Campagne de phishing

Référence : **SECPHISH** Durée : **1 jour** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Aucunes.

PROFIL DES STAGIAIRES

• Tout public.

OBJECTIFS

• Renforcer le maillon humain de protection contre risques induits par le phishing. • Se préparer à se défendre face au phishing.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Qu'est ce que le phishing

• C'est un e-mail usurpant l'identité d'une personne physique ou morale pour tromper le destinataire
• Il invite généralement à se rendre sur un site Internet malveillant mais peut aussi pousser à effectuer une opération sensible illégitime comme vous demander vos identifiants

Simuler une campagne de phishing

Les étapes

• Définition des objectifs, du scénario, des messages (mail, faux portail, message de sensibilisation)
• Cadrage de l'opération, des communications, de la dimension sociale et validation via un pilote
• Lancement de la campagne et suivi
• Recueil des réactions, synthèse, réunion de clôture

Les perspectives

• Campagnes régulières et variées (scénarios, populations,…) et évaluation de la progression
• Déclenchement de séances de sensibilisation & démonstrations sur mesures
• Accompagnement dans la lutte contre le phishing (protection, détection, chaine de réaction,…)

Les informations issues des campagnes

• Type de la campagne (format, message,...)
• Résultats (nombre de clics sur les liens, ouverture de pièces jointes, etc.)

Les livrables

• Une base de statistiques anonymes (analyses par centre de profits, par site, … selon le cadrage de la campagne)
• Les supports utilisés durant la campagne
• Une fiche permettant le recueil des évènements internes (helpdesk contacté, blocage mail, etc.)

- Une synthèse de l’opération directement exploitable reprenant les enjeux, les résultats, le comportement utilisateur, les réponses opérationnelles et les enseignements

Accompagnement

Sensibilisation

- Réaliser une campagne d’exercices de phishing pour améliorer les reflexes des populations et adapter les efforts de communications

Detection

- Observer et challenger le dispositif de détection des incidents de sécurité, sur les plans techniques et organisationnels !

Crise

- Dans un exercice plus global, apporter une couche «cyber» dans les exercices de gestion de crise avec un scénario plausible

Réponse

- Réagir efficacement et avec sang-froid pour limiter les dégâts et apporter les informations attendues

Stratégie d'amélioration

- Campagne initiale : état des lieux
- Campagne enrichie : observation du traitement de l'incident
- Campagne enrichie : Exercice gestion crise cyber