

**11<sup>ème</sup> GS DAYS – 2 AVRIL 2019 – PARIS 3<sup>ème</sup>**  
**APPEL A COMMUNICATION**

« Convaincre sans contraindre »\*, telle est la devise de cet événement dédié à la sécurité de l'information. L'objectif des [GS Days, Journées francophones de la sécurité](#), est d'établir le dialogue entre le monde de la technique (administrateurs, experts sécurité), les RSSI, DSI et les décideurs. Ce colloque, exclusivement en français, proposera, dans un même espace, plusieurs cycles de conférences et de démonstrations d'exploitation de failles informatiques, sous un angle technique, organisationnel et juridique.



\* Citation de Jean-Marc Laloy, ARCSI

La 11<sup>ème</sup> édition des GS Days, qui se tiendra le 2 AVRIL 2019 à l'Espace Saint-Martin - Paris 3<sup>ème</sup>, s'articulera principalement autour du thème : « Comment faire de l'humain le maillon fort de la sécurité ? »

L'humain est un élément essentiel pour la sécurité, économique comme numérique. Qu'il soit utilisateur, manager, développeur, administrateur, expert..., l'humain se trouve au cœur des dispositifs de sécurité mis en place en entreprises, et des bonnes pratiques à appliquer au quotidien. Toutefois, l'humain, de par ses comportements et ses actions, peut aussi s'avérer un vecteur de menaces pour son entreprise. Lors de cette édition des GS Days, l'accent sera à la fois mis sur les risques inhérents au facteur humain, mais aussi l'importance de la sensibilisation et de l'acculturation à la cybersécurité et à la sécurité économique. L'objectif sera également de mieux comprendre le comportement humain et de déterminer comment en faire un levier pour améliorer le niveau de sécurité globale en entreprise, comme ailleurs.

**Quelques exemples de thèmes, à titre indicatif :**

• **L'humain, vecteur d'attaque et/ou vecteur de défense ?**

- ▶ Ingénierie sociale, Phishing, Spear Phishing & Co.
- ▶ Repérer et endiguer la menace interne & externe
- ▶ L'humain en tant que levier et maillon fort pour la sécurité

• **De la sensibilisation à l'acculturation**

- ▶ Comment aborder la sécurité au sein des directions numériques et sensibiliser l'ensemble des collaborateurs (utilisateur, manager, admin, développeur...) ?
- ▶ De quelle manière passer de la sensibilisation à l'acculturation ?
- ▶ Formation & Éducation cyber : quelles démarches privilégier, avec quels acteurs ?
- ▶ Sciences comportementales & cybersécurité

• **Quelle confiance faut-il accorder à l'humain ?**

- ▶ Le besoin d'en connaître : limitation d'accès aux informations, gestion des habilitations et des comptes à privilèges
- ▶ Quelles mesures l'employeur peut-il prendre pour se prémunir des risques (chartes, clause de confidentialité dans les contrats de travail, enquête sur la bonne moralité des employés...) ?

• **Sécurité économique**

- ▶ Espionnage & cyberespionnage
- ▶ Crochetage de serrures et autres techniques d'intrusion...
- ▶ Protection bâtementaire & gestion des accès

- **Cyberattaques & cybersécurité**

- ▶ Vulnérabilités et menaces récentes
- ▶ DevOps & sécurité
- ▶ Comment évaluer le degré de sensibilité du patrimoine informationnel d'une entreprise ? De quelle manière attirer l'attention de l'utilisateur sur cette sensibilité ?
- ▶ Développement sécurisé & security by design

**Le format des conférences sera de 50 minutes, dont 10 minutes de questions. Celui des démonstrations sera de 15 minutes.**

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 comité de Programme est assuré par Global Security Mag, Luména Duluc, CLUSIF, Hervé Schauer, HS2, Philippe Humeau, Paul Such, Hacknowledge, Olivier Revenu, ON-X, Me Diane Mullenex/Annabelle Richard, Cabinet Pinsent Masons, Eric Doyen, CESIN, Emmanuel Garnier, Club 27001, Diane Rambaldini, ISSA France, Jean-Marc Laloy et Francis Bruckmann, ARCSI, Christophe Labourdette, OSSIR. Ce comité a pour objectif la sélection des conférenciers et du contenu du Colloque.

**Dates importantes :**

- ▶ Date limite de soumission : **20 JANVIER 2019** uniquement par mail : [marc.jacob@globalsecuritymag.com](mailto:marc.jacob@globalsecuritymag.com)
- ▶ Notification aux auteurs : 5 février 2019
- ▶ Présentation définitive : 15 mars 2019
- ▶ Conférence : 2 avril 2019

**Processus de soumission**

- ▶ Première étape : Les propositions de communication (1 à 2 pages) parviendront au comité de programme **avant le 20 JANVIER 2019** par mail à l'adresse [marc.jacob@globalsecuritymag.com](mailto:marc.jacob@globalsecuritymag.com). Le format recommandé est PDF. Figurent le titre de la communication et sa catégorie (Technique, Organisationnelle, Juridique ou Démonstration), les nom(s) et prénom(s) 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 de leur proposition le 5 février 2019.

- ▶ Seconde étape : Les auteurs fourniront pour le 15 mars 2019 une version définitive de leur présentation par mail à l'adresse [marc.jacob@globalsecuritymag.com](mailto:marc.jacob@globalsecuritymag.com). Ces versions définitives tiendront compte des remarques du comité de programme. Elles seront fournies de préférence au format PDF ou PPT. 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@globalsecuritymag.com](mailto:marc.jacob@globalsecuritymag.com)

**Date et lieu :**

2 avril 2019 – 8h30 - 18h30

Espace Saint-Martin - 199 bis, rue Saint-Martin - 75003 Paris

[www.gsdays.fr](http://www.gsdays.fr)