**Organisme de formation** : ENDKOO, 4 Rue de la charité 69002 LYON, France sous le numéro SIRET 83475061400028. Enregistré sous le n° de déclaration d'activité :84691626269

ENDKOO›

| | |
|---|---|
| Nom de la formation: | Formation Social Engineering DEBUTANT 3 jours |
| | |
| Résumé de la formation: | Cette formation de 3 jours vise à fournir aux participants une compréhension approfondie des différents types de Social Engineering, des techniques utilisées par les cybercriminels, ainsi que des mesures de prévention et de réaction efficaces pour se protéger contre ces attaques. Les participants auront l'occasion de participer à des exercices pratiques et des analyses de cas réels pour renforcer leurs compétences en matière de sécurité informatique. |
| | |
| Matériel : | Les participants devront apporter leur propre ordinateur portable pour les exercices pratiques. Le reste des matériels de formation seront fournis par l'organisateur. |
| | |
| Pour qui : | Cette formation s'adresse aux professionnels de la sécurité informatique, aux responsables de la sécurité des systèmes d'information, aux employés de soutien informatique et à toute personne souhaitant améliorer ses connaissances en matière de sécurité informatique. |
| | |
| Enjeu : | Les attaques de Social Engineering sont de plus en plus courantes et peuvent causer des dommages considérables à une entreprise. Il est donc crucial de comprendre les techniques utilisées par les cybercriminels et de savoir comment se protéger contre ces attaques. |
| | |
| Prérequis : | Aucun prérequis n'est nécessaire, cette formation est destinée à tous les niveaux. Etre disposé à apprendre de nouveaux concepts et de nouvelles technologies. |
| | |
| Objectifs : | Comprendre les différents types de Social Engineering et les méthodes utilisées par les cybercriminels pour obtenir des informations sensibles.<br>Acquérir les compétences pour identifier les signaux d'alerte et les moyens de se protéger contre les attaques de phishing, de spear phishing, de vishing et de smishing.<br>Apprendre les différentes techniques d'infiltration sociale, d'ingénierie sociale et de persuasion sociale et savoir les identifier.<br>Élaborer un plan de prévention des attaques de Social Engineering pour une entreprise.<br>Savoir réagir efficacement à une attaque de Social Engineering.<br>Récapituler les connaissances acquises durant la formation et recevoir un certificat de formation.<br>Comprendre les différentes mesures de prévention contre les attaques de Social Engineering.<br>Apprendre à utiliser des outils et des stratégies pour se protéger contre les attaques de Social Engineering.<br>Comprendre les risques liés aux réseaux sociaux et comment les gérer efficacement.<br>Apprendre à identifier les comportements à risque et à adopter des pratiques de sécurité efficaces pour protéger les informations sensibles.<br>Comprendre les principales lois et réglementations en matière de sécurité informatique et comment les appliquer dans une entreprise.<br>Échanger des expériences et des idées avec les autres participants pour renforcer les compétences en matière de sécurité informatique. |
| | |
| Durée : | 3 jours (21 heures) |
| | |

**Organisme de formation** : ENDKOO, 4 Rue de la charité 69002 LYON, France sous le numéro SIRET 83475061400028. Enregistré sous le n° de déclaration d'activité :84691626269

ENDKOO›

| | |
|---|---|
| Points forts et méthodes : | La formation est conçue pour être pratique et interactive, avec des exercices pratiques pour tester les compétences acquises. Les participants auront également l'occasion de mettre en pratique les compétences acquises dans un environnement de groupe. Le formateur est spécialisé dans le numérique depuis 2003. Méthodologie avec théorie à 50% et pratique à 50% (exercices en lignes) |
| | |
| Modalités : | Formation à distance uniquement via Microsoft Teams |
| | |
| Délais d'accès : | Formation intra entreprise – Délais à négocier avec l'entreprise dont inférieur à 2 mois |
| | |
| Support pédagogique : | Un support pédagogique et une palette d'exercice sera remis à chaque participant |
| | |
| Les modalités d'évaluations des acquis : | En début et en fin de formation, les stagiaires h/f réalisent un test de positionnement (auto évaluation) via GoogleForms de leurs connaissances et compétences en liens avec les objectifs de la formation. L'écart entre les 2 évaluations permet de mesurer leurs acquis. |
| | |
| Accessibilité aux personnes handicapées : | Le support de formation est disponible en format numérique, il est accessible aux personnes handicapées en utilisant des outils d'accessibilité. |
| | |
| Les modalités d'évaluations de la satisfaction et suivi de la prestation | Dans le cadre de notre démarche qualité, toutes nos formations font l'objet d'une évaluation « à chaud » (en fin de formation) et « à froid » (4 mois après la fin de la formation) par stagiaire h/f. Une feuille d'émargement sera signée par demie journée pour chaque stagiaire ainsi que pour le formateur qui justifiera la présence des participants. |
| | |
| Tarifs : | 2500€HT |
| | |
| Programme de formation: | Jour 1 : Introduction au Social Engineering |
| | |
| | Thématique 1 : Définition et types de Social Engineering (1h) |
| | But : Comprendre les différents types de Social Engineering et les méthodes utilisées par les cybercriminels pour obtenir des informations sensibles. |
| | Exercice : Analyse de cas réels de Social Engineering pour identifier les techniques utilisées et les vulnérabilités exploitées. |
| | Thématique 2 : Étude de cas : Phishing et Spear Phishing (2h) |
| | But : Comprendre les différences entre le phishing et le spear phishing et les moyens de se protéger contre ces attaques. |
| | Exercice : Simulation d'une attaque de phishing pour identifier les signaux d'alerte et les moyens de se protéger contre ces attaques. |
| | Thématique 3 : Étude de cas : Vishing et Smishing (2h) |
| | But : Comprendre les différences entre le vishing et le smishing et les moyens de se protéger contre ces attaques. |

| | |
|---|---|
| | Exercice : Simulation d'une attaque de vishing pour identifier les signaux d'alerte et les moyens de se protéger contre ces attaques. |
| | |
| | Jour 2 : Techniques de Social Engineering |
| | |
| | Thématique 1 : Techniques d'infiltration sociale (2h) |
| | But : Comprendre les différentes techniques utilisées pour obtenir des informations sensibles par la manipulation des individus. |
| | Exercice : Analyse de cas réels d'infiltration sociale pour identifier les techniques utilisées et les vulnérabilités exploitées. |
| | Thématique 2 : Techniques d'ingénierie sociale (2h) |
| | But : Comprendre les différentes techniques utilisées pour obtenir des informations sensibles par la manipulation de la confiance. |
| | Exercice : Analyse de cas réels d'ingénierie sociale pour identifier les techniques utilisées et les vulnérabilités exploitées. |
| | Thématique 3 : Techniques de persuasion sociale (2h) |
| | But : Comprendre les différentes techniques utilisées pour obtenir des informations sensibles par la persuasion. |
| | Exercice : Analyse de cas réels de persuasion sociale pour identifier les techniques utilisées et les vulnérabilités exploitées. |
| | |
| | Jour 3 : Prévention et réaction aux attaques de Social Engineering |
| | |
| | Thématique 1 : Prévention des attaques de Social Engineering (2h) |
| | But : Comprendre les différentes mesures de prévention contre les attaques de Social Engineering. |
| | Exercice : Élaboration d'un plan de prévention des attaques de Social Engineering pour une entreprise. |
| | Thématique 2 : Réaction aux attaques de Social Engineering (2h) |
| | But : Comprendre les différentes mesures de réaction contre les attaques de Social Engineering. |
| | Exercice : Simulation d'une réaction à une attaque de Social Engineering pour identifier les bonnes pratiques à suivre. |
| | Thématique 3 :Conclusion et remise des certificats (1h) |
| | But : Récapitulation des connaissances acquises durant la formation et remise des certificats de formation pour les stagiaires. |
| | Exercice : Évaluation finale des compétences des stagiaires en matière de prévention et de réaction aux attaques de Social Engineering. |
| | |