Orange
Cyberdefense

Managed Cybercrime Monitoring [brand]

Monitoring of web, mobile and social channels to identify any brand exploitation, social media impersonation, malicious or fraudulent mobile apps, and defacement of legitimate websites.

What we do:

- Gather data via proprietary crawlers, as well as strategic partnerships with enterprise Digital Risk Management platforms
- Monitoring of common and alternative app stores
- Monitoring of popular social networks (Twitter, Linkedin, Facebook etc.)
- Triage of all alerts by Intelligence Analysts
- Assist with takedowns if required and where possible

What you get:

- Alert notification upon detection
- Full analysis, qualification and investigation of each case and criticality scoring
- Recommendations
- Takedown options for mobile and social
- Mobile App analysis via P2M proprietary sandbox

A modular approach

Build your digital risk management capabilities according to your needs

The Managed Cybercrime Monitoring service can be consumed in a modular fashion, allowing you to build up your capability depending on your needs now, but also allowing for future expansion.

Our four key areas of focus include:

- Brand: monitoring of web, mobile and social channels to identify any brand exploitation, rogue sites or apps, and defacement.
- Data: Proactive identification of potential data exposure (whether accidental or malicious) across diverse sources, from paste sites to code repositories to Dark Web marketplaces and underground forums.
- Fraud: surveillance of fraudulent activity. Focusing on phishing sites and domain impersonation, as well as specialised areas such as credit card fraud monitoring.
- Email: advanced email analysis, employee security awareness and IOC collection.