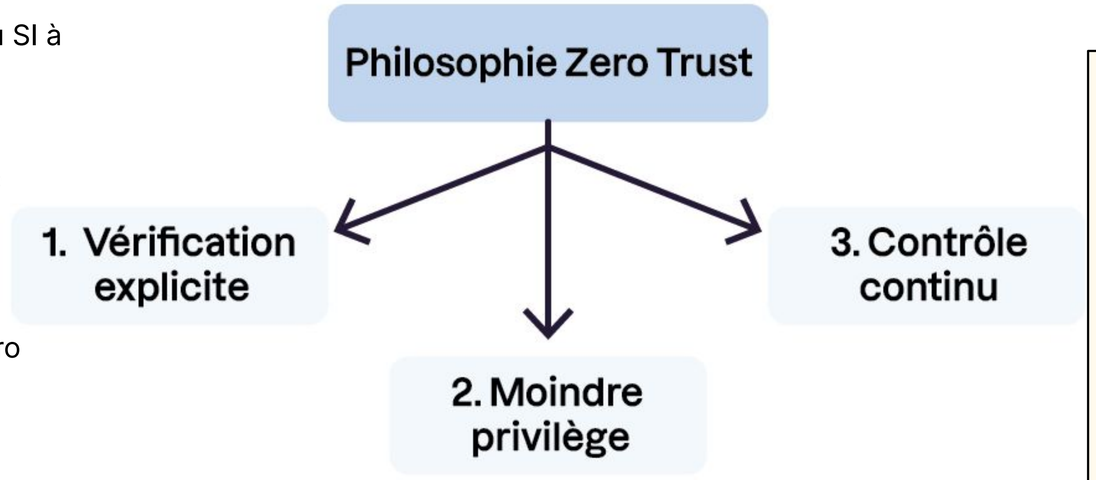
Fiche récap : Concevez votre architecture Zero Trust

Cybersécurité

1. Analyser les scénarios de risques et les vulnérabilités du SI à partir de la démarche EBIOS RM
2. Sensibiliser le COMEX aux limites du modèle de sécurité périmétrique historique
3. Définir une stratégie de transition vers une approche Zero Trust adaptée au SI hybride
4. Initier les chantiers structurants du modèle Zero-Trust, comme la centralisation et le renforcement du contrôle des accès autour d'un fournisseur d'identité unique
5. Prioriser une feuille de route cybersécurité fondée sur les risques et la conduite du changement



Bonnes pratiques

- ✅ Imposer un MFA résistant au phishing pour sécuriser rapidement les accès sensibles
- ✅ Centraliser les authentifications via un fournisseur d'identité unique et simplifier la gestion des accès
- ✅ Appliquer le principe du moindre privilège aux comptes critiques et administrateurs
- ✅ Segmenter les environnements pour limiter les mouvements latéraux en cas de compromission
- ✅ Contrôler les accès SaaS grâce au SSO et aux politiques d'accès conditionnel
- ✅ Superviser les journaux d'accès afin de détecter rapidement les comportements suspects
- ✅ Formaliser les responsabilités cybersécurité via une matrice RACI claire et opérationnelle
- ✅ Prioriser des mesures de sécurité pragmatiques et des quick wins avant les projets complexes de transformation

Erreurs classiques

- ❌ Considérer le réseau interne comme fiable par défaut
- ❌ Exposer des ports d'administration directement sur Internet
- ❌ Autoriser des comptes administrateurs permanents
- ❌ Utiliser des SMS comme second facteur d'authentification
- ❌ Déployer un SaaS sans intégration avec l'IdP central
- ❌ Stocker des mots de passe en clair dans les scripts
- ❌ Négliger les revues périodiques des droits utilisateurs
- ❌ Lancer des projets de transformation lourds sans s'assurer de l'existence des prérequis techniques et organisationnels nécessaires

Définitions

Zero Trust
Approche de sécurité supprimant la confiance implicite liée au réseau et imposant une vérification explicite et continue du contexte utilisateur, appareil et accès à chaque requête (« Never Trust, Always Verify »).

IdP (Identity Provider)
Service centralisant l'authentification et la gestion des identités.

MFA (Multi-Factor Authentication)
Authentification utilisant plusieurs facteurs pour valider un accès.

CASB (Cloud Access Security Broker)
Outil contrôlant et supervisant l'usage des services Cloud.

Micro-segmentation
Isolation des ressources pour limiter la propagation d'une attaque.

PDP (Policy Decision Point)
Concept défini par le NIST dans l'architecture Zero Trust, désignant le composant chargé d'évaluer les règles de sécurité et de décider si un accès doit être autorisé.

PEP (Policy Enforcement Point)
Concept défini par le NIST dans l'architecture Zero Trust, désignant le composant chargé d'appliquer techniquement les décisions d'accès prises par le PDP.