# Managed Cybercrime Monitoring [email]

## Advanced mail analysis, incorporating employee security awareness as well as IOC extraction and collection.

Alongside the more covert operations and previously uncovered data exposure incidents that Managed Cyber-crime Monitoring seeks to address as a service, comes the cybercrime community's long standing weapon of choice – email phishing attacks. Email-borne attacks con-tinue to be a prominent and ever-adapting tactic of cyber-criminals, and Business Executive Compromise (BEC) and Email Account Compromise (EAC) have consistently been responsible for the biggest overall financial losses* related to cybercrime.

As with the broader digital risk management activities, phishing email analysis has grown more popular as a ser-vice that can be handed over as a function to a specialist managed service provider. But this too, has often become a silo within security operations

Orange Cyberdefense enables the integration of this function as part of our broader Managed Detection and Response offering, as well as complementing advisory activities such as security awareness programmes under-taken by our consulting teams.

### What we do:

- Triage, qualification and classification of emails
- Notification to end users
- Identification of IoCs
- Enrichment of third-party tools such as anti-spam, anti-virus etc.
- In-depth analysis (if necessary) of specific threats



Escalation to customer's security team

Suspicious email received by customer employee

forwarded to monitoring

Managed Cybercrime Monitoring [email] infrastructure

Email acknowledgement sent to user

Reply sent to user

Automated Email analysis & classification

Manual review and analysis by CERT

Learning chain