Cynet

# MANAGED DETECTION AND RESPONSE SERVICES

## INCLUDED IN THE CYNET 360 'COMPLETE' PACKAGE

## SECURITY SKILLS ARE CRITICAL

Cyberthreats are on the rise, but not all attacks were created equal. It takes an expert eye to tell between a critical risk and a mere nuisance, as well as to know where to look, what to look for and what the best paths are to confront the threat.

While security products are constantly improving in disclosing risk level and threat metadata in their alerts, human skill remains critical.

## CYOPS: CYNET MDR SERVICES

CyOps is Cynet's team of threat analysts and security experts, operating a 24/7 SOC which manages the initial interaction of Cynet customer alerts.

CyOps continuously monitors and prioritizes alerts, informing customers in real-time of critical security events and guiding them through the response process. The interaction is bi-directional, as Cynet customers can submit files to CyOps for analysis at any time, as well as escalate events that require deeper examination.

## KEY BENEFITS

**24/7 Availability**
Perpetual monitoring and investigation. There are no 'off' work hours.

**Maximize Cynet 360 ROI**
Backed by the masters of Cynet 360 alerts and investigation tools.

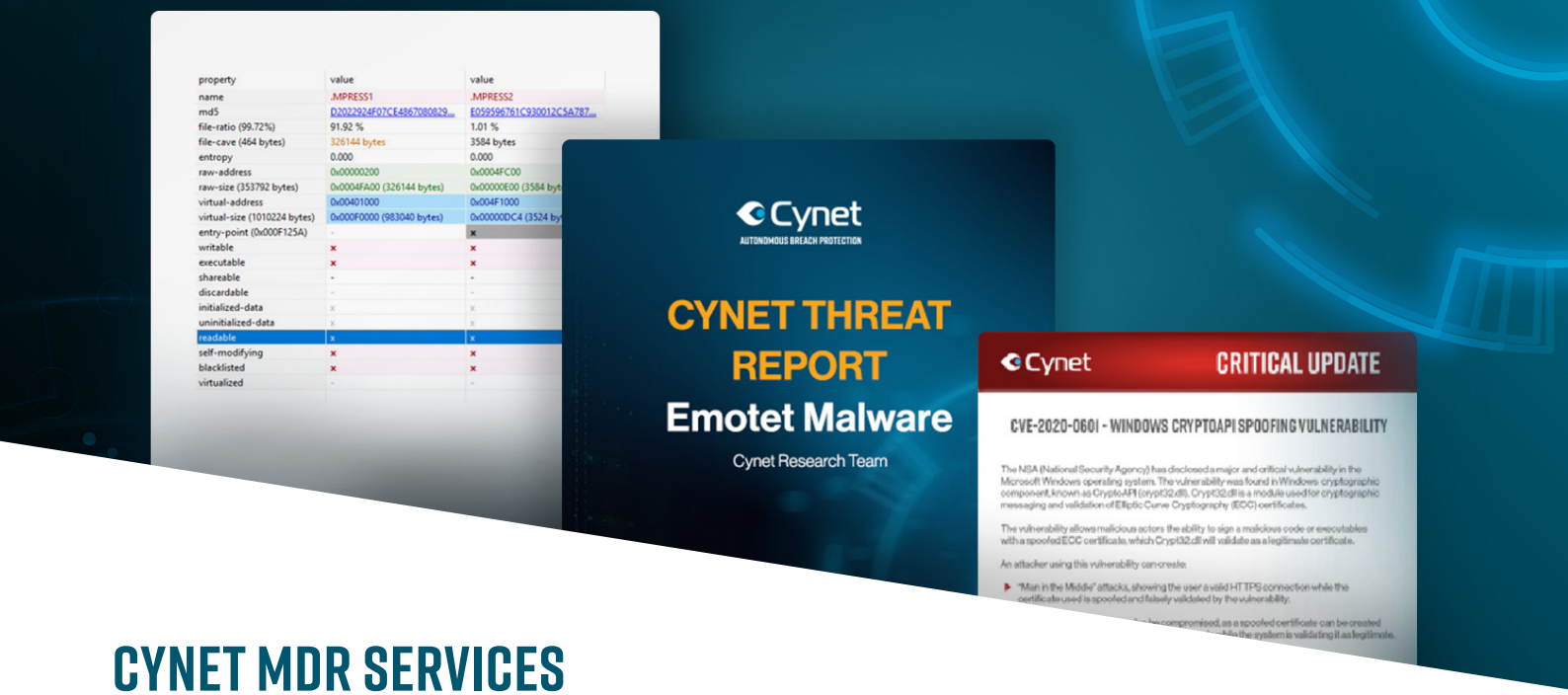
**Top Expertise**
Best-of-breed threat analysts and security experts.

**Single Click Away**
One click on 'engage CyOps' in the Cynet Dashboard app to get a security analyst on the line.

**100% Proactive**
Continuously hunting for critical and evasive threats in your environment.

**Threat Intelligence**
Constant updating from the world's leading threat intelligence feeds.

# CYOPS SAMPLE OUTPUTS




# CYNET MDR SERVICES

## ALERT MONITORING

Continuous management of incoming alerts: classify, prioritize and contact the customer upon validation of active threats.

## THREAT HUNTING

Proactive search for hidden threats leveraging Cynet 360 investigation tools and multiple threat intelligence feeds.

## 24/7 AVAILABILITY

Ongoing operations at all times, both proactively and on demand, per customers' specific needs.

## ON-DEMAND FILE ANALYSIS

Customers can send suspicious files to analysis directly from the Cynet 360 console and get immediate verdicts.

## ONE CLICK AWAY

CISOs can engage CyOps with a single click on the Cynet Dashboard App upon any suspicion of an active breach.

## ATTACK INVESTIGATION

Deep-dive into validated attack bits and bytes to gain full understanding of scope and impact, providing the customer with updated IoCs.

## EXCLUSIONS, WHITELISTING AND TUNING

Guidance in adjusting Cynet 360 alerting mechanisms to the customers' IT environment to reduce false positives and increase accuracy.

## REMEDIATION INSTRUCTIONS

Conclusion of investigated attacks entails concrete guidance for users regarding which endpoints, files, user and network traffic should be remediated.