Fiche Pédagogique

CyberSecurité - Sensibilisation

Organisation

Durée : 1 heure

Mode d'organisation : Présentiel

Contenu pédagogique

Description

Chaque session de formation débute par un tour de table permettant de :

- Vérifier, si nécessaire, les prérequis des participants.
- Rappeler les objectifs pédagogiques ainsi que les compétences visées.
- Identifier les connaissances et compétences déjà maîtrisées par les participants au regard des objectifs de la formation, et adapter le contenu si besoin.
- Recueillir les attentes particulières des participants afin d'ajuster au mieux le déroulé de la session.

Ce programme de formation en cybersécurité aborde des thématiques critiques liées à la protection des environnements industriels. La formation est structurée en plusieurs modules, avec une approche pédagogique classique complétée par une **séquence en réalité virtuelle (VR)**.

Cette partie immersive permet aux participants de se plonger dans des scénarios concrets, tels que la gestion de tentatives de phishing, l'utilisation de mots de passe sécurisés et l'adoption de bonnes pratiques en cybersécurité.

Public visé

Cette formation cible les professionnels du secteur industriel, notamment les responsables de production, ingénieurs, techniciens et opérateurs. **Les participants doivent comprendre les enjeux de la cybersécurité et de la protection des données en production.**

Elle s'adresse aussi aux employés administratifs et équipes de sécurité souhaitant améliorer leurs compétences en détection et prévention des attaques de phishing. **Chaque membre de l'organisation doit être conscient des risques liés à la cybersécurité.**

Objectifs pédagogiques

Cette formation vise à sensibiliser les participants aux enjeux de la cybersécurité dans un contexte industriel. Les objectifs pédagogiques incluent :

- Comprendre la nature et les conséquences des attaques de phishing.
- Développer des compétences pour identifier et éviter les tentatives de phishing.
- Apprendre à gérer les mots de passe de manière sécurisée.
- Acquérir des réflexes de cybersécurité pour protéger les données et les systèmes de production.

À l'issue de la formation, les participants devraient être en mesure de reconnaître les alertes de phishing, de protéger leurs accès avec des mots de passe robustes et de mettre en œuvre des pratiques de sécurité quotidienne dans leur environnement de travail.

Prérequis

Aucun pré-requis spécifique n'est nécessaire pour suivre cette formation.

Modalités pédagogiques

Les modalités pédagogiques de cette formation sont basées sur une approche immersive et interactive, utilisant la réalité virtuelle pour simuler des scénarios réalistes. Les participants seront plongés dans des environnements de travail familiers où ils devront prendre des décisions critiques face à des situations de cybersécurité.

Les sessions incluent des éléments tels que :

- Des mises en situation interactives où les participants doivent réagir à des attaques simulées.
- Des analyses de cas réels pour illustrer les conséquences des erreurs de cybersécurité.
- Des ateliers pratiques pour créer des mots de passe forts et utiliser des outils de gestion de mots de passe.

Cette approche favorise un apprentissage actif et engageant, permettant aux participants de développer des compétences pratiques qu'ils peuvent appliquer immédiatement dans leur environnement professionnel.

Moyens et supports pédagogiques

Les ressources pédagogiques mises à disposition des stagiaires comprennent :

- Une plateforme de réalité virtuelle permettant une immersion totale dans des scénarios de cybersécurité.
- Des supports de cours numériques avec des infographies et des vidéos explicatives sur les bonnes pratiques de cybersécurité.
- Des guides pratiques pour la création de mots de passe et des mesures de sécurité à adopter.
- Un accès à un gestionnaire de mots de passe sécurisé, tel que KeePass, qui sera présenté durant la formation.

Ces supports sont conçus pour renforcer l'apprentissage et fournir aux participants des outils qu'ils pourront utiliser au quotidien.

Le support de présentation est diffusé durant la session.

Modalités d'évaluation et de suivi

Sous le contrôle du formateur/intervenant, l'évaluation des compétences visées est effectuée tout au long de la formation à travers différents moyens et outils, notamment des auto-évaluations, des mises en situation, des exercices pratiques, des jeux de rôle. L'expertise et l'expérience du formateur/intervenant permettent d'apprécier l'atteinte des objectifs visés.

A la fin de formation, le formateur/intervenant valide les compétences dans son outil de gestion et informe le service formation des résultats constatés. Ce dernier délivre un Certificat de réalisation mentionnant l'acquisition des compétences visées. Si l'acquisition d'une compétence ; ou plusieurs, est partielle ou non acquise, le Certificat de réalisation le mentionne. Le Certificat de réalisation, signé par le responsable de l'organisme de formation, est adressé au participant. Le participant, s'il le souhaite, peut le retourner signé.

Les outils utilisés pour l'appréciation de l'atteinte des compétences visées d'un participant peuvent être des auto-évaluations, des mises en situation, des exercices pratiques, des jeux de rôle, des quiz, des QCM, des auto-évaluations. Les outils sont précisés et détaillés dans la fiche pédagogique et/ou le déroulé pédagogique et/ou le support de formation.