Carré des Docks – Le Havre – 31 Août / 1er Sept.

Smart Buildings & Territories SUMMIT

Cyber-Sécurisation des bâtiments

Digital Access
Du Smart au Secure

Nom intervenant : Jean-Christophe Denis

Urbanization director, cyber-security architect @ WALLIX

WALLIX CYBERSECURITY SIMPLIFIED

SBA SMART BUILDINGS ALLIANCE FOR SMART CITIES

Smart Buildings & Territories SUMMIT

Smart to Secure

Bâtiments, villes, territoires…

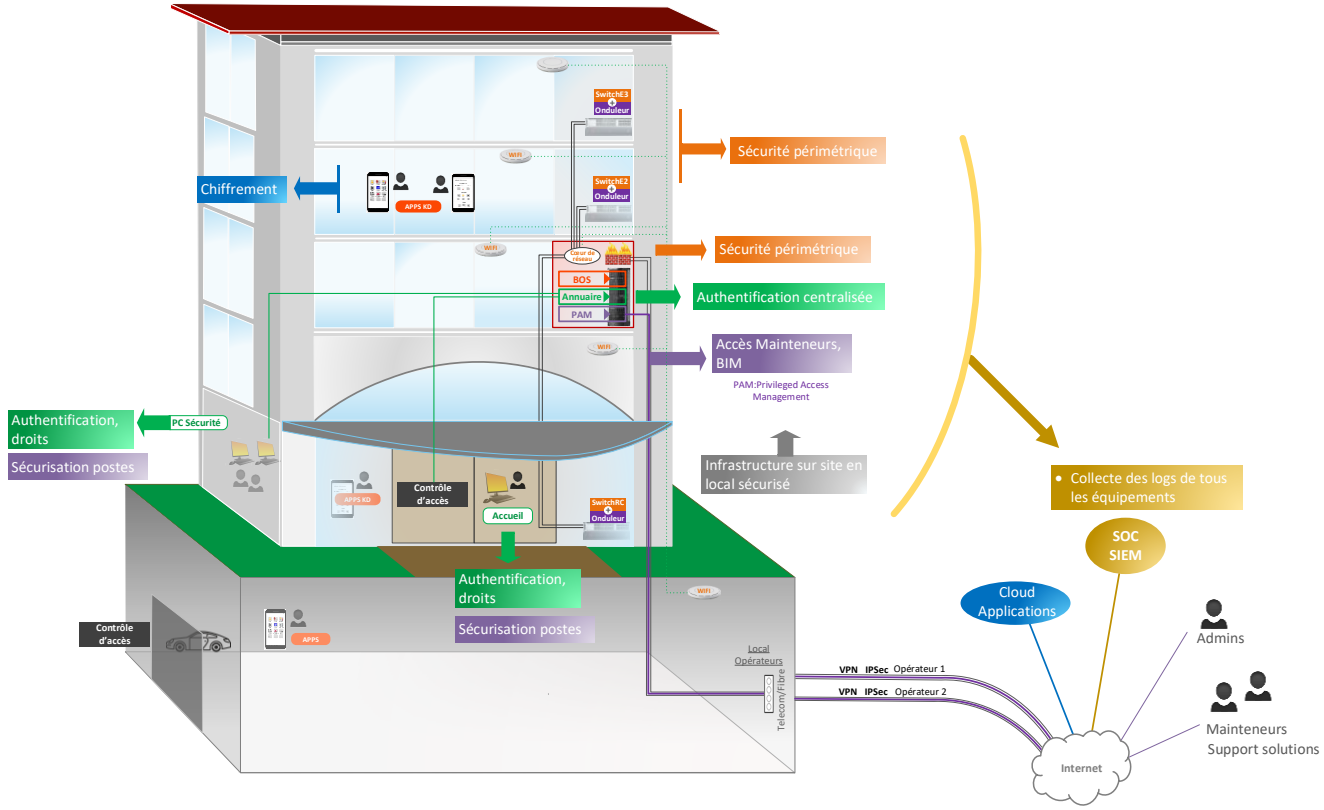
L'ajout d'*intelligence*, d'interfaces, induisent de la complexité
et augmente la surface d'exposition des systèmes aux attaques.
Certains évènements aussi : Crise sanitaire…
La dépendance au numérique ne cesse de croître,
et les données sont le nouvel *or*.
L'*intelligence* ne doit pas nuire à la sécurité :
Il faut un plan et collaborer et le faire dès maintenant
car les menaces n'attendent pas !

Enjeux & défis

- La confiance numérique : un cap à maintenir absolument (Sérénité, dépendance etc.)
- Relier le monde de l'OT et de l'IT : Un problème de tempo et de langages
- Une affaire à mener avec les équipementiers pour être en capacité à réaliser les intégrations avec les solutions de cyber sécurité
- Sensibiliser et amener les acteurs à prévoir les budgets dès l'initiation du projet
- Une collaboration d'architectes (Bâtiment/ville et S.I). Les deux doivent travailler de concert, et ce sera de plus en plus vrai !
- Sensibiliser les mainteneurs et exploitants aux bonnes pratiques et les inclure dans le plan de sécurisation
- Favoriser l'adoption des solutions, former les personnels opérationnels

Smart Buildings & Territories SUMMIT

La cyber, vue d'un bâtiment



Cyber sécurité ?

Confidentialité, Intégrité, Disponibilité et Traçabilité

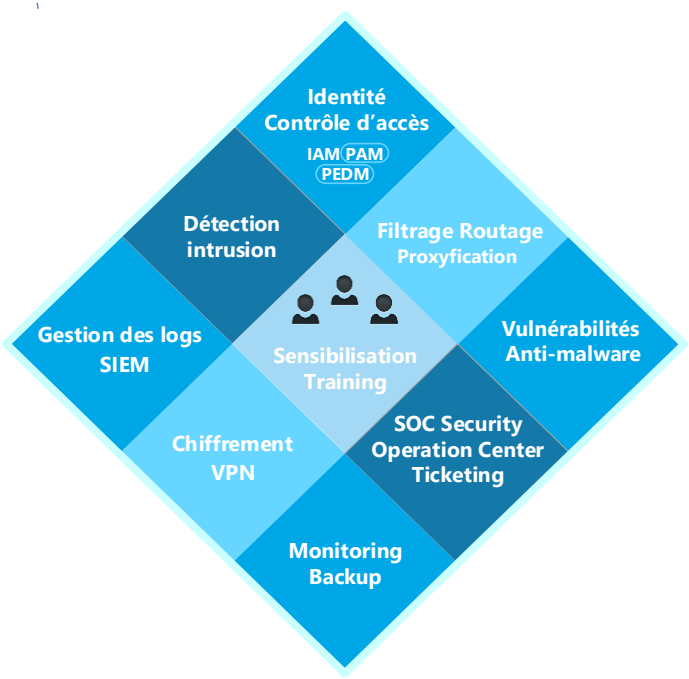
Protection des données, des systèmes **et** des personnes, contre les risques

Concepts

- Least Privilege « POLP »
- Défense en profondeur
- Contrôle des accès
- Traçage et analyse
- Compétences, sensibilisation
- Vision holistique, gouvernance
- Usage des standards
- Principe de Kerckhoffs

Solutions

Hardware, Software,
Organisation, process
Normes… Et du bon sens,
de la matière grise !



N'autoriser que le nécessaire, s'assurer que c'est bien la bonne personne, (re)vérifier et tracer

Méthode

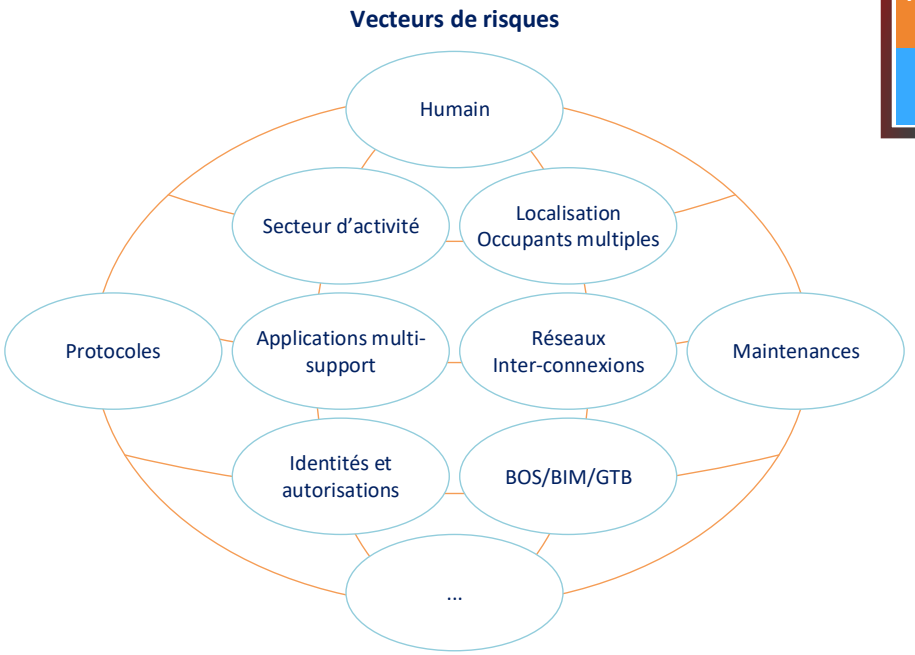
From Design To Run

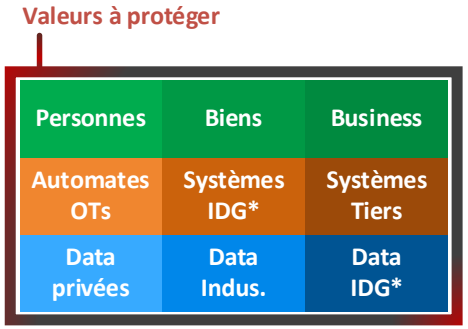
- **Ecouter** : Compréhension fine des besoins et contraintes et du contexte
- **Evaluer** : Périmètre de sécurité, conformité (R2S) / Budget, faisabilité
- **Etudier** : Aspects techniques, organisationnels, conformité, compétences
  - Les **Risques** *(Plan, BIA)*, crises *(RACI*, process)*
- **Communiquer** : Expliquer, sensibiliser aux bonnes pratiques
  Transférer des compétences
- **Orchestrer** : Pour atteindre les objectifs, gouverner. Architecture.
- **Vérifier** : En comités réguliers, validés et documentés
- **Déployer** : Installer et configurer les solutions (⚠ Conformité)
  Documenter *(Architecture et process)* et valider
- **Maintenir** : Assurer la MCO, m-à-j, tracer, analyser, adapter
- **Prévoir** : Déterminer des tendances (monitoring) et faire évoluer

*RACI : Responsible, Accountable, Consulted et Informed

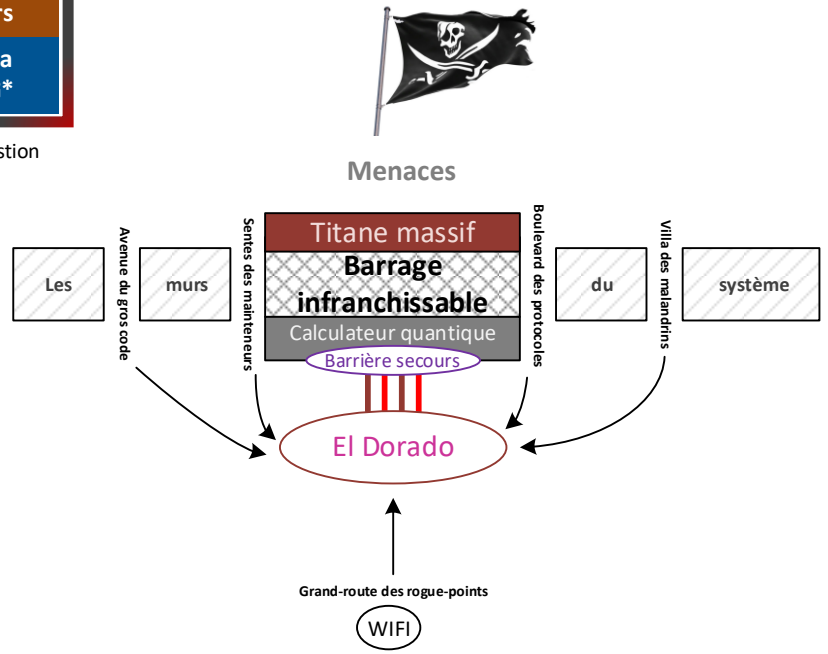
Smart Buildings & Territories SUMMIT

Risques



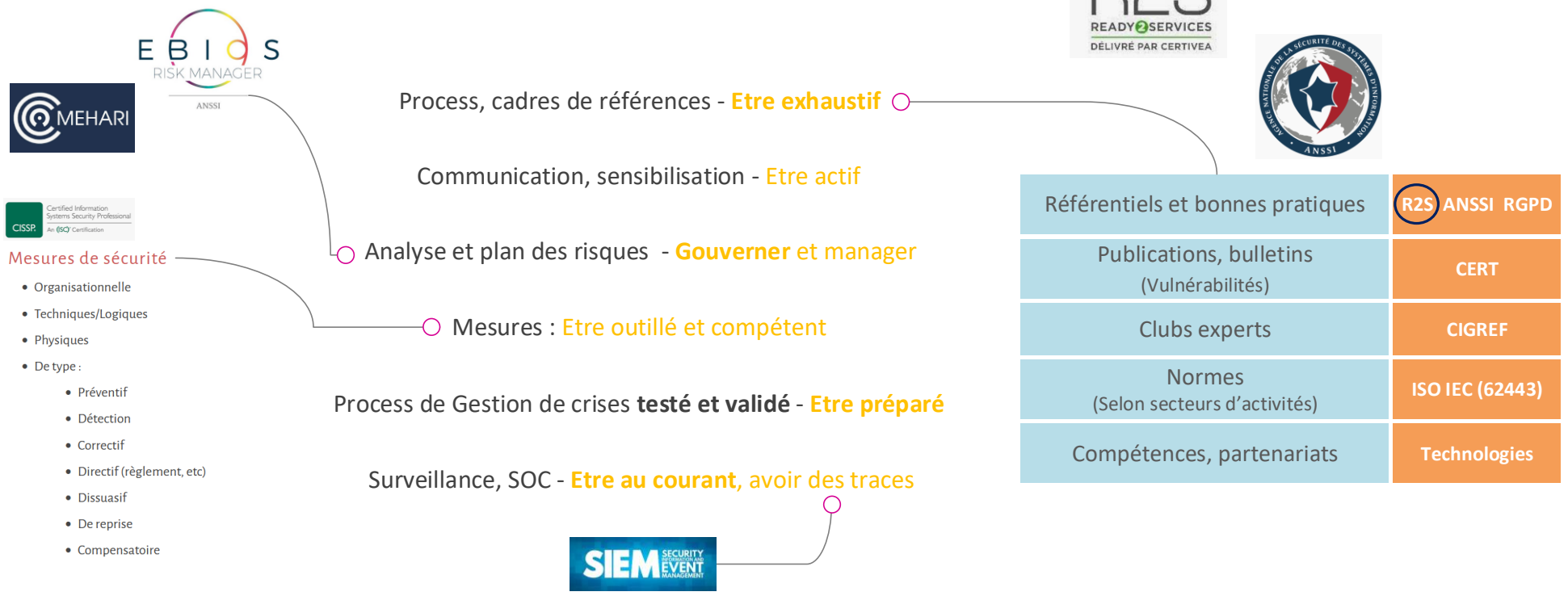


*IDG : Informatique De Gestion



« Faire de la sécurité c'est poser des questions qui peuvent « fâcher » ou faire peur, c'est ingrat et indispensable ». (ANSSI)

Moyens, outils & cadres de références

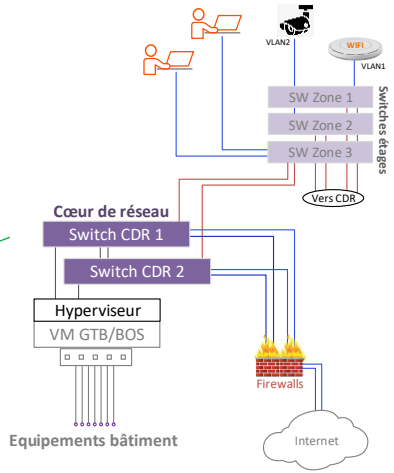


La sécurité à 100% ça n'existe pas. Mais être exhaustif (assets/mesure) permet le maximum.

Programme de cyber sécurisation

S.I Bâtimentaire & ses sous-systèmes, utilisateurs du S.I.B

SSI, GTB-BOS, CA, HVAC, Vidéo, WIFI, IoTs, IRVE, SMé, Visio, Parking etc.
SOC-Ticketing, BIM-GMAO, infrastructure

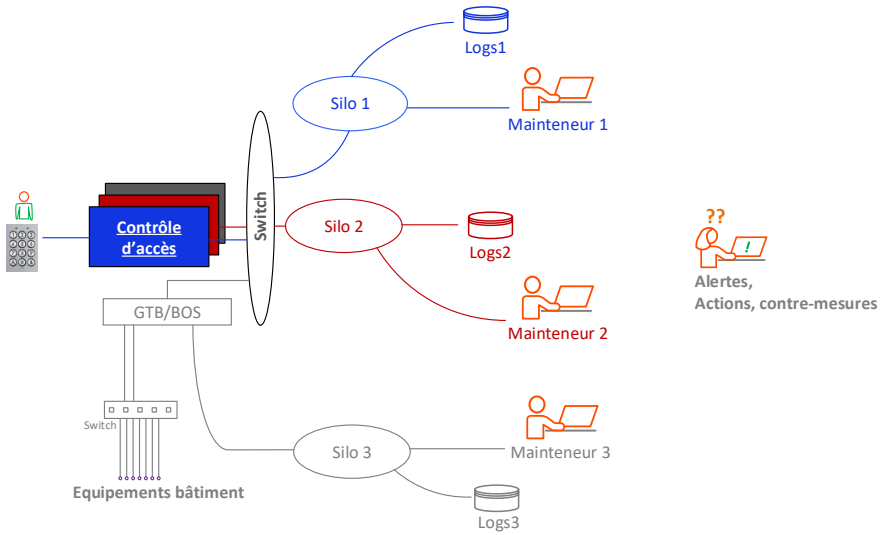


Adapté, conforme
Raisonnable (Légitime)
Modulaire (Evolutif)
Maintenu, surveillé
(Ré)évalué

- Gestion des Risques, accompagnement, sensibilisation
- Sécurité périmétrique et résilience du réseau Smart, VLANs
- Gestion des accès à privilège (Infra, GTB-BOS, BIM…)
- Gestion centralisée des Identités, réglage des autorisations
- Gestion des incidents de sécurité - SOC-SIEM, reporting

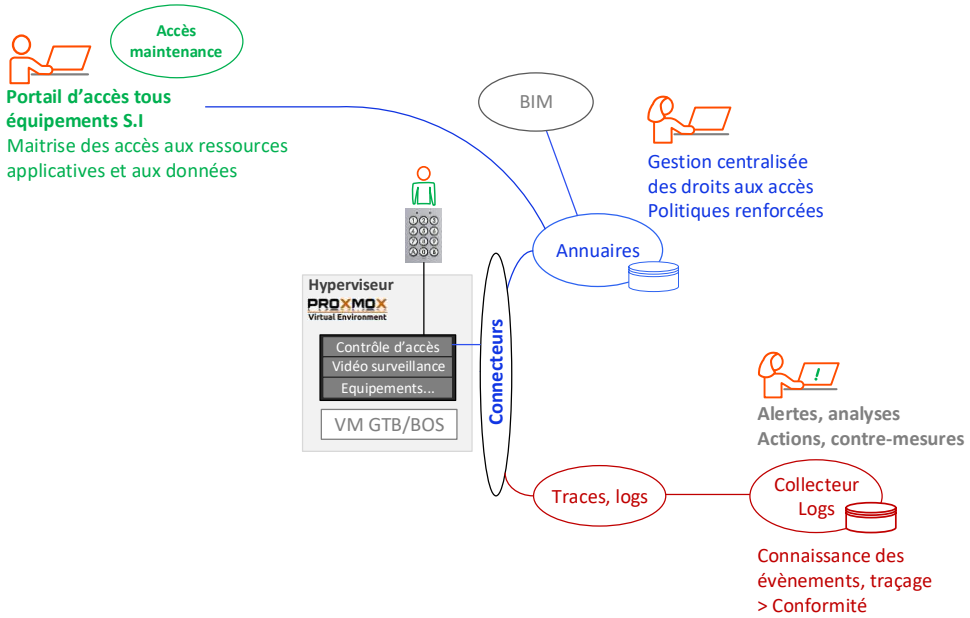
Exemple d'intégration avancée

Contrôle d'accès



Pas de maitrise, logs fastidieux à trouver et sans *end to end,* points d'accès multiples, pas de politique des secrets…

Accès centralisé, maitrisé, sécurisé,
Réutilisation des briques, gestion avancée des secrets, logs centralisés



III Conclusion

Une stratégie, des outils et des Hommes

- Avoir une bonne connaissance de ses actifs (documentée) et des risques
- Déterminer la cible de sécurité et prévoir les budgets adéquats
- Savoir ce qui se passe sur son réseau, disposer d'alertes
- Nature cyclique du risque
- Faire appel au bon sens, à la simplicité
- Sécuriser par l'architecture, pas seulement par l'empilement de solutions
- Utiliser des standards reconnus et leurs communautés
- Communiquer, former, sensibiliser, se certifier
- Nouer des partenariats avec des spécialistes

Smart Buildings & Territories SUMMIT

WALLIX CYBERSECURITY SIMPLIFIED

SBA SMART BUILDINGS ALLIANCE FOR SMART CITIES

MERCI

Retrouvez cette thématique dans le prochain livre blanc de la SBA