MCP008 - Identifiez, analysez et déjouez les biais cognitifs en sécurité numérique

Mis à jour le 01-06-2025

Code : MCP008

Certification de type Experte

Enseignement de type mixte

0 crédits

Responsabilité nationale : EPN05 - Informatique / Stefano SECCI

Contact national :

Cnam Bretagne - PSDR3C

2 rue Camille Guérin
22440 Ploufragan
0972311312

psdr3c@Lecnam.net

Présentation

Prérequis

Cette micro-certification ne nécessite pas de prérequis académiques, ni aucune connaissance technique.

Objectifs pédagogiques

Cette micro-certification s'adresse à tous les acteurs en entreprise quelque qu'en soit la taille, confrontés aux cybermenaces et qui veulent protéger leur organisation face aux menaces numériques.

Cela s'adresse aux cadres dirigeants ou intermédiaires, aux responsables informatiques ou DSI, aux responsables RH ou de formation, aux RSE et RNE, aux référents cybersécurité, aux responsables qualité ou risques ou à toute personne en situation de décision ou d'influence dans les pratiques numériques de l'organisation de l'entreprise.

Compétences

- Reconnaître les biais cognitifs courants affectant les décisions en cybersécurité.
- Évaluer l'impact des erreurs humaines sur la sécurité numérique.
- Analyser des exemples réels d'incidents de sécurité liés aux biais cognitifs.
- Communiquer et sensibiliser les employés aux risques humains en cybersécurité.
- Identifier les comportements à risque.
- Implémenter des actions préventives pour renforcer la sécurité.

Promouvoir une culture organisationnelle axée sur la sécurité et la vigilance

Programme

Contenu

Les objectifs pédagogiques de cette micro-certification visent à renforcer la compréhension et la gestion des risques liés au facteur humain dans la cybersécurité en entreprise :

- les participants apprendront à **identifier et à comprendre les biais cognitifs** courants qui influencent les décisions et comportements en matière de sécurité numérique. Cette connaissance permettra de reconnaître comment ces biais peuvent augmenter la vulnérabilité aux cyberattaques.
- ensuite, la formation se concentrera sur **l'analyse des impacts spécifiques de ces biais cognitifs** sur les pratiques de sécurité au sein des entreprises. Les participants étudieront des cas concrets et des exemples de failles de sécurité dues à des erreurs humaines pour mieux comprendre les dynamiques en jeu.
- enfin, la formation **proposera des stratégies et des techniques pour atténuer les effets des biais cognitifs**. Les participants développeront des compétences pratiques pour promouvoir une culture organisationnelle axée sur la sécurité numérique et la vigilance collective autour des biais cognitifs.

Ces objectifs permettront aux apprenants de maîtriser les éléments de théorie et de pratiques réflexes leur permettant en tant que décideurs ou responsables de mieux anticiper et gérer les risques humains, contribuant ainsi à une culture de sécurité numérique plus solide, efficace et ancrée dans la culture d'entreprise.

Dans un monde professionnel où les cybermenaces sont de plus en plus sophistiquées, le facteur humain demeure l'un des maillons les plus vulnérables (entre 60% et 90% des cyberattaques réussies, comme évoquée dans la recommandation 2024 de Gartner incitant à prendre plus en compte le facteur humain en cybersécurité). Les erreurs de jugement, les automatismes ou encore la surcharge cognitive peuvent compromettre des systèmes autrement bien protégés sur le plan technique. Cette formation intervient donc dans une logique de cybersécurité cognitive, à la croisée des sciences comportementales et de la gestion des risques numériques.

Cette micro-certification trouve pleinement sa place :

- dans des plans de sensibilisation à la cybersécurité pour cadres et managers, notamment dans les entreprises de toute taille.
- en complément des formations techniques, pour renforcer la prise en compte du facteur humain dans les politiques de sécurité de l'information.
- dans une stratégie de cyberrésilience globale, visant à intégrer la psychologie cognitive dans la gestion proactive des risques.

dans le cadre d'une montée en compétence ciblée, notamment en préparation ou accompagnement d'un audit de cybersécurité, d'une démarche RGPD ou ISO 27001 ou encore NYS2.

Modalités de validation

- Examen final

Description des modalités de validation

Réussite du test final

(minimum de 50% des points requis)