration, exercices

↗Analyse, démarche réflexive autour du vécu et des situations de travail

PROGRAMME

Comprendre à quoi sert la SSI dans un établissement de santé et plus particulièrement dans son service

- Quelle est aujourd'hui l'état de la menace cyber ?
- Les principes de base de la SSI.
- L'intégration des personnels techniques dans la SSI.

Comprendre les interactions entre les différents appareils connectés et le service sécurité informatique

- Le rôle de la SSI au sein d'un établissement (la confidentialité, l'intégrité, la disponibilité et la traçabilité).
- La SSI garante de la sécurité des périphériques et des données.

Connaître le risque de piratage des appareils.

- Diagnostiquer son SI et évaluer les risques dans son environnement.
- Méthode d'évaluation des risques équipement par équipement.
- Mise en situation, évaluation de plusieurs objets connecté de l'établissement.
- Debriefing discussion et partage de connaissance sur la méthode AMDEC et le scoring des objets.

Être confronté à des scénarii d'attaque mettant en cause ces appareils connectés

- A l'aide des résultats de l'évaluation des risques le formateur proposera différents scénarii d'attaque.
- Chaque scenarii sera présenté par le formateur d'un point de vue technique avant de laisser au sous-groupe le soin d'évaluer la menace.

Apprendre à réagir efficacement en cas de cyberattaque

- Quels environnements techniques pour quel type de menaces.
- Reconnaitre les cyberattaques les plus courantes
- Réagir à une cyberattaque
- Mise en situation d'une réponse à une cyberattaque.
- Debriefing sur les simulation et mise en place d'un plan d'action pour la mise en place du mode dégradé.