

Cours 2 : Introduction au CyberFundamentals Framework (CyFun) et ethical hacking

Cycle de webinaires - Renforcez la cybersécurité de votre organisation pour contrer les cyberattaques : réglementation et mise en pratique

Webinaire | Vendredi 10 octobre 2025 | Belgique | Valéry Vander Geeten, Jeoffrey Vigneron

Description

Plongez au cœur de **la cybersécurité et de la conformité avec la nouvelle Directive NIS2** grâce à ce cycle de formations complet, réparti en trois webinaires interactifs. Accompagné d'experts chevronnés, vous explorerez les **fondations de la sécurité numérique, les cadres de conformité et de bonnes pratiques, ainsi que l'implémentation technique concrète** pour assurer la résilience de votre organisation.

L'objectif de ce deuxième cours est d'apprendre les bases du CyberFundamentals Framework et de découvrir les principes et la méthodologie de l'ethical hacking.

Pourquoi participer ?

- **Approche opérationnelle** : Familiarisez-vous avec le CyberFundamentals Framework (CyFun), inspiré de standards internationaux (NIST CSF, ISO/IEC 27001, CIS Controls, IEC 62443), ainsi qu'avec les conditions d'application de l'ethical hacking
- **Adapté à votre contexte** : Qu'il s'agisse d'une PME, d'une organisation essentielle ou d'un prestataire de services, ce cycle vous guidera dans la mise en conformité légale, technique et organisationnelle
- **Garantir la résilience et la réputation de votre entité** : Anticipez les risques, réduisez votre surface d'attaque et protégez vos données sensibles pour maintenir la confiance de vos clients, de vos partenaires et des autorités de régulation (ex. Centre pour la Cybersécurité Belgique – CCB)

Ce que vous obtiendrez :

- Des bases solides pour mettre en œuvre le CyberFundamentals Framework (CyFun)
- Des méthodes éprouvées pour planifier, exécuter et maintenir une stratégie de sécurité pérenne

Rejoignez-nous et faites de la cybersécurité un atout stratégique !

Programme

1. Introduction

- 1.1. Objectifs du cours
 - Apprendre les bases du CyberFundamentals Framework.
 - Découvrir les principes et la méthodologie de l'ethical hacking.
- 1.2. Contexte
 - Importance de l'approche proactive en cybersécurité.
 - Lien entre CyFun, conformité NIS2 et prévention des cyberattaques.

2. Présentation du CyberFundamentals Framework

- 2.1. Vue d'ensemble
Cadre basé sur NIST CSF, ISO 27001, CIS Controls, IEC 62443.
Objectifs : renforcer la sécurité des petites entités.
- 2.2. Niveau "Small"
Mesures minimales : Sauvegardes régulières - Gestion des accès - Patchs logiciels - Sensibilisation des employés.
- 2.3. Documentation et outils disponibles
Utilisation de Safeonweb@Work - Guides pratiques pour petites entités.
Exemple : Mise en œuvre des sauvegardes et patchs dans une PME fictive.

3. Ethical hacking : Concepts et méthodologies

- 3.1. Définition et objectifs
Différence entre hacking éthique et hacking malveillant. Rôle des pentests dans la cybersécurité.
- 3.2. Méthodologies
Étapes : reconnaissance, scan, exploitation, rapport.
Normes internationales : OSSTMM, OWASP.
- 3.3. Techniques courantes
Tests de vulnérabilité (scan des ports, reconnaissance réseau) - Attaques simulées (ex. injection SQL).

Exemple : Démonstration d'un test de vulnérabilité simple sur une plateforme de test dédiée.

4. Aspects juridiques et éthiques de l'ethical hacking

- 4.1. Réglementation
Nécessité d'une autorisation préalable - Responsabilités des hackers éthiques.
- 4.2. Sanctions pour un hacking non autorisé
Études de cas : conséquences d'un hacking illégal.
- 4.3. Intégration dans un cadre légal
Clauses dans les contrats avec des prestataires de pentests.

5. Conclusion et Q&A

Synthèse des points abordés et Session interactive pour répondre aux questions.

Orateurs

- **Valéry Vander Geeten** : Juriste du CCB (Centre for Cybersecurity Belgium)
- **Jeoffrey Vigneron** : Avocat au barreau de Bruxelles, coding lawyer, co-fondateur du cabinet Lawgitech

Informations pratiques

Dates et horaire

Vendredi 10 octobre 2025

De 9h30 à 12h30

Cycle de webinaires - Renforcez la cybersécurité de votre organisation pour contrer les cyberattaques : réglementation et mise en pratique

Vendredi 3 octobre : Cours 1 : Introduction à la cybersécurité et à la Directive NIS2

Vendredi 10 octobre : Cours 2 : Introduction au CyberFundamentals Framework (CyFun) et ethical hacking

Mercredi 15 octobre : Cours 3 : Implémentation technique et cas pratiques

Lieu

En ligne

Vous pourrez suivre la formation en direct sur le Web. Vous recevrez les détails de connexion à l'avance par e-mail.

Attention ! L'adresse e-mail par laquelle vous procédez à l'inscription sera l'adresse à laquelle le lien vers le webinaire sera envoyé. Si vous vous inscrivez par l'intermédiaire d'une autre personne (secrétaire, collègue...), cette personne devra vous faire suivre le lien en question pour que vous puissiez vous connecter et suivre la formation. Les inscriptions qui arrivent moins d'une heure avant le début du webinaire ne seront malheureusement pas prises en compte.

Prix

230 € TTC - Participation à un cours

594 € TTC - Participation aux trois cours

Public visé

Ce cycle est proposé à tous les professionnels cherchant à renforcer leurs compétences en matière de cybersécurité, de conformité légale et de protection des systèmes d'informations et des données afin d'assurer la sécurité de leur organisation.

Le cycle peut également être tout autant bénéfique pour les avocats, notaires, huissiers de justice, les juristes d'entreprises, CISO, DPO, RSSI ... qui sont chargés de traiter des questions technico-juridiques liées à la sécurité des données et à la conformité réglementaire et soucieux de se prémunir de toute cyberattaque pour leur organisation.

Formation permanente

Une demande d'agrément a été introduite auprès de AVOCATS.BE, avocats.lu, la Chambre nationales des notaires, l'IJE et SAM-TES.

Ce webinaire peut faire l'objet d'une prime Liberform si vous remplissez les conditions.

Renseignements complémentaires

Larcier-Intersentia

formations@larcier-intersentia.com

Numéro gratuit : 0800 39 067