

PARIS

Espace Saint-Martin
3 avril 2012

GS Days



Le carrefour
de la sécurité des
Systèmes d'Information
exclusivement en français
pour réunir : les RSSI, DSI,
Administrateurs
Réseaux et Sécurité,
Experts Sécurité...

Les Journées Francophones de la Sécurité de l'Information



4^e édition

Un cycle de conférences techniques
organisationnelles et juridiques



SPONSOR PLATINIUM

Partenaires Institutionnels :

Délégation générale du Québec - ANSI (Tunisie)

Partenaires associations :

AFCDP - ARCSI - CLUSIB - CLUSIF - FedISA
Forum ATENA - MEDEF 92 - LE CLUB 27001
OSSIR - OWASP

Partenaires Presse :

Regard sur l'IE - Programmez !
Solutions & Logiciels - Security Vibes - SecuObs

Comité de programme :

Global Security Mag, Olivier Guérin du CLUSIF,
Hervé Schauer, HSC, Philippe Humeau, NBS
System, Paul Such, SCRT, Olivier Revenu,
EdelWeb, et Maître Diane Mullenex, Cabinet
Ichay et Mullenex, Eric Doyen, Generali,
et Emmanuel Garnier, Systalians

Comité de pilotage :

Global Security Mag, Jean-Marc Laloy
de l'ARCSI, Francis Bruckmann, France Telecom
Orange, David Dupré, CommonIT,
Jean-Nicolas Piotrowski, ITrust,
Jean-François Beuze, Sifarès

Nos autres sponsors

Sponsor Gold



Sponsor Silver



Sponsors



www.gsdays.fr

Renseignements : Marc Jacob - SIMP - 17 avenue Marcelin Berthelot - 92320 Châtillon
Tél. : +33 (0)1 40 92 05 55 - Fax. : +33 (0)1 46 56 20 91 - marc.jacob@globalsecuritymag.com

4^{ème} édition GS DAYS - 3 AVRIL 2012 - PARIS

APPEL A COMMUNICATION

Thème : « **La Sécurité par la pratique** »

Sony, RSA, Barracuda, le Ministère des finances... ont été piratés par de profondes défaillances à la fois de déploiement d'outils de sécurité, mais aussi dans le domaine de l'organisation. Ces attaques souvent très connues ont pu aboutir avec les résultats que l'on sait par manque de pragmatisme dans les entreprises. Il est aujourd'hui nécessaire de revenir aux fondamentaux de la sécurité en tirant les enseignements des actes commis par les pirates informatiques. Ainsi, pour cette édition, il s'agira de proposer des sujets (conférences, démonstrations...) sur des thèmes techniques, organisationnels et juridiques pour montrer les dangers de ces attaques et apprendre à les parer.

QUELQUES EXEMPLES DE THÈMES

► Les thèmes techniques :

Les attaques aujourd'hui sur :

- Les Web Services et les navigateurs : XSS, CSRF, etc.
- Les technologies sans-fil : Wifi, RFID, etc.
- Les terminaux mobiles
- Les bases de données...

L'évolution des moyens de protection :

- Sur le Web : WAF, etc.
- Test d'intrusion : les bonnes pratiques...
- Quels outils et quels paramètres adaptés : IDS/IPS, firewall...

► Les thèmes organisationnels :

- Les hommes (ingénierie sociale)
- La guerre de l'information et l'hacktivisme
- Les nouveaux usages du SI : les réseaux sociaux et les applications en ligne
- Pourquoi et comment sécuriser l'information ?

► Les thèmes juridiques :

- Le SI : Droit, devoir et obligations
- Comment protéger son entreprise des risques liés à l'usage des réseaux sociaux en entreprise

- La fraude et les transactions bancaires : la compliance est-elle l'unique moyen d'y remédier ?
- Le droit peut-il quelque chose en cas de fuite d'information ? ...

Les présentations attendues devront proposer une vision technique ou scientifique. Les présentations à fin commerciale ou la présentation d'un produit ne seront pas acceptées. Cependant, les propositions présentant une analyse technique de la sécurité d'un produit, un comparatif fondé sur des tests scientifiques, et les retours d'expérience avec un aspect technologique, seront examinées avec attention.

Le format des conférences sera de 50 minutes dont 5 à 10 minutes de questions.

Le comité de Programme est assuré par Global Security Mag, Olivier Guérin, CLUSIF, Hervé Schauer, HSC, Philippe Humeau, NBS System, Paul Such, SCRT, Olivier Revenu, EdelWeb, Maître Diane Mullenex, Cabinet Ichay et Mullenex, Eric Doyen, Generali, et Emmanuel Garnier, Systalians.

Ce comité a pour objectif la sélection des conférenciers et du contenu du Colloque.

Processus de soumission

► **Première étape** : Les propositions de communication (1 à 2 pages) parviendront au comité de programme avant le 15 décembre 2011, par mail à l'adresse marc.jacob@globalsecuritamag.com. Le format recommandé est pdf. Figureront le titre de la communication et sa catégorie (Technique, Organisationnelle, Juridique ou Démonstration), les nom et prénom du ou des auteurs et leur affiliation, l'adresse de courrier électronique de l'un des auteurs, un résumé (15 lignes environ) et une liste de mots clés. Les auteurs seront prévenus de l'acceptation ou du rejet le 10 janvier 2012.

► **Seconde étape** : Les auteurs fourniront pour le 12 mars 2012 une version définitive de la communication, de 3 à 10 pages, par mail à l'adresse marc.jacob@globalsecuritamag.com. Ces versions définitives tiendront compte des remarques du comité de programme. Elles seront fournies de préférence au format Word. Les communications seront rédigées uniquement en français. Les meilleures communications, désignées par le comité de programme, pourront faire l'objet d'une publication sur le site de Global Security Mag ou dans le magazine trimestriel.

Pour adresser vos soumissions : marc.jacob@globalsecuritamag.com

DATES IMPORTANTES

Date limite de soumission :

15 décembre 2011 uniquement par mail
marc.jacob@globalsecuritamag.com

Notification aux auteurs : 10 janvier 2012

Article définitif : 12 mars 2012

Conférence : 3 avril 2012