Workshop Microsoft Sentinel

Récupération des informations essentielles au Workshop Microsoft Sentinel

Définition du périmètre de déploiement : création d'un document de déploiement

Gestion du changement (si nécessaire) : le client doit suivre son processus de gestion des modifications et obtenir l'approbation des modifications de configuration conformément au périmètre défini.

Configuration :
- Configuration des licences d'évaluation
- Configuration des outils nécessaires

Finalisation de l'installation de Microsoft Sentinel

Phase de lancement → Intégration → Récupération des données (3 semaines) avec gestion des incidents par le SOC Devensys Cybersecurity

Réunion de présentation des résultats :
- Présentation et discussions autour des résultats
- Les prochaines étapes

Besoins Client :
- Les solutions de sécurité Microsoft nécessaires
- Les budgets nécessaires

Démonstration des solutions de sécurité Microsoft

Les prochaines étapes de la sécurisation du SI Client

Décommissionnement :
- Effacer les logs récupérés
- Effacer les changements de configuration effectués
- Désactiver les licences d'évaluation
- Managed Detection and Response (MDR) transition

Journée de restitution → Décommissionnement