C O M M U N I Q U E D E P R E S S E

La 5è édition du Forum International de la Cybersécurité dévoile son programme de conférences.

L'événement dédié aux experts de la sécurité (RSSI, DSI…) et aux décideurs non-spécialistes (chef d'entreprise, DRH, directeur juridique...), issus des secteurs publics et privés se déroulera à Lille Grand Palais les 28 et 29 janvier prochains.

Paris, le 14 novembre 2012 - Organisé conjointement par la Direction Générale de la Gendarmerie Nationale, le Conseil Régional du Nord-Pas-de-Calais et CEIS, société de conseil en stratégie et en management des risques, le FIC 2013 abordera la cybersécurité sous un angle stratégique, en mettant l'accent sur les enjeux géopolitiques, sociologiques, juridiques, managériaux, technologiques liés à la sécurité et à la confiance dans le cyberespace tout en tenant compte des aspects opérationnels.

La 5è édition du FIC, événement européen, dédié aux professionnels issus des sphères publiques (ministères, administrations, collectivités territoriales et établissements publics) et privées (grands groupes, PME-PMI, opérateurs d'infrastructures vitales, pôles de compétitivité) se déroulera à Lille Grand Palais, les 28 et 29 janvier 2013.

Le Forum International de la Cybersécurité 2013 aura l'honneur et le plaisir d'accueillir M. Manuel Valls, Ministre de l'Intérieur, pour la cérémonie officielle, le lundi 28 janvier 2013. L'allocution du Ministre sera suivie de la première séance plénière consacrée au continuum défense-sécurité dans le cyberespace, avec notamment l'intervention de *Patrick Pailloux, directeur général de l'ANSSI.*

Les conférences et tables rondes, regroupées sous trois axes principaux : Gouvernements & administrations – Entreprises (opérateurs d'infrastructures vitales, grandes entreprises, PME) et Collectivités territoriales et Etablissements publics permettront aux participants de s'informer et d'échanger autour des problématiques et des enjeux liés à la cybersécurité :

-> Gouvernements et administrations
- Géopolitique et gouvernance du cyberespace
- Souveraineté des données et cloud computing
- Nouvelles formes de conflictualités dans le cyberespace
- Technologies de l'information et de la communication et ordre public
- OTAN, UE, quelles alliances en matière de cybersécurité et de cyberdéfense ?
- Droit du cyberespace : entre réactivité et proactivité de la loi
- Cyber terrorisme : mythes et réalités
- La modernisation des moyens de prévention et d'investigation dédiés au traitement des infractions criminelles
- Regards croisés sur les stratégies de cyberdéfense

- Partenariat public-privé : comment créer des espaces de confiance ?
- Panorama des cyber-stratégies étatiques

-> Entreprises (opérateurs d'infrastructures vitales, grandes entreprises, PME)
- Panorama de la cybercriminalité (CLUSIF)
- Cyberespace et contrefaçon
- Cyber délinquance ou cybercriminalité organisée : quels sont les profils des cybercriminels ?
- BYOD, réseaux sociaux… les nouveaux risques en entreprise
- SCADAs : menaces cybercriminelles sur les transports
- Quels parcours pour les particuliers et les entreprises victimes d'actes cybercriminels ?
- Monétique et commerce en ligne : quelle sécurité pour les nouveaux moyens de paiement ?
- DRH et cybersécurité : quelles obligations pour l'employeur et le salarié ?
- SCADAs : quelles menaces sur les approvisionnements énergétiques ?
- Usurpation d'identité : quels risques ? Quelles solutions ?
- Existe t-il un marché pour la cybersécurité ?
- Les Advanced Persistent Threat (APTs) : vraie menace ou coup marketing ?
- Comment protéger les smart grids ?
- De l'activisme à « l'hacktivisme »
- Outsourcing : aggravation du risque ou faux problème ?
- Le recrutement, la formation et l'entrainement des professionnels de cybersécurité
- Sécurité des télécommunications
- Cybercriminalité bancaire et financière
- E-réputation : quels risques pour les particuliers et les entreprises ?
- Nouvelles technologies, nouveaux usages, nouveaux risques
- Développement informatique sécurisé : comment intégrer la sécurité en amont ?
- La résilience Internet
- Plans de continuité et reprise d'activité
- Quelle politique de sécurité pour des systèmes d'information adopter en entreprise ?
- Lutte informatique défensive et Security Operation Center : vers une cybersécurité dynamique
- La management des professionnels de la cybersécurité : quelle place pour les « hackers » en entreprise ?
- La cybercriminalité, un risque assurable ?

-> Collectivités territoriales et établissements publics
- Cybersécurité et continuité du service public
- Smart cities : quelle sécurité pour les villes de demain ?
- Dématérialisation et archivage électronique
- Intelligence économique : un atout pour les collectivités territoriales
- Cybersécurité et santé
- Quelle politique pour le système d'information des collectivités ?
- Open data, libération des données publiques et sécurité
- Construire et sécuriser un réseau d'informations stratégiques

Huit parcours thématiques : *Panorama des menaces cybercriminelles – Stratégie de cybersécurité – Ressources humaines – E-santé – Lutte anti-cybercriminalité – Infrastructures sensibles – Sécurité des systèmes d'information – E-administration* permettront aux participants de profiter pleinement du FIC 2013 avec un circuit personnalisé et adapté à leurs centres d'intérêt.

A propos du Forum International de la Cybersécurité

Inscrit dans le programme européen de Stokholm de 2012-2015, le renforcement de la lutte contre la cybercriminalité est devenu une des priorités de l'Union européenne. Convaincue de la nécessité d'être partie prenante de cet effort, la Gendarmerie Nationale a lancé en 2007, la première édition du Forum International de la Cybersécurité.

L'édition 2013 du FIC (www.fic2013.com) est organisée conjointement par la Direction Générale de la Gendarmerie Nationale, le Conseil Régional du Nord-Pas-de-Calais et CEIS.

Organisé à Lille, ville pionnière en matière de réflexions sur la lutte contre la cybercriminalité, le FIC est rapidement devenu un rendez-vous majeur pour les acteurs de la sécurité du cyberespace compte tenu de son envergure internationale et de l'importance des thématiques abordées.

En marge du FIC, l'Observatoire FIC, co-animé par la Gendarmerie Nationale, le Conseil Régional Nord-Pas de Calais et CEIS, est une plateforme de réflexion et d'échanges animée tout au long de l'année. Il propose une veille permanente sur toutes les thématiques développées lors des conférences et des tables rondes.

Pour suivre l'actualité du FIC : @FIC2013 /fic2013

Contact Presse – Agence : Cymbioz – Laëtitia Berché
laetitia.berche@cymbioz.com
06 14 48 02 95