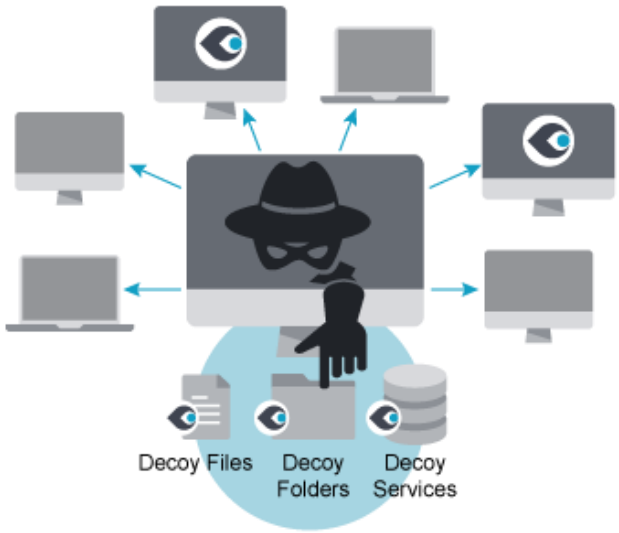
Cynet 360 Use Case: Deception

CYBERSECURITY CDM LEADER 2016

"Deception provides highly deterministic alerts that can easily integrate into other detection methods." - Gartner, November 2016

The Cynet 360 Advanced Threat Detection and Response platform continuously monitors behavioral and interaction indicators in its adversary-centric approach to detection. One of the unique methods is the **use of intelligent deception**, using decoy interaction to pinpoint threat activity.



Deception via Decoy Files and Folders

After an attacker compromises an endpoint, they will attempt to perform reconnaissance or collect sensitive data. Cynet creates decoy files and folders on endpoints throughout the organization that seem valuable to the attacker. These Decoy Files may include custom documents such as Word, Excel and PDFs. They will lead the attackers to pre-deployed traps setting off alerts and tracking mechanisms, even if the Decoy File is exfiltrated and opened outside the organization's network.

Deception via Decoy Servers, Services and Shares

Cynet's deception engine also deploys Decoy Servers, Services and Shares that only the attacker will see. This provides a diversion as the attacker attempts to move laterally throughout the organizational network. If they see and access the Cynet Decoy Servers, Services and Shares, open services such as SSH, RDP and SMB will generate alerts once accessed.

Decoys can be deployed for a specific group of servers or workstations, or for the entire network, to lead attackers to a safe and isolated environment where the threat can be investigated.

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

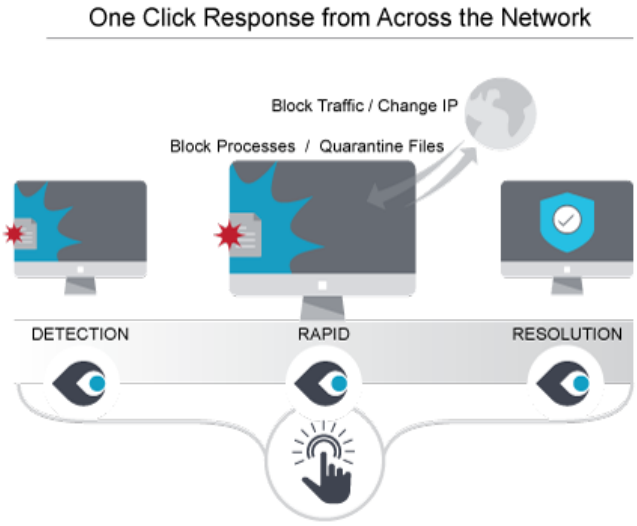
Decoys can be added very rapidly, in a few minutes. By adding Decoying functionality, Cynet provides an additional powerful capability for leveraging against the human weakness of the attacker, creating highly accurate detection alerts and causing threats to be diverted and isolated for advanced inspection and remediation.

Automatic or One-Click Response

Response to detected threats can be accomplished manually with a single click if it fits into your security workflow, or automatically if instant remediation is needed.

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

Searching and reviewing historic and current incident data on endpoints, investigating and validating alerts, and searching for other instances of threats across the network can be accomplish from the main dashboard. 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.



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