5 novembre 2013

Cloud, Big Data et sécurité

Conseils et solutions

solucom
management & IT consulting

Agenda

1. Enjeux sécurité du Cloud et du Big Data
2. Accompagner les projets
3. Quelques solutions innovantes
4. Quelle posture pour les décideurs sécurité ?

Deux enjeux majeurs pour la sécurité dans le Cloud / du Big Data

Enjeu n°1 : Sécurité à la contractualisation

Choisir un fournisseur et une solution adaptés au besoin et à « l'appétence aux risques » de l'entreprise

Enjeu n°2 : Sécurité dans le temps

S'assurer que la solution est correctement mise en œuvre et surveiller le niveau de sécurité au quotidien

Des outils dédiés existent pour évaluer ses risques de sécurité

Une démarche très classique : l'analyse de risque

Des outils spécifiques

Pour le Cloud :

- Guides de l'ANSSI, de la CNIL
- Analyse de risque de L'ENISA
- Cloud Controls Matrix

Encore peu de guides indépendants pour le Big Data…

In fine,
L'entreprise doit décider quels risques sont acceptables ou non pour elle !

Différents moyens de réponse

- **Contractuels**
  - Engagement du fournisseur
  - Assurances
- **Techniques**
  - Chiffrement de données
  - Sécurisation des systèmes, réseaux…
- **Juridiques**

Agenda

1. Enjeux sécurité du Cloud et du Big Data
2. Accompagner les projets
   - *2. 1 Cloud*
   - *2. 2 Big Data*
   - *2. 3 Maintenir la sécurité dans le temps*
3. Quelques solutions innovantes
4. Quelle posture pour les décideurs sécurité ?

Des outils existent pour appuyer la démarche Cloud

De nombreux documents de référence

- **ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)**

« Maîtriser les risques de l'infogérance »

- **ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information)**

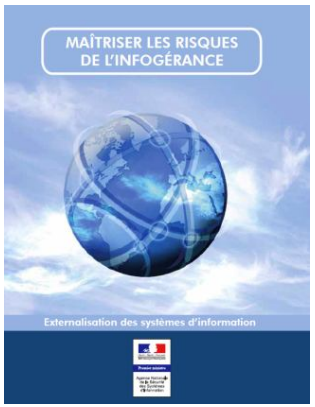
« Cloud computing : Benefits, risks and recommendations for information security »

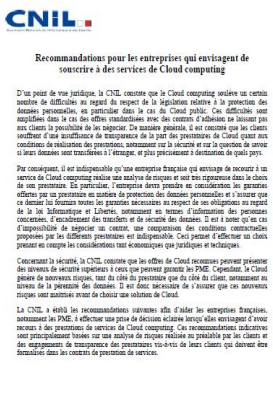
- **CNIL**

« Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing »

- **Syntec Numérique**

« Sécurité du Cloud computing » et « Guide contractuel SaaS »





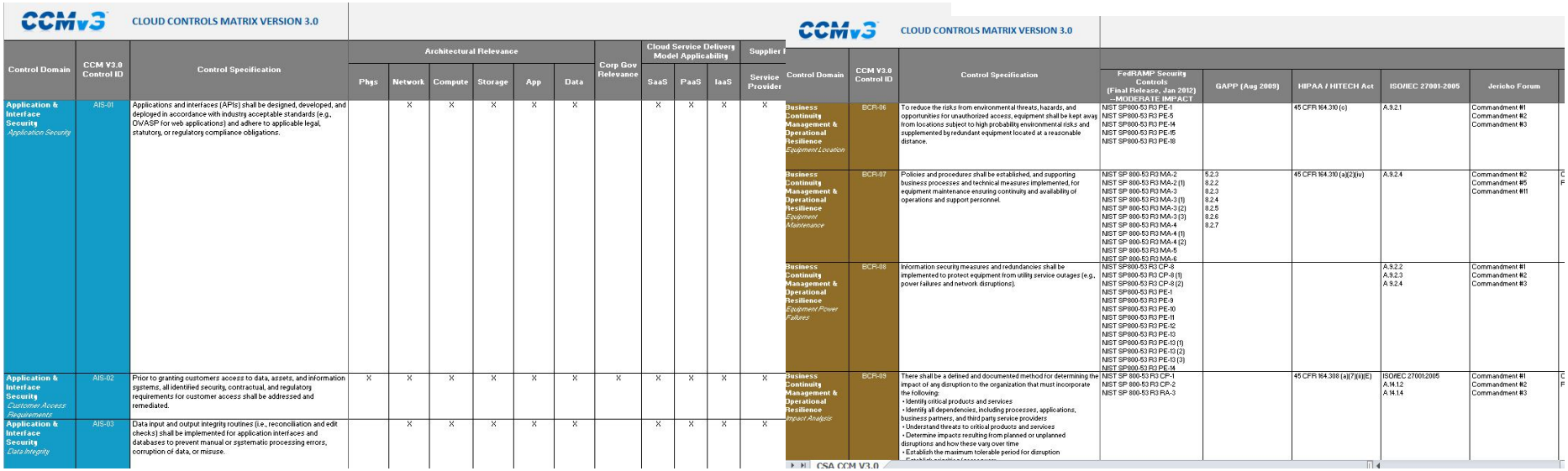
Des outils existent pour appuyer la démarche Cloud

La « Cloud Controls Matrix »

- **Tableau réalisé par la Cloud Security Alliance (CSA) : https://cloudsecurityalliance.org/research/ccm/**
- **Identification détaillée des risques dans un cadre Cloud**
- **Basé sur une démarche de réponse volontaire des acteurs**
- **11 thèmes couverts**

Conformité	Gouvernance des données	Sécurité des installations	Ressources humaines	Sécurité de l'information	Juridique
Gestion des opérations	Gestion du risque	Gestion des changements	Continuité de l'activité	Architectures de sécurité	

- **Donne les correspondances avec de nombreuses normes et réglementations**



Accompagner un projet Cloud

Des certifications dont peuvent se prévaloir les acteurs

ISO 27001

- Mise en place d'un système de management avec une revue annuelle des risques, le référentiel de mesures à respecter et les contrôles associés
- Audit sur site annuel par un organisme de certification

ISAE 3402 / SSAE 16

- Contrôle et certification de la mise en place d'un système de contrôle interne basé sur les risques
- Audit unitaire (type 1) ou sur 6 mois (type 2) par un cabinet d'audit

Données de santé

- Mise en place de mesures de sécurité spécifiques sur les données de santé
- Rédaction d'un dossier d'agrément et audit éventuel par la CNIL

PCI-DSS

- Mise en place de mesures pointues et techniques sur les données de type carte bancaire
- Audit sur site, tests techniques réguliers et certification annuelle par un QSA (PCI-Council)

Autres : ISO 22301 / 9001 / 20000

- Suivant les thèmes (continuité, qualité, services SI…) mise en place de système de management
- Audit sur site annuel par un organisme de certification

Un fédérateur pour toutes les certifications : ISO 27001

Système de management / Déclaration d'applicabilité

Agenda

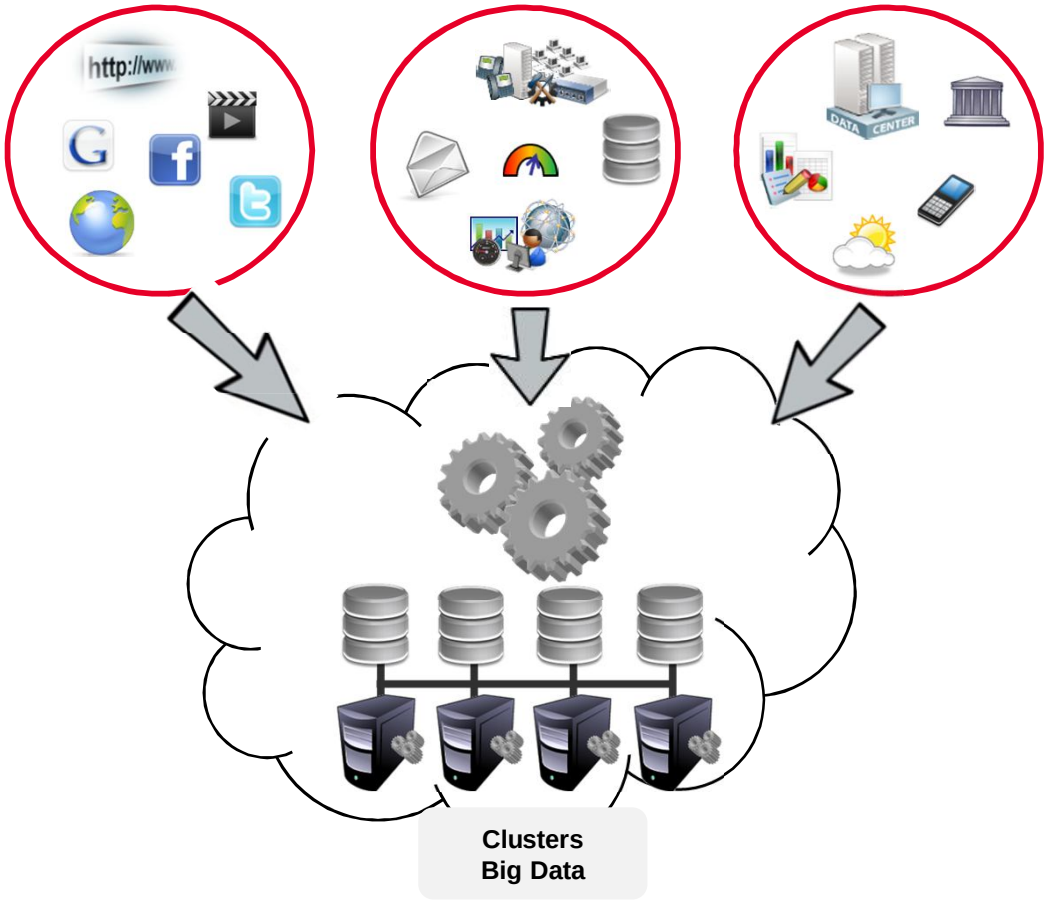
1. Enjeux sécurité du Cloud et du Big Data
2. Accompagner les projets
   - *2. 1 Cloud*
   - *2. 2 Big Data*
   - *2. 3 Maintenir la sécurité dans le temps*
3. Quelques solutions innovantes
4. Quelle posture pour les décideurs sécurité ?

Comment aborder la sécurité du Big Data ?
12 questions à se poser

- **A qui appartiennent les données** que je collecte ?
- Quelle est **leur nature** ? (données spécifiques, données personnelles…)

- Quel est **mon objectif** vis-à-vis de ces données, et est-il **déclaré** ?
- Existe-t-il un risque de non-conformité **réglementaire** ?

- Sais-je **où les données sont stockées** et suis-je capable des les **modifier** ?
- **Combien de temps** seront-elles stockées ?



- Ma technologie est-elle **à jour** ?
- Est-elle entièrement **maintenue**?

- Qui sont mes **fournisseurs externes** et quelle est la structure de mon **contrat** avec eux ?

- Quels **types de traitement** vont être réalisés ?
- Les résultats seront-ils **utilisés légitimement** ?

- Chaque type de donnée est-il **protégé de manière adéquate** contre les différentes menaces ? (modification, accès illégitimes, vol…)

P.10

Comment aborder la sécurité du Big Data ?

4 objectifs de sécurité

Assurer la fiabilité des données

- Contractualiser avec des **fournisseurs de confiance** et / ou certifiés
- Poser des **clauses strictes** quant aux données collectées par des tierces parties
- **Identifier clairement** les données sensibles (bancaires, personnelles)
- Utiliser des protocoles de transfert sécurisés

Protéger les données stockées

- **Former** les équipes aux nouveaux outils à utiliser
- Utiliser les **fonctions de sécurité offertes par les outils**, ou des couches de sécurité supplémentaires (**chiffrement** en particulier)

Sécuriser les processus d'analyse

- Déléguer l'analyse des données à des ***data scientists***
- Définir clairement les **traitements** appliqués et les buts de l'analyse
- **Déclarer** les traitement de données aux autorités/personnes en charge de la protection des données
- **Anonymiser/masquer** les données sensibles

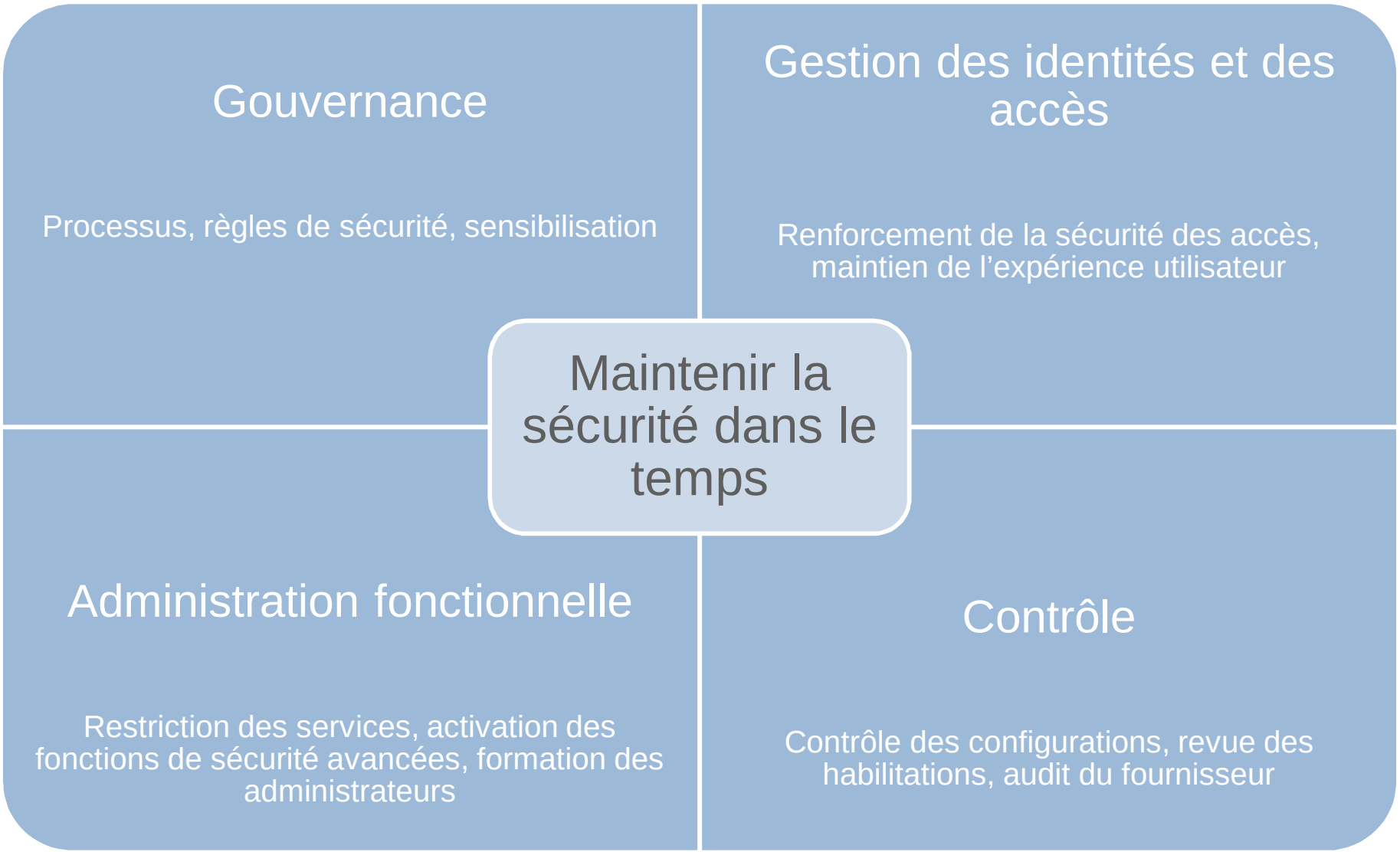
Maintenir la sécurité dans le temps

- Réaliser des **audits** réguliers
- **Insérer le Big Data dans les processus** sécurité existants (patch management, durcissement, gestion de l'administration, DRP…)

Agenda

1. Enjeux sécurité du Cloud et du Big Data
2. Accompagner les projets
   - *2. 1 Cloud*
   - *2. 2 Big Data*
   - *2. 3 Maintenir la sécurité dans le temps*
3. Quelques solutions innovantes
4. Quelle posture pour les décideurs sécurité ?

Responsabilités de l'entreprise



Agenda

1. Enjeux sécurité du Cloud et du Big Data
2. Accompagner les projets
3. Quelques solutions innovantes
4. Quelle posture pour les décideurs sécurité ?

Solutions innovantes

Sécurité grâce au Cloud et au Big Data…

Anti-DDoS : allier une protection sur site et le Cloud

1. Détection de l'attaque par un équipement sur site
2. Activation du système de déviation du trafic
3. Renvoi du trafic vers les infrastructures du fournisseur
4. « Nettoyage » du trafic par le fournisseur qui ne laisse passer que les flux légitimes
5. Fin de l'attaque et désactivation de la déviation

Intelligence dans le Cloud / Big Data

1. Centralisation et traitement des logs (type SIEM) dans un système Cloud
2. Utilisation de systèmes de « réputation » pour profiter des expériences d'autres organisations, notamment pour les antivirus/antimalwares
3. *Advanced Threat Prevention* : identifier des utilisations/comportements anormaux

IAMaaS / IDaaS

1. Solutions hébergée permettant la gestion des habilitations pour des applications internes **et externes** de l'entreprise
2. Incluent des fonctionnalités de gestion des identités, des rôles, d'authentification, de SSO…

Infrastructures de confiance dans le Cloud

1. PKI ou authentification forte
2. Offrent des usages/facteurs d'authentification diversifiés (soft/hard tokens, SMS…)
3. Implique une grande confiance dans le fournisseur

Agenda

1. Enjeux sécurité du Cloud et du Big Data
2. Accompagner les projets
3. Quelques solutions innovantes
4. Quelle posture pour les décideurs sécurité ?

Pour les décideurs sécurité Quels pour le RSSI et le RM ?

Pour le RSSI

- **Expliquer les risques**
  - De manière pragmatique
  - En évitant les réflexes historiques
- **Accompagner (sans *tout* refuser)**
  - Adopter une démarche d'analyse de risque rationnelle
  - Proposer des solutions pour couvrir les risques *différemment*
- **S'assurer du maintien de la sécurité dans le temps**
  - Appliquer les clauses d'audit *(pour de vrai)*
  - Ne pas oublier les contrôles possibles en interne
  - Continuer la sensibilisation

Pour le Risk Manager

- **Auprès des métiers**
  - Comprendre le contexte / le besoin
  - Expliquer les limites et contraintes des technologies, au-delà des seuls discours des fournisseurs
- **Auprès de la DSI**
  - Appliquer des principes de "due diligences" avant contractualisation
  - Valider les possibilités techniques de réversibilité et la capacité à exploiter au quotidien
- **Auprès du service juridique et des achats**
  - Couverture juridique : possibilité de recours, pénalités, sous-traitance…
  - Applicabilité réelle des clauses contractuelles : faillite ou rachat du fournisseur, réversibilité, audits et tests d'intrusion…

The power of simplicity

«Ce qui est simple est fort»

www.solucom.fr

Contact

Chadi HANTOUCHE

Manager

Mail : chadi.hantouche@solucom.fr

Qui sommes-nous ?

Notre mission est d'accompagner nos clients dans la **maîtrise des risques** et la **conduite des projets** au **bénéfice des métiers**

Nos convictions :

- **Prioriser les risques** en fonction des **enjeux des métiers** et accompagner le développement de l'entreprise
- S'adapter à **l'évolution rapide des risques** et apporter des **réponses innovantes**
- Allier protection, **détection et réaction** pour faire face à la diversification des menaces

Une **alliance unique d'expertises de premier plan**

Risk Management	Continuité d'activité	Cyber sécurité	Identité numérique

- ✓ **Plus de 200 consultants spécialisés**
- ✓ **Expertises réglementaires et sectorielles** (banque, assurance, énergie, télécom, transport, santé,…)
- ✓ **Implication forte dans les organismes professionnels et partage de nos partis-pris**

www.solucominsight.fr

Solucom - Practice Risk management et sécurité de l'information

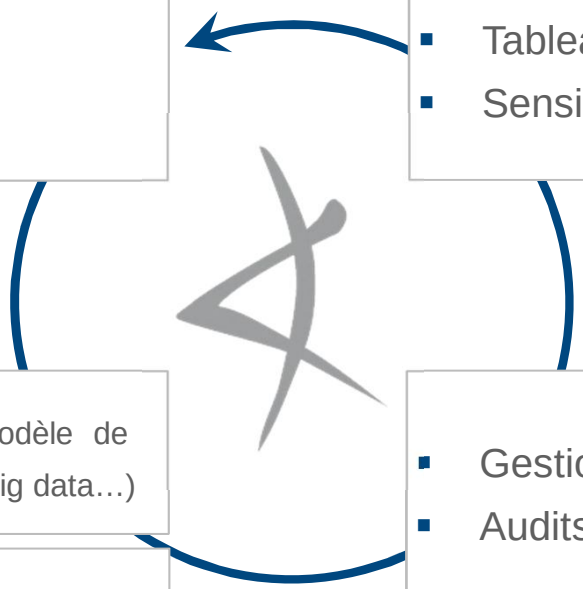
Cybersécurité : la nécessité d'une réponse globale

Anticipation

- Organisation et gouvernance
- Analyse et cartographie des risques
- Schéma directeur et stratégie sécurité
- Cyberassurance et conformité (CNIL/notification, PCI-DSS, OIV, RGS…)

Amélioration

- Animation des systèmes de management 27001
- Centre de compétences architecture/expertise
- Tableaux de bord et contrôle permanent
- Sensibilisation (DG/métiers, développeurs, industriels…)



Protection

- Sécurité applicative et infrastructure (modèle de protection, SI industriels, mobilité, smart, cloud, big data…)
- Gestion des identités et des accès (identité numérique clients/collab., fédération & cloud, biométrie…)
- Continuité d'activité métier et SI (reprise utilisateur, PCI & cloud, tests et exercices, certification ISO 22301…)

Détection & Réaction

- Gestion de crise et forensics (**CERT-Solucom**)
- Audits et tests d'intrusion
- Mise en place de SOC/CERT
- Externalisation de la surveillance (MSSP)

Cybersécurité : nos partis-pris sur les sujets d'actualité

Cyber criminalité	Changer de posture pour s'adapter aux nouvelles menaces
Sécurité applicative	La solution est dans l'organisation !
Cloud	Se focaliser sur la gestion des identités et des accès
Sécurité SI industriel	Agir tout d'abord en mobilisant les opérationnels
Externalisation de la sécurité	Trouver l'équilibre entre industrialisation et expertise

Radar Solucom de la sécurité

Anticipez les évolutions et les futures tendances

Solucom - Practice Risk management et sécurité de l'information

Cybersécurité : le CERT-Solucom, un acteur de confiance à vos cotés

- **Une intervention sur toutes les thématiques cybercriminalité**
  - Étude des menaces et stratégie cybercriminalité
  - Préparation à la gestion de crise
  - Forensics : réaction sur incidents recherche de compromission
  - Veille et innovation

- **L'association d'expertise technique et organisationnelle**
  - La mobilisation de plus de 45 profils expérimentés

Réponse métier	Réponse SI	Réponse forensics

- **Des méthodologies orientées « scénarios d'attaque »**
  (Dénis de service, attaques ciblées, intrusions…)
  - Fiches de réaction, gestion de crise, solution, technique

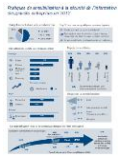
Une expérience avérée au travers de nombreuses références

SFR	Organisation de la gestion de crise cybercriminalité
TELECOMS (confidentiel)	Exercices de crise intrusion et vol de données
INDUSTRIE (confidentiel)	Gestion de crise et forensics intrusion large / APT
TRANSPORT (confidentiel)	Forensics - recherche de compromission antérieure
AIR LIQUIDE	Animation du CSIRT

Solucom - Practice Risk management et sécurité de l'information

Cybersécurité : pour en savoir plus sur nos expertises…

Découvrez nos publications



Sensibilisation
Étude sur les pratiques du marché

Sécurité SI Industriels
Quelle organisation pour réussir ?

Identité numérique
Le futur de la relation client ?

Synthèse Cybercriminalité
Think global!

Nos thématiques d'intervention

- **Gestion de risques** : casser les silos !
- **Cyberassurance** : les clés pour souscrire
- **DDoS** : quelle stratégie de protection ?
- **IAM** : vers de nouvelles perspectives
- **ISO 22301** : le renouveau du PCA
- **Cloud et sécurité** : un mariage impossible ?
- **Modèles de sécurité** : retour d'expérience
- **SOC/CERT** : quel modèle d'organisation ?
- **Comptes à pouvoir** : les clés pour agir

Rejoignez-nous

AMRAE – Septembre
Cloud & RM : les 15 questions clés

Assises de la sécurité – Octobre
Cybercriminalité et gestion de crise

ISC² Secure Paris – Octobre
Panorama de la Cybercriminalité

Nos prises de paroles

www.solucominsight.fr

Nos lettres d'information

La Lettre Risques & Sécurité

Les dossiers CERT-Solucom