Orange
Cyberdefense

Managed Detection & Response

What are your top assets? Are they safe right now?

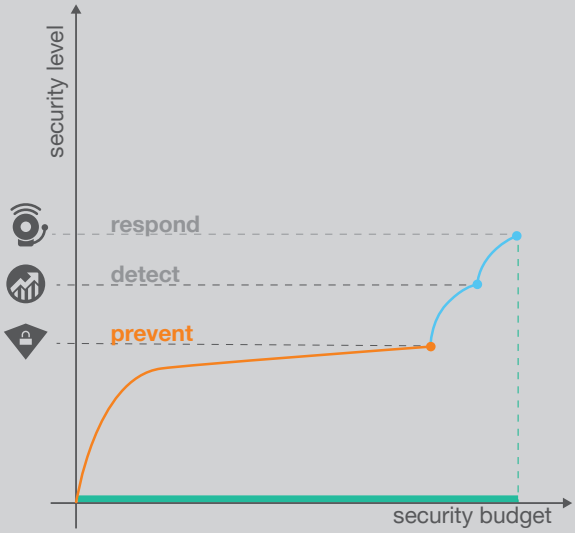
A majority of organizations are unclear about whether they are successfully identifying breaches and incidents!

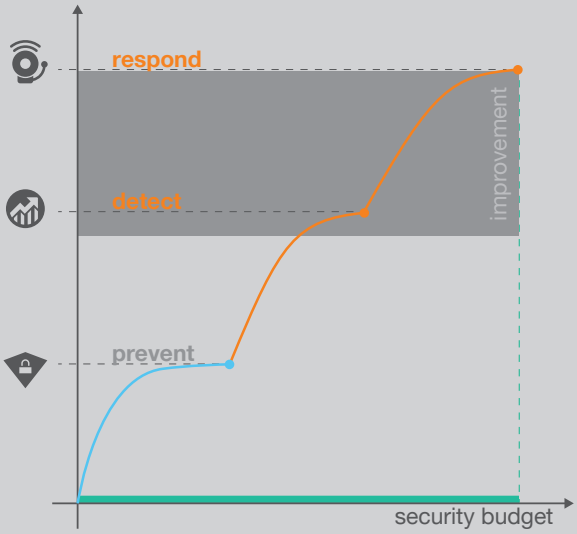
Why is that? For decades the majority of the security budget has been spent on prevention technologies like for example AntiVirus and Firewalls. This has left a small budget for investing in the abilities to detect and respond to the threats that you could not prevent.

Another challenge with detection and response is that has a much higher demand on people and processes and required 24x7 expertise, since the threats are global and very skilled. Building up a 24x7 team with competence, infrastructure and processes is very expensive and time consuming.

This makes investing in Managed Detection & Response (MDR) services the best bet for most customers.

82% of organizations are unclear about whether they are successfully identifying breaches and incidents.
EY Global Information Security Survey 2018





Orange Cyberdefense Detection Services

- SecureDetect SIEM
  Log based detection with Co-managed option
- SecureDetect Network
  Network based detection
- SecureDetect Endpoint
  Endpoint based detection
- SecureDetect Intelligence
  Targeted threat intelligence as a service

Orange Cyberdefense Response Services

- SecureRespond Quarantine
  Threat disruption service
- SecureRespond Incident
  Incident Response service
- SecureRespond Malware
  Malware forensics service

Orange Cyberdefense – a recognized partner to rely on.

- Listed as notable vendor in Gartner Europe Context for MSS
- Listed as representable vendor in Gartner Market Guide for Managed Detection & Response
- Identified by PWC as a European market leading service provider
- Most importantly, we are local. We work closely with our customers to develop the optimal detection and response strategy for their specific company.

Find out more on how to protect your endpoints on:
orangecyberdefense.com/de/mdr/

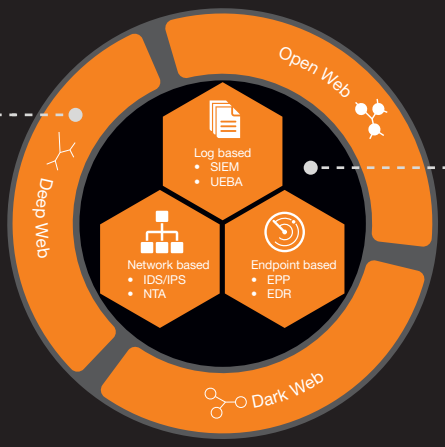
Detection

The challenge with detection is that there is not one type of technology that solve the complete detection needs. There is a need for doing detection across both 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 threat 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.

External activities
- Identify exposed crudentials, IP...
- Identify exposed domains, profiles...
- Access TI feeds & Threat Actor Profiles



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

Response

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

Option A
You have all the capabilities yourself for 24x7 response and only need incident detection & notification.

Option B
You have an incident response team, but no 24x7 threat disruption capabilities.

Option C
You need help with both 24x7 threat disruption and onsite Incident Response services.

Mehr Infos finden Sie auf
https://orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

info@de.orangecyberdefense.com
+49 89 2000148 00