Cynet 360 Use Case: Endpoint Detection and Response (EDR)

CYBERSECURITY CDM LEADER 2016

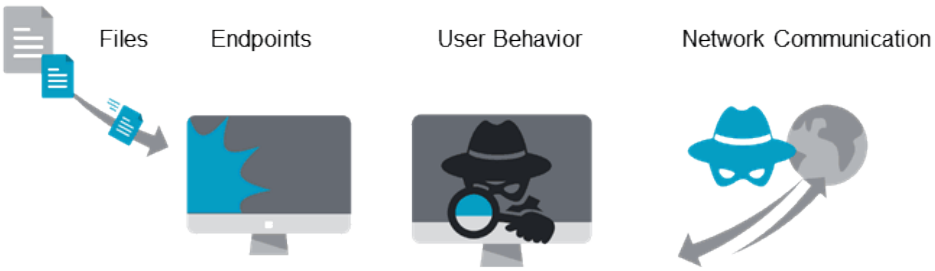
Increased complexity and frequency of today's advanced attacks elevate the need for enterprise-scale response, deep investigations and a rapid forensic process.

The Cynet 360 Advanced Threat Detection and Response platform is perfect for Endpoint Detection and Response purposes. With its visibility to endpoints, servers and the network, and using an adversary-centric approach to detection, Cynet precisely detect threats with near-zero false positives.

Precise Detection and Visibility Across the Attack Chain

Through continuous monitoring of endpoints for behavioral and interaction indicators, in-memory attacks and suspicious network communications, Cynet takes the unique approach of thinking like an adversary.

Cynet sees threats where adversaries try to slip in – detecting threat behaviors and indicators across files, endpoints, users and network communications, giving a complete picture of an attack operation and the associated actionable intelligence, and responding before it can do damage.



Correlating Threat Indicators

Rapid Response and Speed to Resolution:

Because of its access to the endpoint, responding to confirmed threats can be done quickly, even from across the network. Response actions include:

- Blocking of users or killing of processes
- Verifying files with dynamic analysis (sandbox)
- Changing IP or blocking traffic
- Deleting files Quarantining of files
- Isolating or restarting hosts, changing passwords and more.

Benefits

Comprehensive Platform:

- Single platform to detect, disrupt, respond, investigate and remediate

Rapid Deployment:

- Deploy to thousands of endpoints in < 2-hours
- No disruption and low impact to the end-user

Precise Alerts without the Noise

- Alerts of threats, not just pieces of evidence

Complete Understanding of Attacks

- Full picture and chain of events of an attack

Speed to Resolution:

- Quickly investigate, triage, respond and remediate
- Reduce dwell-time of threats

Efficient, Simplified Security:

- Improve productivity of security team

24x7 Monitoring:

- Available CyOps threat analyst assistance and insights

This can be accomplished manually with a single click if it fits into your security workflow, or automatically if instant remediation is needed, as in the case of in-memory attacks or ransomware.

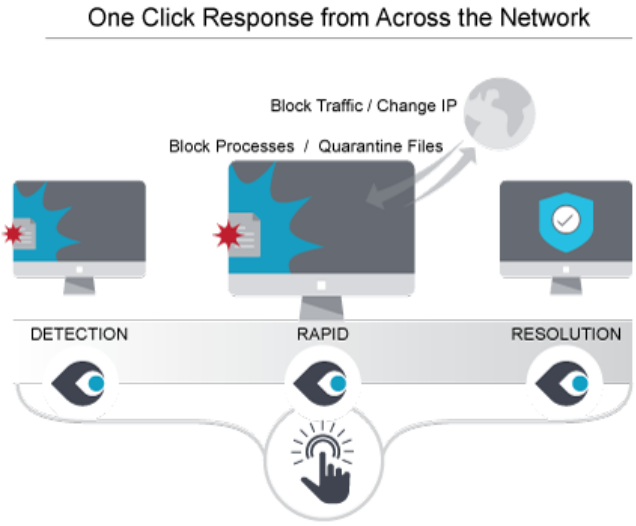
Quickly Search, Hunt and Validate

Cynet is also used for searching and reviewing historic and current incident data on endpoints, investigating and validating alerts, and searching for other instances of threats across the network.

Cynet records threat indicators over time for complete forensics, allowing for a deeper understanding of attack operations for investigators.

Knowing what a threat did, where it went, who it targeted and the root cause, gives investigators the actionable intelligence to respond now and take proactive action for the future.

With its quick search ability, security teams can hunt for other instances of threats, indicators of compromise (IOC), or other security artifacts sought by investigators enterprise-wide. And if you have alerts from other security products, you accomplish efficient validation of those alerts without chasing down endpoints.



About Cynet

Cynet is a pioneer and leader in advanced threat detection and response. Cynet simplifies security by providing a scalable, easily deployable protection platform that delivers prevention, precise findings and automated response to advanced threats with near-zero false positives, shortening the time from detection to resolution and limiting damage to an organization.

Cynet's unique visibility of files, users, network traffic, and endpoints, and continuous monitoring of an environment uncovers behavioral and interaction indicators across the attack chain, giving a complete picture of an attack operation over time. Cynet is enhanced by Cynet CyOps, which delivers additional value to the platform with 24/7 threat expert assistance, insight and intelligence. Staffed by an elite group of cyber threat analysts and investigators, Cynet's CyOps is an extra set of expert eyes dedicated to monitor, prioritize and respond to threats in a customer's environment.

By combining high fidelity detections, decoy interactions, network analytics, and expert analyst assistance, Cynet provides accurate findings with associated risks without a lot of complexity and noise, so security teams can prioritize and respond to what matters.

www.cynet.com | info@cynet.com
Tel: USA: 1-212-634-9358 EMEA: (972) 03-962-2655