Université du Québec

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Guide sur la gestion des courriels d'hameçonnage dans Microsoft 365

Université du Québec

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIERES

INTRODUCTION

Les établissements universitaires sont les cibles de plus en plus fréquentes d'attaques de type hameçonnage. La hausse de ces tentatives peut être expliquée par plusieurs facteurs :

- Importante quantité d'utilisateurs;
- étudiants à l'étranger (souvent plus susceptibles à des campagnes d'hameçonnage);
- informations personnelles conservées par les établissements (dossiers d'employés, dossiers d'étudiants);
- données de recherche de grande valeur (parfois très sensibles et confidentielles);
- partenariats avec des entités manipulant des données hautement confidentielles;
- etc.

Pour les acteurs malveillants, les établissements universitaires sont des sources d'informations très convoitées, et ce non seulement par des attaquants « amateurs » qui cherchent à obtenir ces informations pour la revente ou la rançon, mais aussi par des « cyber-espions » cherchant à obtenir les secrets des compétiteurs commerciaux, des « cyber-terroristes » qui cherchent à créer de la peur et du chaos en perturbant les opérations des organisations, et aussi des « pirates d'état » qui sont subventionnés par leurs gouvernements afin d'obtenir un avantage stratégique (militaire, économique, etc.).

Il devient donc primordial pour les établissements du réseau d'avoir les bons outils en place afin d'être en mesure de bien détecter, bloquer et, dans le cas où les différents automatismes ne les auraient pas capturés, comment bien supprimer et isoler les courriels malveillants qui ciblent leurs utilisateurs.

Les courriels d'hameçonnage sont une menace courante pour les organisations et peuvent entraîner des violations de sécurité importantes si elles ne sont pas gérées correctement. Exchange Online, qui fait partie de Microsoft 365, offre plusieurs méthodes pour gérer les courriels d'hameçonnage.

À QUI S'ADRESSE CE GUIDE

Ce guide s'adresse à toutes les personnes ayant comme responsabilité la gestion de l'environnement **Microsoft 365**, **Exchange Online** ou encore qui jouent un rôle de soutien aux utilisateurs de leur organisation en matière d'hameçonnage, ou qui a un rôle de gestion d'incident en cybersécurité.

Il peut aussi s'adresser à tout établissement du réseau qui exploite l'environnement Microsoft 365 ainsi qu'Exchange Online, et qui aimerait comprendre un peu mieux les différents outils et rôles qui gravitent autour de la conformité et de la sécurité.

AVANT DE POURSUIVRE

Il est important de mentionner que les actions suggérées dans ce guide demandent des privilèges élevés dans l'environnement **Azure**, la section **Microsoft Purview** et dans **Exchange Online**. Et comme avec tous les comptes ayant des privilèges élevés, il est fortement recommandé d'appliquer des politiques d'accès conditionnels exigeant l'authentification multifactorielle afin de sécuriser l'environnement d'attaques pouvant compromettre l'intégrité des informations hébergées.

RÔLES REQUIS

Certains rôles peuvent être affectés aux gestionnaires des courriels et des menaces d'hameçonnage afin d'accomplir les opérations requises pour la recherche et le nettoyage. Dans le cas où vous désirez un rôle plus personnalisé, vous pouvez toujours en créer un qui répond aux besoins de votre établissement.

RÔLES EXISTANTS

Il existe quelques groupes dans la section **Microsoft Purview** qui permettent aux organisations de faire la gestion des courriels d'hameçonnage. Voici un résumé construit par Microsoft qui résume les différents rôles inclus avec chaque groupe :

Rôles RBAC liés à eDiscovery

Le tableau suivant répertorie les rôles de contrôle d'accès en fonction du rôle liés à eDiscovery dans le portail de conformité et indique les groupes de rôles intégrés auxquels chaque rôle est attribué par défaut.

Rôle	Administrateur de conformité	Administrateur eDiscovery Manager &	Gestion de l'organisation	Relecteur
Gestion des cas	✓	✓	✓	
Communication		✓		
Recherche de conformité	✓	✓	✓	
Consignataire		✓		
Exporter		✓		
Suspension	✓	✓	✓	
Gérer les étiquettes d'ensemble de révision		✓		
Aperçu		✓		
Révision		✓		✓
Déchiffrement RMS		✓		
Rechercher et vider			✓	

ADMINISTRATEUR GÉNÉRAL / GLOBAL ADMINISTRATOR

Où retrouver ce rôle : https://portal.azure.com/

Avertissement : Le rôle « **administrateur général** » est un rôle qui doit être attribué de façon limitée dans votre environnement Azure / Microsoft 365. Il est préférable, dans le besoin de gestion des courriels d'hameçonnage, d'utiliser d'autres groupes que l'administrateur général pour assigner les rôles requis.

Lorsqu'un administrateur est membre de ce groupe, il peut assigner des rôles dans la plateforme « **Microsoft Purview / Conformité et sécurité** ». L'**administrateur général** fait automatiquement partie du groupe « **Gestion de l'organisation** », permettant à l'administrateur général de faire des recherches de contenu et de purger les résultats de recherches au besoin.

GESTION DE L'ORGANISATION / ORGANISATION MANAGEMENT

Où retrouver ce rôle : https://compliance.microsoft.com/compliancecenterpermissions

C'est du groupe « **Gestion de l'organisation** » que proviennent les rôles de base que possèdent les administrateurs généraux dans la section **Microsoft Purview**. Ces rôles permettent à l'utilisateur d'ajuster les permissions et les rôles dans la plateforme de **Microsoft Purview**, en plus de permettre à l'utilisateur de lancer une recherche de contenu et de purger les résultats de la recherche.

Un administrateur qui programmerait une recherche serait tout de même limité dans la visibilité des objets trouvés par cette recherche, ne pouvant pas exporter ou visualiser les éléments de la recherche.

GESTIONNAIRE EDISCOVERY / EDISCOVERY MANAGER

Où retrouver ce rôle : https://compliance.microsoft.com/compliancecenterpermissions

Lorsque nous voulons créer un « cas de découverte électronique (eDiscovery case) », le rôle de **Gestionnaire eDiscovery** permet à un utilisateur de créer un cas, créer, lancer et modifier une recherche et d'en exporter les résultats. Le rôle est octroyé lorsque nous désirons permettre à un responsable de trouver un courriel correspondant à certains critères afin de permettre à un autre responsable ayant les droits de suppression de faire le nettoyage final.

Le rôle de **Gestionnaire eDiscovery** ne permet pas, cependant, de faire la suppression des résultats d'une recherche.

Un **Gestionnaire eDiscovery** n'a accès qu'aux cas eDiscovery qu'il a créés, ou ceux auxquels il a été assigné par un **Administrateur eDiscovery**.

Avertissement : Puisque le contenu d'une recherche peut être exporté et consulté par le Gestionnaire eDiscovery, il est important de valider les aspects légaux de faire une consultation de documents et courriels d'utilisateurs de votre établissement.

ADMINISTRATEUR EDISCOVERY / EDISCOVERY ADMINISTRATOR

Où retrouver ce rôle : https://compliance.microsoft.com/compliancecenterpermissions

Un **Administrateur eDiscovery** a tous les mêmes rôles qu'un **Gestionnaire eDiscovery**, à la différence que l'**Administrateur eDiscovery** peut faire la gestion de tous les cas de découverte eDiscovery. Il peut aussi assigner des **Gestionnaires eDiscovery** à certains cas de découverte.

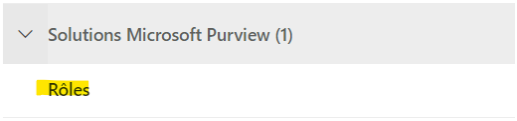
RÔLES PERSONNALISÉS

Parfois, pour répondre aux besoins plus particuliers dans votre établissement, il se peut que vous optiez pour un groupe ayant des rôles personnalisés. En procédant de cette façon, vous pourrez assigner des rôles permettant la recherche, l'exportation et la suppression des courriels, si tel est le besoin. Cependant, notez bien que chaque rôle doit être octroyé en ayant une pleine connaissance de l'impact qu'ils pourraient représenter. L'exemple suivant ne représente en aucun cas une « bonne pratique » recommandée, mais uniquement une démonstration sur la création d'un groupe avec des rôles personnalisés. Il faudra voir, selon votre structure organisationnelle et les tâches assignées aux responsables Exchange dans votre établissement, quels rôles seront appropriés.

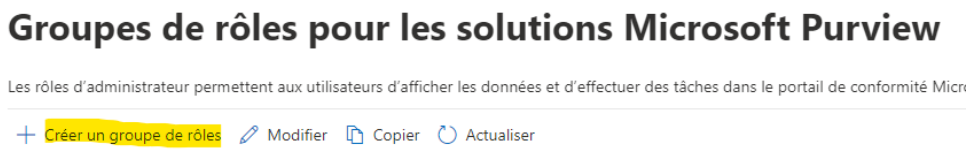
CRÉATION D'UN GROUPE AVEC DES RÔLES PERSONNALISÉS

- Sur la plateforme Microsoft Purview, accédez à la section « **Autorisations** » dans le menu de gauche.

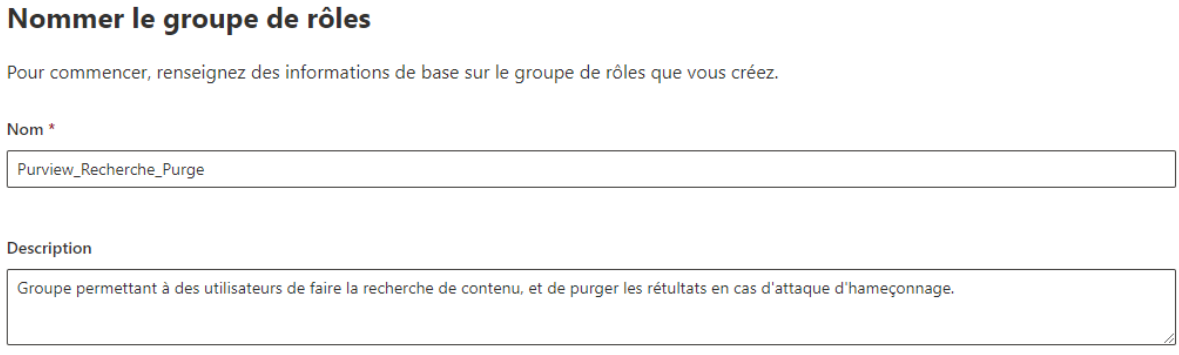
- Par la suite, choisissez **« Rôles »** qui se trouvent sous **« Solutions Microsoft Purview »**. Ceci nous permettra de créer un groupe avec des rôles personnalisés directement dans la plateforme Purview.



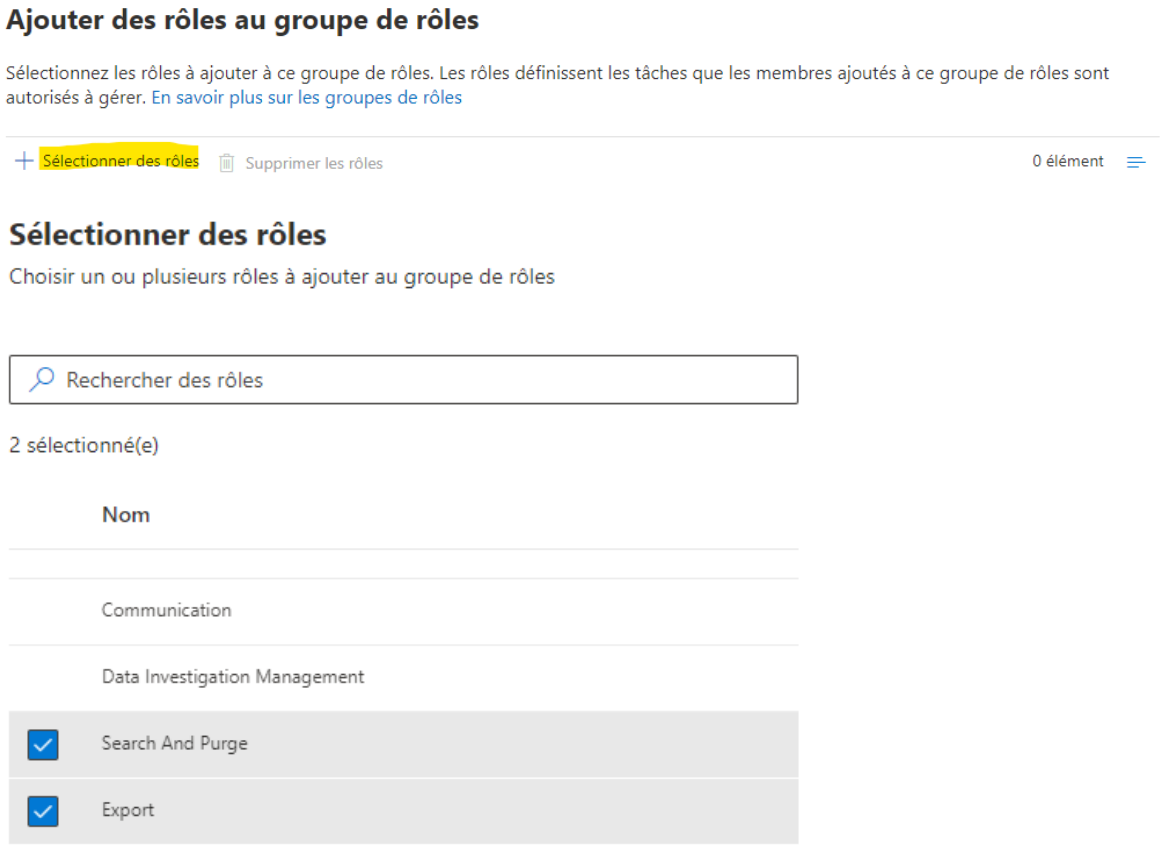
- La liste complète des groupes de rôles sera affichée. Pour créer un nouveau groupe, cliquez sur l'option « **Créer un groupe de rôles** » qui se trouve en haut de liste.



- Vous serez amenés vers la première étape de la création du groupe de rôles, où vous serez demandé de donner un nom et une description au nouveau groupe. Soyez concis avec le nom et la description, puisque parfois, les rôles peuvent se ressembler, il est important de bien décrire leur utilisation.



- Dans la section suivante, vous pourrez sélectionner dans la liste de rôles disponibles pour les différentes opérations possibles de la plateforme Microsoft Purview les rôles que vous désirez assigner au groupe. Dans cet exemple, nous avons choisi les rôles « **Search and Purge** » et « **Export** », permettant de faire la recherche, d'exporter les résultats, et de faire la suppression du contenu trouvé.



- La section suivante vous permettra de sélectionner des utilisateurs qui seront membres du groupe. Il n'est pas requis d'ajouter des membres immédiatement, vous pourrez toujours retourner réviser les appartenances du groupe par la suite.

- La dernière section affichera un résumé des configurations du groupe de rôles. Lorsque tout est validé, terminez la création du groupe. Vous pourrez par la suite assigner des membres au groupe, leur octroyant les rôles qui y sont attachés.

Purview_Recherche_Purge

Modifier Copier Supprimer

Nom du groupe de rôles
Purview_Recherche_Purge

Description du groupe de rôles
Groupe permettant à des utilisateurs de faire la recherche de contenu, et de purger les rétultats en cas d'attaque d'hameçonnage.

Rôles dans le groupe de rôles
Search And Purge
Export

Membres dans le groupe de rôles

Nom d'affichage	Type	Étendue
Jean-François Blais	Utilisateur	Organisation

RÉFÉRENCES

https://learn.microsoft.com/fr-ca/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide

https://learn.microsoft.com/en-us/microsoft-365/compliance/ediscovery-assign-permissions?view=o365-worldwide

https://msftcompliance.com/blog/microsoft-purview-ediscovery-compliance-boundaries/

OUTILS DE RECHERCHE

Microsoft Purview est un outil de gestion de données qui fournit des fonctionnalités telles que la gestion des métadonnées, la classification des données et la découverte des données. Deux fonctionnalités clés de Purview sont la recherche de contenu et l'eDiscovery, qui sont souvent utilisées de manière interchangeable, mais ont des fonctionnalités différentes.

La recherche de contenu ou la recherche eDiscovery ne sont généralement pas les méthodes les plus efficaces pour le nettoyage de courriels d'hameçonnage sur Exchange Online. Ces méthodes sont plus couramment utilisées pour rechercher et récupérer des messages spécifiques pour des besoins de conformité ou d'enquête.

Pour le nettoyage de courriels d'hameçonnage, il est recommandé d'utiliser des méthodes spécifiques de filtrage et de nettoyage, telles que le filtrage des courriels, la suppression manuelle, le signalement de courriels d'hameçonnage, le nettoyage automatique, les règles de transport et les solutions tierces. Ces méthodes sont conçues pour identifier et supprimer les courriels d'hameçonnage de manière efficace, tout en minimisant les risques pour les autres messages légitimes et importants de l'entreprise.

Les outils de recherche peuvent être utilisés pour récupérer des messages suspects ou malveillants dans des enquêtes ou des audits de conformité, mais ils ne sont pas conçus pour nettoyer ou supprimer automatiquement les courriels d'hameçonnage. Il est important de noter que l'utilisation d'un de ces outils de recherche pour supprimer des messages peut entraîner la suppression de messages légitimes et importants pour l'entreprise.

Malgré tout, le besoin peut se présenter où il devient important de retrouver et supprimer rapidement des courriels d'hameçonnage qui auraient été distribués à une grande échelle dans votre établissement. Parfois, même avec le signalement d'un utilisateur, le

processus automatisé de quarantaine peut prendre un certain temps, laissant vos utilisateurs risquant de tomber victimes. C'est pourquoi les outils de **Recherche de contenu** et les cas **eDiscovery** peuvent être exploités afin d'accélérer le processus.

RECHERCHE DE CONTENU

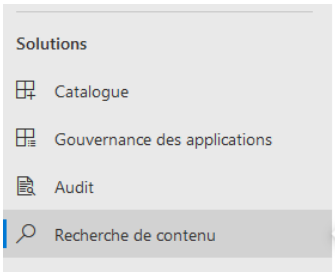
Où retrouver : https://compliance.microsoft.com/contentsearchv2?viewid=search

La recherche de contenu dans Purview est une fonctionnalité qui permet aux utilisateurs de rechercher des données spécifiques dans le contenu des fichiers, tels que des documents texte, des PDF et des feuilles de calcul.

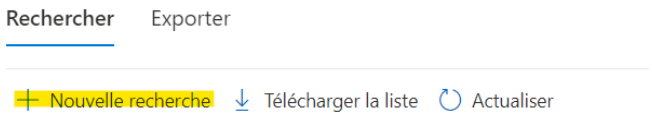
La recherche de contenu peut être utile pour trouver des mots clés spécifiques dans des messages, mais cela ne permet pas d'identifier spécifiquement les courriels d'hameçonnage. En effet, les courriels d'hameçonnage peuvent contenir des mots et des phrases qui ne sont pas forcément des indicateurs fiables pour les identifier. C'est pourquoi il est important, avant de procéder à la suppression des courriels, de bien valider les résultats de la recherche afin de minimiser les impacts pouvant survenir à la suite de la suppression de courriels légitimes.

COMMENT LANCER UNE RECHERCHE DE CONTENU

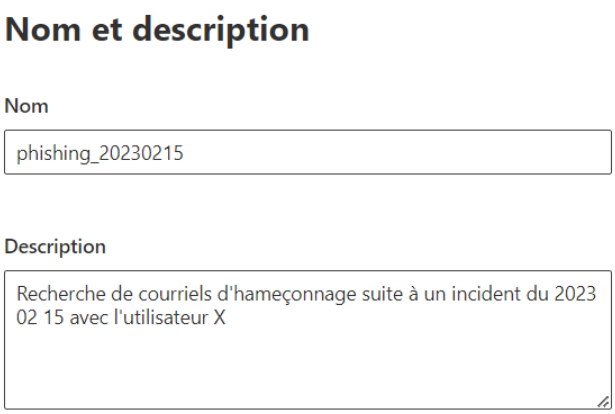
- Dans la console de Microsoft Purview, chercher dans le menu de gauche la section « **Recherche de contenu** ».



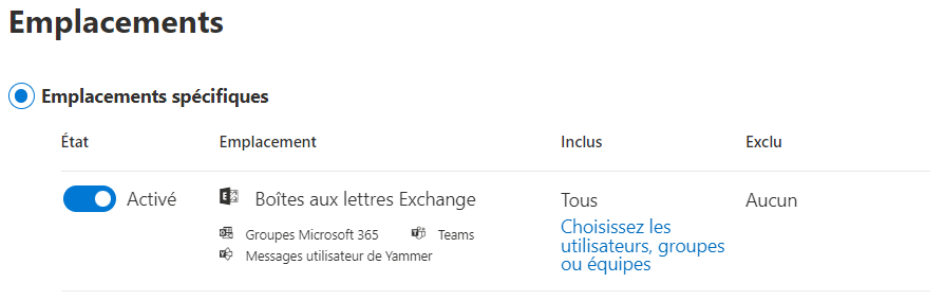
- Sur la page qui s'affichera, vous pourrez voir la liste des recherches de contenu déjà créées, où vous pourrez voir leur état, et consulter les détails qui les concernent. Pour créer une nouvelle recherche, cliquez sur « **Nouvelle recherche** » qui se trouve en haut de liste.



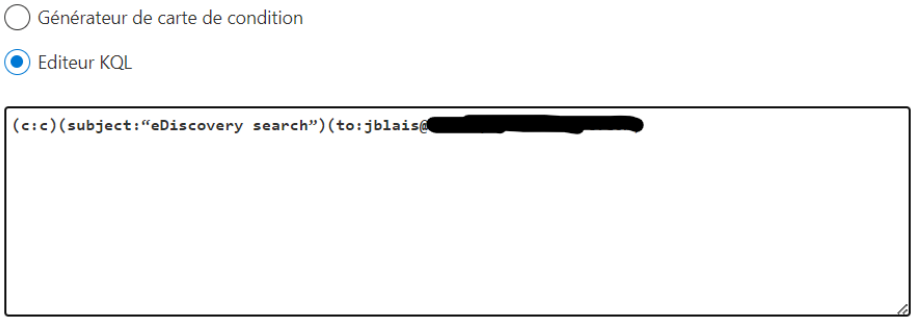
- Vous serez amenés vers la première étape de la création de la nouvelle recherche, où vous serez demandé de donner un nom et une description.



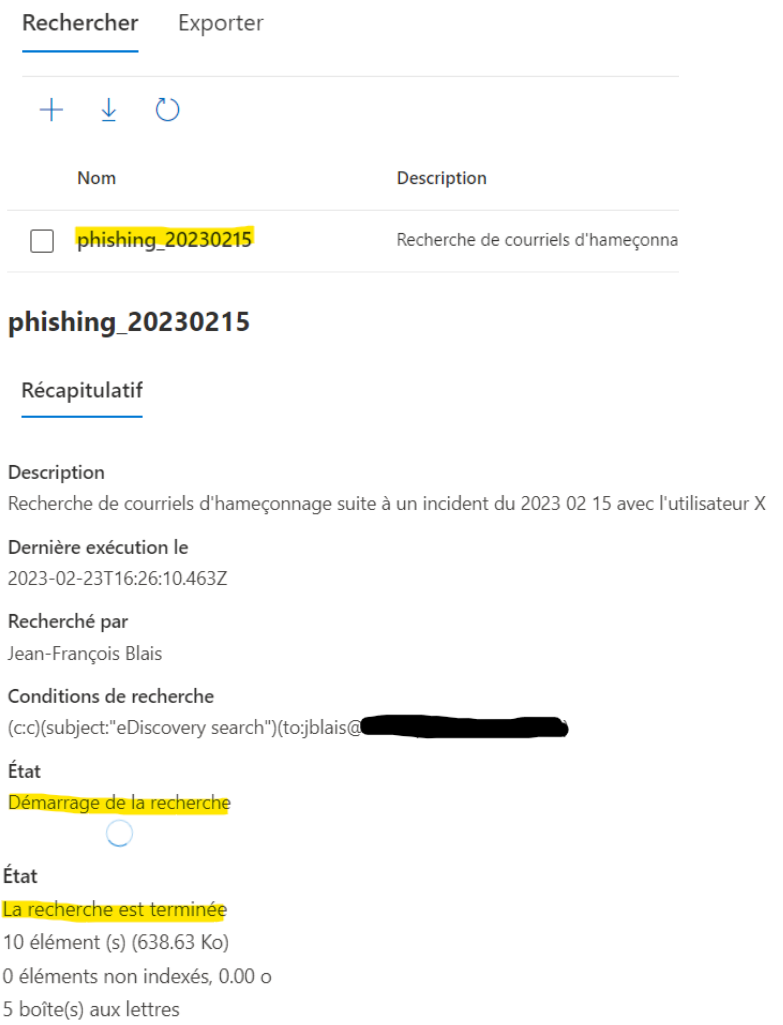
- La section suivante vous demandera les emplacements qui doivent être inclus dans la recherche. Ici, « Boites aux lettres Exchange » a été activé, nous permettant d'effectuer des recherches de courriels. Il est important de prendre connaissance que la recherche dans cet emplacement pourrait trouver des résultats sur Teams ou Yammer, qui sont inclus dans cette catégorie d'emplacement. Cependant, lorsque vous ferez la suppression, les éléments trouvés sur Teams ou Yammer ne seront pas supprimés, uniquement les courriels seront purgés.



- La section suivante est sûrement la plus importante. C'est ici où nous devons indiquer quels sont les critères de recherche. Nous avons le choix d'utiliser les cartes de condition ou l'éditeur KQL (que certains vont préférer puisque l'éditeur KQL a une présentation des critères de recherche identique que l'outil EXO de PowerShell). Pour avoir plus de détails sur les options possibles lors de la création de nos critères de recherche, vous pouvez consulter le guide de Microsoft sur les mots clés et les conditions de recherche. Dans l'exemple suivant, nous allons rechercher les courriels ayant « eDiscovery search » dans le titre, envoyé à une adresse particulière (qui pourrait être incluse dans un groupe, CCI ou CC).



- Lorsque la recherche est créée, elle sera automatiquement lancée. Vous pouvez voir l'état de la recherche en retournant dans la liste des recherches de contenu, et en cliquant sur la nouvelle recherche.



- Lorsque la recherche est terminée, vous pouvez vérifier que les résultats trouvés par la recherche correspondent bien à ce que vous voulez trouver. Il est important de valider les résultats afin de s'assurer que notre recherche n'inclut pas de courriels qui sont légitimes. Dans ce cas, vous pouvez réviser les critères de recherche afin d'exclure ces éléments légitimes.
- Il n'y a malheureusement pas de méthode dans l'interface graphique de recherche de contenu permettant de faire la suppression des résultats d'une recherche. Pour ce faire, il faudra procéder avec le module Exchange Online v.3.0 (EXO) de PowerShell (qui sera expliqué un peu plus tard dans ce guide).

CAS DE DÉCOUVERTE EDISCOVERY

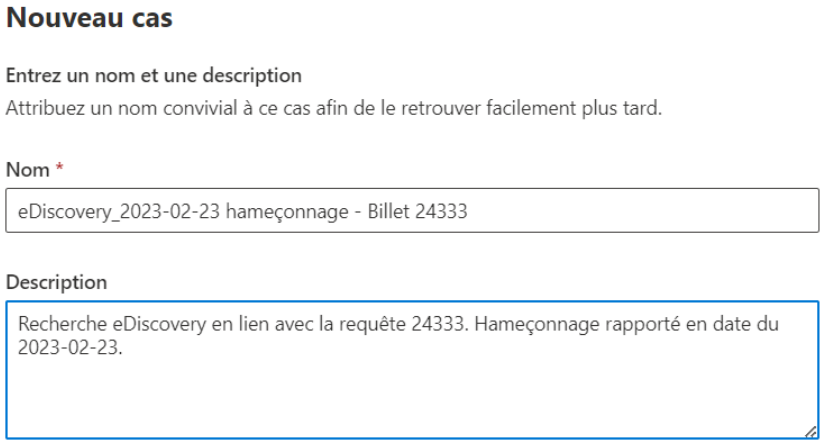
L'eDiscovery dans Purview est une fonctionnalité plus complète qui permet aux utilisateurs de rechercher et d'analyser l'ensemble des données de leur organisation, y compris les courriels, les messages dans les discussions et d'autres sources de données non structurées. L'eDiscovery est généralement utilisé dans des contextes juridiques, tels que lorsqu'une entreprise est tenue de produire des données pertinentes dans le cadre d'une enquête juridique ou réglementaire. Avec l'eDiscovery, les utilisateurs peuvent collecter, traiter et analyser de grandes quantités de données provenant de sources multiples pour identifier des informations pertinentes.

En résumé, l'eDiscovery est une fonctionnalité plus complète conçue pour les enquêtes juridiques ou réglementaires qui impliquent la recherche et l'analyse de données provenant de sources multiples.

COMMENT CRÉER UN CAS DE DÉCOUVERTE EDISCOVERY

- Accéder à la section eDiscovery (standard)
- Dans la page de eDiscovery, vous pouvez voir la liste des cas ouverts auxquels vous avez des accès (dépendant du groupe Gestionnaire ou Administrateur eDiscovery auquel vous êtes membre).
- Pour créer un nouveau cas de recherche eDiscovery, sélectionnez l'option « **+** » qui se trouve en haut de la liste

- La première section à remplir sera composée d'un champ pour le nom et la description du cas eDiscovery. Notez qu'à cette étape, nous ne sommes pas encore rendus à la création de la recherche, mais plutôt à la création d'un conteneur privilégié où pourront se retrouver plusieurs recherches.



- De retour sur la liste des cas eDiscovery, nous pouvons sélectionner le nouveau cas créé pour ouvrir les différentes options qui s'offrent à nous. Pour créer une nouvelle recherche de contenu à l'intérieur du cas eDiscovery, sélectionnez l'onglet « **Recherches** ».

- Tel que mentionné dans un point précédent, un cas eDiscovery peut contenir plusieurs recherches différentes (tout dépendant du besoin pour le cas). Les recherches à l'intérieur d'un cas eDiscovery sont identiques (avec quelques exceptions) à la « **Recherche de contenu** » présentée précédemment dans ce guide. Vous pouvez créer la recherche en utilisant les mêmes critères.

- Les recherches nouvellement créées sont démarrées automatiquement. Lorsque complétées, vous pouvez exporter et analyser les résultats de la recherche afin de vérifier qu'elle ne contient aucun courriel légitime (dans ce cas, vous pouvez revoir vos critères de recherche afin de les exclure de la recherche).
- Comme avec la recherche de contenu, il n'y a pas d'options dans l'interface graphique de recherche eDiscovery permettant de faire la suppression des résultats d'une recherche. Pour ce faire, il faudra procéder avec le module Exchange Online v.3.0 (EXO) de PowerShell.

  Notez bien que l'utilisation présentée de eDiscovery est uniquement pour démontrer comment effectuer une recherche de contenu, et pas une explication approfondie sur les outils supplémentaires de rétention, d'exportation et de tous les aspects légaux attachés aux cas eDiscovery.

POWERSHELL (EXO V.3.0)

https://learn.microsoft.com/fr-ca/powershell/exchange/exchange-online-protection-powershell?view=exchange-ps

PowerShell est un outil de ligne de commande de Microsoft qui peut être utilisé pour automatiser les tâches de gestion de messagerie, y compris la recherche et la suppression de courriels d'hameçonnage. Les administrateurs peuvent utiliser les cmdlets PowerShell Exchange Online (EXO) pour rechercher les courriels en fonction de divers critères tels que l'expéditeur, le destinataire ou le contenu du message. Une fois les courriels identifiés, les administrateurs peuvent les supprimer de manière sélective ou en bloc.

Le module EXO exige des privilèges administrateur (local ou domaine) afin d'être installé sur un système d'exploitation, mais n'en requiert pas pour être exploité par un utilisateur (mis à part les rôles requis dans la plateforme Microsoft Purview).

INSTALLATION DU MODULE EXO

Si vous n'avez pas encore installé le module Exchange Online sur votre système, vous devrez le faire. Ouvrez une fenêtre en tant qu'administrateur, et exécutez la commande suivante :

```
Install-Module -Name ExchangeOnlineManagement -Force -Verbose -Scope CurrentUser
```

IMPORTATION DU MODULE EXO

Comme mentionné, l'utilisation du module n'exige pas de privilèges élevés sur le système, alors vous pouvez ouvrir une nouvelle fenêtre PowerShell, et débuter avec l'importation du module.

```
Import-Module ExchangeOnlineManagement -Verbose
```

POLITIQUE D'EXÉCUTION DE SCRIPTS

Lors de la connexion à Exchange Online et la plateforme de conformité, le module EXO exige une politique d'exécution de scripts particulière, exigeant que les scripts distants soient signés.

```
Set-ExecutionPolicy RemoteSigned
```

LANCER LES CONNEXIONS REQUISES

L'utilisation des cmdlets EXO exigent une connexion réussie à deux consoles, soit à Exchange Online et à la console de conformité (Purview). Si votre organisation utilise l'authentification multifactorielle, vous devrez la compléter pour poursuivre.

```
Connect-ExchangeOnline -UserPrincipalName %courriel_administrateur%
Connect-IPPSSession -UserPrincipalName %courriel_administrateur%
```

CRÉER UNE NOUVELLE RECHERCHE

Pour créer une nouvelle recherche, vous devrez lui donner un nom, et spécifier les critères de recherche.

```
New-ComplianceSearch -Name %Nom% -ExchangeLocation All -ContentMatchQuery %Criteres_de_recherche%
```

LANCER UNE RECHERCHE

Contrairement aux interfaces graphiques de création de recherche (« Recherche de contenu » et « eDiscovery »), lorsque vous ferez la création d'une nouvelle recherche avec PowerShell, la recherche ne sera pas automatiquement lancée. Il faudra donc lancer la recherche manuellement.

```
Start-ComplianceSearch -Identity %Nom%
```

CONSULTER L'ÉTAT D'UNE RECHERCHE

Afin de valider l'état d'une recherche (en attente, en cours et terminée), vous pouvez lancer la commande suivante. Si la recherche mentionnée n'existe pas, un message d'erreur sera affiché.

```
Get-ComplianceSearch -Identity %Nom% -ErrorAction SilentlyContinue
```

SUPPRIMER LES RÉSULTATS D'UNE RECHERCHE

La suppression des résultats d'une recherche exige la création d'une nouvelle action de recherche de conformité. Afin de supprimer les courriels trouvés, nous pouvons choisir entre « **SoftDelete** » qui déplacera les courriels dans les boites « Courrier indésirable » des utilisateurs en question, ou « **HardDelete** » qui déplacera les courriels dans une corbeille où les utilisateurs n'ont pas accès. La suppression sera lancée automatiquement, selon les résultats trouvés par la recherche.

```
New-ComplianceSearchAction -SearchName %Nom% -Purge -PurgeType SoftDelete
```

FERMER LES SESSIONS ACTIVES

Il existe une limite de trois sessions concurrentes lors de l'utilisation d'EXO. Sans soucis de fermeture de session, il se peut que, rapidement, vous atteigniez la limite permise, vous empêchant pendant un certain temps d'initier une nouvelle connexion à Exchange Online et de traiter les courriels d'hameçonnage qui peuvent être urgents. Il est donc important, à la fin de chaque utilisation d'EXO, de bien fermer la session active.

```
Disconnect-ExchangeOnline -Confirm:$false
```

OUTILS COMPLÉMENTAIRES

Si vous désirez avoir un outil un peu plus « clé en main », le CESI a développé un script permettant de créer, lancer et faire le nettoyage de recherches avec EXO. L'outil permet de relancer la recherche et le nettoyage automatiquement dans les boites de courriel qui auraient plus de 10 résultats par recherche (limite concurrente avec la suppression PowerShell par boite de courriels). La boucle permettra, dans le besoin, de s'assurer que tous les résultats liés à la recherche seront bien nettoyés.

Noter bien, cependant, que la révision de code est une étape requise lors de l'utilisation de scripts externes, et qu'aucun outil « clé en main » ne pourra répondre entièrement à vos besoins. L'idée est de simplement fournir un exemple fonctionnel avec une recherche simple afin de permettre aux établissements du réseau de modifier et utiliser le module EXO de façon correspondante à leurs besoins.

CESI-NETTOYAGEEXCHANGE.PSM1

Module PowerShell créé par le CESI exploitant les cmdlets de Exchange Online V3.0. Le module fait certaines validations lors de la création, l'exécution et la suppression des courriels. Il permet aussi d'afficher les boites Exchange et la quantité de courriels correspondant aux critères de recherche ont été trouvés. Il peut aussi se charger de l'installation du module EXO (moyennant que l'utilisateur exploitant le script ait des droits d'administration sur son système d'exploitation).

Archive : Téléchargement ici

CESI-EXEMPLEUTILISATION.PS1

Exemple d'utilisation du module CESI-NettoyageExchange.psm1.

Archive : Téléchargement ici

RÉFÉRENCES

Mots clés et conditions pour la recherche

https://learn.microsoft.com/fr-ca/microsoft-365/compliance/ediscovery-keyword-queries-and-search-conditions?view=o365-worldwide

Recherche et suppression de messages électroniques

Recherche et suppression de messages électroniques dans votre organisation - Microsoft Purview (compliance) | Microsoft Learn

SERVICES CONNEXES

PROTECTION EXCHANGE EN LIGNE / EXCHANGE ONLINE PROTECTION (EOP)

Vue d'ensemble de Exchange Online Protection (EOP) - Office 365

Protection Exchange Online (EOP) est un service basé sur l'infonuagique qui fournit une filtration des courriels et une protection contre les pourriels, les virus et les courriels d'hameçonnage. EOP utilise l'apprentissage machine et d'autres technologies pour analyser le contenu des courriels et déterminer s'il s'agit d'une tentative d'hameçonnage ou non. Il permet également aux administrateurs de configurer des stratégies personnalisées pour la gestion des courriels d'hameçonnage, comme les rediriger vers un dossier de quarantaine ou les bloquer complètement.

ADVANCED THREAT PROTECTION (ATP)

Microsoft Defender for Office 365 (Plan 1) anciennement Protection avancée contre les Menaces (ATP) – Openhost Network (openhost-network.com)

Microsoft Defender pour Office 365 | Sécurité Microsoft

Office 365 Advanced Threat Protection (ATP) est un service complémentaire pour Exchange Online qui offre des fonctionnalités de sécurité supplémentaires, notamment une protection contre les attaques d'hameçonnage avancées et les attaques de harponnage (spear-phishing). ATP utilise l'apprentissage machine et l'analyse comportementale pour identifier et bloquer les courriels suspects, et fournit des rapports en temps réel et des alertes pour les administrateurs.

SIGNALEMENT DE COURRIELS D'HAMEÇONNAGE

Exchange Online offre aux utilisateurs la possibilité de signaler les courriels d'hameçonnage en utilisant la fonction "Signaler le message". Lorsqu'un utilisateur signale un courriel d'hameçonnage, Exchange Online peut analyser le courriel et mettre à jour ses stratégies de protection contre l'hameçonnage pour bloquer des courriels similaires à l'avenir.

Comment activer le module complémentaire de signalement de courriels d'hameçonnage
Activer les compléments Signaler le message ou Signaler l'hameçonnage - Office 365 | Microsoft Learn

SENSIBILISATION DES UTILISATEURS

L'une des méthodes les plus efficaces pour prévenir les attaques d'hameçonnage est la sensibilisation des utilisateurs. Exchange Online fournit des outils aux administrateurs pour créer une formation personnalisée sur la sécurité pour les utilisateurs, ce qui peut les aider à identifier et à éviter les courriels d'hameçonnage.

RÉVISIONS

Date	Action	Auteur	Ver.
2023-03-02	Première version	Jean-François Blais CESI de l'UQ	1.0