Orange
Cyberdefense

Managed Cybercrime Monitoring

Taking managed detection and response beyond the enterprise perimeter.

Protecting your brand and intellectual property in the digital world is paramount. Cybercrime is big business and in 2021 it is expected to inflict 6 trillion US dollars in damages globally.

Brand abuse by malevolent actors is at epidemic level in the digital world, destroying reputations and denting bottom lines. The impact can be enormous, from legal action and regulatory fines to damaged customer loyalty. The techniques used by attackers change as fast as the attack landscape and most threats come from organized and sophisticated cybercriminal networks with global reach.

Alongside this problem, further digital risk and exposure comes from the accidental dissemination of information on the internet from using data sharing apps in the cloud, naïve use of code repositories such as GitHub by development communities, and data mistakenly published by an employee or a third party.

Orange Cyberdefense's Managed Cybercrime Monitoring services extend managed detection and response capabilities outside your organization's perimeter by continuously monitoring the internet, deep and dark web for digital fraud, brand exploitation and data leaks.

Addressing cybercrime across a number of different attack surfaces and use cases, Orange Cyberdefense allow you to introduce digital risk management as a business function without the huge outlays it would otherwise require. The service is also an integrated part of our wider Managed Detection and Response (MDR) service offering, meaning that this crucial component of security operations is no longer a silo, but instead expands MDR coverage beyond traditional internal monitoring of endpoint, network and log data.

Challenges of monitoring cybercriminal activities:

Access: Access to underground marketplaces and cybercriminal forums is getting tougher as they fragment amidst high profile law enforcement operations.

Language: Cybercriminals speak a different language, both literally but also figuratively. The cybercriminal community has its own unique tone and rules of engagement.

Intelligent data processing: Huge amounts of data can be collected to profile a business and their digital footprint – but amongst that is also an incredible amount of content that is completely legitimate and irrelevant to cybercrime monitoring activities.

Mitigation: It is much tougher to act on external digital risks identified than the traditional activities of incident response in environments that are under your control. Often legal teams are not built for such a specialist purpose, nor do they have the resources to act quickly and efficiently.

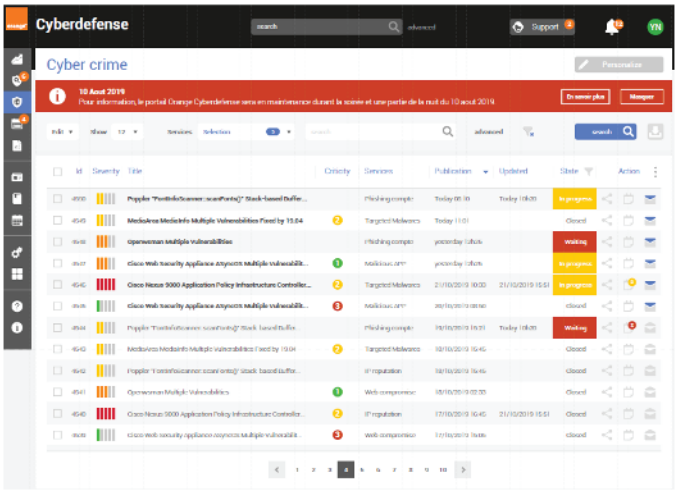
Find out more on our modular approach on:
orangecyberdefense.com/global/cert/

A modular approach

Build your digital risk management capabilities according to your needs

For a long time, securing our digital footprint and the inherent risk it carries has been too costly, even with the savings made by pushing that capability out to a trusted MDR specialist such as Orange Cyberdefense.

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. All of this is presented in our Threat Defense Center portal, so that you can easily view, filter and report on the findings of the service. You can also submit additional assets when new digital assets are created or discovered.



About the Orange Cyberdefense CERT:

- Our in-house Computer Emergency Response Team (CERT) is recognized as the top European private CERT. It has relationships with 20 law enforcement agencies across multiple continents including the FBI, Interpol and Europol.
- Dedicated Cybercrime Monitoring team with 20+ intelligence analysts across 3 locations coming from specialised intelligence backgrounds and with over 16 years' experience in this field.

Our proprietary, hidden web crawlers and bots specialize in analyzing huge numbers of pages on the open internet, the deep web and the dark web seeking out potential threats against your organization's brand and IP addresses.

- This is complemented by in-depth qualification by multilingual experts, who are available 24/7/365. They monitor more than 10,000 brands and take down around 20,000 rogue websites each year.

The Managed Cybercrime Monitoring lifecycle process

Anticipate
- Understand intelligence goals
- Understand business context
- Collect the right asset data

Identify
- Millions of sources crawled
- Proprietary Orange Cyberdefense CERT tools and infrastructure
- Best in class DRM platforms

Respond
- Collect the evidence required to resolve the incident
- Formalize recommendations and escalate appropriately
- Take action where possible (e.g. domain- or content takedowns)

Detect
- Millions of sources crawled
- Proprietary Orange Cyberdefense CERT tools and infrastructure
- Best in class DRM platforms