CYNET 360: ADVANCED THREAT DETECTION & RESPONSE

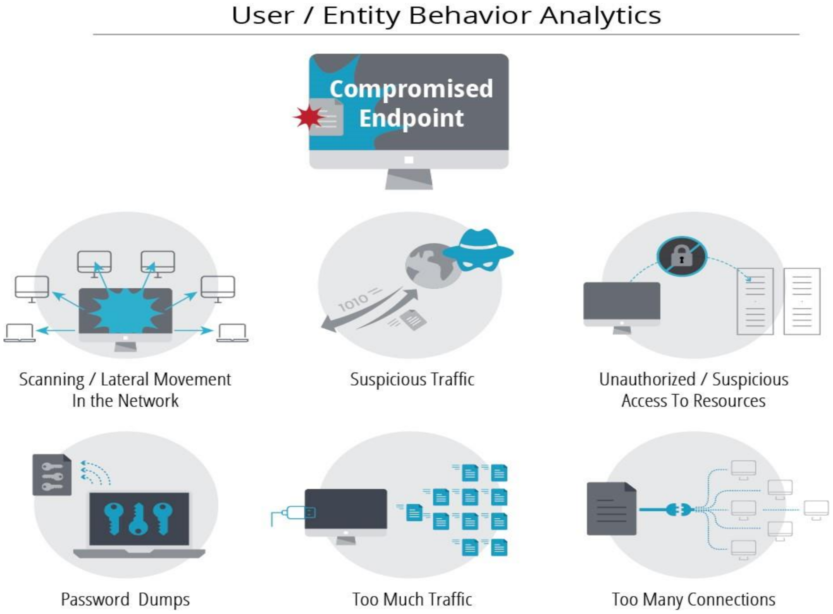
Cynet 360 Use Case:
User & Entity Behavior Analytics (UEBA)

"UEBA successfully detects malicious and abusive activity that otherwise goes unnoticed, and effectively consolidates and prioritizes security alerts sent from other systems." — Gartner

Departments tasked with protecting an organization's assets require visibility into the behavior and activity of users and devices across the enterprise, in order to detect and respond to threats, while weeding out the noise. The Cynet 360 platform for advanced threat detection and response monitors and analyzes behavioral and interaction indicators across endpoints, users, network traffic and files, unifying insights and issuing risk rankings to identify malicious activity, before damage is done.

UEBA: Part of a Comprehensive Security Platform

User & Entity Behavior Analytics (UEBA) joins Endpoint Detection & Response (EDR), Network Analytics, Forensics, Threat Intelligence, Deception and more – as part of the comprehensive Cynet 360 advanced threat detection and response platform. Together, they accurately detect inside threats, prioritize alerts across systems and initiate rapid response.


User / Entity Behavior Analytics
Compromised Endpoint
Scanning / Lateral Movement In the Network
1010
Suspicious Traffic
Unauthorized / Suspicious Access To Resources
Password Dumps
Too Much Traffic
Too Many Connections

Identify the Bad Players

Cynet's UEBA feature rapidly hones in on suspicious activity to accurately identify malicious users. Capabilities include:

- Quick detection of suspicious activity (lateral movement, c&c activity, accessing bad domains, etc.)
- Identification of compromised devices and machines
- Enablement of UBA verification for user identity
- Protecting networks and servers by reducing threat dwell-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:

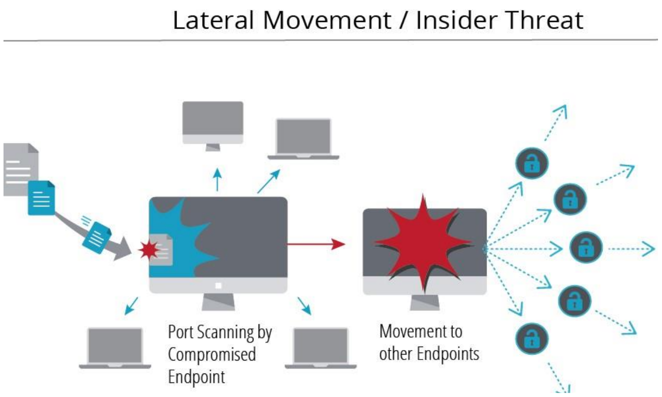
- Improve productivity of security team

24x7 Monitoring:

- Available CyOps threat analyst assistance and insights

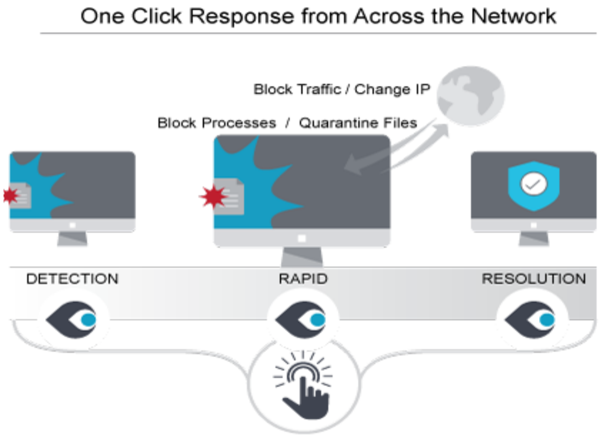
Hone in on Anomalous Behavior

The Cynet 360 platform utilizes machine learning and heuristic analysis to monitor and understand the activities of users and entities within an organization's systems. Cynet then compares the activity in real-time to historical activity, establishing a baseline for what is normal, and accurately honing in on malicious behaviors.


Lateral Movement / Insider Threat
Port Scanning by Compromised Endpoint
Movement to other Endpoints

Full Picture, Automated Response

Security IT teams get actionable intelligence telling them exactly what happened during a breach, where an attacker went, what they accessed and laying out every step of the attack process. This allows them to create rules for automated response, so that the next time the same type of threat occurs, the Cynet platform isolates and remediates suspicious items, before assets are


One Click Response from Across the Network
Block Traffic / Change IP
Block Processes / Quarantine Files
DETECTION
RAPID
RESOLUTION

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.