Cynet

CYNET 360: ADVANCED THREAT DETECTION & RESPONSE

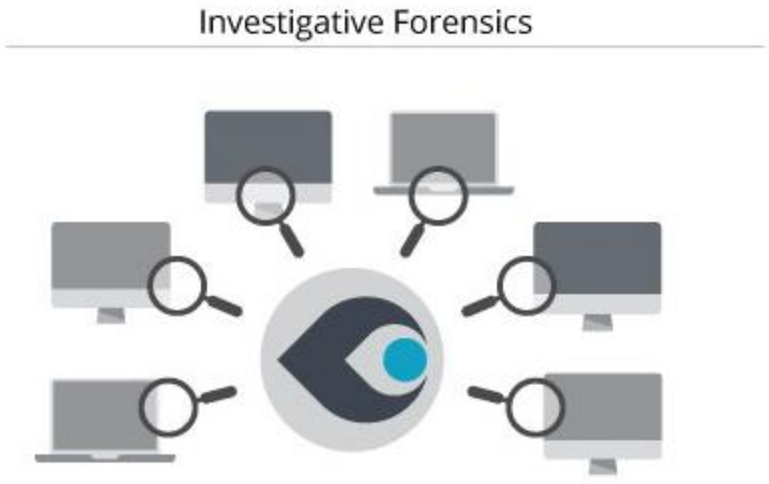
Cynet 360 Use Case: Forensic Investigations

CYBERSECURITY CDM LEADER 2016

"Adding technology alone won't stop advanced persistent threats. An effective strategy must include improvements in your forensics and incident response (IR) capabilities." - Gartner

In times of crisis, rapid, expert response is critical to ensuring business continuity. The Cynet 360 Advanced Threat Detection and Response platform provides the IT security team with a ready-to-go set of tools for the entire range of an enterprise's cybersecurity needs.

A crucial aspect of response, whether focused on network traffic, the endpoint, within user behavior, or the framework of Incident Response, is the ability to carry out precise, focused Forensic Investigations, to detect, understand and react to threats as they develop.



Deep-dive Forensic Investigations

Identifying a potential threat is the first step to protecting the organizational perimeter. Cynet correlates between indicators across files, endpoints, users, and the network, to identify anomalies and provide true alerts.

Once a potential threat has been detected and an alert received, the Cynet platform enables the IT security team to quickly isolate and investigate utilizing its advanced Forensic Investigation capabilities. Threat evidence can be examined and associated with a host, processes, users or network traffic data.

Static and Dynamic Sandbox

The Cynet 360 platform provides a static and dynamic sandbox environment in which enterprise security staff can isolate and investigate suspicious items. This allows them to safely gain data and behavioral evidence, for a clear picture of threats and attack operations over time.

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:

- CyOps threat analyst assistance and insights

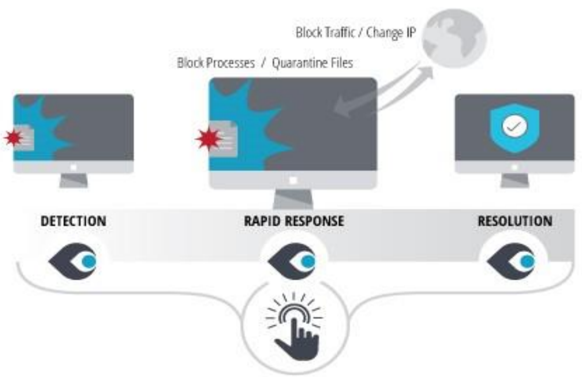
CyOps: 24/7 Expert Analyst Assistance & Monitoring

In addition to independent response capabilities such as one-click manual and auto-remediation, the Cynet 360 platform offers 24/7 expert assistance, in the form of CyOps.

A frontline threat insight and intelligence team, CyOps is composed of elite cyber analysts and investigators who are online and available, all day, every day. The CyOps team can serve as your organizational SOC, or as an elastic extension to an organization's existing SOC, providing an extra set of eyes at a fraction of the cost of a fully staffed Security Operations Center.

Cynet's CyOps provides expert assistance – continual monitoring, prioritizing, and response, when threat activity occurs.

One Click Response from Across the Network



Cynet Incident Response

When an attack is detected, immediate response is of the essence. For an organization already using the Cynet 360 platform, Incident Response is a built-in capability.

For the organization new to Cynet, the platform can be deployed across thousands of endpoints and begin scanning, analyze and provide results, in under 2-hours. Investigations and forensics provide a complete picture of the attack over time. Cynet's main dashboard provides information regarding threat activity, including who was targeted and the root cause.

The Cynet 360 platform gives investigators the actionable intelligence needed to respond, and to take action for the future.

Files
Endpoints
User Behavior
Network Communication

Correlating Threat Indicators

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.

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.