Orange
Cyberdefense

Managed Threat Detection [endpoint]

Visibility is key and the endpoint is where you get it. Respond immediately.

There is no such thing as 100% protection. Once you have accepted this fact it is time to implement a strategy on how to detect the threats you couldn't prevent. The challenge with detection is that today's threats are not using old malware that is easy to detect and remediate.

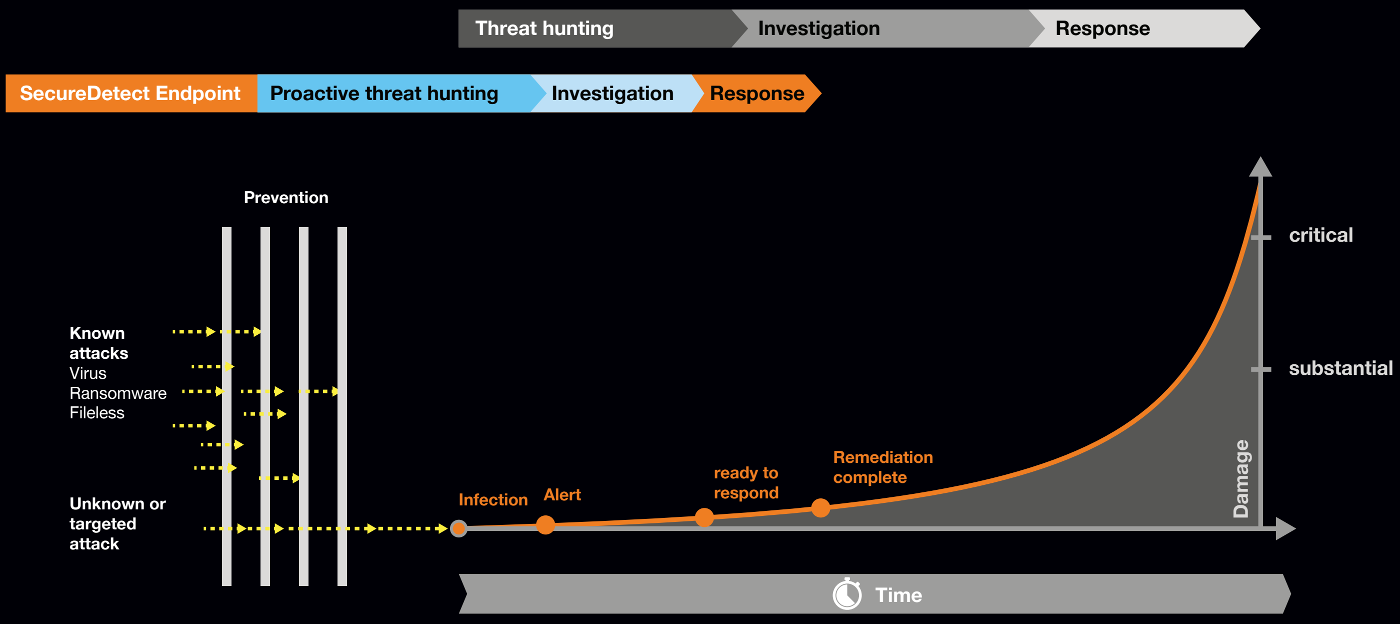
77%* of successful attacks used fileless malware that traditional security tools could not prevent. Since detection of fileless malware and similar types of advanced attacks cannot be done with the help of static rules or signatures, you need the ability for behavior anomaly detections on the endpoint. This behavior needs to be analyzed and also correlated across other endpoints to be able to separate the false positives from the real incidents. Without the right tools and competences this can take a very long time. Once the investigation is done, often you need to do a rapid response. The time from infection, to detection, to remediation takes too long, causing uncontrollable cost and damage.

* Ponemon 2018 Endpoint Security Statistics Trends

Service overview

The Managed Threat Detection [endpoint] service is a managed detection and response service (MDR) based on endpoint detection and response technology (EDR). By deploying small sen-sors on the endpoints, behavior data is collected, enriched and correlated across all endpoints with the help of an AI hunting engine and a massive in-memory graph database. By doing up to 8M correlations per second this outper-forms the amount of correlations you can do on a tradition-al SIEM platform massively.

This provides detection abilities far beyond what traditional signature or rule-based platforms can do. The caveat is that the detections are not black or white. In most cases it requires manual work from a skilled analyst to verify and classify the incident. This is where the Orange Cyberdefense Cyber SOCs come in.



Mehr Infos zur Endpoint-Verteidigung finden Sie unter:
orangecyberdefense.com/de/endpoint/

Benefits:

- Quick time to value (versus for example, deploying a SIEM)
- Advanced detection abilities based on endpoint behaviors
- 24x7 manual analysis and classification of incidents
- Threat disruption by isolating infected endpoints
- Optional: Threat Hunting and Incident Response Retainer services

	Standard	Premium
Analysis and classification of MalOps	🟧	🟧
Notifications with recommended actions	🟧	🟧
Isolation of infected endpoints (SecureRespond service incl.)	🟧	🟧
Monthly security report	🟧	🟧
Recurring service delivery meetings	🟧	🟧
Orange Cyberdefense custom detection rules		🟧
Orange Cyberdefense threat intelligence integration		🟧
Manual threat hunting	optional	optional
Incident Response Retainer Service	optional	optional

Learn more

If you’d like to know more about how our Managed Threat Detection [endpoint] service, simply call us to arrange a free, no obligation consultation, or visit **orangecyberdefense.com**.