Conformité : quelles exigences réglementaires ?

WALLIX
Infrastructure and Security Solutions

WallixAdminBastion

Quelles normes ?

- Sécurité des données des titulaires de cartes bancaires

- Régulation des jeux en ligne

- Sécurité des données nominatives de santé

- Equilibrer sécurité et externalisation

WallixAdminBastion

Problématiques communes

Mot de passe

- PCI-DSS : 8.5.10 à 8.5.13

Mots de passe forts (7 caractères, alphanumériques) et archivés(4 derniers interdits , 6 échecs)

- Hébergement des données de santé à caractère personnel : P6 -> PSI 14 et 15

Présentation des critères suivants : Taille des mots de passe, complexité, expiration, historisation

- ARJEL

10 caractères minimum

Issus d'au moins 3 des 4 groupes de caractères suivants : minuscules, majuscules, spéciaux, chiffres

Ex : Wallix2011

WallixAdminBastion

Problématiques communes

Traçabilité des actions

- PCI-DSS : 10.2, 10.3

Toutes les actions des administrateurs sont enregistrées et consignées dans des journaux d'audit

- Hébergement des données de santé à caractère personnel : P6 -> 2.7

Présentation de la typologie des éléments tracés : Actions réalisées, comptes, etc..

- ARJEL : 5.7.2.a

Préciser les contrôles sur les sous-traitants

Traces activées et consolidées pour retrouver l'exécutant d'un e action

WallixAdminBastion

Problématiques communes

Authentification

- PCI-DSS : 10.3

Toutes les tentatives d'authentification sont logguées (succès/échec)

- Hébergement des données de santé à caractère personnel : P6 -> 2.7

Présentation de la typologie des éléments tracés : Authentification (succès/échec)

- ARJEL : 5.7.3.e.1

Authentification via certificat X509 V3

WallixAdminBastion

Maîtriser les risques d’infogérance

ANSSI Agence nationale de la sécurité des systèmes d'information

- Risques inhérents aux interventions distantes :2.2.2
  - Mots de passe par défaut ou faibles
  - Absence de traçabilité des actions
  - Possibilité d’effacer les traces a posteriori

WallixAdminBastion

Maîtriser les risques d'infogérance

ANSSI Agence nationale de la sécurité des systèmes d'information

- Recommandations:2.2.3
  - Dispositifs techniques de sécurité : filtrage des accès réseau, droits d'accès
  - Traçabilité des actions
- Mise en œuvre d'une passerelle sécurisée:2.2.4
  - Authentifier la machine distante et la personne en charge du support
  - Assurer une traçabilité de confiance des actions effectuées
  - Audit de la passerelle sécurisée

http://www.ssi.gouv.fr/fr/bonnes-pratiques/

Conclusion

ANSSI Agence nationale de la sécurité des systèmes d'information

PCI Security Standards Council ™

- Sources

  - www.pcisecuritystandards.org
  - www.esante.gouv.fr
  - www.arjel.fr
  - www.ssi.gouv.fr

arjel Autorité de régulation des jeux en ligne

asipsanté AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

WAB

Traçabilité des administrateurs internes et externes : une garantie pour la conformité

WALLIX
Infrastructure and Security Solutions

WallixAdminBastion

Wallix en Bref

- Création en 2003 – siège social à Paris, France
- 1er éditeur Européen de solutions de traçabilité et de contrôle des accès des Utilisateurs à privilèges et des prestataires
- Actionnariat solide : Thierry Dassault Holding, Auriga Partners, Caisse des Dépôts …
- Chiffre d'affaire : Progression de 100% par an depuis 3 ans
- 35 collaborateurs, 80% effectif support et R&D
- Bureaux au Royaume-Uni et au USA
- Forte présence sur les grands comptes
- Plus de 130 clients
- Un réseau de partenaires certifiés dans le monde entier
- Modèle de distribution Indirect
- Des solutions déployées dans 10 pays

WallixAdminBastion

Quelques références

Collectivités locales

- Mairie de Boulogne Billancourt
- Mairie d'Alès
- Mairie des Mureaux
- Mairie de Nanterre
- Mairie de Châteauroux
- Communauté Urbaine de Bordeaux
- Conseil Général des Hauts de Seine
- Conseil Général de la Sarthe
- Conseil Général de l'Oise ...

Administration / Education / Santé

- CNAM TS
- Ministère de l'Ecologie
- Ministère de l'Economie
- Météo France
- INSERM
- BRGM
- INERIS
- IRSN
- DILA
- Gendarmerie Nationale
- DGA Techniques Navales
- Hôpital de Carcassonne
- Hôpital de Poissy St-Germain
- SIIH
- Académie d'Amiens
- Académie de Versailles
- Université de Rennes 2 ...

Industrie / Energie

- PSA Peugeot Citroën
- EDF
- ST Microelectronics
- Thales
- Boost Aerospace
- Arcelor Mittal
- SPIE
- SPEIG
- Fenwick
- Groupe Soufflet ...

Banque / Assurance

- MGEN / Choregie
- GMF
- Crédit Agricole SA
- CA Monecam
- Amundi
- Casden
- Harmonie Mutualité
- Generali
- Euler Hermes ...

Transport / Logistique

- Geodis
- Chronopost
- Coliposte
- Régie des Transports Marseillais
- Aéroport de Marseille Provence ...

Services / Luxe / Medias

- LVMH
- Hermes
- France Télévisions
- M6
- Quick
- Alain Afflelou
- GALEC (Leclerc)
- Wolters Kluwer
- TDF
- Maisons du Monde ...

Télécom / Hébergement

- Bouygues Telecom
- SFR
- Numericable
- GRITA
- Pharmagest
- Coreye / Pictime
- OPT (Polynésie Française)
- Mipih ...

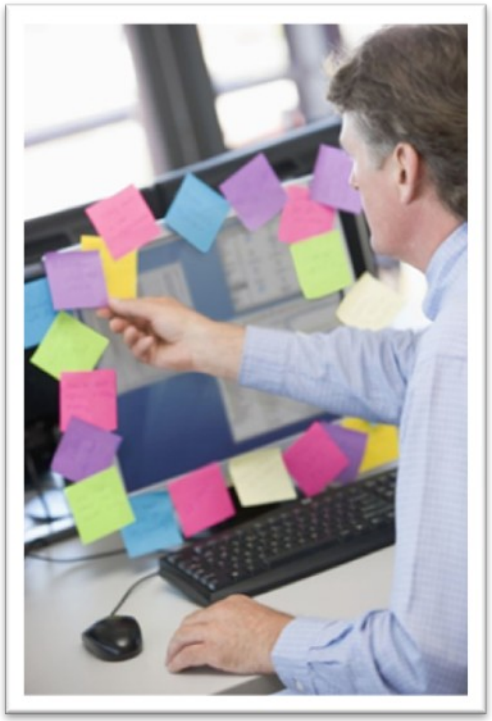
International

- Maroc Telecom
- Millicom (Luxembourg)
- Naxoo / Télégenève (Suisse)
- Tigo (El Salvador, Ile Maurice, RDC ...)
- Université du Luxembourg
- Service Public de Wallonie ...

Comptes à privilèges : quelles problématiques ?

Mots de passe administrateurs

- Les administrateurs doivent apprendre les mots de passe, les retenir et en changer régulièrement
- Les post-it se multiplient autour de l'écran ou sur le bureau
- Les mots de passe sont gérés à droite et à gauche, parfois ils restent dans la tête de l'administrateur !



Comment gérer les mots de passe administrateurs de mon entreprise dans la durée ?

Le turnover des équipes IT

- L'un de mes administrateurs s'en va. Où sont ses mots de passe ?
- Il faut recenser ses accès, les désactiver et les changer sur tous les équipements
- Il faut communiquer les changements en interne
- Comment s'assurer qu'il ne pourra plus accéder au SI de l'entreprise ?

Les employés qui volent ou divulguent les données d'entreprise le font à l'occasion de leur départ vers un concurrent (70 % des cas) ou de la création de leur propre affaire (23 % des cas)

ORIGINE D'UN INCIDENT ET TRAÇABILITÉ DES ACTIONS

- La base de données clients est tombée suite à une intervention de maintenance durant une migration de version
- Pas de responsable et pas de moyen de le désigner !
- Difficile de retrouver la cause

D'où vient l'erreur ?
Peut-on rejouer le scénario ?
Comment retrouver l'origine de l'incident ?

Les intervenants externes…

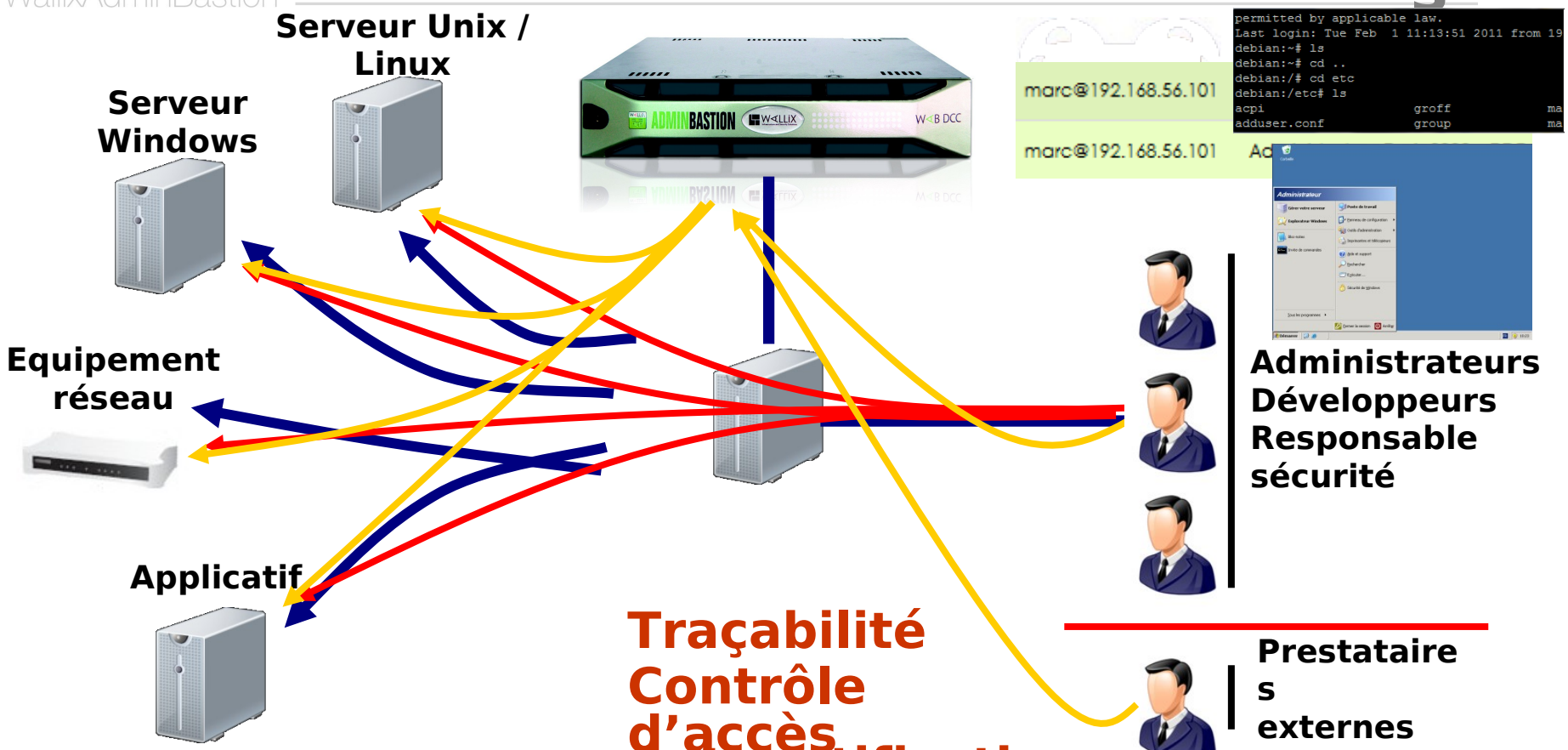
GESTION DES CHANGEMENTS DE PRESTATAIRES

- Je n’ai aucune visibilité sur leurs actions de mes prestataires !
- Les connexions aux serveurs et équipements sont multiples : je ne sais pas qui se connecte, quand et comment !
- Je dois contrôler leurs accès et les cadrer en cas d’interventions ponctuelles et pouvoir changer de prestataire si nécessaire

Comment m’assurer que les accès sont bien contrôlés ? Comment remonter à l’origine d’un incident ?
Qui est responsable ?

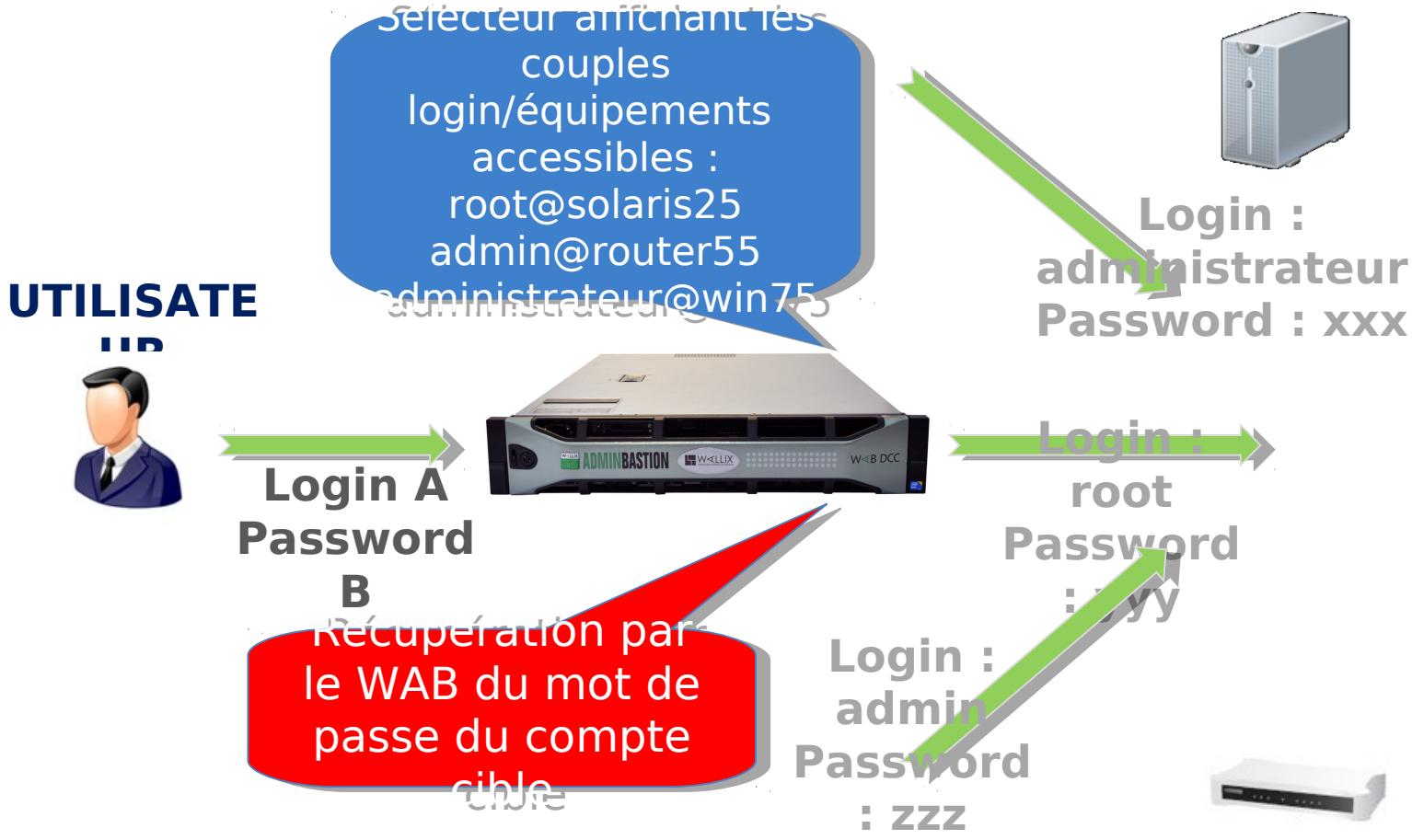
Accès sécurisé aux comptes à privilèges avec Wallix AdminBastion

Concepts



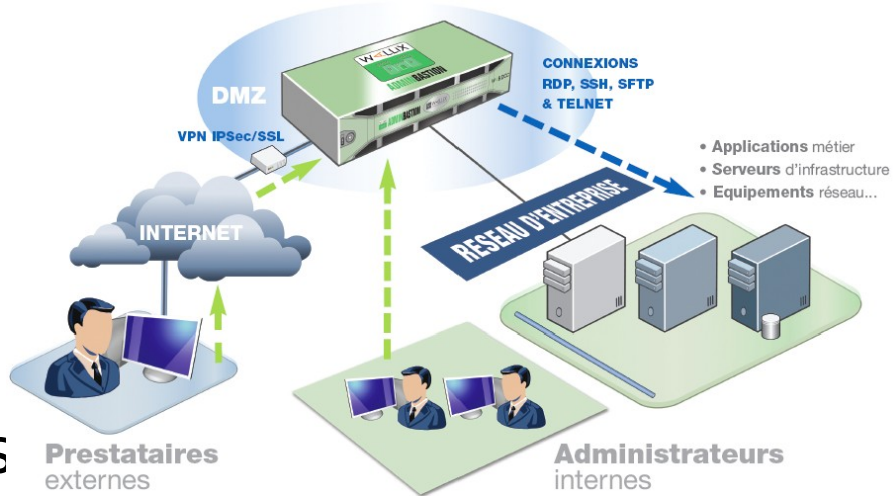
Traçabilité
Contrôle d'accès
Authentification centralisée
Gestion des mots de passe cibles

Contrôle d'accès



Types d'utilisation

- Contrôle des accès des prestataires internes et externes
- Traçabilité des connexions internes vers des équipements sensibles



- Gestion centralisée et simplifiée des accès, des identifiants et des mots de passe
- Authentification forte des administrateurs système (via solutions externes)
- Alerte (ex : envoi de message) en cas de connexion à des serveurs critiques

Protocoles supportés

EQUIPEMENTS CIBLES

UTILISATEUR

RDP
VNC
SSHv2
http/https
SFTP
Telnet
rlogin

RDP

SSHv2
https
SFTP

Autorisation (ou non) des fonctions SSH

- **Shell Session**
- **Exécution de commandes distantes**
- **SCP (upload & download)**
- **X11 Forwarding**

Enregistrement des sessions

SESSIONS RDP (WINDOWS)

- Conservation d'une vidéo au format Flash du contenu de la session (visualisation de l'écran du PC de l'utilisateur)
- Récupération automatique d'informations sur le contenu de la session

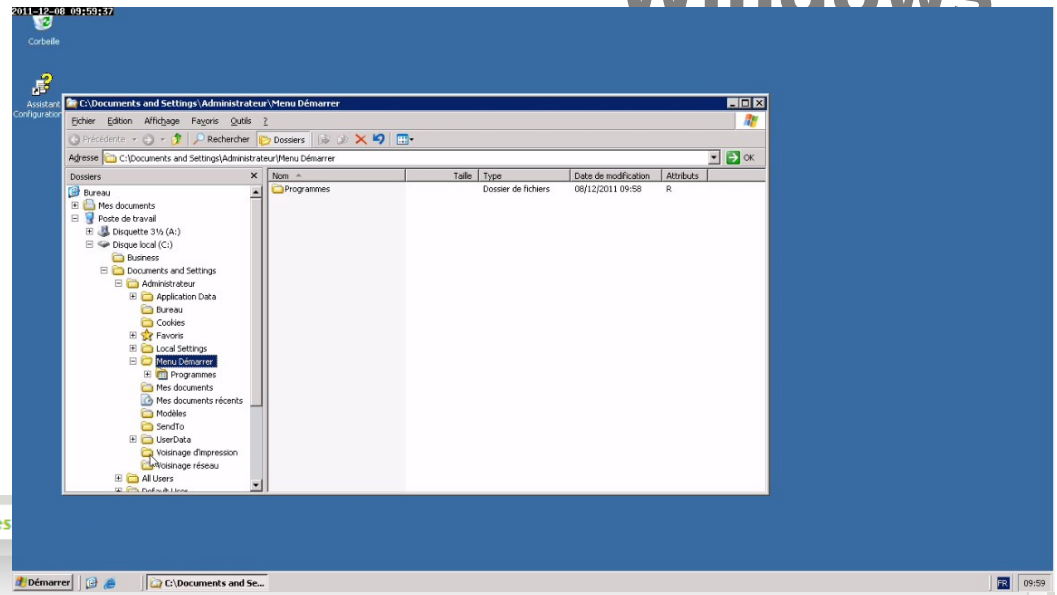
SESSIONS SSH/TELNET

- Conservation des lignes de commande entrées par l'utilisateur et du "retour" de l'équipement
- Informations disponibles dans un fichier texte ou bien dans un fichier semi-vidéo

WallixAdminBastion

OCR sur les sessions Windows

Obtenir automatiquement d'une session Windows enregistrée ...



Les informations pertinentes !

Titres des fenêtres

2011-12-08_09:59:15	Gérer votre serveur
2011-12-08_09:59:20	Document - WordPad
2011-12-08_09:59:31	bonjour.rtf - WordPad
2011-12-08_09:59:37	C:\Documents and Settings\Administrateur\Menu Démarrer
2011-12-08_09:59:42	C:\WINDOWS
2011-12-08_09:59:46	C:\Business
2011-12-08_09:59:48	Business Plan 2012.rtf - WordPad

1-7 / 7

< << Page 1 of 1 >> > 25 Reset

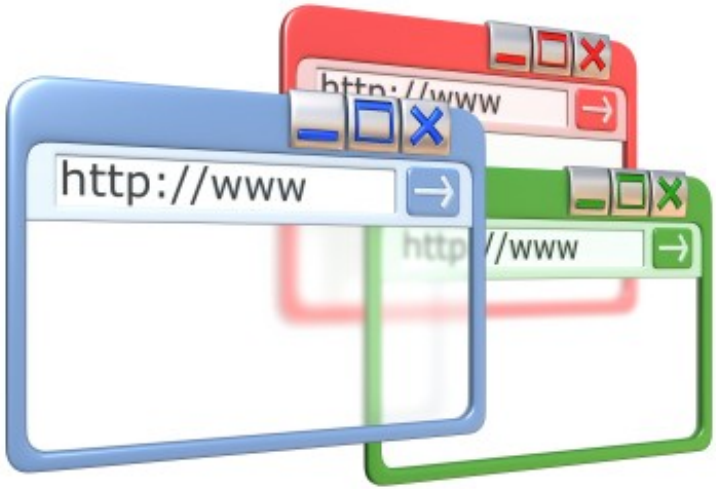
Qui peuvent également être exploitées dans un SIEM !

Support natif http/https

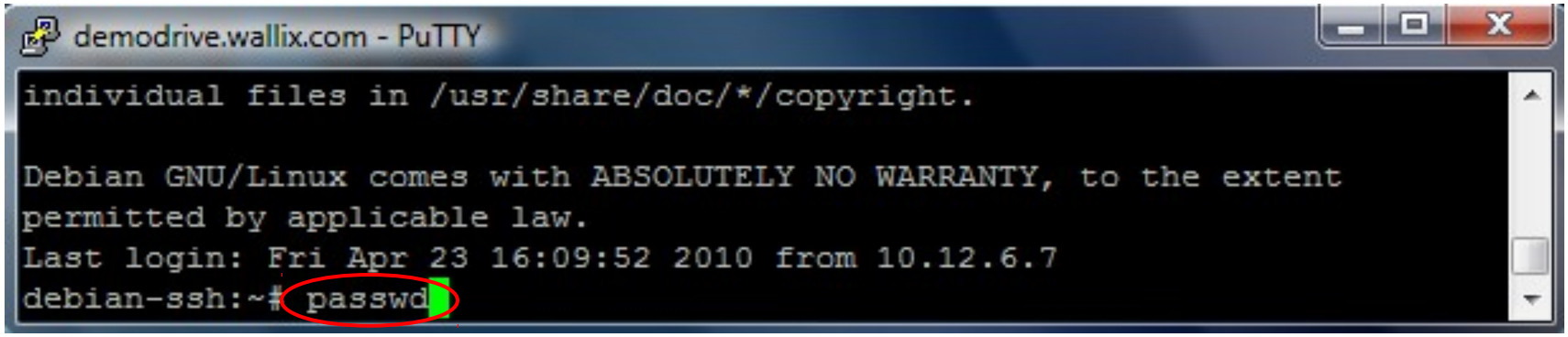
WAB vous permet de contrôler et de tracer les accès aux interfaces web d'administration d'équipements ou d'applications.

• Permet de tracer les connexions vers les applications métiers exploitant une interface web

• Evite d'avoir à installer une solution spécifique pour tracer les connexions vers des interfaces Web



Contrôle des flux SSH



Dans l'exemple ci-dessus, l'expression « passwd » figure dans la liste des commandes interdites

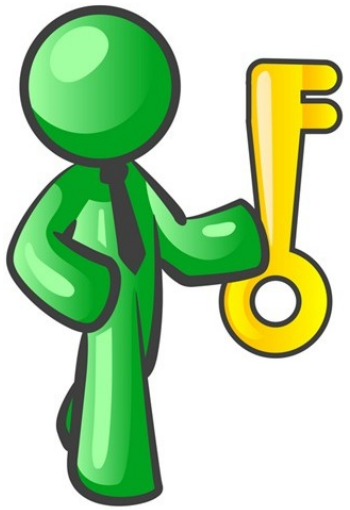
La détection de l'expression « passwd » déclenche l'envoi d'une alerte et/ou la coupure de la connexion.

Gestion des mots de passe cibles

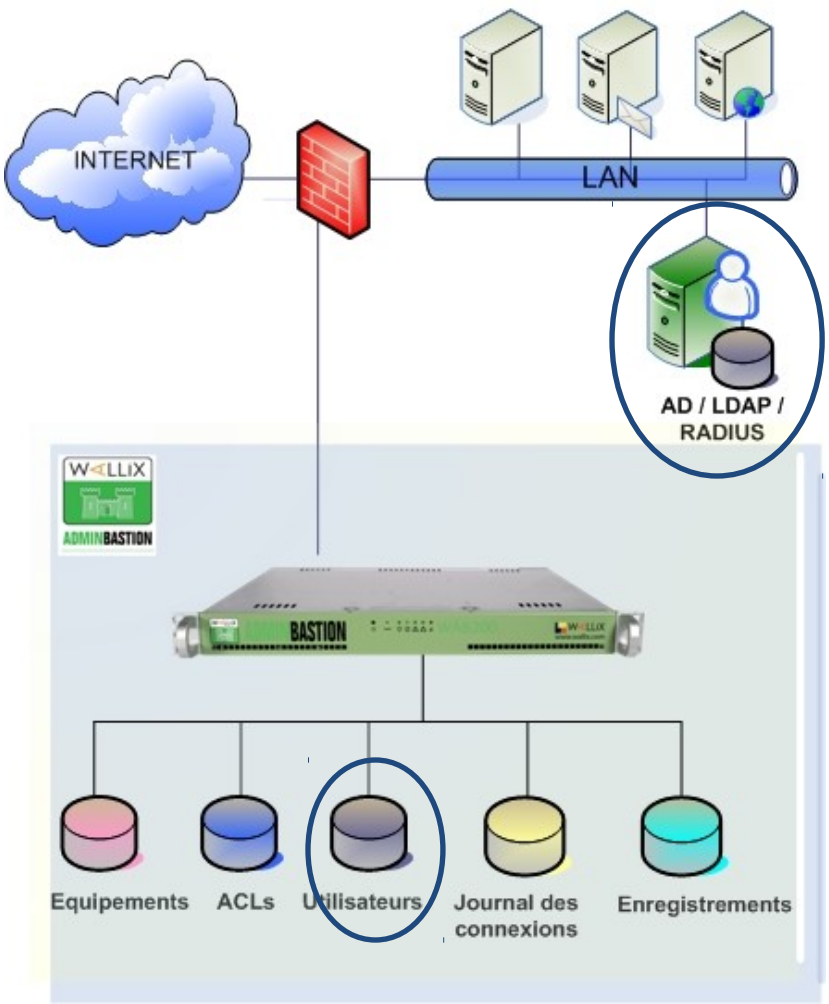
WAB permet d'appliquer une politique de gestion de mots de passe des comptes cibles avec notamment le changement automatique des mots de passe

Il est possible de déterminer la périodicité du changement de mots de passe ainsi que la taille minimale des mots de passe

Cela permet de répondre aux exigences réglementaires concernant les mots de passe des comptes critiques



Architecture interne



OPTION 1

L'appliance WAB héberge les bases de données utilisateurs, les ACL* et les bases équipements

OPTION 2

L'appliance WAB se connecte à un annuaire extérieur** pour l'authentification utilisateur

* Access Control List

** Annuaires LDAP/LDAPS, Active Directory, Radius

Authentification forte

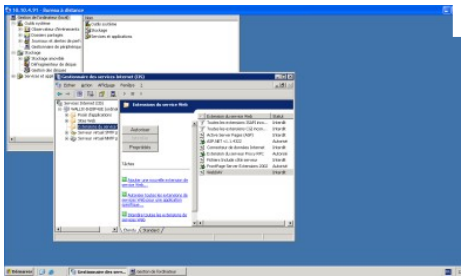
Technologies

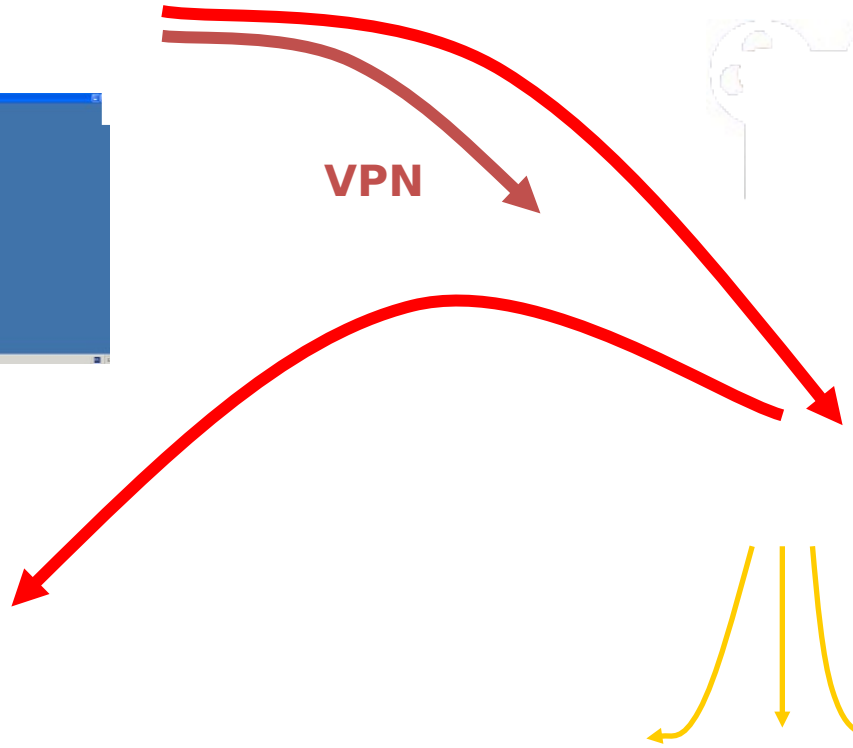
- **RSA SecurID**
- **Radius**
- **ActivCard**
- **Autres**

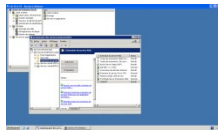
En option
Support des certificats X509v3

WallixAdminBastion

Cas concret d'utilisation

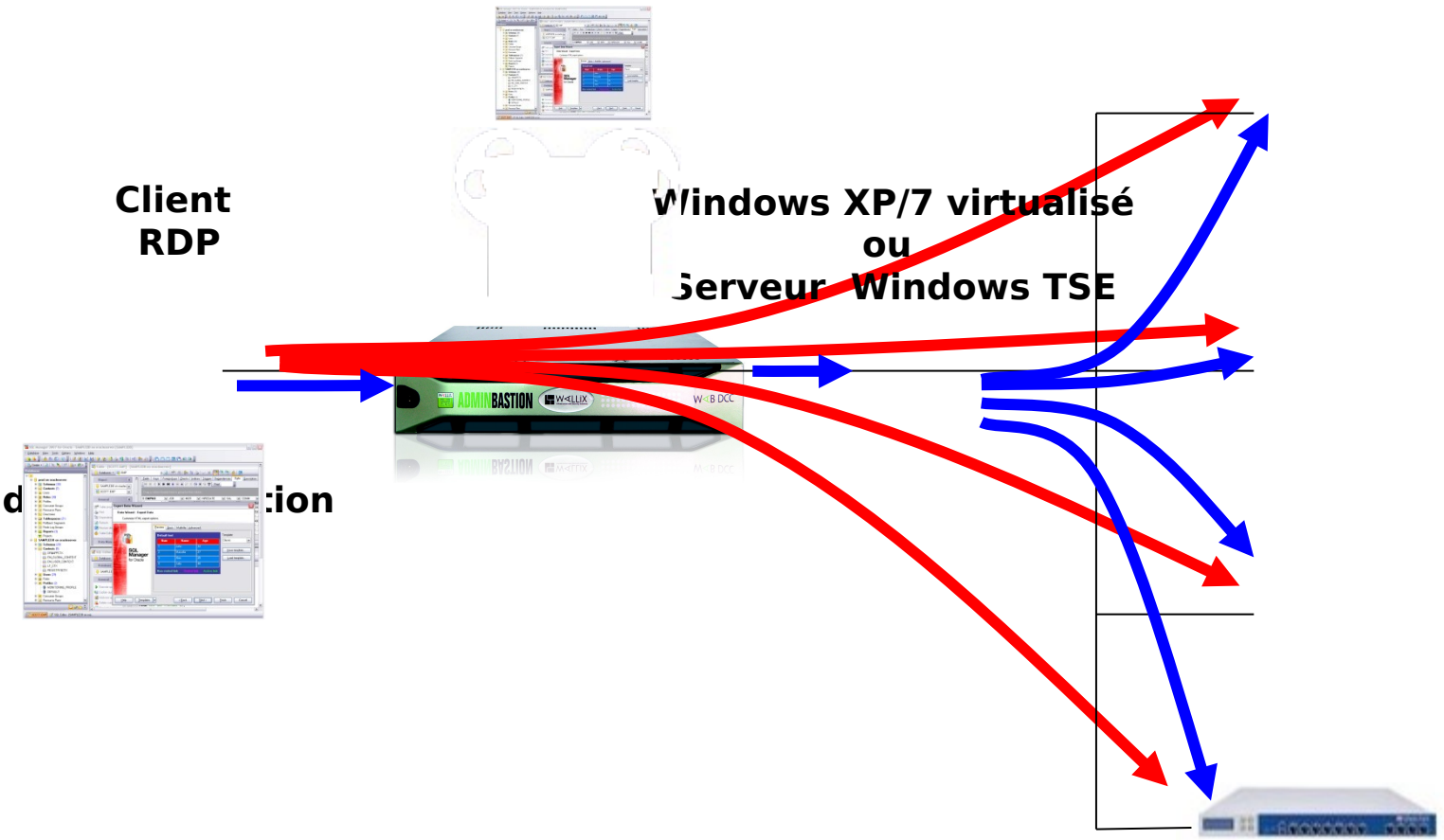






WALLIX TRACE, AUDIT & TRUST

Cas concret -Applications client-serveur



WAB - Facilité de déploiement

Aucun agent à installer sur les serveurs ou sur les équipements

- Gain de temps de déploiement
- Intégration aisée dans l'infrastructure existante
- Baisse du coût de possession (TCO)

Aucune formation nécessaire pour les utilisateurs de WAB

- WAB ne change pas les méthodes de travail
- Conservation des outils actuels (client TSE/RDP, Putty, WinSCP, navigateur Web, ligne de commande ...)

Appliance ou software

Appliances

10 modèles disponibles : du WAB 5 au WAB 2000

Package logiciel

Disponible sous la forme d'appliance virtuelle VMWare

WallixAdminBastion

Appliances WAB

Appliance	Processeur	RAM	Disques	Alimentation
WAB 5 – 15	Pentium G620 (2,6 GHz) – Dual Core	4 Go	500 Go utile	Simple
WAB 50	Core i3 540 (3 GHz) - Dual Core	4 Go	RAID 1 - 250 Go utile – Hot-plug	Redondante - Hot-plug
WAB 100 – 200	Xeon X3480 (3 GHz) - Quad Core	8 Go	RAID 1 - 1 To utile – Hot-Plug	Redondante - Hot-plug
WAB 400 – 600	Xeon X5675 (3 GHz) - Hexa Core	16 Go	RAID 10 - 2 To utile – Hot-Plug	Redondante - Hot-plug
WAB 800 – 1000	2 * Xeon X5675 (3 GHz) - Hexa Core	32 Go	RAID 5 - 14 To utile – Hot-Plug	Redondante - Hot-plug
WAB 2000	2 * Xeon E7-4850 - Deca Core	64 Go	RAID 10 - 1,8 To utile (SAS) – Hot-plug	Redondante - Hot-plug

Support Silver

- Accès aux mises à jour mineures & correctifs logiciels
- 2 interlocuteurs accrédités pour contacter le support.
- Support téléphonique & e-mail : Prise en main des tickets en J + 1
- Disponibilité : du lundi au vendredi de 9h00 à 19h00 (GMT+1)
- Garantie matérielle : Intervention en J+1 *
- Protection des données **

Support Gold

- Accès aux mises à jour mineures & correctifs logiciels
- 4 interlocuteurs accrédités pour contacter le support.
- Support téléphonique & e-mail : Prise en main des tickets en 8 H
- Disponibilité : 7 jours sur 7 de 9h00 à 19h00 (GMT+1)
- Garantie matérielle : Intervention en H+4 *
- Protection des données **

Support Platinum

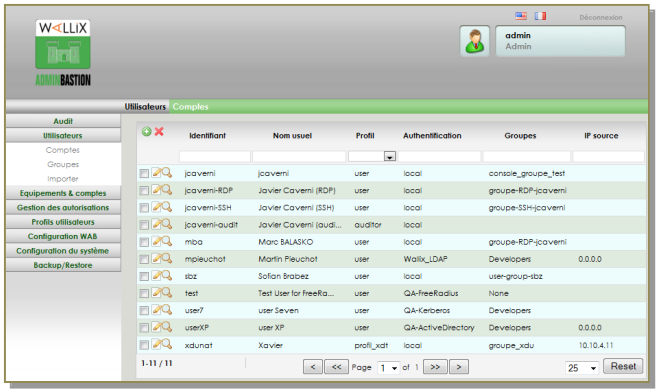
- Accès aux mises à jour mineures & correctifs logiciels
- 6 interlocuteurs accrédités pour contacter le support.
- Support téléphonique & e-mail : Prise en main des tickets en 2 H
- Disponibilité : 7 jours sur 7 - 24 heures sur 24 (GMT+1)
- Garantie matérielle : Intervention en H+2 *
- Protection des données **

* Toutes nos appliances bénéficient d'une garantie matérielle comprenant un service d'intervention sur site. La demande d'intervention est effectuée par nos services dès la qualification de l'incident par nos équipes techniques.

** Cette option, incluse dans toutes nos offres de support, permet aux clients de garder le contrôle de leurs données sensibles en conservant leurs disques durs lors du remplacement de matériels défectueux.

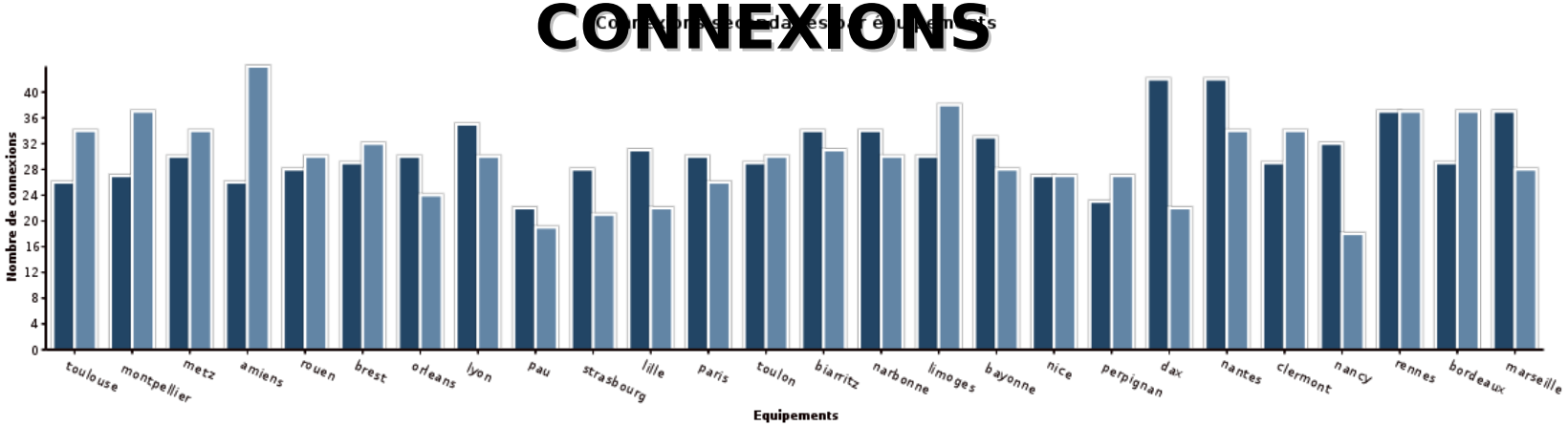
WALLIX TRACE, AUDIT & TRUST

Facilité d'administration



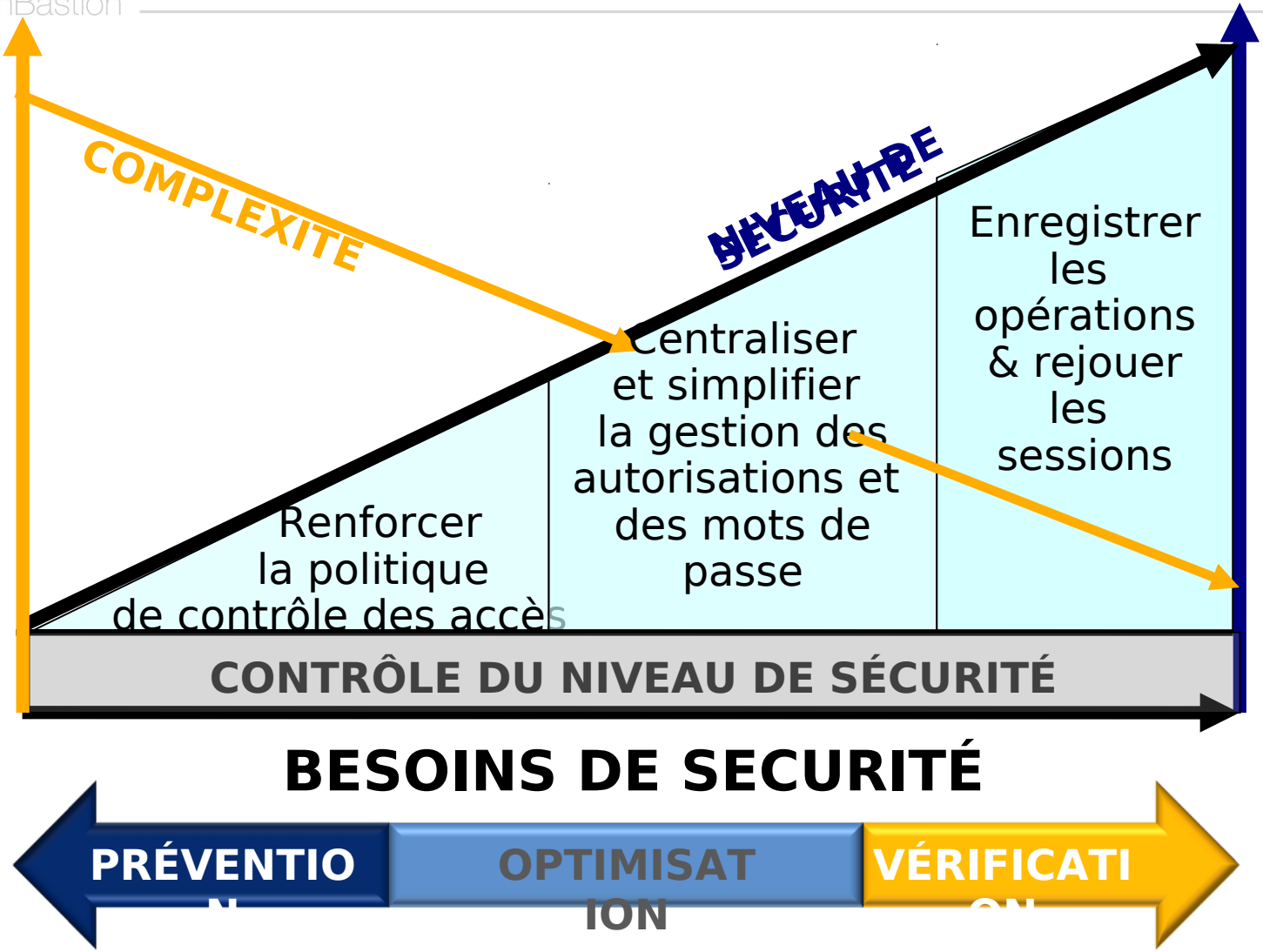
- Interface Web (https) en anglais et en français
  - Compatible IE7+ et Firefox
- Interface « CLI »
  - Pilotage possible du WAB via scripts externes ou applications tierces
- Possibilité de définir des profils avec des droits spécifiques (ex : auditeur)
- Possibilité de définir des périmètres d'actions par administrateur du WAB – en terme d'utilisateurs et/ou de comptes cibles

REPORTING GRAPHIQUE SUR LES CONNEXIONS



- Export au format csv des données pour exploitation ultérieure
- Alertes temps réel (mail & logs) paramétrables :
  - Détection de chaines de caractères interdites (SSH)
  - Echec d'authentification sur le WAB
  - Echec de connexion sur le compte cible …
- Envoi par mail d'un rapport quotidien sur les connexions

Élever le niveau de sécurité



Réponses aux besoins

Questions

Merci de votre attention

Marc BALASKO
marc.balasko@wallix.com
Tel : 01.70.36.37.52
Mob : 06.61.84.78.03