CYNET 360: ADVANCED THREAT DETECTION & RESPONSE

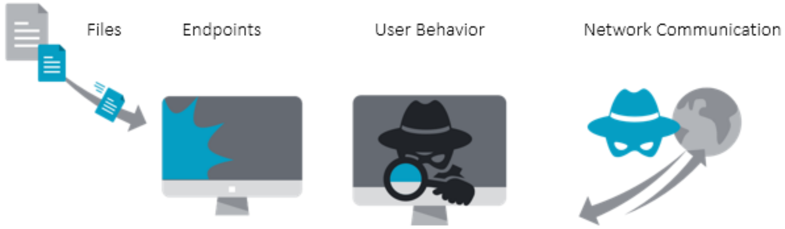
Cynet 360 Use Case: Incident Response

CYBERSECURITY CDM LEADER 2016

Precise Detection Across the Attack Chain

The Cynet 360 Advanced Threat Detection and Response platform is a work horse for incident response teams. Today's threats are complex and multi-staged, with continually changing variants that bypass traditional controls.

Using an adversary-centric approach to detection, and visibility of indicators on endpoints, user behavior, files and network communications, Cynet puts together the complete picture of an attack operation, precisely pinpointing when, where, and what threats are lurking, and the details behind them.

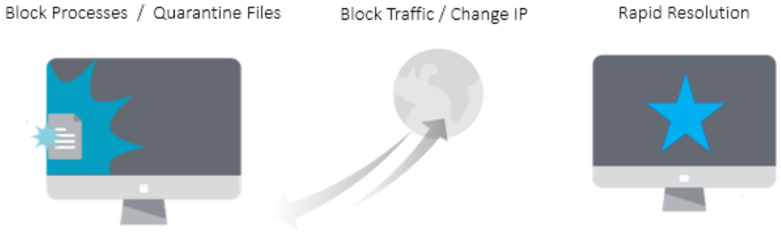


Correlating Threat Indicators

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
- Quarantine/Deleting files
- Isolating or restarting hosts, changing passwords and more.



One Click Response from Across the Network

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.

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

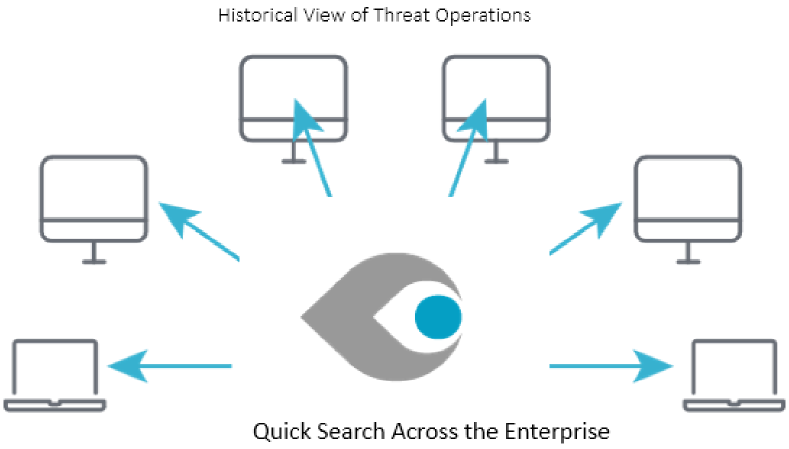
24x7 Monitoring:

- Available CyOps threat analyst assistance and insights

Investigative Forensics

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.

Quick search ability also enables responders to find other instances of the threat across the network, and centralized information ensures continuous availability.


Historical View of Threat Operations
Quick Search Across the Enterprise

Risk Ranking and What Matters

With Cynet's machine learning algorithms profiling what's normal for your environment, found threats can be scored and risk ranked so responders can triage the most dangerous attacks, isolating affected endpoints and dealing with what matters most in a quick and streamlined manner.

Cynet provides enterprise security teams a powerful, yet simple way to detect, disrupt and respond to the most dangerous and stealthy threats before they can do damage.

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.