

Projet Sécurité des SI

« Groupe Défense »



Auteurs Candide SA

Diffusion : limitée

Type de document Compte rendu Projet Sécurité

Destinataires P. LATU

M2 STRI

Date 14/12/09



Version 1.2

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion



Plan

- **Introduction**
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Introduction



Sous-traitance d'une industrie convoitée



Cas d'exploitation typique

Groupe Attaque



Groupe Défense



Groupe Audit



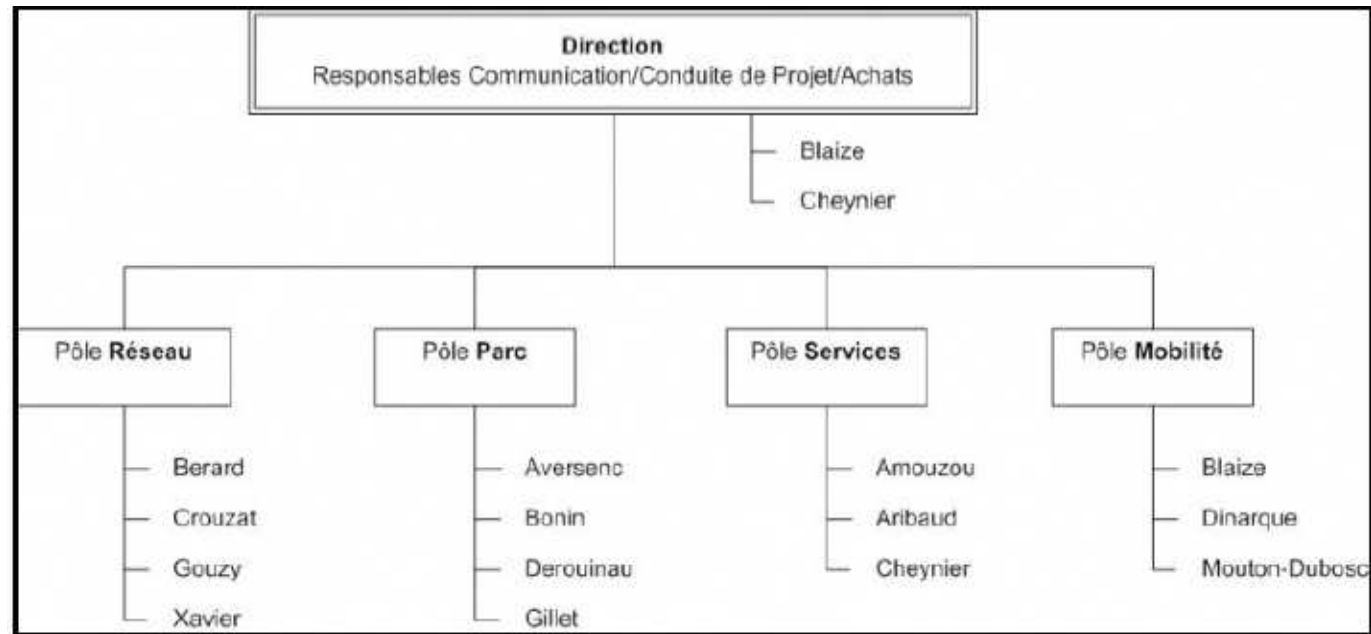
3 Confrontations :

- **Scénarios préalablement définis**
- **Niveau de sécurité évolutif**

Plan

- Introduction
- **Présentation organisationnelle**
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Présentation organisationnelle



Plan

- Introduction
- **Présentation organisationnelle - groupes**
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Présentation organisationnelle : groupes

Direction :



- Collecte des informations
- Rédaction des comptes-rendus d'activités
- Planification et priorisation d'activités
- Gestion des aspects contractuels :
(Audit)

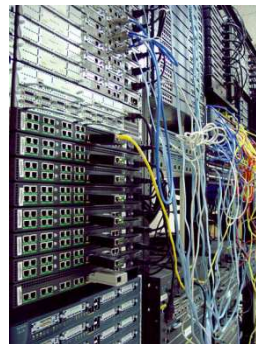


Plan

- Introduction
- **Présentation organisationnelle - groupes**
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Présentation organisationnelle : groupes

Réseau:



- Etude Schémas d'interconnexion
- Installation & configuration
- Maintenance & évolution
- Principaux thèmes :
 - Configuration équipements
 - VLAN
 - Adressage IP
 - Filtrage
 - Routage

Plan

- Introduction
- **Présentation organisationnelle - groupes**
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Présentation organisationnelle : groupes



Services:



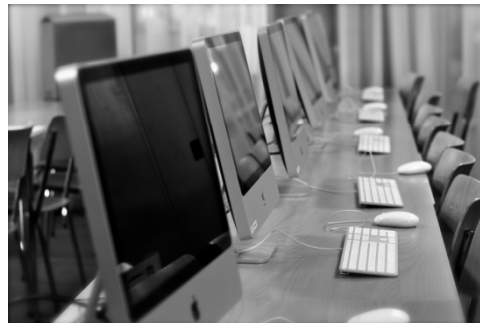
- **Portail Web collaboratif**
- **Service de messagerie**
- **Sécurisation de la partie applicative**
- **Définir une charte d'utilisation**
- **Thèmes :**
 - Serveurs et Relais de messagerie
 - Politiques de sécurité applicative
 - Services Web
 - FTP

Plan

- Introduction
- **Présentation organisationnelle - groupes**
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Présentation organisationnelle : groupes

Parc :



- Définir les ressources système
- Configuration des terminaux
- Reprise d'activité
- Gestion du domaine
- **Thèmes :**
 - Configuration des différents OS
 - Sauvegarde & synchronisation
 - Virtualisation
 - Active Directory...

Plan

- Introduction
- **Présentation organisationnelle - groupes**
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Présentation organisationnelle : groupes

Mobilité :



- **Mise en place accès distant**
- **Gestion du niveau de sécurité**
- **Etude de l'impact de la mobilité**
- **Thèmes :**
 - VPN
 - Wifi
 - Clients Nomades
 - Impact sécurité

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- **Architecture technique**
 - **contraintes**
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Architecture technique : contraintes

Difficultés à maintenir un contexte professionnel



Locales

- Disponibilité des ressources
- Accès physiques
- Premier niveau FW / Proxy



Distante

- Configuration changeante du VPN UPS

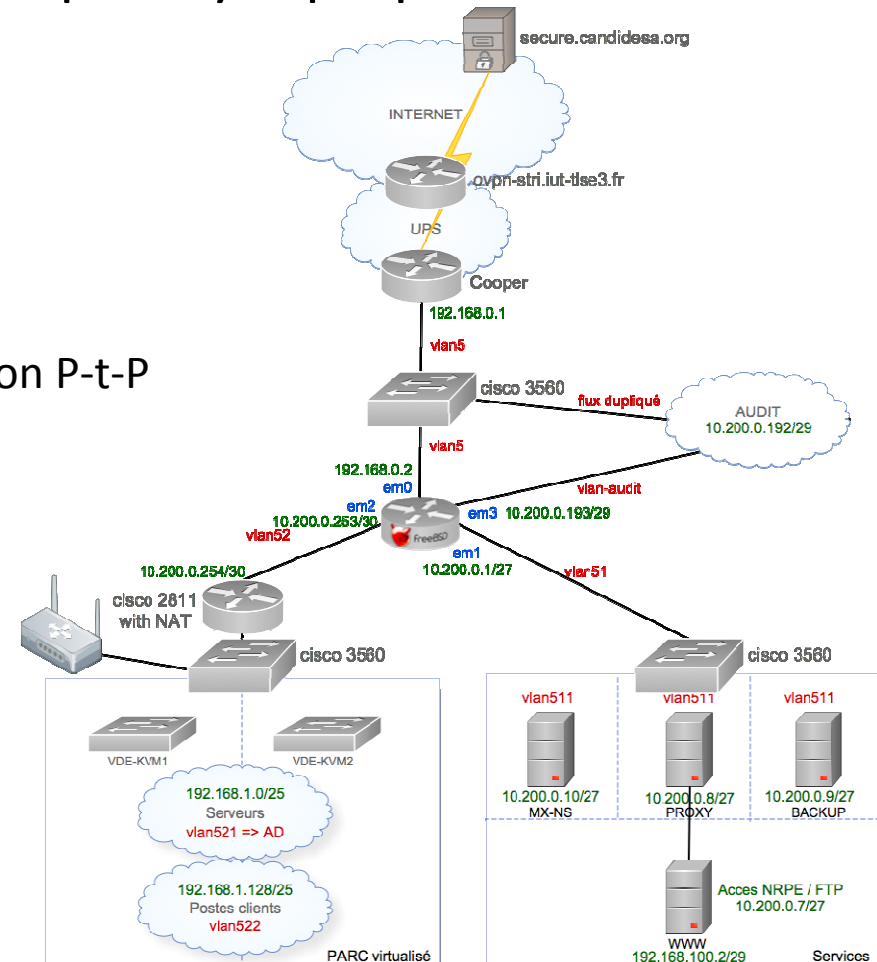


Plan

- 🕒 Introduction
- 🕒 Présentation organisationnelle
 - groupes
- 🕒 **Architecture technique**
 - contraintes
 - **synoptique & éléments**
 - évolutions
 - communication
- 🕒 Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- 🕒 Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- 🕒 Conclusion

Architecture technique : synoptique & éléments

- Découpage en VLANs
- Routage OSPF
- Simulation d'une liaison P-t-P
- Equipements réseaux
 - CISCO
 - FreeBSD



Plan

- Introduction
- Présentation organisationnelle
 - groupes
- **Architecture technique**
 - contraintes
 - synoptique & éléments
 - **évolutions**
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Architecture technique : évolutions

Première confrontation



Défense

- Serveur Web NATé derrière proxy (blog, wiki, site)
- Serveur DNS
- Serveur KVM pour le parc
- Firewall de tête



Audit

- Déversement des logs serveurs
- Déversement des résultats NetFlow

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- **Architecture technique**
 - contraintes
 - synoptique & éléments
 - **évolutions**
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Architecture technique : évolutions

Seconde confrontation



Ajout des services et serveurs :

- FTP sur le serveur Web
- site Web dynamique + B.D
- service de mail
- serveur de sauvegarde distante
- duplication des disques durs des serveurs



Parc :

- suite Office sur postes clients
- XP SPO

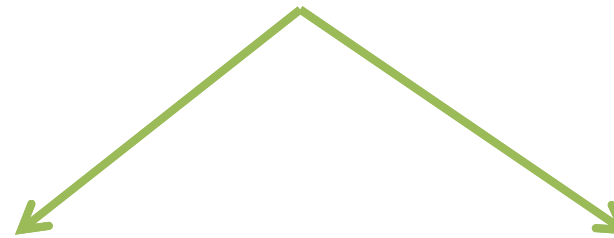
Plan

- Introduction
- Présentation organisationnelle
 - groupes
- **Architecture technique**
 - contraintes
 - synoptique & éléments
 - **évolutions**
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Architecture technique : évolutions

Troisième confrontation

Publication d'informations par l'Audit



Ajustement sécurité



Ajout d'une borne Wifi



Plan

- Introduction
- Présentation organisationnelle
 - groupes
- **Architecture technique**
 - contraintes
 - synoptique & éléments
 - évolutions
 - **communication**
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Service de communication inter-groupes

Domaine candidesa.org



Webmail, roundcube



Wiki



VPN OpenVPN



Monitoring



Accès SSH, clés GPG

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- **Réaction face aux attaques**
 - **confrontations**
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Réactions : face aux confrontations

Première attaque



Attaque Wordpress, v2.8.4



Mise à jour Wordpress, v2.8.6



Web Apache2 : *Max client*
PHP : *max time*

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- **Réaction face aux attaques - confrontations**
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Réactions : face aux confrontations

Deuxième attaque



Faible PDF FoxitReader



✓ Changement du lecteur PDF

✓ Mise en place d'un antivirus



Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- **Réaction face aux attaques**
 - **confrontations**
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Réactions : face aux confrontations

Troisième attaque



Faiblesse du chiffrement WEP



Implémentation de WPA2



Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- **Réaction face aux attaques**
 - **confrontations**
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Réactions : face aux confrontations

Tentatives sans conséquences



Serveur dissimilé



Injection XSS et de bruteforce sur le site web



Scan de ports



Mail Bombing

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - **initiatives audit**
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Réactions : initiative de l'audit

La fuite d'informations



- ✓ Mots de passe serveur
- ✓ Contenu de certains serveurs

Intrusion détectée



- ✓ Attaque Bruteforce sur le Wiki
- ✓ Intrusion sur le Routeur Firewall

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Réactions : initiative de l'audit

Actions entreprises



✓ Modification de la « passphrase »



✓ Modification des mots de passes



✓ Limitation des tentatives de connexion sur le Wiki

✓ Méfiance vis-à-vis du matériel de la salle de TP



✓ Restauration des serveurs

Plan

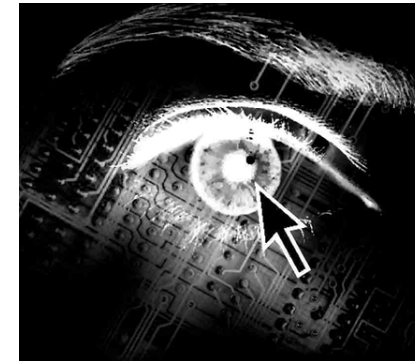
- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- **Réaction face aux attaques**
 - confrontations
 - initiatives audit
 - **dérive audit**
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- Conclusion

Réactions : dérives de l'audit

L'audit bascule dans le groupe attaque

Publication intégrale de :

- ✓ l'architecture
- ✓ la configuration
- ✓ la communication
- ✓ la sécurité



Le + :

Mesure de notre réactivité

Les - :

- **Attaque hors contrat**
- **Attaque physique**

difficilement réalisable (dans le cadre réel)

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- **Retour sur expérience**
 - **sécurité & disponibilité**
 - politique de défense
 - cloisonnement
- Conclusion

Retour sur expérience : sécurité & disponibilité

Principes



Authentification

« *Qui êtes vous?* » : identification par mots de passes



Confidentialité

Stockage des mot de passe dans des fichiers chiffrés avec GPG

+ **Simplification d'utilisation**

+ **Evite la dispersion d'information**

+ **Augmentation de la complexité**

- **Vulnérabilité du chiffrement GPG**

- **Criticité de la machine de stockage**



Autorisations

« *Qu'avez-vous le droit de faire?* » : cloisonnement métier

→ **Principe de moindres privilèges**

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- **Retour sur expérience**
 - **sécurité & disponibilité**
 - politique de défense
 - cloisonnement
- Conclusion

Retour sur expérience : sécurité & disponibilité

Principes

➔ **Audit et journalisation**

Journalisation de l'activité des serveurs

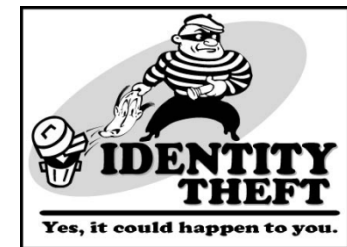
➔ **Intégrité**

- Signatures numérique et authentification de messages
- Garantie par Architecture Multi-tiers

➔ **Disponibilité**

Reprise d'activité après incident :

- ✓ Archivage pour restauration : Backup centralisés
- ✓ « Snapshots » : Sauvegarde des disque via LVM



Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- **Retour sur expérience**
 - **sécurité & disponibilité**
 - politique de défense
 - cloisonnement
- Conclusion

Retour sur expérience : sécurité & disponibilité

Critiques du projet



Architecture Multi-tiers

- Couche Présentation
 - Présente le produit fini
- Couche Middleware
 - Composition/Construction
 - Logique applicative
- Couche Database
 - Stocke l'information brute
 - Persistance des données



Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- **Retour sur expérience**
 - **sécurité & disponibilité**
 - politique de défense
 - cloisonnement
- Conclusion

Retour sur expérience : sécurité & disponibilité

Critiques du projet



Firewall matériel

- + **Intégré**
- + **Administration simple**
- + **Niveau de sécurité → bon**
- **Maj liées aux constructeurs**
- **Peu flexibles**



Firewall applicatif

- + **Personnalisables**
- + **Niveau de sécurité très bon**
- **Charges d'administration accrues**

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- **Retour sur expérience**
 - sécurité & disponibilité
 - **politique de défense**
 - cloisonnement
- Conclusion

Retour sur expérience : politique de défense

Politique de défense en 5 axes :

Se prémunir des attaques

- Eviter l'apparition de failles : systèmes en versions stables

Bloquer

- Les attaques avant propagation : solutions de filtrage statefull

Renforcer

- la défense : Chiffrement des disques par « passphrase » ?

Détecter et identifier

- Les incidents > Apport de corrections

Intervenir

- Sur le Système d'Information : Processus de reprise sur activité

Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- **Retour sur expérience**
 - sécurité & disponibilité
 - politique de défense
 - **cloisonnement**
- Conclusion

Retour sur expérience : la nécessité du cloisonnement

▪ Contexte typique entreprise :

- Intra entreprise : externalisation de services
refonte organisation métiers/projets
- Prestataires : solutions « clé en main » vulnérables

▪ Dérive de candidesa.org : ressources extérieures

- Passerelle VPN
- Centralisation des informations propre au projet
- Support des communications électroniques des collaborateurs



Plan

- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- **Conclusion**

Conclusion

Cibles des compromissions :

- Disponibilité des infrastructures
- Intégrité des données
- Confidentialité
- Crédibilité et image publique de l'entreprise

Problèmes intra et inter-équipes mis en évidence :

- Facteurs humains
- Absence de visibilité globale sur les systèmes et les applications
- Niveau de sécurité applicables à une architecture structurée

Plan

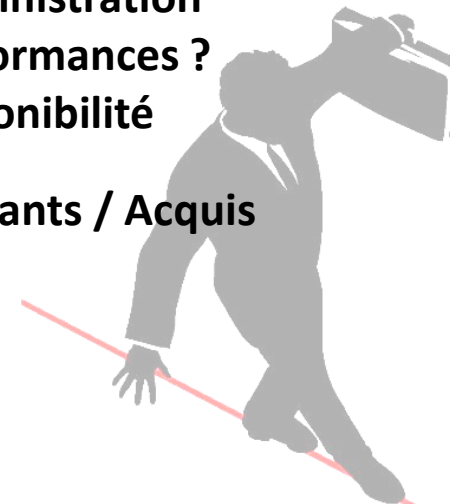
- Introduction
- Présentation organisationnelle
 - groupes
- Architecture technique
 - contraintes
 - synoptique & éléments
 - évolutions
 - communication
- Réaction face aux attaques
 - confrontations
 - initiatives audit
 - dérive audit
- Retour sur expérience
 - sécurité & disponibilité
 - politique de défense
 - cloisonnement
- **Conclusion**

Conclusion

➔ **Exigences fonctionnelles satisfaites**

➔ **Virtualisation =** - Coûts
- Administration
- Performances ?
+ Disponibilité

➔ **Sensibilisation des participants / Acquis**



Projet Sécurité

« Groupe Défense »



Auteurs	Candide SA	Diffusion : limitée
Type de document	Compte rendu Projet Sécurité	
Destinataire	P. LATU	M2 STRI
Date	14/12/09	
Version	1.2	