

DISPOSITIF Cyberdéfense : Simuler une attaque/défense pour les agents des services informatiques hospitaliers

Contexte

Les professionnels des services informatiques sont au cœur 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
- Informier / 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

Renseignements complémentaires

Pour plus d'informations :

Alicia GARDE (a.garde@anhf.fr) 04.20.61.01.46

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 virtualisé (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%

Public

Professionnel des SI - Equipe SSI - Administrateur

Exercice

2024

Code de formation

4.08

Nature

AFR

Organisé par

Ascent Formation

Durée

N/C