THALES
Building a future we can all trust

Sûreté et sécurité, du processeur jusqu'au cloud

Emmanuel GUREGHIAN
Wladimir KSINANT
14 novembre 2024

www.thalesgroup.com

Qui sommes-nous ?

Wladimir Ksinant

Expert cybersécurité
Sécurité des produits et solutions du groupe

MA CARRIERE

1990 développeur soft
1999 6WIND R&D
2004 Thales cybersecurité

UNE COMPETENCE ESSENTIELLE POUR MOI

Le travail d'équipe pour concevoir des solutions sécurisées

UNE ANECDOTE À PARTAGER

Désolé, c'est classifié !

Prouvez-moi votre besoin d'en connaître et je serai heureux de partager des anecdotes ☺

MON SITE WEB PRÉFÉRÉ

https://datatracker.ietf.org/wg/#sec

CE QUE JE CRAINS LE PLUS

La malhonnêteté et le manque de transparence

UNE INVENTION QUI A ATTIRÉ MON ATTENTION

Confidential Compute

CYBERHACKER OU CYBERTRACKER?

CyberTracker

QUELQUE CHOSE D'ESSENTIEL POUR LA CYBERSÉCURITÉ

Rester calme et être prêt

Qui sommes-nous ?

Emmanuel Gureghian

Responsable Laboratoire Systèmes & Embarqués Critiques @ Thales Research

MA CARRIERE

1995 OS Multi-niveaux
2012 Project Design Authority Cyber Aéro THALES
2019 Resp. lab. Safe & Secure

UNE COMPETENCE ESSENTIELLE POUR MOI

Argumenter sans se fâcher

UNE ANECDOTE À PARTAGER

J'ai quand même crée un compte linkedin

MON SITE WEB PRÉFÉRÉ

La voie de l'épée

CE QUE JE CRAINS LE PLUS

Que le ciel nous tombe sur la tête

UNE INVENTION QUI A ATTIRÉ MON ATTENTION

La fusée R7 de Sergueï Korolev

CYBERHACKER OU CYBERTRACKER?

Tracker

QUELQUE CHOSE D'ESSENTIEL POUR LA CYBERSÉCURITÉ

Paranoïaque sur les menaces mais rationnel sur nos ambitions et humble sur nos réalisations

De nouveaux services apparaissent, le plus souvent dans le cloud

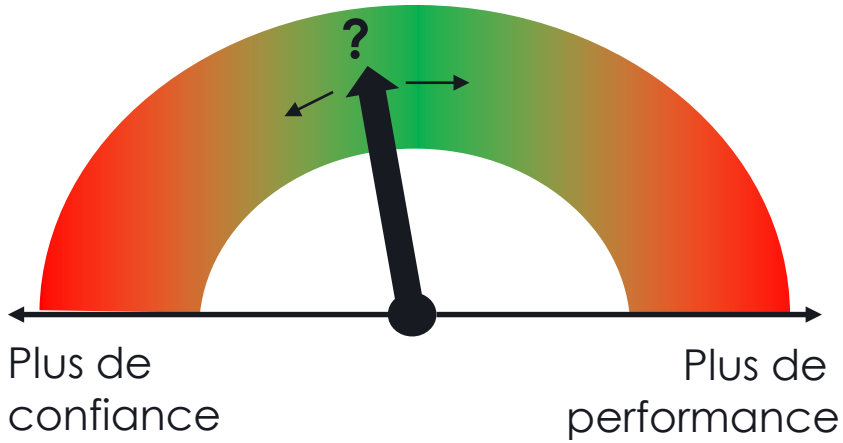
> Exemples de nouveaux services :

- IA, nouvelles chaines de production des logiciels…
- Services SaaS…

> Les avantages du cloud sont importants

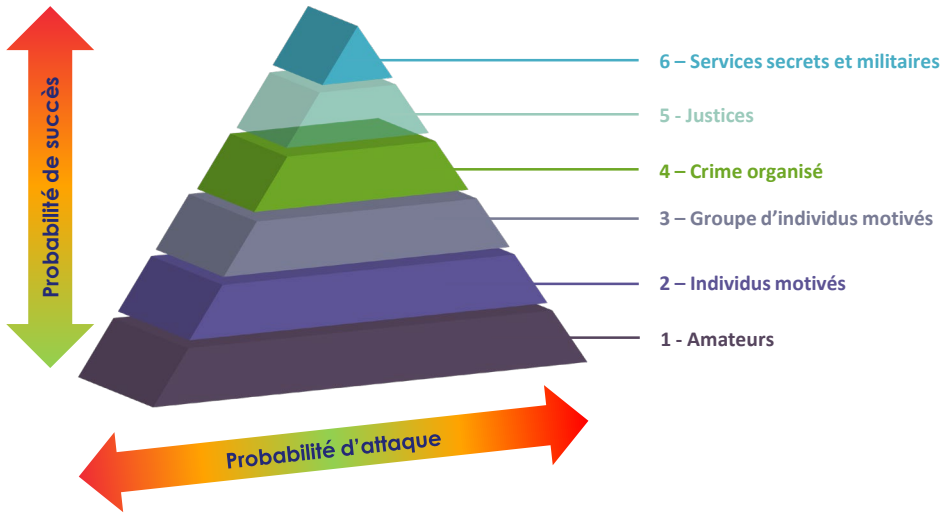
- Moins d'investissement initial (CAPEX)
- Les outils y sont souvent plus efficaces que ceux disponibles sur site client

> Mais cela peut poser des problèmes de confidentialité (et plus largement de cyber-sécurité)



Les risques de cybersécurité à considérer

> De qui veut-on se protéger ?

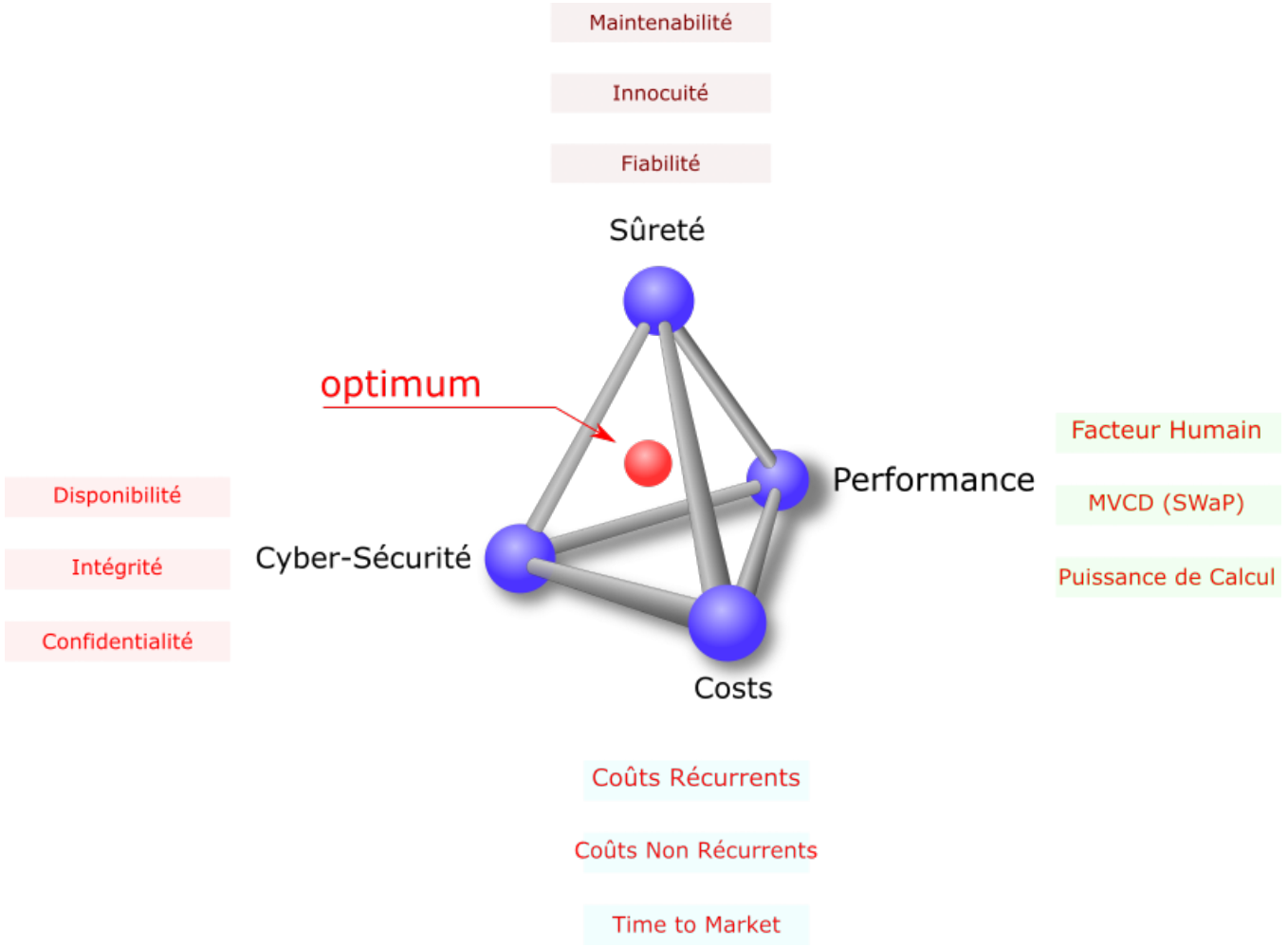


> Les principaux risques à considérer

- Perte de contrôle pour l'utilisateur
- Réglementations et lois
- Les ressources partagées
- Les interfaces de gestion
- Les erreurs de configuration

Quelques grands principes pour la sécurité dans le cloud

Replacer la cyber dans son contexte



Des technologies plus ou moins maitrisées

> Souveraineté des composants

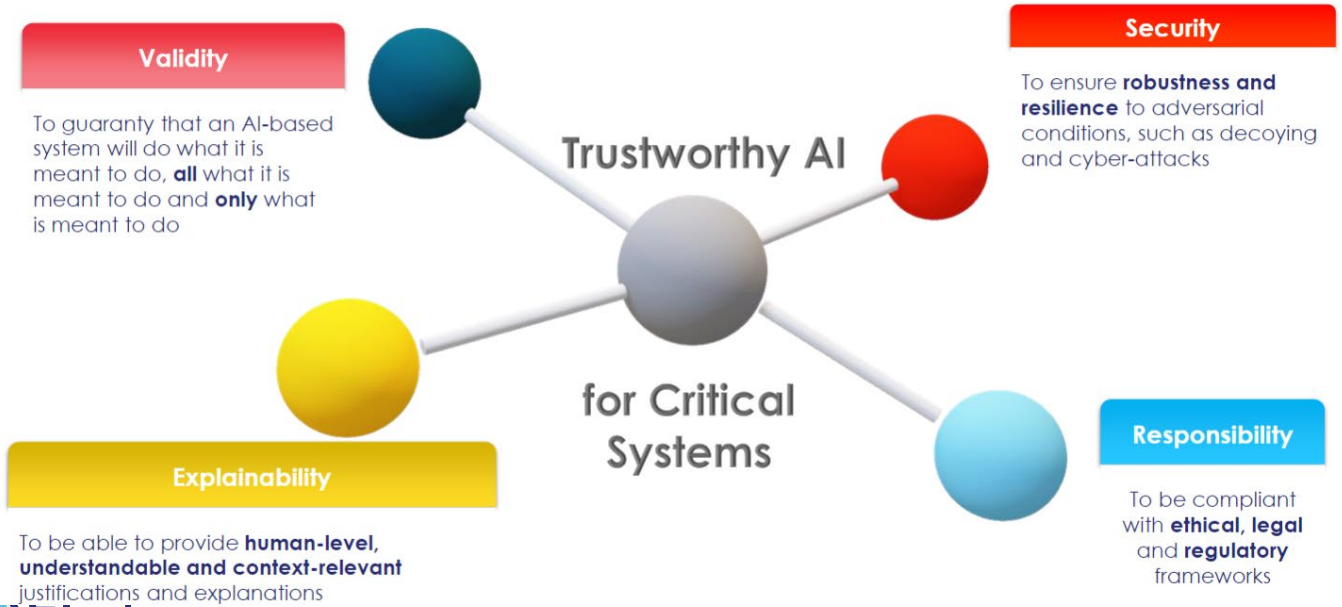
> Complexités du micro au macro des architectures systèmes

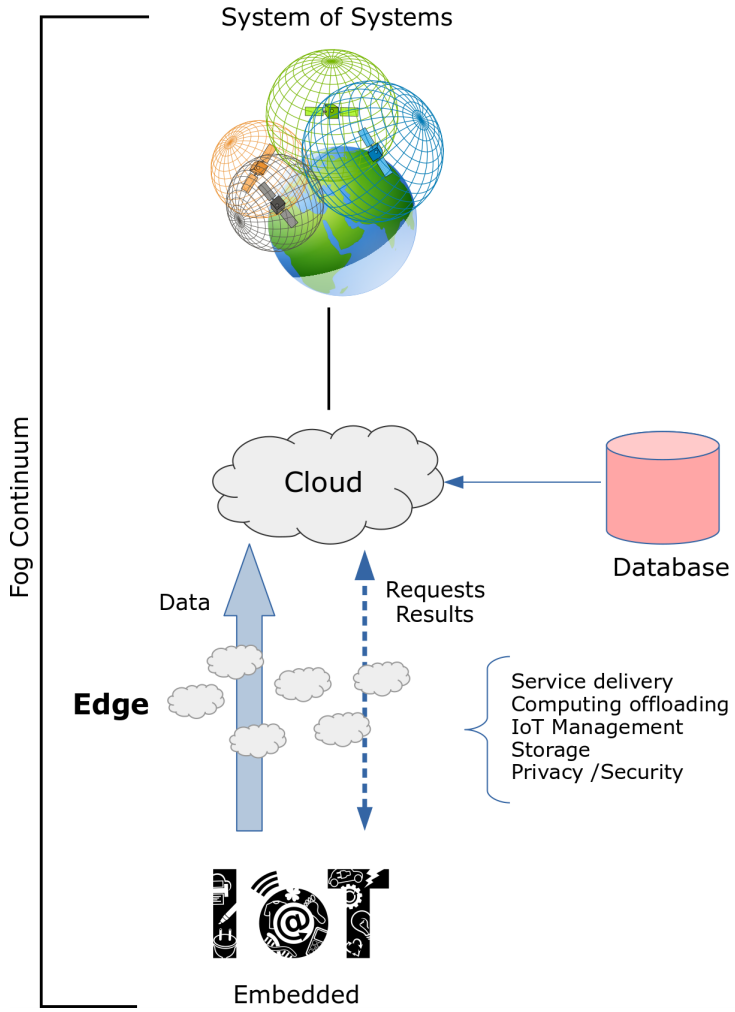
- ➔ **Identifier & contractualiser les interfaces est indispensable**

> Des réglementations de plus en plus contraignantes :

> IA omniprésente

- délicate à maîtriser : validité, explicabilité, sécurité, responsabilité

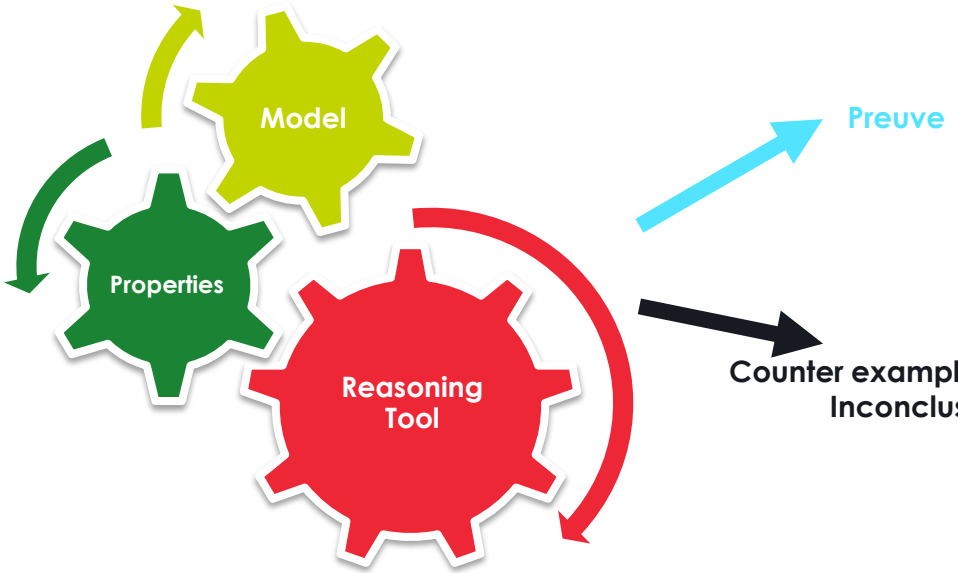




Mettre du rationnel et de la confiance : Intérêt des méthodes formelles

> La « mécanique newtonienne » de l'informatique

- Tout ce que l'on peut faire avec une bonne sémantique
- Convaincre depuis la spécification jusqu'à l'analyse de binaires :
  - Spécifier / Raffiner / Tester / Prouver / Synthétiser / Compiler

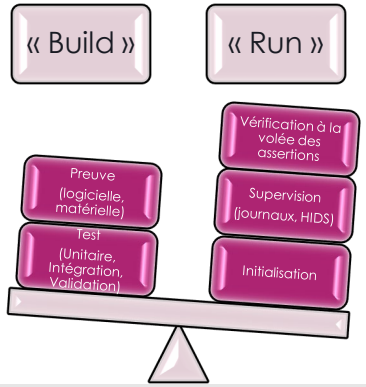


> Architecture & Méthodes formelles

- Tout n'est pas critique ➔ la bonne méthode pour le bon composant
- Le test, encore le test, toujours le test mais …
  - Orchestré & rejouable
  - Généré & vérifié automatiquement
- Intégré dans votre chaîne de CI/CD

> Plusieurs voies à explorer :

- IA & Méthodes formelles :
- - L'IA peut rendre la marche d'entrée moins haute
- - Les méthodes formelles peuvent aider à produire une IA de confiance (cf. manifeste)
- **Prolongez l'utilisation des MF du « build » au « run »**



Quelques recommandations

> Côté Industrie

- Le continuum s'impose à nous,
- Implémentations de confiance pour la crypto :
  - De préférence dans des enclaves non observables
  - Déjà compatibles post-quantique
- L'utilisation des Méthodes Formelles doit amener à repenser l'organisation vers le DevSecOps
- ➔ décloisonner les équipes architectes, développeurs, exploitants, certificateurs
- ➔ aménager les rôles notamment en agile,

> Côté Enseignement & Recherche :

- Systématiser l'enseignement Méthodes Formelles en tronc commun
- Démontrer le passage à l'échelle pour conviancre : le libre à la rescousse
- L'inscription dans l'écosystème est primordiale pour valoriser l'innovation apportée par les briques technos

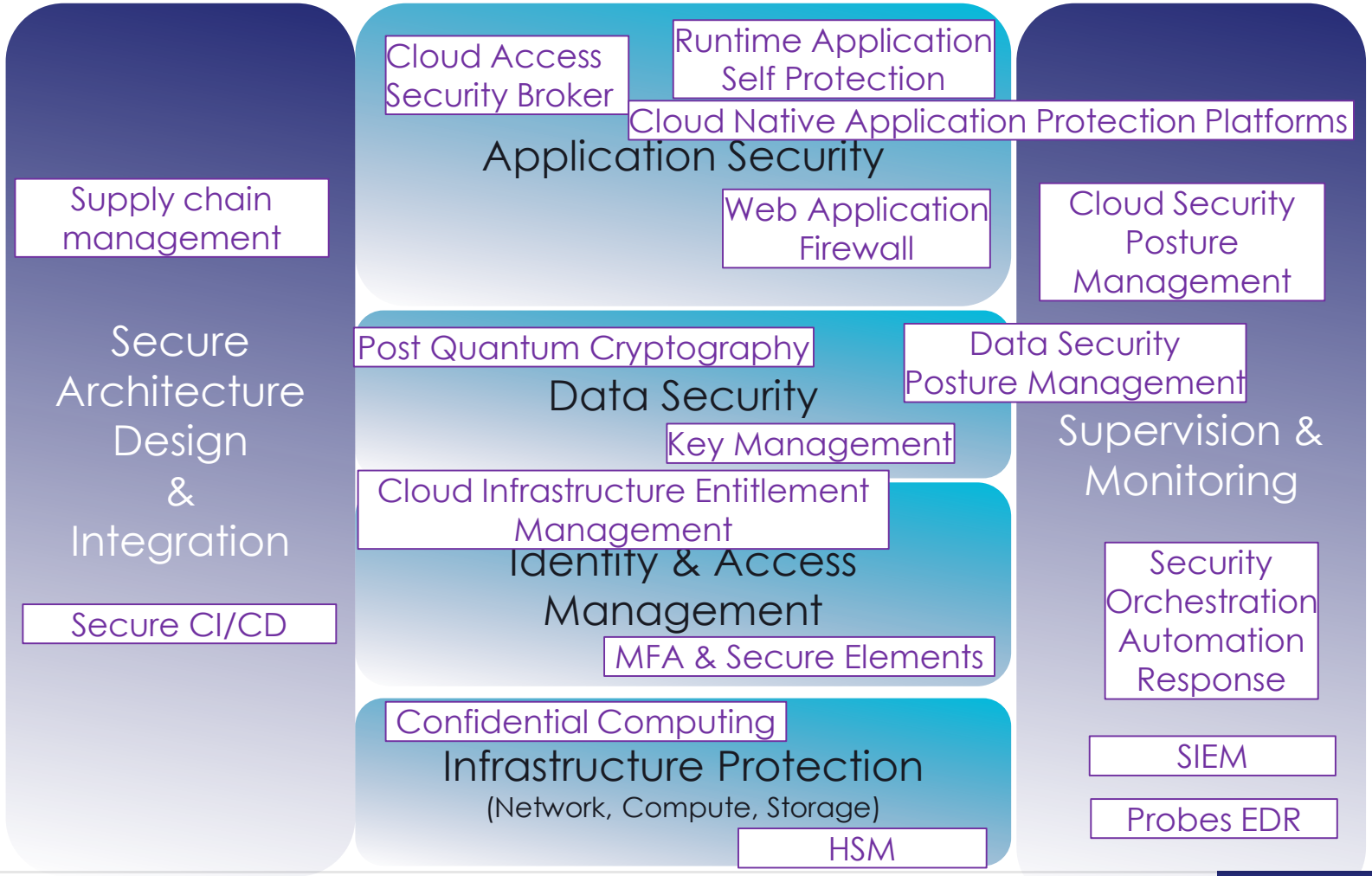
Autres recommandations

> Accompagner le changement plutôt que de tenter d'y résister

> Bien connaître ses risques

- Que devons-nous protéger ?
- De qui voulons-nous nous protéger ?
- Identifier les risques
- Proposer des mesures de sécurité par exemple :
  - Cryptographie robuste avec gestion de clé maîtrisée
  - Des moyens de supervision efficaces
  - Maîtriser sa posture

> Quelques éléments techniques à surveiller



THALES
Building a future we can all trust

Thank you

www.thalesgroup.com