

# CWATCH MAIL REPORT

For a long time, email has been the **major attack vector** for adversaries to target users of your information system: phishing / credential theft operation, compromise of a workstation by a malicious payload in an attachment, fraud and identity theft.

Your email systems and user awareness are essential security measures against these threats.

The **CWATCH Mail Report** solution completes your security measures by giving an active role to your users by allowing them to easily report a suspicious email, with all the technical data required for investigations, and to benefit from the expertise of the CWATCH CERT in their analysis.

The service helps to shorten detection times and enable effective responses. In addition, SOC CWATCH managed services can enhance your organization's security.

## HOW DOES IT WORK FOR USERS ?

The user selects the suspicious email in their email client and clicks on the **CWATCH Report button**

**CERT CWATCH** warns the user of the result and notifies your security team in case of a proven threat

CWATCH CERT can directly **remove malicious emails** in O365 mailboxes if you allow it

A **notification email** including all the necessary technical information is prepared automatically, ready to send

**CWATCH CERT** analyzes email on its investigation platform



**NB: The CWATCH Mail Report solution** can also be used on its own and configured to send the notification email to your security team, without the services of the CWATCH SOC / CERT.

# CWATCH MAIL REPORT

## WHAT ARE THE ADVANTAGES OF THE CWATCH MAIL REPORT SOLUTION?

01

The reporting function is extremely simple for users, and unlike the common use of the «forward» function of an email to the internal IT support team, **the use of CWATCH Mail Report ensures that all data relevant to the investigation** (message headers including SPF, DKIM fields, sender IP address, etc.) are **delivered right from the start**, without any back and forth with the support team or complex handling.

02

Your IT support does not have to handle malicious emails with the risks that it implies: **the analysis of emails is carried out by the experts of the CWATCH SOC / CERT Almond teams** on our investigation platform, where they can control the content of the email, the attachments and the links, without risk for your information system.

03

**The technical analysis is coupled with a human analysis to identify cases of fraud or manipulation** and make an appropriate response to the user + a notification to your IT teams if the threat is highlighted with an action plan proposal.

04

If you authorise it, the CWATCH SOC / CERT team can **automate the deletion of malicious emails in your users' mailboxes** on your Office 365 email.

05

The CWATCH SOC / CERT team can help you to **measure the effectiveness of your users awareness** by analyzing reports from **phishing campaign tests**.

### Email client

#### Windows

Office365 ProPlus  
Outlook 2019

#### Mac

Office365 ProPlus  
Outlook 2019  
Outlook 2016

### Email platform

#### Exchange Online (Office365)

Exchange 2019 on-premise  
Exchange 2016 on-premise

**Access to the site hosting the supplement and managed by Almond from all user workstations**

# CWATCH MAIL REPORT

## WHAT IS THE COST?

Cost of deployment of the CWATCH Mail Report	1 900€
Cost of usage of CWATCH Mail Report button (per user) year 1	1,50€
Cost of usage of CWATCH Mail Report button (per user) year 2 and following	0,25€
Annual CWATCH base service for alert analysis capability	Contact us

## HOW TO GO FURTHER?

By subscribing to Almond SOC's detection services, you can gain an **advanced automated detection and response capability**. For example:

- **Identify malicious emails** that have been delivered through alerts generated by your email security solutions and proactively remove them before they become a problem.
- Identify when a user has actually **clicked on a malicious link** in an email and **adapt the response**.
- Proactively adapt **filtering on your email gateways**.

Also, **if you need assistance** with a security incident, do not hesitate to contact our **dedicated CERT team** who can help you to deal with it **quickly**:



+33 (0)1 83 75 36 94



[alerte@cwatch.almond.eu](mailto:alerte@cwatch.almond.eu)