harmonie [TECHNOLOGIE]

Mardi 18 mars 2014

GS DAYS

GESTION DES COMPTES À PRIVILÈGES

GS Days
LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ

harmonie [TECHNOLOGIE]

Présentation

HARMONIE TECHNOLOGIE

Cabinet de conseil et d'expertise technique
Spécialiste de la sécurité du système d'information

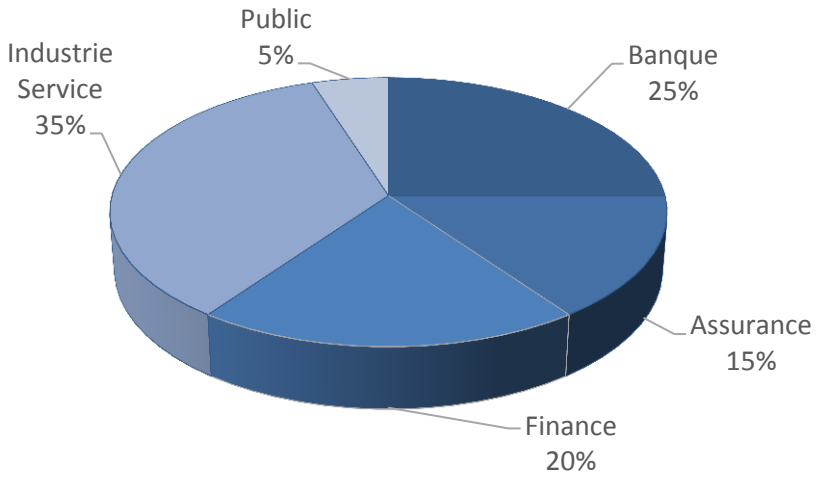
PRÉSENTATION D'HARMONIE/ STRATÉGIE 2016

Un cabinet de conseil et d'expertise

Spécialiste de la sécurité du système d'information

Une **double compétence fonctionnelle et technique** pour un accompagnement global sur les sujets sécurité

- AUDIT
- INTEGRATION
- CONSEIL
- FORMATION

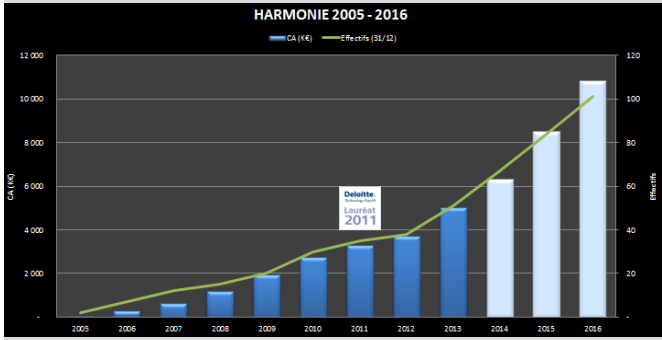


Nos clients
Relation partenariale avec les grands comptes avec une forte présence Banque, Finance, Assurance

harmonie [TECHNOLOGIE]

HARMONIE 2005-2016
Société indépendante financièrement
Croissance organique soutenue depuis 2005, supérieure à 20% par an

- 2005 : Création sur le métier de l'intégration de solutions IAM
- 2009 : Création du pôle Conseil
- 2010 : Achat d'une société spécialisée dans la protection des données
- 2011 : Récompense Deloitte
- Objectif 2014 : 70 collaborateurs et CA de 7M€
- Projection 2016 : 100 collaborateurs CA de 11M€



OFFRES SSI

Une double compétence fonctionnelle et technique pour un accompagnement global en SSI

GOUVERNANCE, RISQUES & CONFORMITÉ

- Schéma directeur SSI et mise en place de SMSI
- Politique de sécurité et tableaux de bord SSI
- Sensibilisation à la sécurité
- Analyse de risques (MEHARI, EBIOS, ISO 27005)
- Plan de continuité d'activité / informatique

GESTION DES IDENTITÉS ET DES ACCÈS

- Annuaire, contrôle d'accès
- Gestion des habilitations
- Role Management et revue d'habilitation
- Gestion des comptes à privilèges
- SSO, fédération d'identité
- Authentification forte et card management

SÉCURITÉ DES SERVICES ET DE L'INFORMATION

- Protection des données sensibles, DLP
- Confiance numérique : PKI, chiffrement, etc.
- Sécurité des développements et des applications
- Supervision de la sécurité : log management et SIEM

AUDIT DE SECURITE

- Organisation et processus
- Politiques et normes
- Technique : architecture, code, …
- Tests d'intrusion

CONSEIL

- Etude d'opportunité, cadrage, aide au choix de solutions
- AMOA de projet SSI, conduite du changement
- Accompagnement RSSI

EXPERTISE TECHNIQUE ET INTEGRATION

- Conception et mise en œuvre d'architecture de sécurité
- Intégration de solutions IAM, DLP, SIEM
- TMA corrective et évolutive de solutions de sécurité

CENTRE DE FORMATION AGREE

- Concepts et méthodologies
- Produits

harmonie [TECHNOLOGIE]

Extrait conférence **GSDAYS 2014**

GESTION DES COMPTES À PRIVILÈGES

Christophe Gueguen – Directeur du Pôle Technique Harmonie Technologie

QU'EST CE QU'UN COMPTE À PRIVILÈGES?

Compte d'administration générique partagé
Compte d'administration des composants ou des applications
Exemple : compte « root » sous Unix ou « SYS » sous Oracle

Compte à privilège personnel
Compte nominatif possédant des droits étendus sur un système

Compte de service
Compte technique utilisé pour exécuter un service sur une machine

Compte d'applications
Compte utilisé par les applications pour se connecter à une base de données, un annuaire ou une autre application

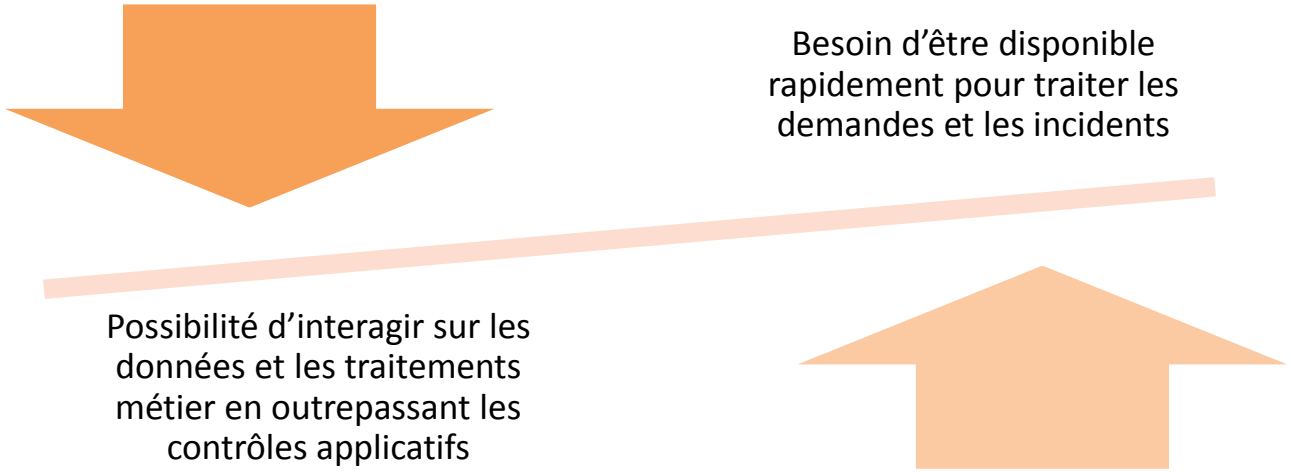
Compte « urgence »
Compte générique stocké dans un coffre pour permettre de traiter des incidents majeurs.
Exemple : activation d'un PRA

PRINCIPALES CARACTÉRISTIQUES DES COMPTES À PRIVILÈGES

Ces comptes sont des clés pour accéder au cœur des systèmes d'information et vont permettre :

- Aux composants de fonctionner et de communiquer les uns avec les autres
- Aux équipes opérationnelles d'assurer l'administration et la maintenance des composants du SI

De fait, ces comptes sont critiques à deux titres



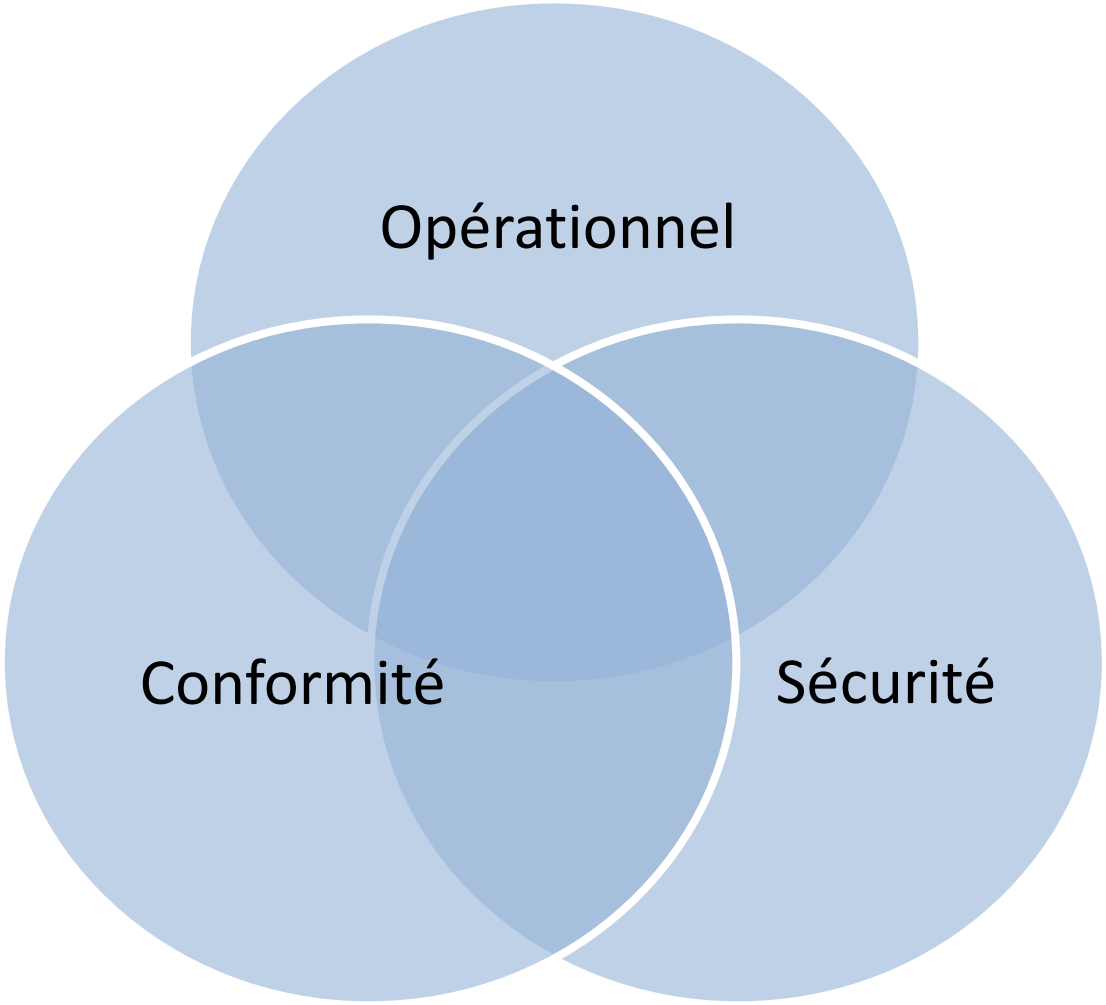
GESTION HÉTÉROGÈNE DES COMPTES

Lors des audits et tests d'intrusion interne,
les constats suivants se retrouvent (trop) fréquemment :

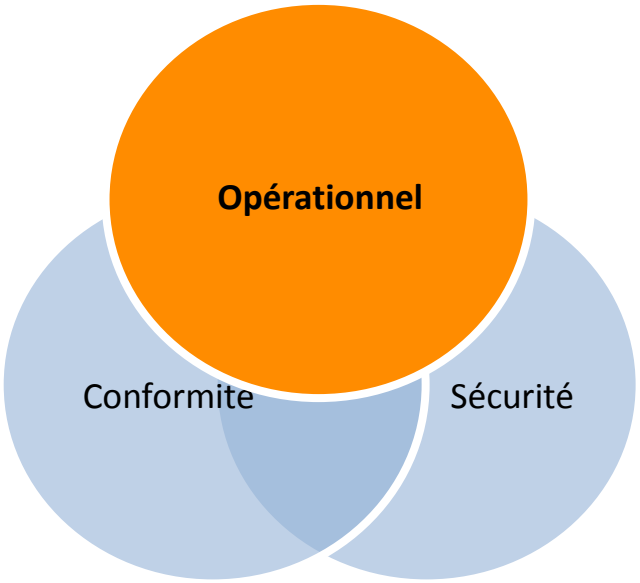
- Les membres des groupes d'administration sont trop nombreux et vont au-delà de la liste des besoins (exemple « Administrateurs du domaine » sous active directory)
- Une complexité hétérogène des mots de passe d'un système à l'autre (A titre d'exemple, les mots de passe d'accès aux bases de données sont souvent trop faibles au vu des enjeux)
- Les mots de passe sont partagés de manière assez large au sein des équipes et rarement (voir jamais) changés
- Les mots de passe sont stockés en clair dans des fichiers de configuration ou des scripts
- Certains comptes vont cumuler des droits au fil des années et des projets au point de pouvoir contrôler intégralement le SI
- Faiblesse de l'auditabilité : Il est complexe de connaitre la personne qui a réalisé une opération.

3 GRANDES FAMILLES DE RISQUES

La non-maîtrise des comptes à privilèges fait courir 3 natures de risques aux entreprises



3 GRANDES FAMILLES DE RISQUES

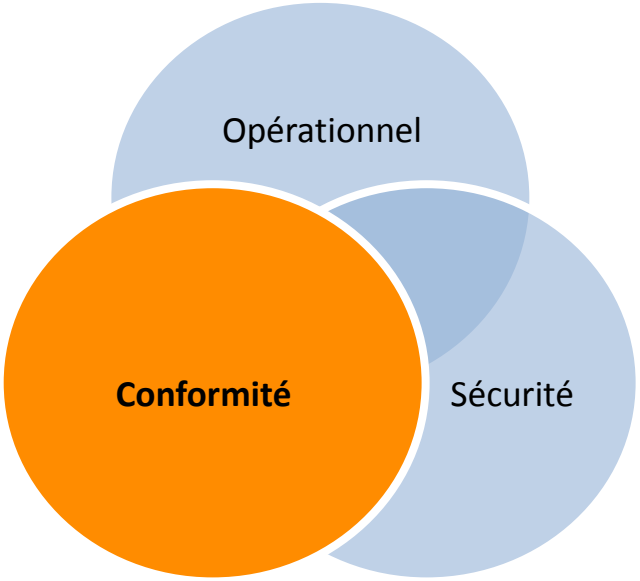


Les risques opérationnels correspondent à des erreurs ou à des fausses manipulations qui peuvent entrainer des perturbations des services.

Ces risques sont d'autant plus importants que les contraintes liées aux activités d'administration des composants le sont également :

+ à gérer	Nombre de plus en plus important de systèmes à gérer
- de personnes	Volonté d'optimisation des coûts de gestion - Réorganisation des activités - Réduction des équipes internes - Externalisation de certaines activités
+ Vite	« time to market » réduit

3 GRANDES FAMILLES DE RISQUES



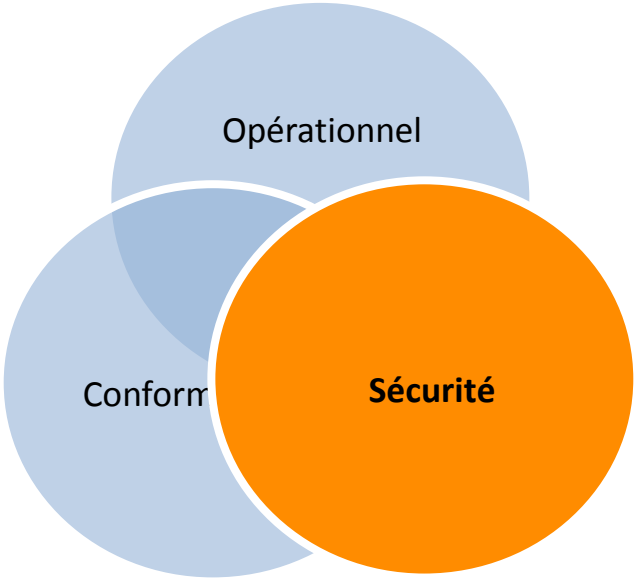
Les réglementations nécessitant des conformités sont de plus en plus nombreuses et variées

PCI · HIPAA Health Insurance Portability and Accountability Act · asipsanté · GLBA · SOLVENCY II · Bâle III

Les exigences des politiques et des réglementations sont généralement de quatre types

Identifier et suivre **la localisation des informations de connexion** des comptes à privilèges	Renforcer la **politique de mot de passe** (force, changement)
Limiter les accès des comptes aux personnels en ayant le besoin et appliquer le principe du moindre privilège	**Auditer l'utilisation des comptes à privilèges** (demandeur, historique d'accès, justification, …)

3 GRANDES FAMILLES DE RISQUES



Une mauvaise gestion des accès privilégiés peut avoir des conséquences graves pour l'entreprise :

- Perte financière
- Dégradation de l'image de marque
- Discontinuité de services
- Vol de données

"48% des vols de données sont liés à une mauvaise gestion des privilèges" Gartner.

Multiplication des attaques ciblées sur les administrateurs

DES SOLUTIONS À LA CROISÉE DES CHEMINS

Pour couvrir ces risques, il est nécessaire d'apporter un ensemble de fonctionnalités autour de la gestion des comptes d'administration et des administrateurs

IAM
Gestion des mots de passe des comptes partagés

SSO
Gestion des accès des comptes à privilèges

SIEM
Supervision

Les solutions de gestion des comptes à privilèges couvrent trois grands thèmes

Gestion des comptes d'administration et des administrateurs

LES SOLUTIONS DE GESTION DES COMPTES À PRIVILÈGES

Principales solutions du marché

beyondtrust securing the perimeter within

BalaBit IT Security

Cyber-Ark

Centrify

ca technologies

IBM

QUEST SOFTWARE now a part of Dell

WALLIX TRACE, AUDIT & TRUST

Les offres proposées par ces éditeurs ne sont pas équivalentes :

- Même si les éditeurs couvrent toutes les fonctionnalités de la gestion des comptes à privilèges , il peut s'agir de produits différents
- Certaines solutions sont plus orientées « agent » ou « bastion »
- Les deux familles de solutions ne sont pas incompatibles et peuvent répondre à des besoins différents

COUVERTURE DES RISQUES

En conclusion, les solutions permettent

- une meilleure auditabilité de l'utilisation des comptes à privilèges
- une capacité de mener des analyses à posteriori des activités des administrateurs
- de circonscrire l'utilisation des comptes partagés
- de déployer des profils pour les équipes techniques

De fait, elle concourt à la couverture des 3 familles de risques citées

Conformité	Opérationnel	Sécurité
Réponse aux quatre types d'exigences ▪ Localisation des informations ▪ Renfort de la politique de mot de passe ▪ Limitation des accès ▪ Renfort des capacités d'audit	▪ Les fausses manipulations sont circonscrites au périmètre de responsabilité de l'administrateur ▪ Ses actions peuvent être limitées à une liste des commandes autorisées	▪ En cas de compromission du poste d'un administrateur, les possibilités de rebond de l'attaquant sont réduites

EST-CE SUFFISANT POUR INITIER UN PROJET ?

Trois familles principales d'éléments déclencheurs de projet

Une attaque avérée

La commercialisation d'un service réglementé

L'externalisation d'activité pour améliorer la traçabilité

PRÉSENTATION DU CONTEXTE – EXIGENCES DE PCI-DSS

PCI-DSS / Comptes à privilèges

Implémenter des mesures strictes de contrôle d'accès	
Exigence 7 :	Restreindre l'accès aux données bancaires grâce au principe « besoin de connaître ».
Exigence 8 :	Attribuer un identifiant unique à chaque personne ayant accès à un ordinateur.
Exigence 9 :	Restreindre l'accès physique aux données bancaires.
Suivre et tester régulièrement les réseaux	
Exigence 10 :	Tracer et suivre tous les accès aux ressources du réseau et aux données bancaires.
Exigence 11:	Tester régulièrement les systèmes et les processus de sécurité.
Gérer une stratégie de sécurité des informations	
Exigence 12 :	Mettre en œuvre une stratégie répondant aux problèmes de sécurité de l'information.

- ❑ **S'assurer de l'identité des l'individus**
- ❑ **Authentification forte pour les accès distants**
- ❑ **Non-réversibilité du mot de passe**
- ❑ **Politique commune de sécurité du mot de passe**
- ❑ **Principe de l'ID unique**
- ❑ **S'assurer du principe de moindre privilège**
- ❑ **Tracer les demandes d'élévation des privilèges**
- ❑ **S'assurer des actions que peuvent réaliser ou ne pas réaliser les individus (RBAC)**
- ❑ **Tracer les tentatives d'accès**
- ❑ **Tracer les actions des comptes à pouvoir**

GENÈSE DU PROJET – PROJET D'ÉVOLUTION

Définition du besoin

- Respect des préconisations PCI DSS (Payment Card Industry Data Security Standard)
- Mise en place du principe du moindre privilège (« least privilege principle »)
- Outil de gestion des rôles de comptes Unix, de type Role Based Access Control (RBAC)
- Configuration simple de l'attribution de privilèges (par exemple, pouvoir attribuer le privilège d'exécuter telle commande avec tel argument sous telle identité)
- Administration simplifiée des comptes et des rôles associés (de manière centralisée, typiquement)
- Intégration à l'architecture actuelle (partitions AIX clientes LDAP de l'AD)
- Fonctionnalités de log + reporting évoluées : centralisation des logs, détail des commandes utilisées, production facile de rapports

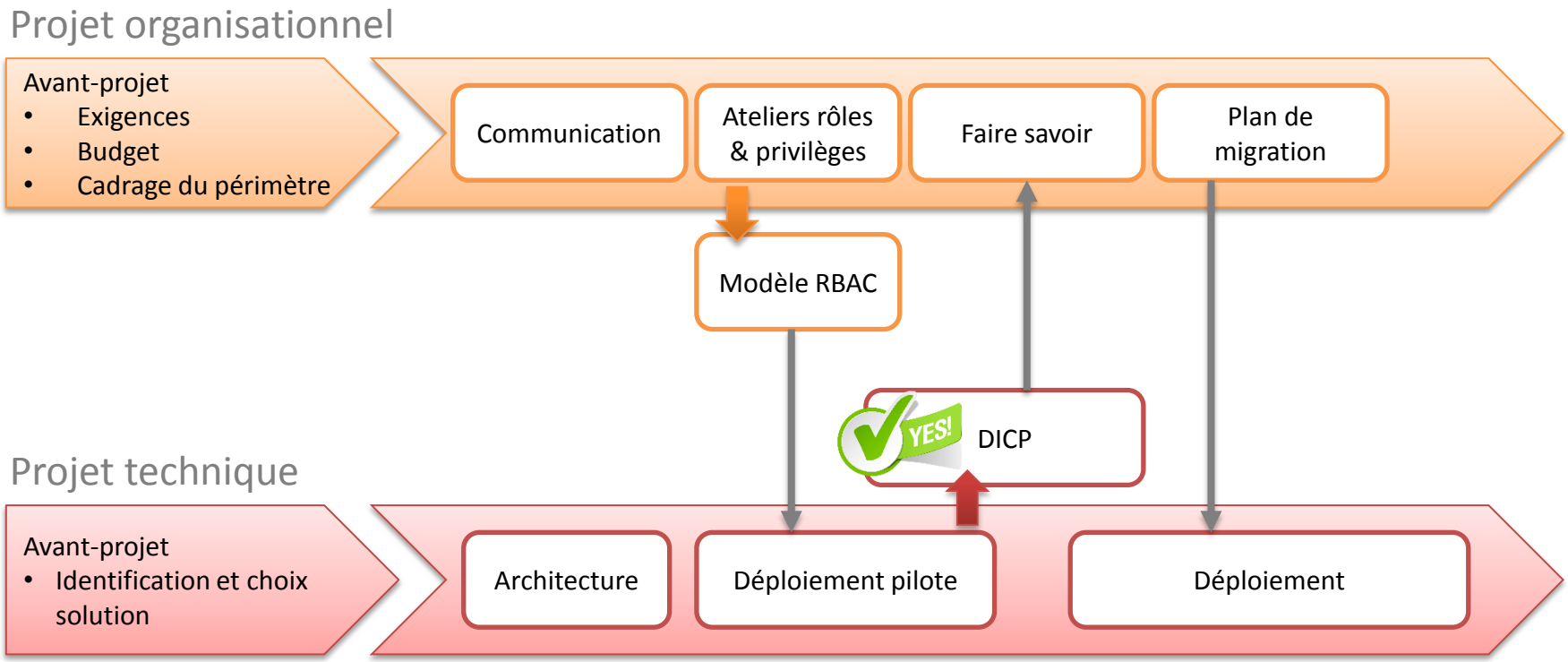
Contraintes

- Pas d'impact sur les performances, fonctionnement en mode dégradé possible…
- Contrainte sur l'AD : Pas de modification de schéma AD tolérée (Hors Microsoft)
- Utilisation d'authentification par carte à puce sur les Workstations du périmètre PCI-DSS
- Evolution pressentie vers une plateforme multi-OS (Unix, Linux & Windows)
- Interfaçage possible avec le workflow des habilitations

Un mot d'ordre semble important: « la simplification de la gestion de l'ensemble fera gagner de l'efficacité et de la sécurité »

ORGANISATION GÉNÉRALE DU PROJET

Un projet technique et organisationnel



STRATÉGIE DE DÉPLOIEMENT

❑ Généraliser la solution de gestion des comptes à privilèges

- ↗ Généralisée à tous les projets, à tous les environnements
- ↗ Bénéfices
  - ⇨ Processus et outillage homogènes quelque soit le projet
  - ⇨ Permet de « faire ses preuves » sur les projets moins critiques, avant d'aborder les projets critiques

❑ Une planification pragmatique mais volontariste

- ↗ Nécessité de rencontrer chaque projet pour tenir compte de ses contraintes
- ↗ Nécessité d'affirmer la volonté de l'entreprise de mener le projet à bien
  - ⇨ Soutient des sponsors
  - ⇨ Escalade pour les projets qui « ne jouent pas le jeu »

COMPLEXITÉS D'UN PROJET DE GESTION DES COMPTES À PRIVILÈGES

La mise en œuvre d'un projet de gestion des comptes à privilèges va bien au delà du « simple » déploiement de produits
Il nécessite a minima des réflexions sur

- L'architecture en place
- Les modes opératoires des équipes

Plusieurs aspects structurants sont à considérer.

- Inventaire des comptes à privilèges
- Mise en œuvre de règles de traitement des comptes dans les applications
- Définition et maintenance des profils d'administration
- Mise en œuvre une gouvernance
- Définition d'une gestion du changement

harmonie [TECHNOLOGIE]

Contact

HARMONIE TECHNOLOGIE

Cabinet de conseil et d'expertise technique
Spécialiste de la sécurité du système d'information

VOS CONTACTS

Pour recevoir le support complet * présenté à l'occasion des GS Days 2014 ou organiser un rendez-vous, merci de nous contacter via info.ssi@harmonie.technologie.com ou au +331 73 54 30 00

**Le support de la conférence est exclusivement réservé à des utilisateurs finaux RSSI & DSI*

Jennifer Bellagamba
Manager commercial

Christophe Gueguen
Directeur du pôle technique

harmonie [TECHNOLOGIE]

Site www.harmonie-technologie.com
Email contact@harmonie-technologie.com
Adr. 60 rue la Boétie, 75008 Paris
Std. +331 73 54 30 00
Fax +331 73 54 30 01