

CWATCH MAIL REPORT

L'email est depuis longtemps le **vecteur d'attaque** important pour les adversaires souhaitant toucher les utilisateurs de votre système d'information : **phishing** / opération de collecte d'identifiants, **compromission** du poste de travail par une charge malveillante dans une pièce jointe, fraudes et usurpation d'identité.

Vos systèmes de messagerie et la sensibilisation de vos utilisateurs sont des mesures de sécurité essentielles face à ces menaces.

La solution **CWATCH Mail Report** complète votre dispositif de sécurité en donnant un rôle actif à vos utilisateurs en leur permettant de signaler facilement un **email suspect**, avec toutes les données techniques nécessaires aux investigations, et de bénéficier de l'expertise du CERT CWATCH dans leurs analyse.

Le service permet de raccourcir les **délais de détection** et de permettre des réponses efficaces, et peut être complété des services managés **SOC CWATCH** pour améliorer la sécurité de votre organisation.

COMMENT CELA FONCTIONNE-T-IL POUR LES UTILISATEURS ?



NB : La solution **CWATCH Mail Report** peut également être utilisée seule et configurée pour envoyer l'email de signalement à votre équipe sécurité, sans les services du SOC / CERT CWATCH.

CWATCH MAIL REPORT

QUELS SONT LES AVANTAGES DE LA SOLUTION CWATCH MAIL REPORT ?

01

L'utilisation de la fonction de signalement est extrêmement simple pour les utilisateurs, et, contrairement à l'utilisation courante de la fonction « transmettre » d'un mail vers un support, l'utilisation de **CWATCH Mail Report garantit que toutes les données déterminantes pour l'investigation** (en-têtes du message dont les champs SPF, DKIM, adresse IP de l'expéditeur, etc.) **sont bien transmises dès le départ**, sans aller-retour avec le support ou manipulation complexe

02

Votre support informatique n'a pas à manipuler des emails malveillants avec les risques que cela implique : **l'analyse des emails est réalisée par les experts des équipes SOC / CERT CWATCH Almond** sur notre plateforme d'investigation, sans risque pour votre système d'information, et permettant de contrôler le contenu de l'email, des pièces jointes et des liens.

03

L'**analyse technique** est **doublée d'une analyse humaine** permettant d'**identifier des cas de fraude ou de manipulation** et de faire une réponse adaptée à l'utilisateur + une notification vers vos équipes IT si la menace est avérée avec une recommandation de traitement.

04

Si vous l'autorisez, l'équipe SOC / CERT CWATCH peut **automatiser la suppression des mails malveillants** dans les BAL de vos utilisateurs sur votre messagerie Office 365.

05

L'équipe SOC / CERT CWATCH peut vous aider à **mesurer l'efficacité de la sensibilisation de vos utilisateurs** en analysant les signalements réalisés dans le cadre de **tests de campagne de phishing**.

Client de messagerie

Windows

Office365 ProPlus
Outlook 2019

Mac

Office365 ProPlus
Outlook 2019
Outlook 2016

Plateforme de messagerie

Exchange Online (Office365)
Exchange 2019 on-premise
Exchange 2016 on-premise

Accès au site hébergeant le complément et géré par Almond depuis tous les postes utilisateurs

CWATCH MAIL REPORT

QUELS SONT LES AVANTAGES DE LA SOLUTION CWATCH MAIL REPORT ?

Coût de déploiement du CWATCH Mail Report	1 900 €
Coût utilisation bouton CWATCH Mail Report (par utilisateur) année 1	1,50 €
Coût utilisation bouton CWATCH Mail Report (par utilisateur) année 2 et suivantes	0,25 €
Service annuel CWATCH socle pour capacité d'analyse de signalements	Nous consulter

COMMENT ALLER PLUS LOIN ?

En souscrivant aux services de détection du SOC Almond, vous pouvez vous doter d'une **capacité de détection et de réponse automatisée plus poussée**, permettant par exemple :

- **D'identifier** par les alertes produites par vos solutions de sécurisation de la messagerie, des **emails malveillants** ayant été délivrés et les **supprimer proactivement** avant qu'ils ne posent problème.
- De repérer les cas où un **utilisateur** a effectivement **cliqué sur un lien malveillant** dans un email et d'**adapter la réponse**.
- D'adapter de façon proactive le **filtrage sur vos passerelles** de messagerie.

Par ailleurs, si vous avez **besoin d'assistance** sur un incident de sécurité, n'hésitez pas à **contacter notre équipe CERT** dédiée qui peut vous aider à y faire face rapidement :



+33 (0)1 83 75 36 94



alerte@cwatch.almond.eu