



David Bizeul – CERT Société Générale

Immersion dans un CERT® d'entreprise

16/06/2011



|

SOMMAIRE

|

Activités d'un CERT®

Entre la théorie...
... et la réalité

Incident de sécurité

Par la détection...
... le traitement ...
... et la communication

Cas concret

Synthèse

Quelles leçons ?
Quelles perspectives ?

Activités d'un CERT®

Entre la théorie...
... et la réalité

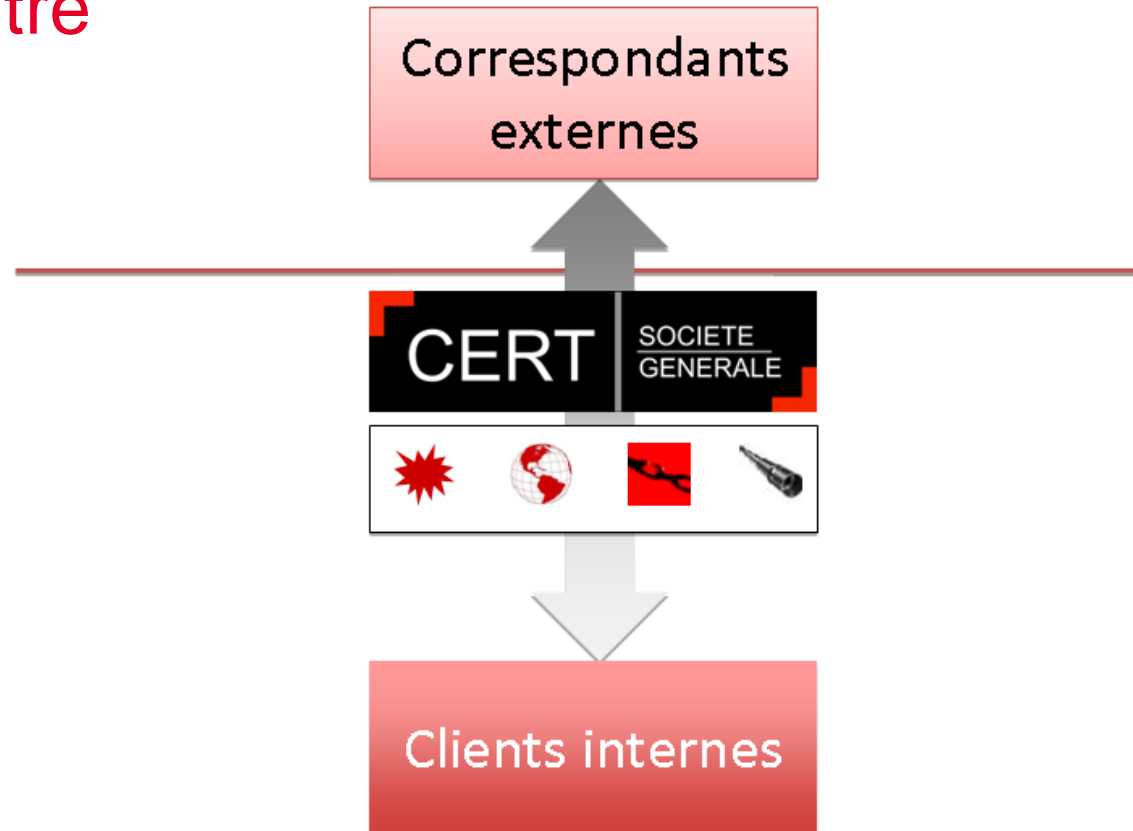
La théorie CERT





La réalité CERT




Périmètre



 Gestion d'incidents

 Lutte cybercriminalité

 Alertes vulnérabilités


 Veille technologique

Image perçue



Image réelle



Accessoires nécessaires



2 – Savoir traiter les incidents



1 – Veille techno

7 – Utiliser la manière forte si nécessaire



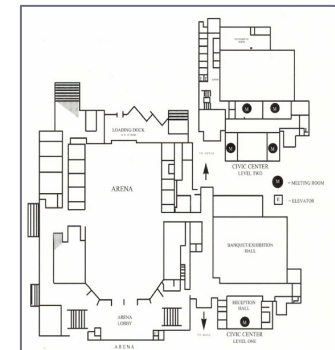
3 – Pouvoir se raccrocher à des éléments de poids

5 – Avoir des référentiels à jour



4 – Avoir les clés pour ouvrir les portes

6 – Pouvoir communiquer de manière autonome



||

Incidents de sécurité

Par la détection...
...le traitement...
... et la communication

Détection

► Technique

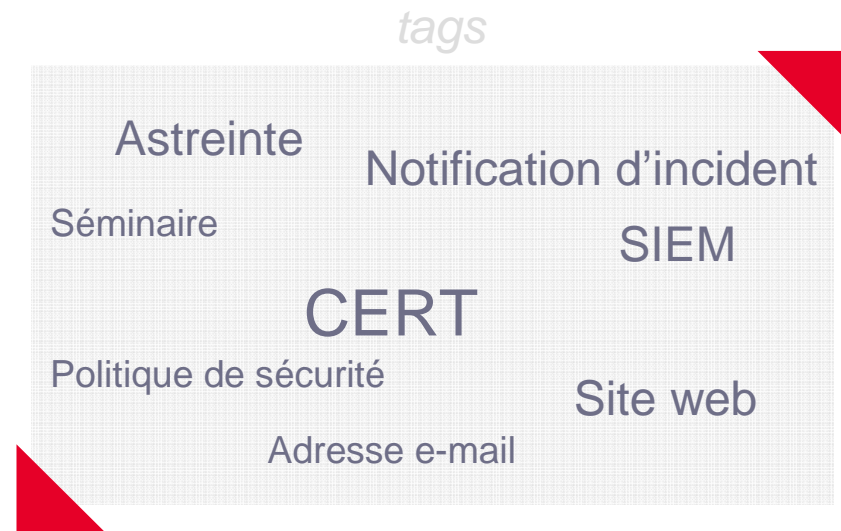
- Alertes de sécurité
- Inquiétude équipes opérationnelles

► Contacts

- Sensibilisation interne
- Succès passés

► Utilisateurs

- Visibilité publique
- Adresse email accessible et pérenne



Traitement

► Réponse immédiate

- **Priorité pour les incidents**
- **Pas de ségrégation**

► Valeur ajoutée

- **Expertise sur des domaines non maîtrisés**
- **Veille de qualité**

► Assistance de bout en bout

- **Travail collaboratif**
- **Ne pas laisser de zone de flou**



Communication

► Proximité

- **Toujours une réponse !**
- **Responsabilité de bout en bout**

► Point de centralisation

- **Sensibilisation basée sur la réalité**
- **Vue globale**

► Point d'entrée externe

- **Relai interne / externe**

tags



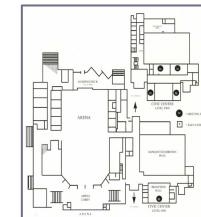
III

Cas concret

...

Vulnérabilité XSS

- ▶ Identification d'un XSS par un internaute et notification Twitter
- ▶ Réponse à l'internaute + relai en interne
- ▶ Suivi de la correction de la vulnérabilité + pentest
- ▶ Recadrage de la communication



IV

Synthèse

Quelles leçons?
Quelles perspectives ?

Quelles leçons ?

- 1** La confiance se crée dans le temps
- 2** Rassurant pour les victimes d'avoir un CERT à disposition
- 3** Structure adaptée pour les interactions internes / externes
- 4** Nécessité d'anticiper les incidents

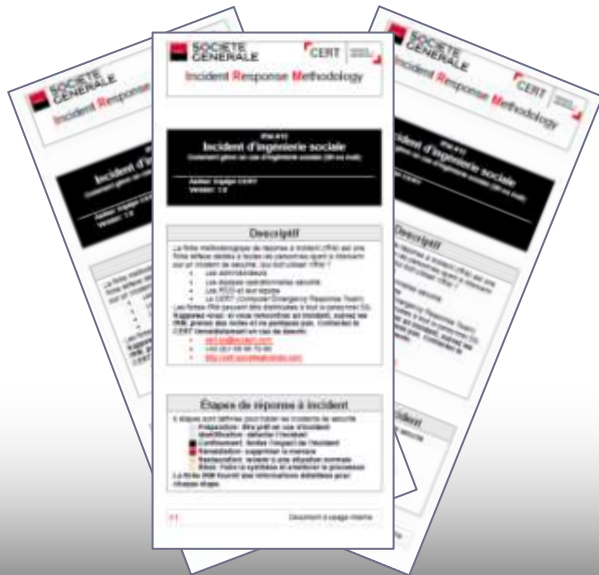
Quelles perspectives ?

1 Les incidents sont souvent en dehors des frontières de l'entreprise

2 La communication devient de plus en plus libérée

3 La réglementation pousse à la notification d'incident

4 Une veille globale et connectée à l'entreprise est nécessaire



Fiches de réponses à incident

► <http://cert.societegenerale.com/fr/publications.html>

Questions ?

CERT Société Générale

David Bizeul

► cert.sg@socgen.com

► 01 58 98 72 00

► <http://cert.societegenerale.com>

► david.bizeul@socgen.com