Service de détection et réponse des boîtes de messagerie (IDR) GoSecure Titan^MC

Guide de l'utilisateur

GoSecure

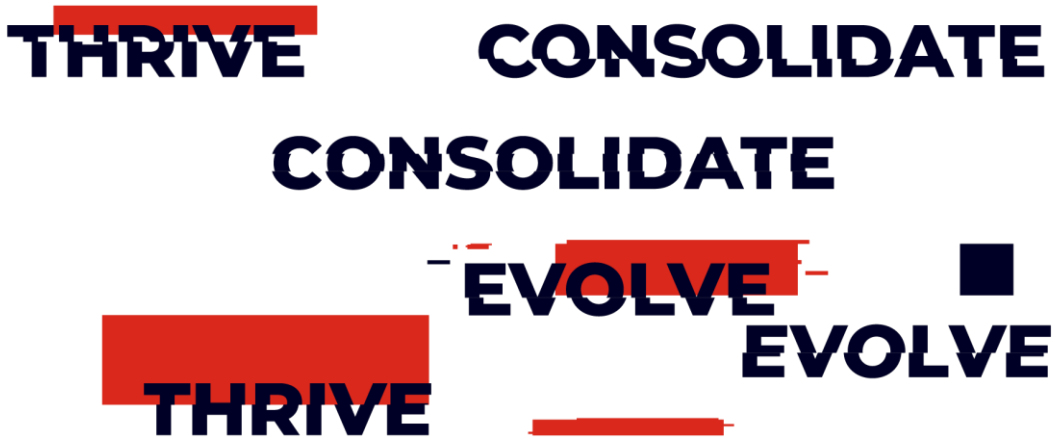
HAMEÇONNAGE

L’hameçonnage est devenu la principale menace informatique ciblant les entreprises à l'ère numérique, ce qui en fait un sujet de discussion majeur à l'heure actuelle.

UNE MEILLEURE PROTECTION CONTRE LES COURRIELS SUSPECTS

[Que faire lorsque vous recevez un courriel ?]

1. Déterminer la source du courriel
2. Identifier l'expéditeur réel
3. Examiner le contenu



DÉTERMINER LA SOURCE DU COURRIEL

- Lorsque vous recevez un courriel, la première étape consiste à faire la distinction entre ceux provenant de **collègues** et ceux provenant **d'expéditeurs externes**.
- Il est **ESSENTIEL** de noter que les courriels provenant d'expéditeurs externes présentent potentiellement une **menace plus élevée**.

IDENTIFIER L'EXPÉDITEUR RÉEL

- Pour identifier l'expéditeur, il est **ESSENTIEL** de se fier à l'adresse électronique plutôt qu'au nom affiché dans Outlook.
- Une adresse électronique au format <expeditor@domain> vous offre la possibilité de discerner l'origine du courriel en identifiant le domaine d'envoi.
- Cependant, les pirates informatiques incitent souvent leurs victimes à utiliser le nom affiché, car il est facile à personnaliser pour gagner la confiance du destinataire.

EXAMINER LE CONTENU

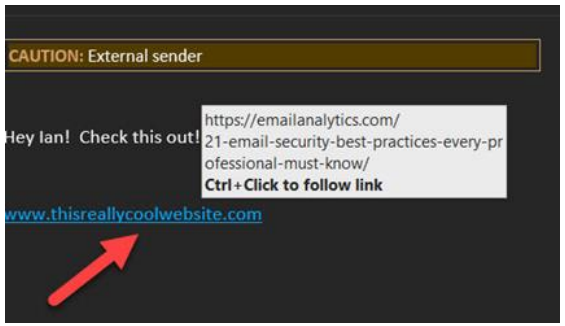
Un courriel suspect contient généralement l'un des éléments suivants :

- Une situation d'urgence est communiquée
- Une menace directe
- Un lien vers un domaine inconnu
- Une pièce jointe potentiellement malveillante

LA TECHNIQUE "HALT"

SURVOLEZ

- Survoler les hyperliens pour voir où ils vont VRAIMENT !



REGARDEZ

- Valide = www.walmart.com
- Non valide = wa1mart.com
- Valide = help@walmart.com
- Non valide = help@wal-mart.com

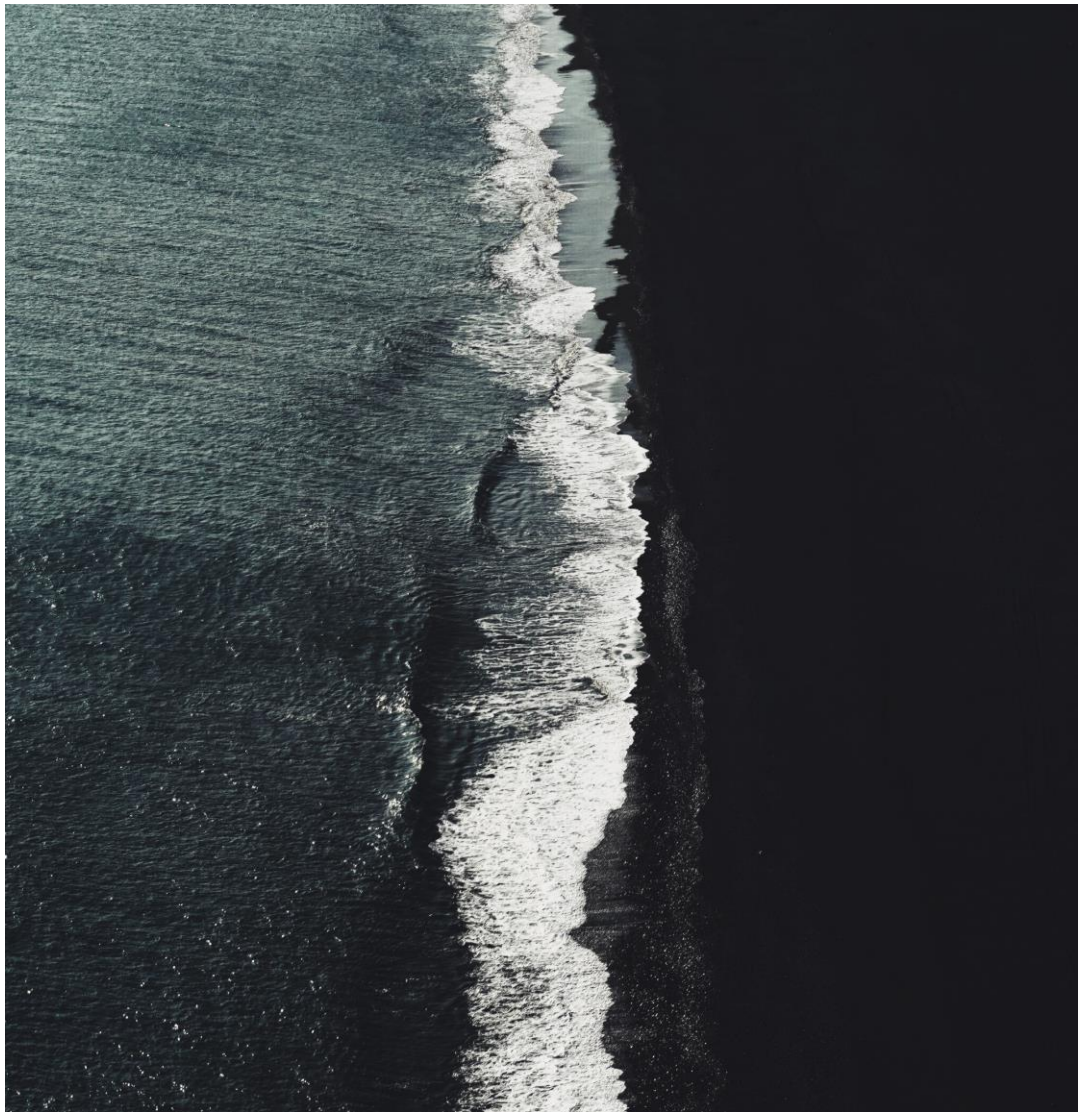
ANALYSEZ

- La partie domaine de l'adresse électronique
- Doit être une organisation valide
- Doit être cohérente

TESTEZ

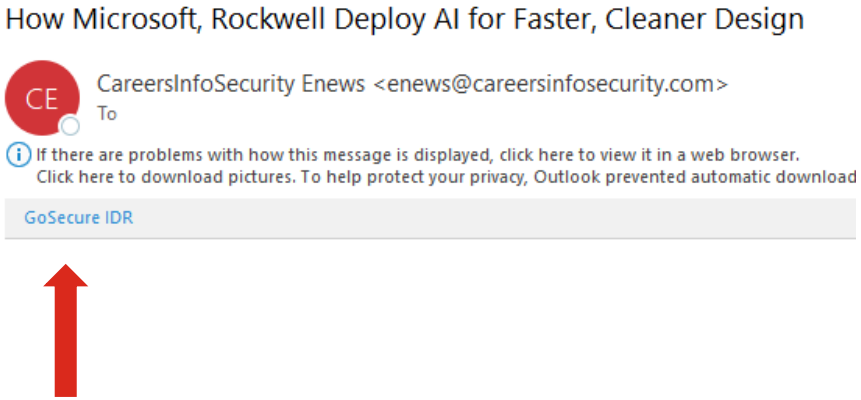
- Cherchez sur Google !
- Vérifier l'adresse réelle

QUELS TYPES DE COURRIELS DOIS-JE SOUMETTRE À GOSECURE IDR ?

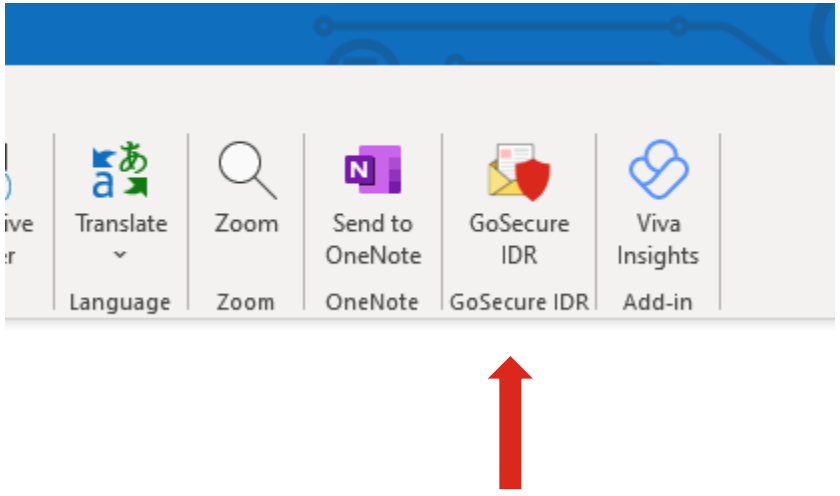


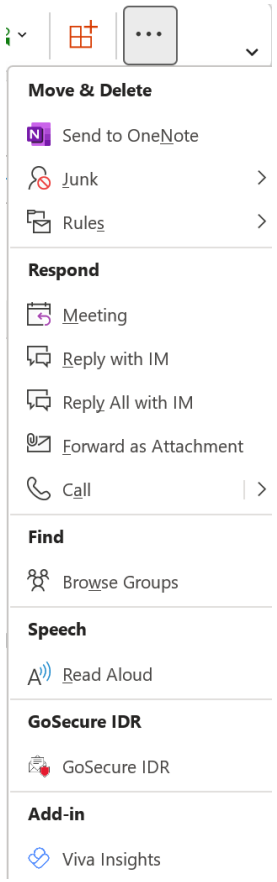
EN CAS DE DOUTE, IL FAUT SOUMETTRE

- Tout courriel semblant être interne et demandant de modifier les informations relatives au dépôt direct ou une demande étrange de la part de la direction de faire quelque chose pour elle, l'expéditeur est souvent usurpé dans ces cas-là.
- Tout courriel provenant d'un expéditeur inconnu et contenant une demande de services, de produits ou de facturation.
- Tout courriel d'un expéditeur connu qui semble ne pas correspondre à la réalité (même des contacts connus et fiables peuvent être compromis et le sont effectivement). Il peut s'agir d'un lien ou d'un document inattendu, ou d'un changement de ton dans le corps du message.
- Tout courriel vous demandant de signer ou d'examiner un document. Tout courriel contenant une pièce jointe, en particulier un fichier zip ou un document de bureau tel que .doc ou .xls.
- Tout courriel qui éveille vos soupçons

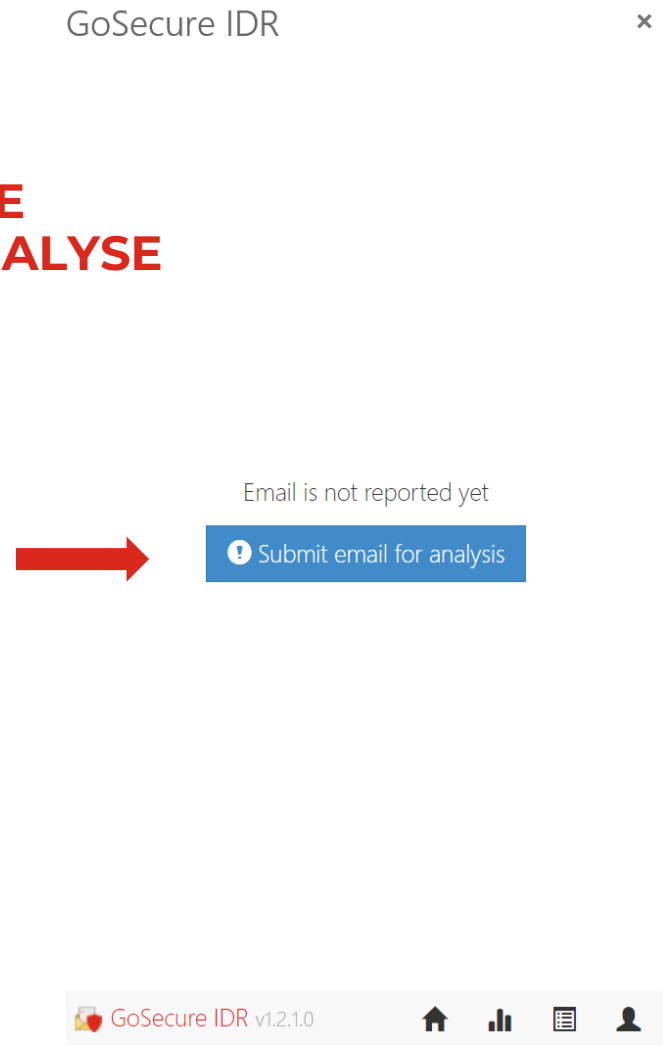


UTILISEZ LE BOUTON GOSECURE IDR



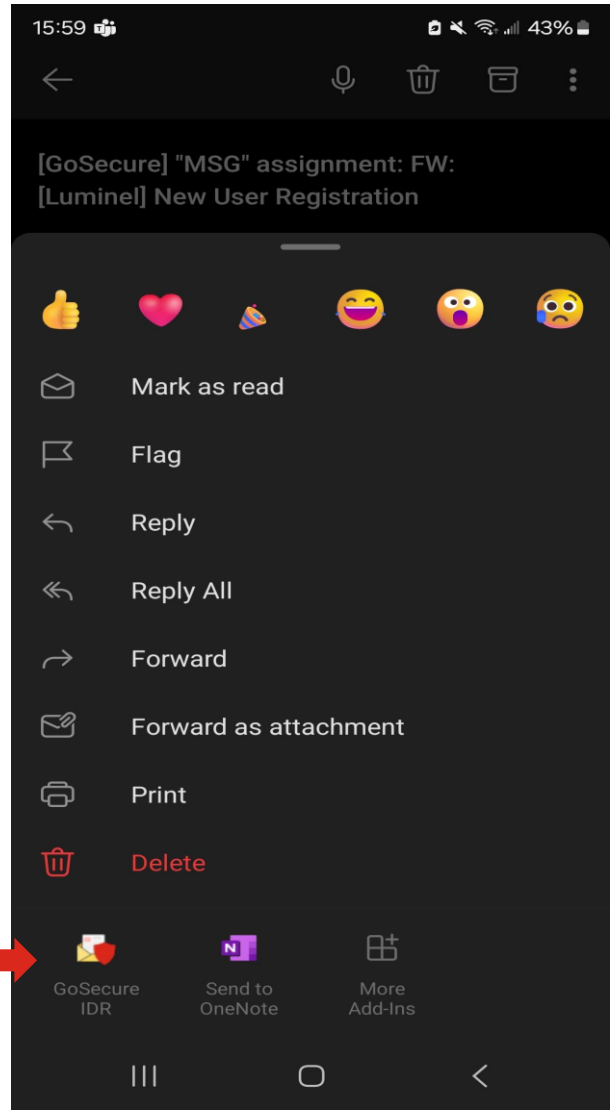


ET SOUMETTRE LE COURRIEL À L'ANALYSE



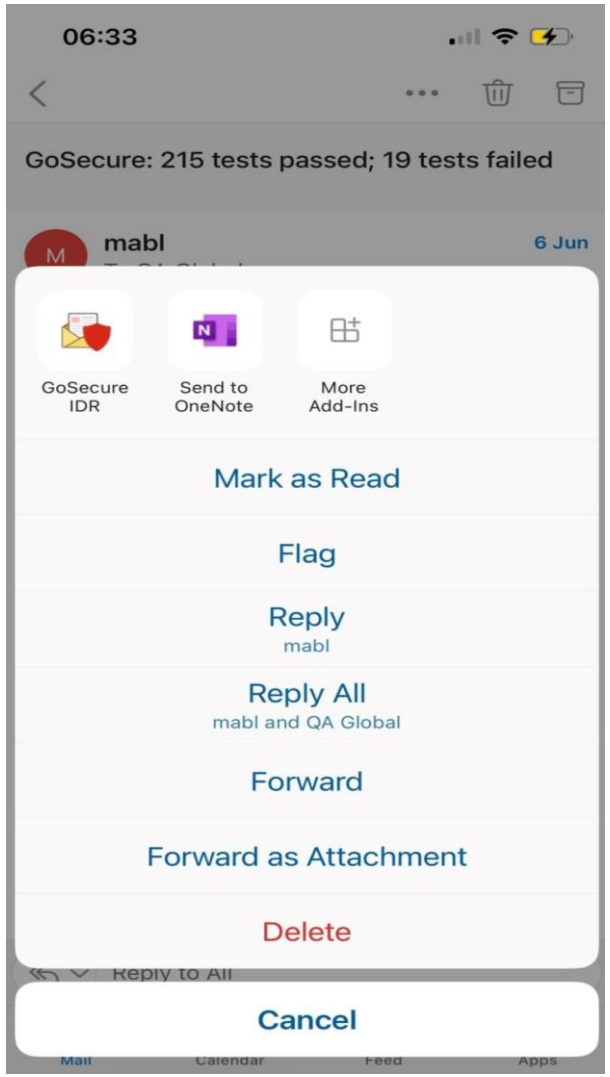
ANDROID

Dans un courriel, cliquez sur les points de suspension, faites défiler vers le bas et cliquez sur le bouton IDR.

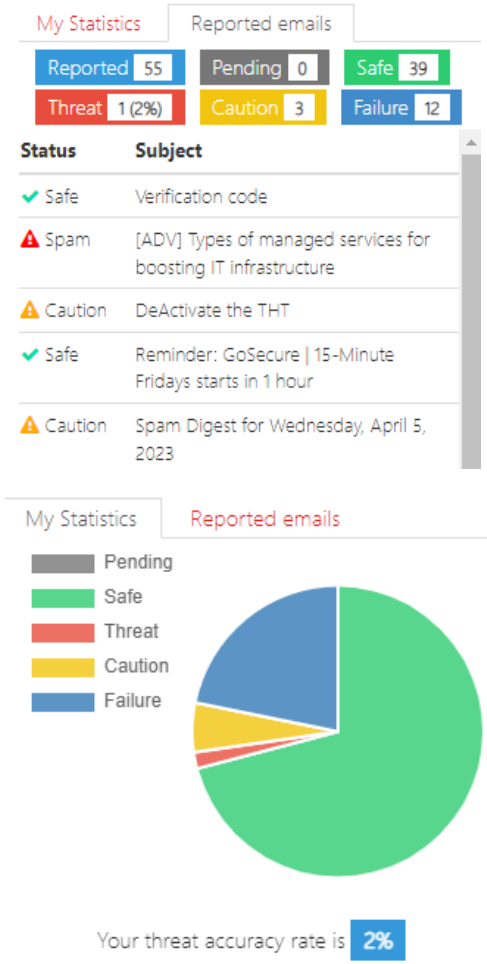


IPHONE

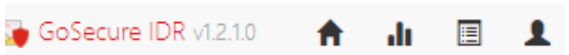
Dans un courriel, cliquez sur les points de suspension et sur le bouton IDR.

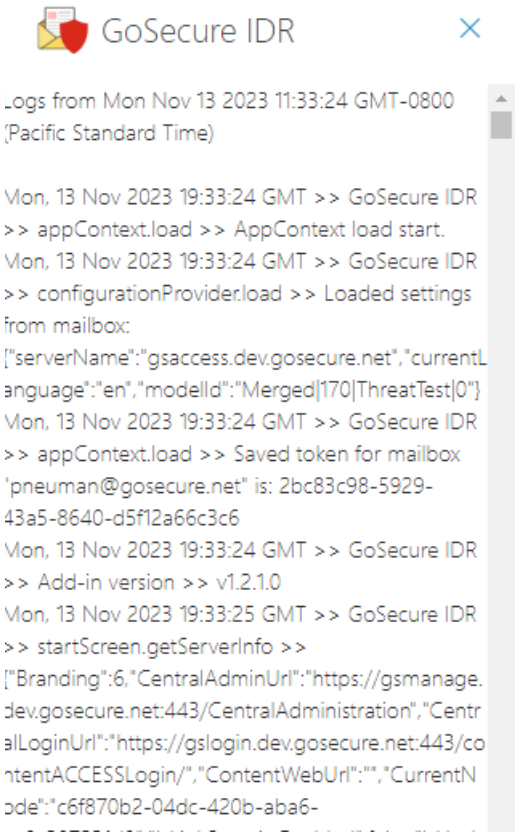


FONCTIONS IDR

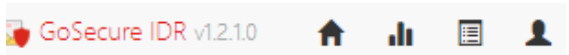


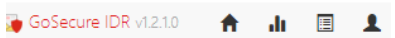
Statistiques





Journaux d'assistance





DÉCISION

FEU VERT

Bien joué !

Cette réponse indique que le courriel n'est pas malveillant, ce qui a conduit GoSecure à le placer dans votre boîte de réception.

FEU JAUNE

Soyez prudent

Cela signifie que le service n'a pas clairement identifié que le courriel est malveillant, mais qu'il a repéré des éléments qui soulèvent des doutes quant à sa légitimité, ce qui a conduit à la mise en quarantaine du courriel ou à son retour dans votre boîte de réception, en fonction des paramètres de sécurité de votre organisation.

Si le courriel a été renvoyé dans votre boîte de réception, nous vous recommandons de contacter l'expéditeur par téléphone avant d'effectuer toute demande.

FEU ROUGE

Nous avons trouvé une menace !

Cette réponse indique que le courriel est suspect, ce qui a entraîné sa mise en quarantaine.

QUESTIONS FRÉQUENTES

Pourquoi est-ce que j'obtiens un feu jaune lorsque je soumets un courriel interne à GoSecure pour analyse ?

- Nous vous recommandons de contacter l'expéditeur par téléphone pour confirmer toute demande.

Que dois-je faire si je me rends compte que j'ai cliqué sur un lien douteux dans un courriel frauduleux ?

- Changez votre mot de passe immédiatement
- Informez votre équipe de sécurité
- Ne manquez pas d'en informer votre responsable

Puis-je récupérer un courriel mis en quarantaine par GoSecure ?

- Bien entendu, vous pouvez demander à l'équipe d'assistance informatique de votre entreprise de lever la quarantaine placée sur un e-mail par GoSecure.

Notre équipe a reçu un courriel, mais il semble avoir disparu de toutes nos boîtes de réception. Pouvez-vous nous expliquer pourquoi ?

- Ceci indique qu'un membre de votre équipe avait des inquiétudes concernant ce courriel. Il l'a soumis à GoSecure IDR pour analyse et a reçu un avertissement jaune ou rouge. En conséquence, le courriel a été supprimé de toutes les boîtes de réception et placé en quarantaine.

J'ai des inquiétudes concernant la cybersécurité. Qui dois-je contacter ?

- Votre équipe d'assistance informatique sera toujours votre premier point de contact pour toute question relative à l'informatique et à la cybersécurité.

GoSecure.net

Merci !