Hameçonnage

Méthodologie de réponse à incident

IRM-01 08/09/2023

Introduction

Cette méthodologie de réponse à incident est une feuille de route dédiée aux gestionnaires et aux cellules de crise menant une investigation sur un problème de sécurité précis.

- La fiche IRM s'adresse aux personnes ou fonctions suivantes :
  - Les RSSI et leurs adjoints
  - Les DSI et leurs adjoints
  - Les administrateurs

Rester calme et contacter immédiatement l'équipe de réponse à incident Cyna.
Nos canaux de discussion :

- **Cybersecurity@cyna-it.fr**
- **+33 9 70 70 41 81 (Heure ouvrés)**

En cas d'urgence, veuillez insérer la balise [URGENT] dans l'objet du courriel. Veuillez noter que notre CERT est disponible 24 heures sur 24 et 7 jours sur 7, mais que l'assistance téléphonique n'est pas disponible en dehors des heures de bureau.

Identification & Processus d'endiguement

Objectif : Détecter l'incident, déterminer son ampleur et impliquer les acteurs appropriés.

1.1. Détection d'hameçonnage

Comment Détecter une Tentative d'Hameçonnage par E-mail

1. **Vérification de l'Expéditeur :**
   - Vérifiez attentivement l'adresse e-mail de l'expéditeur. Faites attention aux erreurs de noms ou de domaines.
2. **Analyse du Message** :
   - Recherchez des erreurs de grammaire, des fautes d'orthographe ou un ton inhabituel.
   - Soyez méfiant envers les messages urgents ou trop prometteurs.
3. **Liens et Boutons** :
   - Ne cliquez pas directement sur les liens. Passez le curseur dessus pour vérifier l'URL.
   - Ne cliquez jamais sur les boutons douteux sans vérifier leur destination.
4. **Pièces Jointes** :
   - Évitez de télécharger les pièces jointes à moins d'être sûr de leur provenance.
5. **Confirmation de l'Expéditeur :**
   - Contactez l'expéditeur par un autre moyen pour confirmer la demande si vous avez des doutes.

1.2. Appliquer le bon processus.

→ Dès qu'un mail semble être un phishing et qu'il est détecté par vos collaborateurs ou vos équipes IT, contactez cybersecurity@cyna-it.fr.

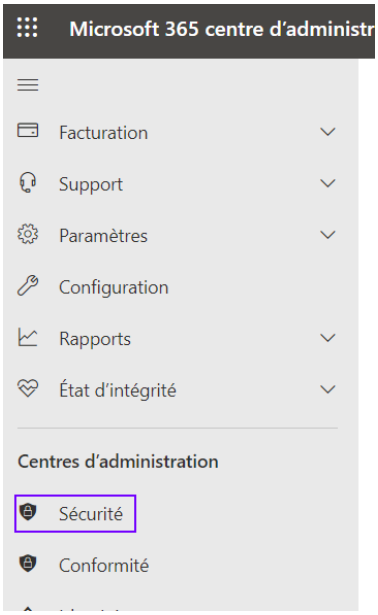
Pour ce faire, rien de plus simple :

- **CTRL + ALT + F** via le raccourci afin de transférer le mail douteux en Piece Jointe.
- Via l'interface graphique « **Plus** » / « **Transférer en tant que pièce jointe** ».

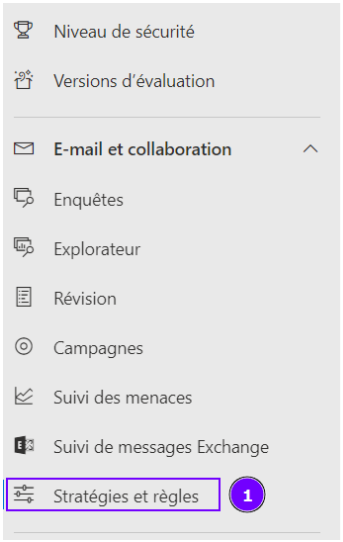
Une analyse ne peut être réalisée uniquement lorsque nous avons la **pièce jointe** du mail, le corps du mail n'est pas assez verbeux pour nos équipes dans le cadre d'une investigation.

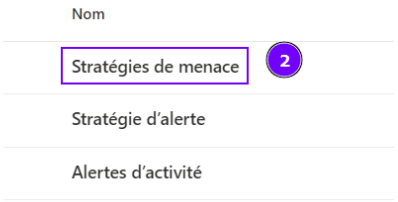
Remédiation

Nous vous proposons un tutoriel à suivre afin de blacklister les domaines malveillants sur vos tenants o365.

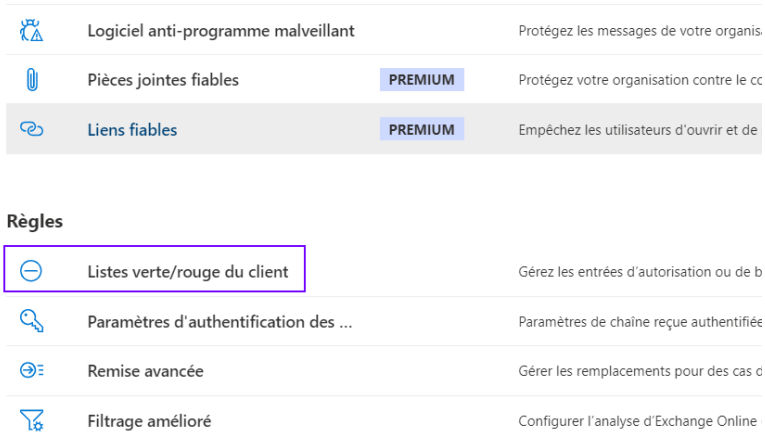


➡ Pour commencer il faut se connecter à la console Admin Microsoft 365

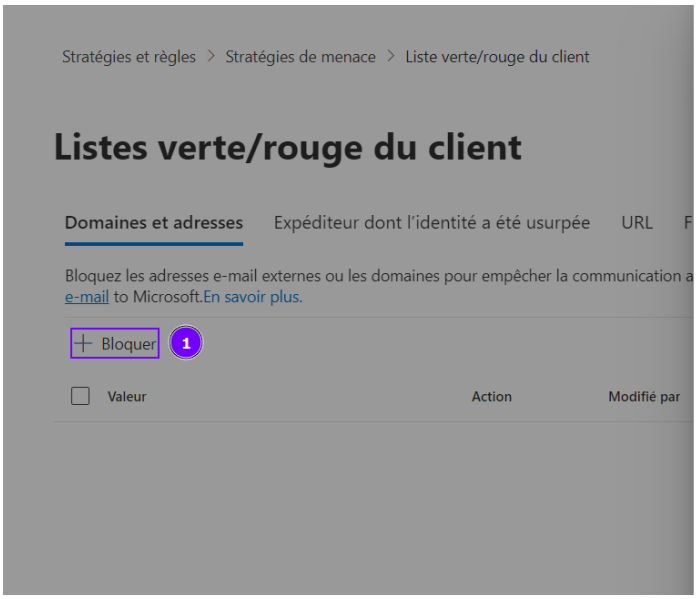


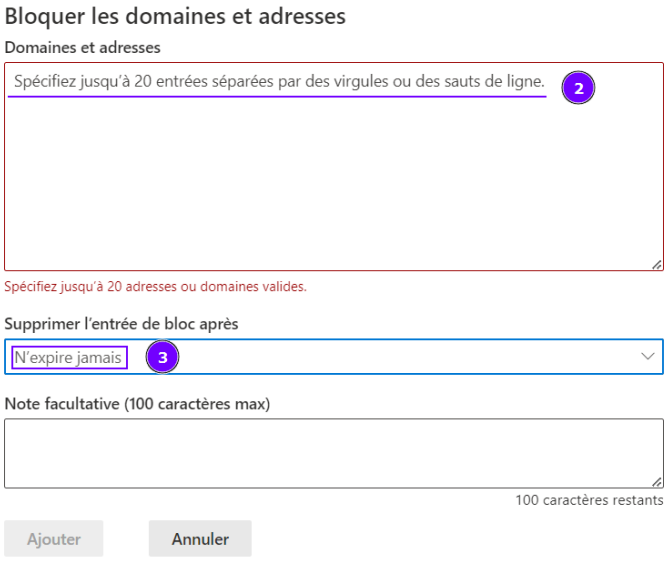


➡ On clique sur stratégies de règles puis stratégies de menace



➡ Une fois dessus nous allons cliquer sur liste verte/rouge





➡ Ici il suffit de rentrer les domaines que nous voulons bloquer et choisir n'expire jamais.