
# Contrôle de la Sécurité des S.I.

*La restitution*

# Le rapport

⇨ **Le rapport de contrôle détaillé constitue le résultat analytique des investigations. Il doit :**

- ✓ Rappeler les objectifs et le périmètre
- ✓ Mettre en évidence les points forts et les points à améliorer
- ✓ Présenter les résultats :
  - ✓ Avec une vision managériale
  - ✓ Avec une vision technique et opérationnelle
- ✓ Présenter les preuves se rapportant au constat
- ✓ Estimer les vulnérabilités au regard des risques


# Le plan de recommandation

⇨ **Plan de recommandations structuré**

- ✓ Recommandations sur l'organisation, les moyens de sécurisation en place, les moyens d'accompagnement,…
- ✓ Estimation des coûts, difficultés de mise en oeuvre,
- ✓ Identification des vulnérabilités résiduelles
- ✓ Planning de mise en oeuvre


# Le suivi des actions

⇨ **Tout plan d'action (ou de de recommandation) doit faire l'objet d'un suivi :**

- ✓ En fonction de la criticité des vulnérabilités traitées
- ✓ En fonction des dates de réalisation
- ✓ En fonction d'un planning pré-défini


# Rapport et recommandations

SOMMAIRE Page


# Rapport et recommandations

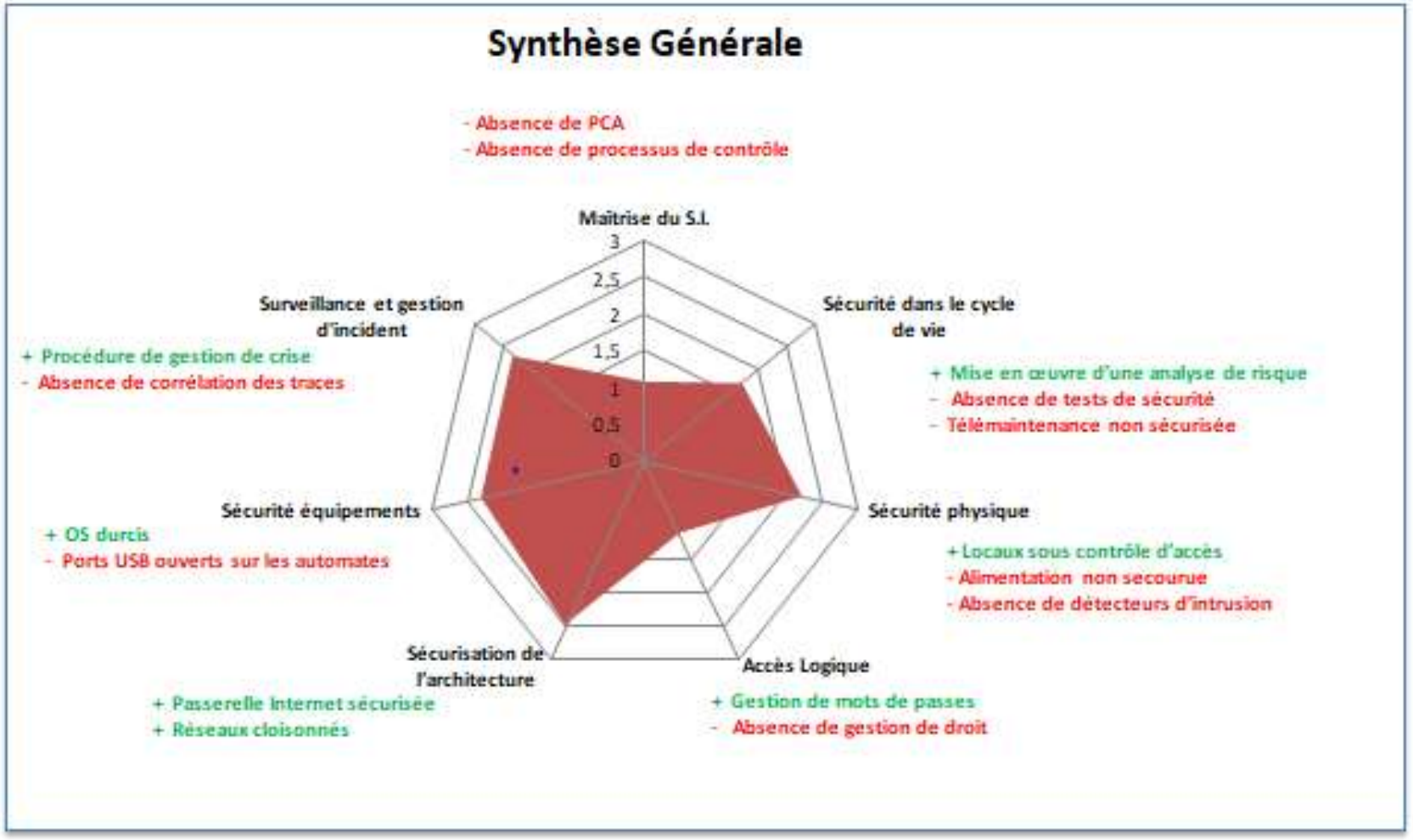

# Rapport et recommandations

| Points positifs | Points d'amélioration | Recommandations |
| --- | --- | --- |
| | | |

Ne pas oublier de citer les preuves

Audit & contrôle

# Rapport et recommandations




# Rapport et recommandations

| Vulnérabilités | Risques Induits | Axes de progrès |
|---|---|---|
| Absence de règles en matière de Sécurité | Systèmes exposés aux menaces | Formalisation des règles de bases en matière de sécurité au sein d'une Politique de Sécurité<br>→Mise à niveau des contrats<br>→Pratiques internes |
| Absence de politique d'authentification | Contrôle des accès aux S.I. non efficient | Mise en place de règles en matière de gestion des accès adaptés aux rôles (Administrateurs / Utilisateurs) |
| Locaux d'hébergement inadaptés | Systèmes exposés aux vols, incendies, accidents, …<br>Faible résilience | Mise à niveau des locaux existants |
| Accès externes non sécurisés | Intrusion externe ou via le SI de gestion | Mise en place de moyens d'accès sécurisés et de surveillance des flux échangés |
| Matériels non sécurisés | Vulnérabilités facilement exploitables | Durcissement des matériels<br>Maintien du niveau de sécurité |

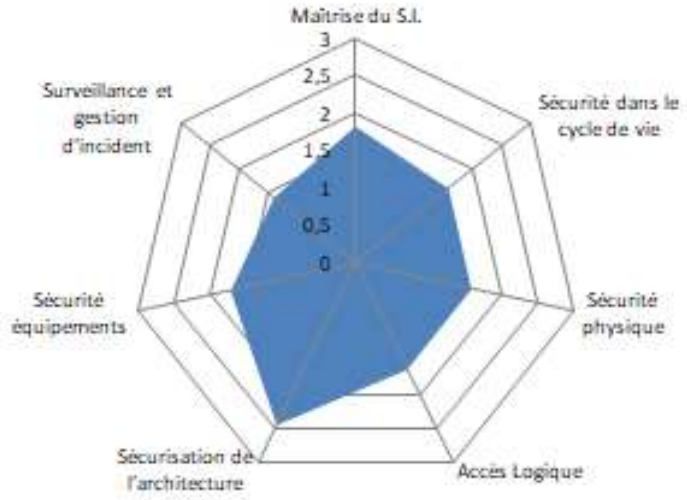
Audit & contrôle

# Rapport et recommandations

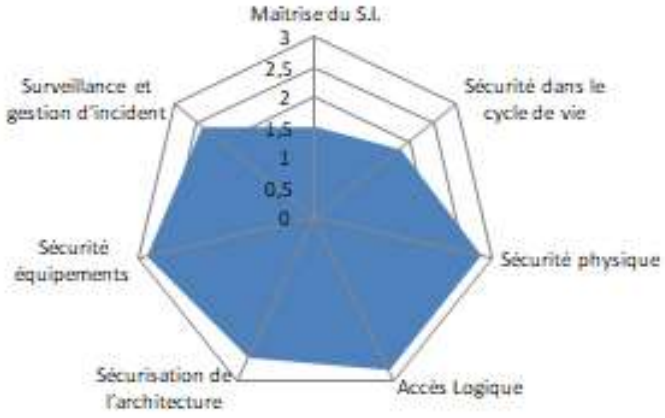
## Synthèse générale

Ventilation Formalisation / Mise en œuvre

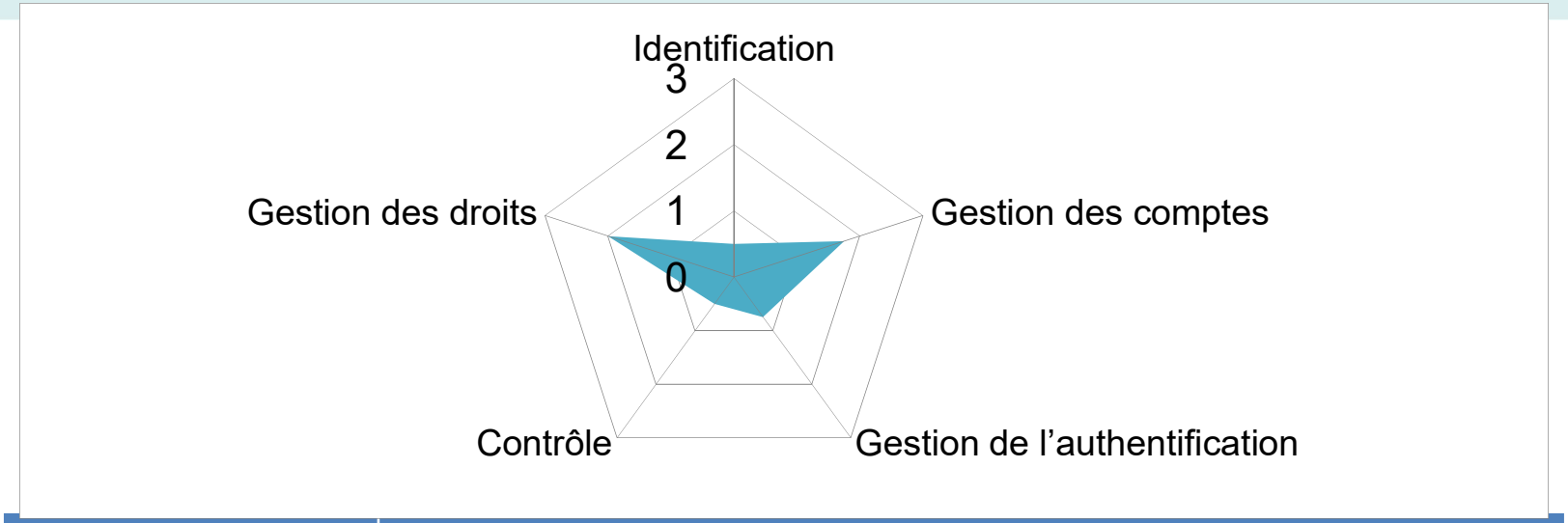
**Niveau de formalisation**




**Niveau de mise en oeuvre**

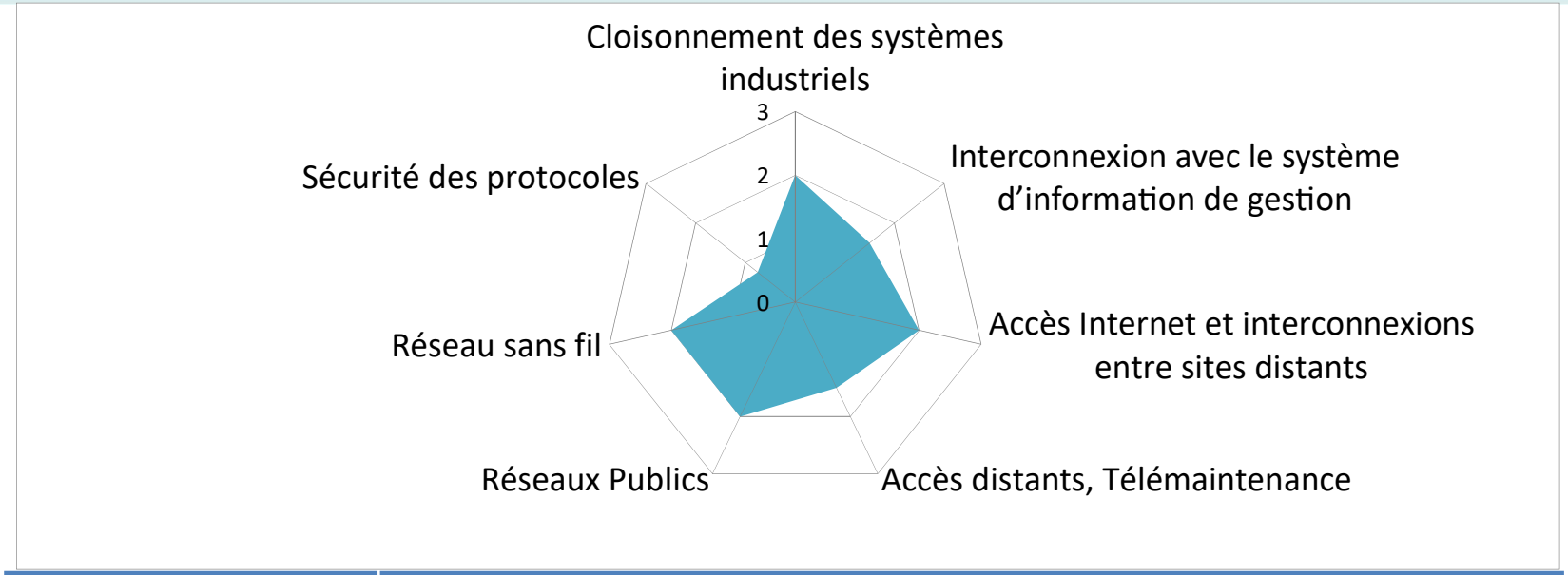



# Rapport et recommandations




| Sous-thème | |
|---|---|
| **Gestion des comptes / droits** | La gestion des comptes pour le volet "Application" (fonctionnel) répond aux exigences d'affection des droits aux personnes devant en connaître. Ce principe n'est ni mis en œuvre, ni contrôlé sur le volet "Infrastructure« ,où les comptes liés aux sessions sont majoritairement en mode "Administrateur". Les risques en cas d'attaques (intrusion) ou d'erreurs (manipulation utilisateurs) sont élevés. En outre, l'usage de comptes génériques pour des rôles ayant des droits élevés ne permet pas d'identifier les intervenants sur les S.I. Industriels. |
| **Authentification** | Les principes d'authentification ne sont pas posés. En conséquence, les mots de passe sont faibles (jusqu'à une seule lettre), jamais renouvelés, ... ce qui ren,d se moyens de protection très relatif. |


# Rapport et recommandations




| Sous-thème | |
|---|---|
| **Cloisonnement** | L'utilisation de réseaux dédiés favorise un cloisonnement physique qui limite les risques en cas d'intrusion. La compromission en cas d'intrusion, ou d'accès via le réseau de gestion, se limiterait à un seul S.I. industriel. |
| **Réseau** | L'absence d'usage du WIFI ou de réseaux publics, ainsi que l'usage très limité d'Internet à partir du S.I. Industriel limitent l'exposition aux risques d'intrusion. |
| **Télémaintenance** | Les infrastructures d'accès pour la télémaintenance sont hétérogènes et peu sécurisées pour certaines.. |

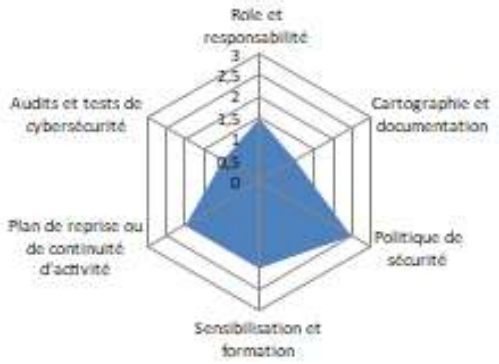
Audit & contrôle

# Rapport et recommandations

## Synthèse par thème

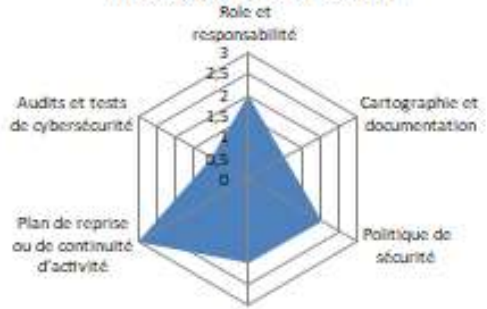
### Maîtrise du S.I.

**Synthèse générale**



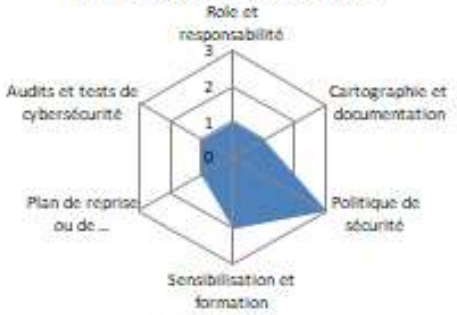

| Sous-thème | + | - |
|---|---|---|
| Rôle et responsabilité | •Hgdhhghgh<br>•hgfdjht | •Hgfhughgf<br>•Ghjgdg gjhg<br>• gr |
| Cartographie et documentation | •hgfdh | •fhfgh |
| Politique de sécurité | •Hfgsh gfd j hj ml h u<br>•jfhjhfg jhgj | •gjfhsfgjhs |
| Sensibilisation et formation | •Hsfhgfs<br>•jhgjhdj | •djhsdh |
| PRA / PCA | •shgs | •shghgh |
| Audits et tests de cybersécurité | •Hg hghgh ghg | •Hghs hghs hgsh |

**Niveau de formalisation**




| Niveau de formalisation | Niveau de mise en œuvre | Note finale |
|---|---|---|
| 1,8 | 1,5 | 1,7 |

**Niveau de mise en œuvre**




Société XXXX Diagnostic SSI 08/2017 14


# Rapport et recommandations

| | Objectif | Risques traités | Charg. | Plann. | Diffic. | Budg. |
|---|---|---|---|---|---|---|
| P1 | Formaliser les règles essentielles en matière de sécurité des S.I. industriels | • Exposition aux menaces externes & internes<br>• Difficultés dans le traitement des incidents<br>• Incapacité à remettre en service suite à incident | | | | |
| P2 | Prise en compte de la sécurité dans les contrats | • Dysfonctionnement majeur suite à une menace introduite par le « Mainteneur »<br>• Perte de maîtrise du S.I | | | | |
| P3 | Sécurisation des environnements physiques | • Dysfonctionnement majeur suite à<br>  • Intrusion, Vol, dégradation<br>  • Incendie, dégats des eaux<br>  • Accidents | | | | |
| P4 | Durcissement des équipements et mise à niveau logiciel | • Dysfonctionnement majeur suite à :<br>  • Virus, malware<br>  • Intrusion logique | | | | |
| P5 | Renforcement de la gestion des droits et accès aux S.I. | • Intrusion facile de personnes non autorisées<br>• Difficulté de traçabilité des actions | | | | |
| P6 | Maitrise des accès à distance / Télémaintenance | • Intrusion de personnes non autorisées<br>• Incapacité à comprendre un incident<br>• Non détection d'un incidents | | | | |
| P7 | Mise en œuvre des pts spécifiques issus de la PSSI | • Niveau de vulnérabilité élevé<br>• Incapacité à remettre en service suite à incident | | | | |

EPITA


# Rapport et recommandations

| Fiche Recommandation | n°3 | Criticité | Important |
|---|---|---|---|
| Objectif | Renforcer le processus de surveillance autour du STCA Intranet, notamment à travers la définition d'une échelle et des exigences en termes de traçabilité des accès et des activités et la mise en œuvre d'un e gestion des traces des activités des exploitants (identifiant, les dates et heures, le type d'action, rétention des logs...). | | |
| Principaux constats | Constat 1 : Absence de processus de gestion de la traçabilité des accès et des activités des exploitants<br>Constat 2 : Absence de protection des logs contre les modifications<br>Constat 3 : Absence de Directive sur les exigences en termes de traçabilité | | |
| Risques induits | Incapacité de prouver l'auteur d'une malveillance ou d'une erreur<br>Incapacité de s'assurer que les logs n'ont pas été modifiés<br>Compromission d'informations sensibles présentes dans les logs | | |

**Exemples d'actions pouvant participer à la réalisation de l'objectif**

- Formaliser et mettre en œuvre un processus de gestion des traces des activités des exploitants, afin de disposer d'une granularité plus fine sur les actions réalisées sur les systèmes du STCA Intranet (identifiant, les dates et heures, le type d'action, rétention des logs...) (N°604)
- Sécuriser le stockage des journaux dans le puits de logs et gérer les habilitations en fonction du niveau de criticité des socles (N°605)
- Spécifier une échelle et des exigences en termes de traçabilité des accès et des activités dans les Directives de la [illegible] (N°606)
- Garantir l'intégrité des traces stockées dans le puits de logs (N°815)

| Délais | Coûts | Leader/ soutien |
|---|---|---|
| TT | €€ | [illegible] |

| Thèmes majeurs couverts | Gestion de l'exploitation, des communications et des réseaux<br>Développement et maintenance des systèmes |
|---|---|


# Rapport et recommandations

**Objectif** Sécurisation des environnements physiques

**Constats**
- Locaux informatiques non adaptés
- Locaux techniques à améliorer
- Armoires terrain non protégés

**Risques**
- Dysfonctionnement majeur (ou vol de données sensibles) suite à :
  - Intrusion, Vol, dégradation
  - Incendie, dégats des eaux
  - Accidents

| | Description |
|---|---|
| P3.1 | **Local PARIF et local PARKING :**<br>-Condamnation des accès vitrés, mise sous contrôle d'accès et alarmes de surveillance<br>- Mise aux normes des étagères ou baies d'accueil des matériels, identification des équipements,<br>- Mise au normes des câblages courant faible (réseaux), dépose des câbles non utilisés, ...<br>- Exclusion de toute activité autre que l'hébergement<br>- Positionnement d'une armoire regroupant la documentation |
| P3.2 | **Local SONO**<br>-Protection de la centrale incendie (cloisonnement) si déménagement non possible<br>-Sécurisation du lien SSI – Sono |
| P3.3 | Fermeture et mise sous alarme (contact ) des armoires terrains en priorisant celles en zone technique |
| P3.4 | **Tri-bagage** : Sécurisation de l'hébergement du serveur (Accès, climatisation, ...) |


# Rapport et recommandations

⇨ **Le rapport est sensible :**

- ✓ Sécuriser la transmission
- ✓ Numéroter les exemplaires papiers
- ✓ Protéger le stockage

❑ **Deloitte (2017)** *Fuite des emails du cabinet à destination des clients (livrables, recommandations, échanges…) et des collaborateurs pendant au moins quatre mois*

❑ **Accenture (2017)** *Fuite de secrets de chiffrement, d'identifiants et de mots de passe qui auraient permis un accès aux données du cabinet et de ses clients*

❑ **Forrester (2017)** *Attaque du site web et fuite de données commerciales : études de marché, analyses et statistiques*


# Rapport et recommandations

***Exemple de solution***

Shadline

TIME FOR TRUST

www.shadline.com

⇨ **Espace d'échange confidentiel et temporel entre des acteurs habilités de différentes organisations**

- ✓ Echange de messages et de fichiers
- ✓ Destruction définitive ou archivage réglementaire des documents à l'issue des projets

⇨ **Transferts permettant de livrer les rapports en maîtrisant les destinataires et les durées d'accès**

- ✓ Lien individuel, temporel et sécurisé par destinataire
- ✓ Traçabilité sur les téléchargements réalisés
- ✓ Relances si nécessaire

⇨ **Espace individuel permettant aux auditeurs d'accéder aux outils de référence pour leur mission en cas:**

- ✓ De déplacement dans certains pays sensibles
- ✓ D'indisponibilité du SI

EPITA