Cours 3 : Implémentation technique et cas pratiques

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

Webinaire | Mercredi 15 octobre 2025 | Belgique | Sandra Denghien, 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 troisième cours est de fournir des outils et méthodologies pratiques pour une implémentation réussie et tester la résilience organisationnelle à travers des exercices concrets.

Pourquoi participer ?

- **Mise en pratique immédiate** : Grâce à des études de cas, des exercices de simulation d'incidents et des checklists issues de l'expérience terrain, vous serez en mesure de concevoir et déployer des solutions concrètes, tout en vous appuyant sur des outils de référence
- **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 méthodes éprouvées pour planifier, exécuter et maintenir une stratégie de sécurité pérenne
- Un accompagnement pratique vers une conformité durable

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

Cycle de webinaires - Renforcez la cybersécurité de votre organisation pour contrer les cyberattaques : règlementation 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

Programme

1. Introduction et objectifs du Cours

- 1.1. Contexte :
  Importance de l'implémentation technique pour la conformité à NIS2 et CYfun. Challenges spécifiques liés à la mise en œuvre technique.
- 1.2. Objectifs :
  Fournir des outils et méthodologies pratiques pour une implémentation réussie et tester la résilience organisationnelle à travers des exercices concrets.

2. Planification technique de l'implémentation

- 2.1. Évaluation de la situation actuelle :
  - Analyse des actifs critiques : Identification des systèmes, données, et infrastructures prioritaires.
  - Évaluation des risques : Exemples d'outils : analyse avec un scanner de vulnérabilités (ex. Nessus) - Modèle d'évaluation des risques basé sur les critères de NIS2.
- 2.2. Choix des outils et technologies :
  - Solutions de gestion des accès (IAM) - Outils de sauvegarde et de reprise après sinistre - Solutions de détection des menaces (SIEM, EDR).
  - Exemple : Présentation d'un cas fictif avec le choix d'un outil SIEM pour une PME.
- 2.3. Planification détaillée avec checklists :
  - Élaboration d'un plan d'implémentation : Étapes clés : priorisation, ressources nécessaires, délais.
  - Exemples de checklists pour garantir la conformité aux exigences techniques de CYfun. Exemple pratique : Discussion en groupe pour compléter une checklist basée sur un scénario.

3. Gestion des incidents et réponse

- 3.1. Procédures de détection et de réponse :
  - Mise en place de protocoles :
    Détection : configuration d'alertes (via un SIEM).
    Réponse : exemple d'un plan de réponse structuré pour un ransomware.
  - Coordination avec les autorités : Processus de notification d'incidents en Belgique via Safeonweb@Work.
- 3.2. Exercices de simulation d'incidents :
  - Objectifs des simulations : Tester la réactivité et identifier les failles dans les procédures existantes.
  - Scénario pratique : Exercice basé sur une attaque par phishing ciblée (simulation) - Analyse post-exercice : points forts et améliorations nécessaires.

4. Retours d'expérience et ajustements

- 4.1. Analyse post-implémentation :
  Audit interne : évaluation des mesures mises en place et Identification des lacunes persistantes.
- 4.2. Amélioration continue :
  Processus de retour d'expérience (RETEX) :
  - Organisation d'ateliers internes pour ajuster les processus.
  - Utilisation des rapports d'incidents pour prioriser les actions futures. Exemple : Discussion d'un RETEX fictif après une simulation d'attaque.
- 4.3. Maintien de la conformité :
  Planification des audits réguliers et documentation mise à jour en fonction des nouvelles exigences ou menaces.

5. Conclusion et Q&A

- 5.1. Synthèse des points clés :
  Importance de l'évaluation initiale et rôle des exercices et ajustements dans l'amélioration continue.
- 5.2. Discussion interactive :
  Questions des participants et partage d'expériences et bonnes pratiques.

Lire plus

Orateurs

Orateurs

- **Sandra Denghien** : Program Manager chez Asfalys
- **Jeoffrey Vigneron** : Avocat au barreau de Bruxelles, coding lawyer, co-fondateur du cabinet Lawgitech

Informations pratiques

Dates et horaire

Mercredi 15 octobre 2025

De 9h30 à 12h30

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 et l'IJE.

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