CYBERSÉCURITÉ : STOPPEZ LES CYBER ATTAQUES EN DIRECT !

Vivez l'expérience du wargame pour déjouer le plan des hackers

2 JOURS, 14 HEURES

TRANSFORMATION NUMÉRIQUE

CODE : GNU26

Objectifs de la formation

Appréhender le cadre général de la directive Européenne NIS2 et les principes de cyber sécurité

Tester les processus définis dans le cadre de la cellule de crise

Développer son agilité face à un imprévu

Parmi nos formateurs

- **REMEUR Patrice**
  Expert cybersécurité : Directeur de l'Innovation & DPO,

Public concernés

- DSI, DPO, Direction juridique, toute direction opérationnelle impliquée dans la protection des données d'entreprise

Critères d'admission

- Cette formation entre dans le champ d'application des dispositions relatives à la formation professionnelle continue car considérée comme une action d'adaptation et de développement des compétences des salariés.

Prérequis

- Apporter un ordinateur portable

A tout moment, la sirène d'alarme indiquant une cyberattaque peut se déclencher. Vous ne saurez pas quand ni comment. Votre équipe et vous devrez alors contrer l'attaque (plus ou moins complexe) et assurer la continuité de la formation. C'est parti !!

Dans une société de plus en plus connectée, les entreprises doivent prendre des mesures prioritaires pour protéger leur système d'informations contre les menaces cyber qui les visent.

Les données récentes sont très préoccupantes : 69 % des cyberattaques ont ciblé des entreprises, 20 % des collectivités territoriales, et 11 % des établissements de santé en 2023. Face à cette réalité inquiétante, il est impératif de renforcer les défenses en matière de cybersécurité. Dans ce contexte, la directive NIS2, parue au Journal Officiel de l'Union européenne en décembre 2022, offre une opportunité sans précédent. Cette réglementation ambitieuse élargit les objectifs et le champ d'application de NIS1, visant à renforcer la sécurité des systèmes informatiques et à prévenir plus efficacement les incidents cyber.

Nous vous proposons une immersion formative innovante, fondée sur un serious game et des ateliers interactifs. Vous plongerez dans une simulation d'attaque réelle. Cette approche vous permettra de mieux comprendre les obligations découlant de cette directive et de mieux gérer une crise cyber.

Introduction : Mode opératoire du wargame

- Mettre en place d'un plan de réponse
- Renforcer la résilience aux cybermenaces et améliorer la réactivité en cas d'incident cyber selon les recommandations de l'ANSSI
- Définir les actions immédiates à entreprendre dès la découverte d'une cyberattaque
- Piloter la crise : Organiser et coordonner une équipe de réponse à l'incident
- Élaborer une stratégie de communication claire

Scénarios cyberattaques

- Les stagiaires sont confrontés à une série de scénarios réalistes de cyberattaques. Dès l'alarme déclenchée, ils doivent prendre des décisions stratégiques pour protéger les systèmes, les données, l'organisation, e-réputation et de communiquer en temps réel avec les parties prenantes.

Cerner le cadre général de la directive Européenne NIS2 et autres réglementations

- Appréhender le cadre réglementaire de la directive NIS2
- Tour d'horizon des principales exigences de la directive NIS2
- Décrypter la feuille de route des réglementations
- Comment mettre en place des mesures de sécurité pour protéger les réseaux et systèmes d'information contre les cybermenaces
- Quelles sont les sanctions en cas de non-respect des textes ?
- La mise en conformité NIS2 : où en est-on ?

ATELIER Discussions sur l'état actuel du niveau de sécurité informatique

Rappeler le cadre théorique de la cybersécurité

- Principes de la cybersécurité
- Quels sont les impacts d'une cyberattaque ?
- Identifier les risques et les vulnérabilités : évaluer les menaces potentielles et les points faibles dans les systèmes d'information
- Mettre en place un plan de réponse efficace
- Former ses équipes aux risques cyber : quels sont les protocoles d'intervention en cas d'incident
- S'approprier les actions clés à mener en cas de cyberattaque

ATELIER à travers une application interactive, les stagiaires définissent les risques cyber

Constituer sa cellule de crise

- Choisir les acteurs à impliquer dans l'équipe
- Définir les rôles et responsabilité de chaque partie prenante
- Coordonner la lutte contre les cyberattaques via des processus de sécurité éprouvés

ATELIER Travail en plénière sur la constitution de la cellule de crise

Se préparer et mettre en place un plan de continuité et de reprise d'activités (PCA/PRA)

- Définir le plan de continuité et de reprise d'activités
- Identifier les processus critiques et les ressources essentielles nécessaires pour assurer la continuité des activités après une cyberattaque
- Quels sont les éléments clés d'un PCA/PRA
- Intégrer les procédures de sauvegarde, de restauration des données et de récupération des systèmes
- Identifier les rôles et les responsabilités des acteurs
- Personnaliser le PCA/PRA en fonction des besoins spécifiques de l'organisation
- Faire le point sur l'importance de tester le PCA/PRA
- Présenter les différentes méthodes de test
- Analyser des résultats des tests
- Assurer la mise à jour du PCA/PRA

ATELIER Les stagiaires travaillent sur leur feuille de route pour la préparation et des dispositifs et la mise en conformité NIS2 et autres réglementations

Evaluation des acquis et débriefing final

Dates

Modalités pédagogiques, d'évaluation et techniques

- **Modalités pédagogiques:**

Pour les formations synchrones-présentiel ou classes virtuelles (formations à distance, en direct), les stages sont limités, dans la mesure du possible, à une douzaine de participants, et cherchent à respecter un équilibre entre théorie et pratique. Chaque fois que cela est possible et pertinent, des études de cas, des mises en pratique ou en situation, des exercices sont proposées aux stagiaires, permettant ainsi de valider les acquis au cours de la formation. Les stagiaires peuvent interagir avec le formateur ou les autres participants tout au long de la formation, y compris sur les classes virtuelles durant lesquelles le formateur, comme en présentiel peut distribuer des documents tout au long de la formation via la plateforme. Un questionnaire préalable dit 'questionnaire pédagogique' est envoyé aux participants pour recueillir leurs besoins et attentes spécifiques. Il est transmis aux intervenant(e)s avant la formation, leur permettant de s'adapter aux publics. Pour les formations en E-learning (formations à distance, asynchrones), le stagiaire peut suivre la formation à son rythme, quand il le souhaite. L'expérience alterne des vidéos de contenu et des activités pédagogiques de type quizz permettant de tester et de valider ses acquis tout au long du parcours. Des fiches mémos reprenant l'essentiel de la formation sont téléchargeables. La présence d'un forum de discussion permet un accompagnement pédagogique personnalisé. Un quizz de validation des acquis clôture chaque parcours. Enfin, le blended-learning est un parcours alternant présentiel, classes virtuelles et/ou e-learning.

- **Modalités d'évaluation:**

Toute formation se clôture par une évaluation à chaud de la satisfaction du stagiaire sur le déroulement, l'organisation et les activités pédagogiques de la formation. Les intervenant(e)s évaluent également la session. La validation des acquis se fait en contrôle continu tout au long des parcours, via les exercices proposés. Sur certaines formations, une validation formelle des acquis peut se faire via un examen ou un QCM en fin de parcours. Une auto-évaluation des acquis pré et post formation est effectuée en ligne afin de permettre à chaque participant de mesurer sa progression à l'issue de la formation. Une évaluation à froid systématique sera effectuée à 6 mois et 12 mois pour s'assurer de l'ancrage des acquis et du transfert de compétences en situation professionnelle, soit par téléphone soit par questionnaire en ligne.

- **Modalités techniques FOAD:**

Les parcours sont accessibles depuis un simple lien web, envoyé par Email aux stagiaires. L'accès au module de E-learning se fait via la plateforme 360Learning. La durée d'accès au module se déclenche à partir de la réception de l'invitation de connexion. L'accès aux classes virtuelles se fait via la plateforme Teams. Le(a) stagiaire reçoit une invitation en amont de la session lui permettant de se connecter via un lien. Pour une bonne utilisation des fonctionnalités multimédia, vous devez disposer d'un poste informatique équipé d'une carte son et d'un dispositif vous permettant d'écouter du son (enceintes ou casque). En ce qui concerne la classe virtuelle, d'un microphone (éventuellement intégré au casque audio ou à la webcam), et éventuellement d'une webcam qui permettra aux autres participants et au formateur de vous voir. En cas de difficulté technique, le(a) stagiaire pourra contacter la hotline au 01 70 72 25 81, entre 9h et 17h ou par mail au logistiqueformations@infopro-digital.com et la prise en compte de la demande se fera dans les 48h.