

Préparation au zéro confiance : un plan directeur pour l'excellence en évaluation

***Avertissement de traduction :** Ce document a été traduit de l'anglais original à l'aide du traducteur alimenté par l'IA de Microsoft. Veuillez noter qu'il n'a **pas** été vérifié par un humain pour vérifier l'exactitude, la terminologie correcte ou une lecture fluide. Si vous trouvez des erreurs ou des différences, le document original en anglais est la version correcte et officielle à suivre.

Ce guide détaille le **Quatre Étapes du Zero Trust Assessment Blueprint**, un processus éprouvé pour évaluer et faire progresser la posture Zero Trust (ZT) de votre organisation. Construite à partir de deux ans d'évaluations auto-assistées et assistées, cette approche permet de dépasser les inconnues, offrant aux dirigeants des rapports clairs et des équipes techniques une feuille de route précise, ce qui permet souvent d'économiser des mois de planification.

Le plan d'évaluation en 4 étapes de la confiance zéro

Le plan est conçu pour construire un programme d'évaluation robuste, reproductible et évolutif, centré sur vos besoins spécifiques.

Pas	Zone de focus	Livrable clé
1	Définissez votre cadre ZT	Un cadre structuré et fondamental avec des résultats vérifiables.
2	Établir les critères d'évaluation	Des données claires et quantifiables pour mesurer la maturité et les progrès.
3	Développer l'ensemble d'outils d'évaluation	Des outils automatisés et conçus sur mesure pour collecter et analyser les données d'évaluation.
4	Déployez le processus d'évaluation	Un plan structuré pour la communication, le pilotage, la mise à l'échelle et le soutien.

Étape 1 : Définir votre cadre ZT

Une évaluation réussie commence par un cadre bien défini qui fournit structure et objectifs mesurables. Cela fait passer ZT d'un changement de paradigme à un plan concret.

- **Fondation :** Commencez par exploiter des modèles reconnus de normes ZT :
 - **Stratégie Zero Trust et Feuille de route d'exécution du DoW américain**
 - **Modèle de maturité zéro trust CISA v2.0**

- **NIST SP 800-207, Architecture Zéro Confiance**
- **Composants de structure :** Par exemple, le modèle ZT de la DoW américain décompose la stratégie ZT en quatre couches distinctes, garantissant que chaque élément soit mesurable et reliable à des outils défensifs :

Couche de cadre	But & Cartographie
Piliers	Zones fondamentales/de haut niveau ZT.
Capacités	Peut être assigné aux Outils/Fournisseurs de cybersécurité défensive.
Activités	Peut être mappé à des fonctionnalités spécifiques de l'outil nécessaires à l'implémentation de ZT.
Résultats	Fonctions vérifiables.

Ciblage : Mettre en œuvre une **approche de niveau cible** pour tous les composants afin d'atteindre un statut ZT de référence à une date fixée, avec un **niveau avancé** pour la maturité future.

Étape 2 : Établir des critères d'évaluation

Définir les points de données spécifiques collectés lors d'une évaluation afin d'évaluer le statut de mise en œuvre de ZT selon le cadre établi à l'étape 1.

Critères pour les capacités ZT :

Point de données	Description
Outils / Fournisseur	Rassemblez une liste de tous les outils cyber défensifs utilisés dans votre environnement pour implémenter ZT.
Liaison d'outils	Associez les capacités ZT à des outils cyberdéfensifs spécifiques qui y répondent.
Statut de maturité	Indique le stade du cycle de vie de l'outil (par exemple, Approvisionnement, Entièrement Intégré).

Critères pour les activités ZT :

1. **Statut de maturité :** Un statut granulaire pour montrer des progrès au fil du temps.
2. **État du résultat :** statut de vérification pour tous les sous-résultats (Terminé, partiellement complété, non terminé).

3. **Réponse écrite** : Une description de la manière dont l'activité ZT a été réalisée et comment les résultats sont mis en œuvre.
4. **Téléchargement d'artefacts** : preuve de réussite de la mise en œuvre (par exemple, captures d'écran, PDF de configuration, documentation).

Exemples de statuts d'échéance :

	Maturité	Description
1	Non applicable (NA)	Cette activité n'est pas applicable dans votre architecture.
2	Incomplet	Réponse en attente.
3	Planification	Outils identifiés mais pas encore acquis.
4	Obtenue	Outils acquis, mais aucune ressource allouée à l'intégration.
5	En cours	Les outils sont en cours d'acquisition et leur mise en œuvre.
6	Partiellement implémenté	Certains résultats obtenus (Oui/partiel).
7	Implémenté	Tous les résultats atteints.
8	Hérité	Tous les résultats sont obtenus via un fournisseur externe ou un service cloud.

Étape 3 : Développer l'ensemble d'outils d'évaluation

Construire un ensemble d'outils ZT est essentiel pour standardiser la collecte de données et automatiser l'analyse.

Évolution des jeux d'outils	État actuel et caractéristiques
Phase 1 : Commencer	Basé sur un tableauur : Très laborieux mais crucial pour la définition initiale du flux.
Phase 2 : Réutilisation/Échelle	Outil basé sur une enquête : Réutilisation des outils existants d'enquête/collecte de données pour les auto-évaluations initiales.
Phase 3 : Outil spécialement conçu	Un outil dédié, déployable localement, conçu spécifiquement pour l'évaluation des ZT. Fonctionnalités principales : collecte de données, automatisation et rapports. Avantages clés : Leave Behind pour une maturité continue et un environnement sûr pour tester la mise en œuvre de ZT.

Étape 4 : Déployer le processus d'évaluation

Un déploiement structuré et progressif garantit l'adoption et le succès dans toute l'organisation.

1. **Communiquer** : Initiez des échanges techniques et des conférences pour communiquer le processus d'évaluation, recueillir les premiers retours et susciter l'adhésion.
2. **Pilote** : Identifier une **organisation ou une équipe d'actifs de haute valeur (HVA)** et réaliser une **évaluation assistée** pour affiner le processus et démontrer sa valeur. C'est un investissement dans le succès précoce.
3. **Échelle** : Une fois l'écoulement prouvé, échellez en deux dimensions :
 - **Auto-évaluation** : Ajustez l'évaluation de préparation ZT basée sur une enquête pour le volume d'évaluation en vrac (cela peut prendre des mois par composante).
 - **Évaluation assistée** : Ajustez les ressources/équipes pour **les évaluations sur site** (simplifiées à environ **une semaine** pour un engagement complet).
4. **Soutien** : Établissez une « **porte d'entrée** » pour le programme :
 - **Support utilisateur** : portail pour l'aide à l'auto-évaluation et les demandes d'évaluation assistée.
 - **Soutien aux rapports** : Équipe dédiée à l' **analyse des tendances** et au reporting exécutif pour communiquer efficacement les progrès de ZT dans la hiérarchie.

Liens de ressources Zero Trust

Ressource	Lien
Modèle de maturité CISA ZT v2.0	https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
NIST SP 800-207, ZT Architecture	https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
Stratégie ZT du DoW américain	https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
Feuille de route pour l'exécution du ZT du DoW aux États-Unis	https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-CapabilitiesActivities.pdf

Centre d'orientation
Microsoft ZT

<https://learn.microsoft.com/en-us/security/zero-trust/>