

Programme de formation

Purview

Publié le 15/12/2023

DESCRIPTION DE LA FORMATION : Cette formation complète vous guidera à travers les étapes essentielles de l'EDRM, en commençant par une initiation à eDiscovery Premium. Vous apprendrez à cibler efficacement les données et les personnes pertinentes, à créer des collections de données, à analyser les informations et à filtrer les contenus de manière stratégique. Enfin, vous maîtriserez l'exportation des données tout en assurant une conformité totale à chaque étape de votre investigation. À travers de Microsoft eDiscovery Premium, explorez la manière de conduire une investigation numérique sur vos données d'entreprise tout en respectant les étapes essentielles de l'EDRM.

OBJECTIFS PÉDAGOGIQUES :

À l'issue de cette formation, les participants seront en capacité de :

- Démarrer avec eDiscovery Premium et comprendre les modèles EDRM
- Cibler les données et les personnes cibles et créer les collections de données
- Analyser les données et filtrer les contenus
- Exporter et garantir la conformité de l'investigation

MÉTHODES & MODALITÉS PÉDAGOGIQUES :

- Cette formation sera constituée de théorie et d'ateliers techniques qui permettront d'être rapidement opérationnel.
- Support : un support de cours sera remis aux participants au format électronique.
- Evaluation : Les acquis sont évalués tout au long de la formation par le formateur (Questions régulières, travaux pratiques, QCM ou autres méthodes).
- Satisfaction : à l'issue de la formation, chaque participant répond à un questionnaire d'évaluation qui est ensuite analysé en vue de maintenir et d'améliorer la qualité de nos formations.

PROGRAMME DE FORMATION : Suivi d'une feuille d'émargement par demi-journée de présence est signée par chacun des participants.

Comprendre les modèles EDRM

- Découvrir le modèle EDRM
- Connaître les étapes prises en charge par eDiscovery Premium
- Chercher, auditer et enquêter sur les données

Démarrer avec eDiscovery Premium

- Connaître les permissions requises au sein de Microsoft Purview

- Accéder à eDiscovery Premium
- Appliquer le paramétrage global
- Créer un case
- Fermer ou supprimer un case

Gérer un case eDiscovery Premium

- Ajouter des custodians
- Ajouter des data source
- Consulter les activités d'un custodian
- Ajouter des intervenants sur un case
- Communiquer avec les custodian

Effectuer les requêtes préliminaires

- Créer, configurer et tester une collection de données
- Consulter les statistiques pour décider de la prochaine étape
- Modifier la configuration de la collection et la régénérer
- Valider la collection
- Conserver et consulter un historique de la collection

Indexer et traiter des données

- Traiter et indexer des données

Opérer sur un Review Set

- Analyser les données d'un review set
- Ajouter des données externes à un review set
- Ajouter des données d'un review set à un autre
- Consulter les contenus d'un review set
- Filtrer les résultats par requête (et enregistrer les requêtes)
- Classer / Tagger les résultats d'une requête
- Analyser les conversations Teams et Yammer

Analyser et épurer les données

- Analyser les données d'un Review Set
- Bâtir un tableau de bord
- Détecter des doublons et des chaines d'e-mails
- Analyse via Machine Learning

Consulter, annoter, occulter les contenus

- Consulter des contenus d'un Review Set
- Annoter des contenus d'un Review Set
- Occulter des contenus d'un Review Set

Tagger les résultats d'un Review Set

Filtrer les résultats d'un Review Set

- Filtrer/requêter les résultats d'un Review Set

Finaliser l'investigation et la production d'un rapport

Constituer un rapport

- Sélectionner et extraire les informations pertinentes
 - Récapitulatif des acteurs impliqués
 - Récapitulatif des sources de données sélectionnées pour le case
 - Récapitulatif des communications avec les custodians
 - Récapitulatif des collections de données
- Exporter un Review Set

Pour suivre cette formation, il est nécessaire d'avoir une bonne connaissance du fonctionnement de Microsoft 365 et de ses services ou de comprendre le processus d'investigation sur des données numériques.

PRÉREQUIS :

Une connaissance du langage KQL est un plus pour suivre cette formation.

: 2 jours (14 heures)

Administrateur technique, expert en investigation numérique

DUREE

INTERLOCUTEUR : Intermédiaire

NIVEAU :