



Gestion des incidents

Paris, 16 juin 2011

Evénement organisé en partenariat avec :

Orange Business Services

TelecityGroup



**Business
Services**





Le CLUSIF : *agir pour la sécurité de l'information*

Association **sans but lucratif** (création au début des années 80)

> 600 membres (pour 50% fournisseurs et prestataires de produits et/ou services, pour 50% RSSI, DSI, FSSI, managers...)

Partage de l'information

Echanges homologues-experts, savoir-faire collectif, fonds documentaire

Valoriser son positionnement

Retours d'expérience, visibilité créée,
Annuaire (Formations, Membres Offreurs)



*Logo pour vos actions commerciales,
votre site web*

Anticiper les tendances

Le « réseau », faire connaître ses attentes auprès des offreurs

Promouvoir la sécurité

Adhérer...

Groupes de travail en progression

Les groupes actifs en 2011

- Documentation de MEHARI™
- EFIS (Evaluation Financière des Incidents de Sécurité)
- Fiches de sécurité pour la micro-informatique
- Gestion de clés cryptographiques
- Gestion des incidents
- Glossaire
- Guide d'audit de sécurité physique
- PA-DSS
- Panorama de la cybercriminalité
- PCI-DSS
- Principes, mécanismes et bases de connaissances de Méhari
- Sécurité des Applications Web - Suite
- Sécurité des Outils de Communication
- Série 27000
- Virtualisation et Sécurité

... et de nouveaux GT

- 👉 **MEHARI-PRO** : fournir une méthodologie appropriée aux PME/PMI pour l'analyse des risques concernant leur organisation
- 👉 **Malware** : mise à jour du document « virus », extension à d'autres formes de programmes « malveillants »
- 👉 **MIPS-2012**



Une collaboration à l'international,
des actions en région



CLUSI Côte d'Ivoire

Boite Postale 2409 Abidjan 25

Contact : M. KOUAKOU Clauba Jean de la Croix (Président)
Tel/Fax : (00225) 22 42 42 66
Secrétariat : contact@dusici.org
Web : <http://www.dusici.org/>.



Club de la Sécurité de l'Information Région Tahiti

Adresse physique : Immeuble SALMON Faa'a Pamatai - Tahiti - Polynésie Française
Adresse postale : B.P. 60123 - Hotuarea - 98704 Faa'a - Tahiti - Polynésie Française
Contact : Matthieu DRUILHE, clusir.tahiti@gmail.com, téléphone : +689 79 82 27
Site web : <http://www.dusif.asso.fr/clusir-tahiti/>



Club de la Sécurité des Systèmes d'Information du Languedoc-Roussillon

954, avenue Jean Mermoz
34000 MONTPELLIER
Contact : Christian FERRAND
Site web : www.clusir.info



Club de la Sécurité des Systèmes d'Information de la Région Midi Pyrénées

5/C INSA
Département de Génie Electrique et Informatique
135, Avenue de Rangueil
31077 TOULOUSE CEDEX 04
Contact : Laurent PELUD
Site web : www.clusir-mp.asso.fr



Club de la Sécurité des Systèmes d'Information de la Région Est

16, rue de Pont-à-Mousson
57000 METZ
Contact : Thierry RAMARD
Site web : www.clusir-est.fr



Club de la Sécurité des Systèmes d'Information de la Région Provence-Alpes-Côte-d'Azur

500, rue de Paradis
13008 MARSEILLE
Contact : Claude LELOUSTRE
Site web : <http://www.clusif.fr/clusir-paca/>



Club de la Sécurité des Systèmes d'Information de la Région Rhône-Alpes

SITIV
Passage de l'Avenir
69200 VENISSIEUX
Contact : Yvanick BOUCHET
Site web : www.clusir-rha.fr



Club de la Sécurité des Systèmes d'Information de la Région Nord Pas de Calais Picardie

CLUSIR InfoNord IES
RSSI
www.clusif.fr/clusir-npp/



Club de la Sécurité de l'Information de Poitou-Charentes

Technopôle Venise Verte
Rue Euclide
BP 8421
79024 NIORT cedex 9
Contact : Sébastien Gloria
Site web : <http://www.clusir-poi.fr/>



Club de la Sécurité de l'Information Région Aquitaine

s/c Philippe Marty (Vice-Président)
51 rue Manon Cormier
33000 Bordeaux
Contact : Marc Ferrigno



Surveiller les flux...

 [RSS/docs CLUSIF](#)

 [RSS/actus CLUSIF](#)

- Nouveaux GT
- Nouveaux documents :
« Gestion des Incidents »

... prochainement un RSS/CLUSIRs

... aujourd'hui, test de video-streaming :

Conférence “ Gestion des incidents ” [beta test]

Pour accéder au live, merci de saisir votre e-mail ci-dessous. Un jeton vous sera envoyé sur cette adresse e-mail, vous permettant d'accéder à la retransmission.

Votre e-mail :

LES DOSSIERS TECHNIQUES

Gestion des incidents de sécurité
du système d'information (SSI)

Mai 2011



Groupes de travail « Gestion des incidents »

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS
11 rue de Mogador - 75009 Paris
Tel. : +33 1 53 25 08 80 - Fax : +33 1 53 25 08 89
clusif@clusif.com.fr - www.clusif.com.fr

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les responsables successifs du groupe de travail :

Robert	BERGERON	<i>CAPGEMINI</i>
Witold	POLOCZANSKI	<i>CAPGEMINI</i>

Les contributeurs :

Michel	BERTIN	
David	BIZEUL	<i>SOCIETE GENERALE</i>
Annie	BUTEL	<i>BNP PARIBAS</i>
Philippe	LARUE	<i>CBP</i>
Sébastien	MAUPTIT	<i>SYSTALLANS</i>
Lionel	MOURER	<i>ESR CONSULTING</i>
Gérard	PETITIT	<i>GRAS SAVOYE</i>
Dominique	POURCELLIE	<i>CNAMTS</i>
Manuel	PRIEUR	<i>HP ENTERPRISE SERVICES</i>

Nous remercions aussi les nombreux adhérents du CLUSIF ayant participé à la relecture.

Le thème...

- **L'identification** des incidents de sécurité: quelle définition à l'incident de sécurité ? Comment passe-t-on de l'événement de sécurité à l'incident de sécurité ? Quels moyens d'identification ?
- **Quel outillage** technique et organisationnel ? Les outils techniques (SIM, SEM, SIEM...), les compétences humaines, la cellule d'urgence (CERT)...
- **Les traitements** d'un incident : quelles compétences ? Quelle organisation ? Sous quelle autorité ? Avec quel séquençement ? Quelles précautions respecter ?
- **Quel apport des cadres normatifs et juridiques** ? Le contexte ISO27001, les obligations de communiquer ou pas, les réglementations spécifiques et légales (PCIDSS, CNIL, données de santé...)
- Les conditions d'**établissement d'un bilan après la résolution** de l'incident et d'apprentissage (mesures mises en œuvre afin d'éviter sa répétition).

Agenda de session

➤ **Supervision de la sécurité : une approche MSSP**

M. David MAILLARD - Security Global Competence Center, TMS - **Alcatel-Lucent France**

david.maillard@alcatel-lucent.com

➤ **Traitement d'incidents et coopération avec des CERTs**

M. Olivier CALEFF - Responsable du CERT-DEVOTEAM - **DEVOTEAM B.U. Sécurité**

olivier.caleff@devoteam.com

➤ **Immersion dans un CERT d'entreprise**

M. David BIZEUL - Responsable CERT Société Générale - **Société Générale**

david.bizeul@socgen.com

➤ **La gestion des incidents par la technologie du SIEM**

M. Alexandre DEPRET-BIXIO - Regional Sales Manager - **HP ArcSight France**

alexandre.depret-bixio@hp.com