

Eurosec'2007 : dernier appel à communication / last call for paper

APPEL A COMMUNICATION - EUROSEC'2007. Intervenez à la plus importante conférence européenne sur la Sécurité des Systèmes d'Information.

1- Qu'est-ce que le Forum EUROSEC ?

Le Forum EUROSEC est la Conférence Européenne de référence sur la sécurité des systèmes d'information. EUROSEC'2007 se déroulera à Paris au CAP 15 du 23 au 25 mai 2007. Pour la 18ème année consécutive, près de 400 participants issus de tous domaines d'activités confronteront leurs expériences et attentes sur la Sécurité des Systèmes d'Information, sur chacun des volets : managérial, fonctionnel, humain, technique et scientifique. EUROSEC s'adresse en particulier aux : Directeurs d'entreprises et d'administrations, DRH, contrôleurs généraux, . Directeurs des Systèmes d'Information, responsables des télécoms, d'exploitation ou d'études, chefs de projet, concepteurs et développeurs d'applications, Risk managers, responsables de la sécurité des systèmes d'information, consultants et auditeurs. Nous sollicitons des présentations de qualité dans tous les domaines de la Sécurité des Systèmes d'Information et de la protection des informations, comme en témoigne la liste de thèmes ci-dessous. Les propositions d'intervention portant sur des orientations nouvelles ou prospectives seront examinées avec une attention particulière. Les propositions qui concernent des offres de service ou de solution et qui apparaissent destinées à la promotion d'un produit ne sont pas acceptées, sauf si elles présentent une analyse sérieuse et complète d'un service basé sur un retour d'expérience pratique. Pour tous les intervenants pourront assister gratuitement à toutes les présentations le jour de leur intervention.

2- Le programme EUROSEC'2007.
L'édition 2007 reprend les principes structurants qui font le succès d'Eurosec depuis plus de 18 ans : un Comité de Programme indépendant, un programme sur trois jours, des sessions plénières et sessions parallèles "à la carte". Deux axes seront plus particulièrement développés pour l'édition 2007 : Une priorité absolue donnée aux retours d'expérience précis et outillés ou aux visions stratégiques averties, Une emphase particulière sur l'international, notamment avec l'implication d'acteurs majeurs de la sécurité en Europe et aux USA. Tous les supports d'intervention seront disponibles à la fois en anglais et en français. Vos interventions feront de nouveau le succès d'EUROSEC'2007. Elles doivent contenir la présentation d'une vision, démarche, technologie ou d'une solution de sécurité répondant à une problématique d'entreprise ou d'administration et illustrée d'une expérience pratique de mise en oeuvre. Des propositions d'intervention sous forme d'atelier pratique ou de démonstrations techniques sont bienvenues. Nous attendons des propositions sur l'ensemble des thématiques de la protection des informations et des systèmes qui la traitent, la liste suivante n'étant pas exhaustive : 1. Evolution du contexte de la sécurité. Le développement de l'intelligence économique. Politique de l'IE, enjeux, retours d'expérience et approches, Le rôle du RSSI : obligation ou opportunité ? Les nouvelles menaces et incidents. Mobilité, convergence, grid computing, instant messaging, dématérialisation, RFID, . Fuite d'informations, social engineering, phishing / pharming, évolution de la menace virale, spam, adware, spyware, . Evolution en matière de cyber-terrorisme, dispositifs mis en oeuvre, notamment par les opérateurs et Fournisseurs d'Accès à Internet (FAI). Le cadre législatif, réglementaire et normatif. Protection des données personnelles et vie privée, retour d'expérience de CIL, signature électronique, chiffrement, cadre juridique des blogs, . Comment se retrouver dans l'explosion des contextes réglementaires (SOX, Bâle II, SOLVENCY, HIPAA, PRIS.) et normatifs (ISO 27000, ISO 15408, PAS 56, .) ? Responsabilités juridiques - délégation de responsabilités. Sécurité de l'externalisation et externalisation de la sécurité. Les problématiques des PME/PMI. 2. Gouvernance de la sécurité et risk management. Le juste prix de la sécurité. Lien entre gouvernance IT et gouvernance sécurité. Organisation de la sécurité. Convergence ou collaboration entre risk management / sécurité du SI / sécurité physique / sécurité des biens et des personnes - télésurveillance / audit / contrôles opérationnels / intelligence économique / . Evolution du RSSI : rôle, positionnement, outils, moyens, . Risk management. Obligations et enjeux, organisation et démarches, Développement de la « culture du risque », transferts et financement des risques. Cadre de la sécurité. Evolution du cadre interne de sécurité (politiques, chartes, .), Vers une protection temporaire des informations et des données . Communication sécurité. La sécurité, un moteur pour les activités et un atout commercial ? Certification : est-elle incontournable pour le professionnel de la sécurité ? Sensibilisation à la sécurité. La sécurité avec moyens et expertises minimales [Orientation PME] 3. Continuité des activités. Evolution de la menace et suivi de la sinistralité, Poussées normatives, Evolution du Responsable PCA : rôle, positionnement, outils, moyens, . Gestion de crise, Rôle et limites des assureurs, Comment optimiser le maintien et les tests des plans ? 4. Protection des infrastructures et gestion opérationnelle de la sécurité. Evolution des solutions techniques. Téléphonie et voix sur IP, mobilité et sécurité (postes nomades, smart phones, .), chiffrement, biométrie, supervision de la sécurité / corrélation d'événements, . Offres « packagées » : forces et écueils, Protection des données. Gestion opérationnelle de la sécurité. Patch management - antivirus et anti spam, supervision de la sécurité, Pilotage opérationnel des indicateurs de sécurité - quelle vision temps réelle de la sécurité ? Quels outils de test de conformité des postes ? Archivage et stockage, cyber-squatting, traçabilité des

opérations et objets, . Industrialisation et externalisation de services de sécurité. SOC : quel positionnement ? Sécurité offshore ? Retours d'expérience de crise / incident. 5. Les contrôles et la conformité. Bonnes pratiques de mise en conformité et de contrôle Investigations : méthode et outils Suivi et contrôle de la sécurité - Tableaux de bord - . Contrôle effectif des prestataires (fournisseurs de ressources critiques, infogérance). 3- Soumissions des communications.

Les langues officielles de la conférence sont le français et l'anglais, les articles et les présentations d'auteurs doivent être transmis dans les deux langues. Chaque proposition doit comprendre : le nom de l'auteur, son affiliation et adresse (postale et électronique), une biographie de l'intervenant avec référence, entre 5 et 10 slides PowerPoint présentant le sommaire de l'intervention et les points forts. La soumission des propositions se fait par email à l'adresse suivante : eurosec2007@devoteam.com . Le Comité de Programme attachera une grande importance au caractère innovant et original, à la qualité technique et à la rigueur des propositions. Les propositions de communication doivent parvenir au plus tard le 17 novembre 2006. Pour toute information complémentaire, contacter : Philippine de Reilhac ou Hervé Morizot Tel : +33 (0)1 41 49 48 48 Mobile : +33 (0)6 70 45 77 58 Fax : +33 (0)1 41 49 55 66 5- Calendrier.

17 novembre 2006 : date limite de réception des propositions de communication, 15 décembre 2006 : notification aux auteurs, 8 mars 2007 : date limite de réception des textes définitifs, 23, 24 et 25 mai 2007 : Forum EUROSEC'2007. Devoteam novembre 2006

http://www.mag-securs.com/article.php3?id_article=6455