Orange
Cyberdefense

Managed Detection and Response

Managed Detection and Response is about discovering breaches in real time, and responding in a way that minimizes damage for your organisation.

According to research the current average time to identify and contain a data breach is 280 days*. It is high time to identify and fix this apparent gap in security operations. An adaptive, modular service package, backed by in-depth awareness of the threat landscape is the solution.

Prevention is not enough

There are many ways to become "almost" good enough with your cybersecurity. Investing in different security vendors and upskilling existing staff can provide a decent protection against a variety of threats.

"Almost good" is not sufficient. The number of threats we now face, combined with their impact demands more.

Investing in good protection is not wrong. But if you think about it, all data we have today, and the news stories we read on a regular basis, tells us that protection alone is not good enough.

For decades the majority of the security budgets has been spent on prevention technologies like antivirus and firewalls. This has left little resources for investing in the abilities to detect and respond to the threats that could not be prevented.

82% of organizations are unclear about whether they are successfully identifying breaches and incidents.

EY Global Information Security Survey 2018

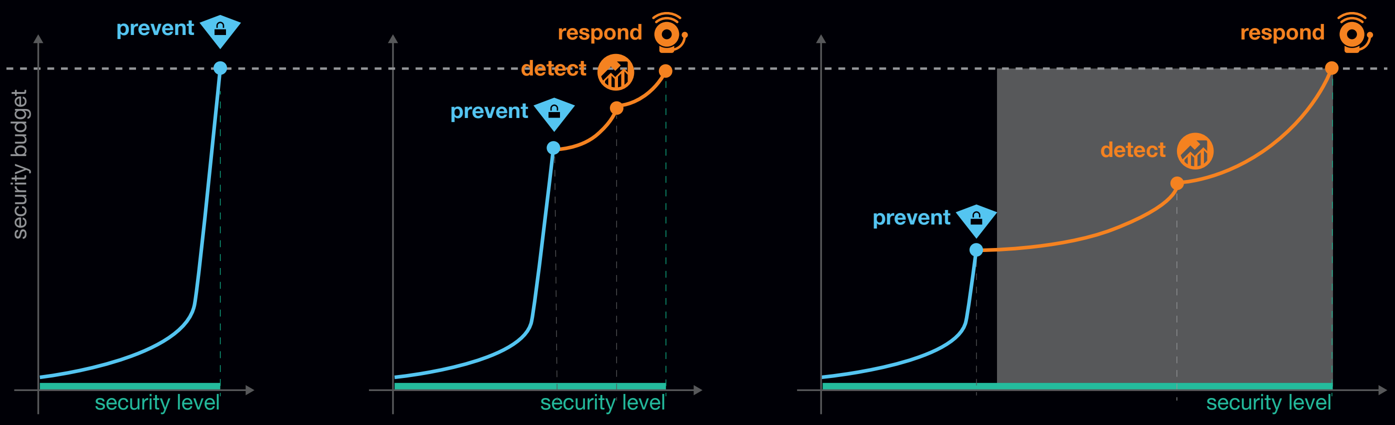
A challenge with detection and response is that it has a much higher demand on people and processes. Threat actors are global, work across all time zones and are very skilled. Building up a 24x7 team with competence, infrastructure and processes is very expensive and time consuming.

This makes investing in Managed Detection and Response (MDR) services your best option.

* IBM Security: Cost of a Data Breach Report 2020

Get more out of your budget

Balancing the scales with detection & response



Chosing the right path

The layers and the type of protection, detection and response is unique for every business. But don't worry, the way to find out what's right for you does not need to be so complex. Focused assessments help to define your next step closer to achieving your threat detection and response goals.

Try our Buyer's Guide for a head-start!

Find out more about how to boost your defenses with MDR: orangecyberdefense.com/global/mdr/

Benefits:

Complete detection visibility: gain insight inside and outside of your organisation to detect cybersecurity threats.

Intelligence-led security: we invest heavily in research and development to detect and respond to the latest tactics, techniques and procedures.

Active response: a broad range of active response options are available 24x7 to suit your security operations needs.

Save time and costs: we use innovative techniques to ensure that incidents are investigated in context and noise is reduced as much as possible.

Intelligent detection

The challenge with detection is that there is not one type of technology that solves all detection needs. There are options for doing detection across log data, network data and endpoint data.

There are threat activities that happens outside of your infrastructure that may cause a risk to your business that needs to be detected. You can probably not solve all problems at the same time, but you can choose a security partner with a complete MDR portfolio that can guide you to your best investments.

Orange Cyberdefense offers a complete detection portfolio that covers not only the SOC triad of log, network and endpoint, but also detection of threats to your business on the Open, Deep and Dark Web. You can start with the one most relevant for your current need, and then expand as your business requires.

Our Intelligence Backbone pulls in and pushes out threat data across our different services and global customer set to enable us to provide a global as well as local perspective on detecting anomalous behavior.

We have you covered!

Orange Cyberdefense MDR services are modular and a customer can select one or several of these components depending on their own resources – or more importantly where Orange Cyberdefense can effectively plug the gaps where those resources don't exist.

Once you have your Managed Threat Detection service in place, this can be combined with the response service that you need in order to compliment your own abilities.

All of the services are backed by our global network of 18 SOCs and 11 CyberSOCs that have 24x7 eyes on the screen, and our internationally recognised CERT teams who hold memberships with CREST, TF-CSIRT and FIRST.

Whatever your needs in the area of response are, our Managed Threat Response services complement and extend your capabilities as required. We assist to contain threats before they cause long lasting damage, while our Incident Response retainer and digital forensics services give you on-demand access to one of the largest and most skillful CSIRT teams in Europe.

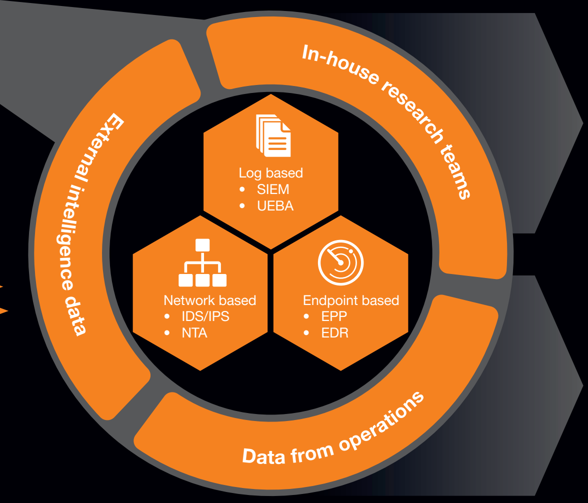
Intelligence-led MDR: Benefits

Orange Cyberdefense Intelligence Backbone

- Intelligence from MDR, CERT, CSIRT operations
- External intelligence
- Collaboration with law enforcement
- In-house R&D

Internal activities

- Detection of suspicious actitivities
- Analyzing and classifying incidents
- Notification and reporting



Better detection

- Advanced knowledge of IoCs
- Early detection of major campaigns
- Superior analysis & correlation
- Efficient filtering of "noise" and false-positives
- 24x7 CyberSOC

Better response

- Faster tracking of incident causes
- Faster detection of attack vectors
- Rapid containment & forensics
- 24x7 CSIRT