

Évaluation de la préparation au zéro confiance : Guide des processus sur site

***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 les étapes et les meilleures pratiques pour mener une évaluation ciblée de la préparation au Zero Trust (ZT) assistée sur site, généralement conçue pour être réalisée dans une semaine. Ce processus vise à travailler en collaboration avec les membres de l'équipe Composante pour valider et faire progresser leur implémentation ZT.

Phase I : Pré-évaluation et mise en place

Cette phase garantit que toute la logistique et la collecte de données sont achevées avant le début de l'engagement sur site.

Étape 1 : Définir le périmètre et initier la collecte des données

Avant d'arriver sur place, définissez clairement le sujet de l'évaluation et lancez immédiatement le processus de collecte des données afin de gagner du temps.

1. **Identifier le composant et l'environnement :** Déterminer précisément **quel composant/organisation** est évalué et **quel environnement** (par exemple, développement, production, cloud ou instance hybride spécifique) est dans le champ d'application.
2. **Enquête initiale/Auto-évaluation :** Créez une instance d'enquête dans votre outil **d'évaluation de préparation ZT** (ou système équivalent) pour que le Composant commence son auto-évaluation initiale.
3. **Déploiement RFI :** Envoyez une demande d'information (RFI) à l'équipe de gestion de projet/direction du composant. Cette RFI doit être exportée ou guidée par votre outil d'évaluation de la préparation ZT afin de s'assurer que tous les points de données requis sont demandés.

Phase II : Engagement sur site

C'est la phase centrale, axée sur la collecte collaborative d'informations, la validation et les entretiens approfondis.

Étape 2 : Lancement et inventaire des outils

L'évaluation sur site commence par une réunion de lancement avec le chef de projet afin de structurer l'engagement et de saisir le paysage technique.

1. **Rencontrez le chef de projet** : Tenez une réunion avec le chef de projet supervisant l'environnement de la composante évaluée.
2. **Inventaire des outils de capture** : documentez systématiquement les outils cyber **défensifs utilisés** dans l'environnement. Pour chaque outil, capturez les éléments suivants :
 - **Cartographie** : Comment l'outil correspond aux **capacités ZT spécifiques** de votre framework.
 - **Statut de maturité** : L'état actuel du cycle de vie de l'outil (par exemple, acquis, configuré, entièrement intégré).
 - **Brève description** : Un résumé concis de la fonction de l'outil dans l'environnement évalué.
3. **Identifier les experts en la matière (PME)** : Recueillir les noms des **PME** responsables de la mise en œuvre, de l'exploitation et de la maintenance de **chaque outil** spécifique.

Étape 3 : Mener des entretiens structurés et la collecte de données

C'est l'étape la plus chronophage, impliquant des entretiens détaillés et ciblés avec les PME identifiés.

1. **Programmez des entretiens** : Programmez des entretiens avec chaque SME. Préparez un programme d'entretien et des questions **spécifiquement basées sur les outils associés aux capacités ZT** à l'étape précédente.
2. **Revue et validation des capacités** : Examinez les capacités ZT qui ont été mappées à leur outil :
 - Confirmez que la cartographie est exacte. Demandez au PME : « **Cet outil répond-il vraiment à ces capacités ? On en ajoute ou on en retire ?** »

3. **Capture des réponses d'activité** : Pour les activités liées à l'outil et aux capacités de la PME, capturez directement les points de données nécessaires à partir de la PME :
- **Statut de maturité** : L'état actuel de la mise en œuvre de l'Activité.
 - **Statut des résultats** : État des fonctions vérifiables (Terminées, partielles ou non terminées).
 - **Réponse écrite** : Une explication détaillée de la manière dont l'activité est mise en œuvre.
 - **Artefacts** : Collectez ou confirmez l'accès aux **artefacts** (captures d'écran, fichiers de configuration, etc.) qui fournissent une preuve documentée de la mise en œuvre.

Phase III : Finalisation et rapport

La dernière étape consiste à clore les questions restantes et à fournir des résultats d'évaluation formels.

Étape 4 : Derniers trous et stratégie de sortie

Assurez-vous que toutes les lacunes restantes soient comblées et que l'équipe composante soit informée avant de conclure la visite sur place.

1. **Capturez le suivi** : Documentez toute **question de suivi** ou **lacune dans vos connaissances** qui n'a pas pu être résolue lors des entretiens. Celles-ci constituent la base des actions finales.
2. **Programmez un entretien de départ** : Planifiez un entretien de sortie formel avec le chef de projet et la direction de la composante. Utilisez cette réunion pour :
 - Examinez les conclusions préliminaires.
 - Répondez aux manques documentées et aux questions de suivi.
 - Donnez du contexte sur le score final de l'évaluation et les prochaines étapes pour la remédiation/maturité.