

SOLUTION BRIEF

CYNET 360 AUTONOMOUS BREACH PROTECTION

Abstract blue and white geometric patterns, including circles, arcs, and lines, overlaid on a dark blue background.

INTRO

SECURITY STACKS ARE COSTLY AND COMPLEX TO OPERATE, RESULTING IN FLAWED PROTECTION

There are a multitude of advanced technologies to confront both advanced and legacy threats. However, their overall consolidation into a cohesive protection environment is still an unsolved challenge.

The common integrated security architectures are subject to the following weaknesses:

- **Complex stack:** there is no security product that covers the entire attack surface. Piecing together disparate products that were not built to work together results both in overlaps and blind spots.
- **Manual workflows:** post-compromise breach protection technologies require manual operation that, by definition, cannot scale to the volume of generated alerts. Additionally, the required skills to efficiently operate these technologies are in high shortage, practically placing security out of reach for most to all organizations.

DISPARATE POINT PRODUCTS

Each product covers a mere subset of threats without communicating with its peers.



HARD DEPLOYMENT

40% avg. security products implementation rate.



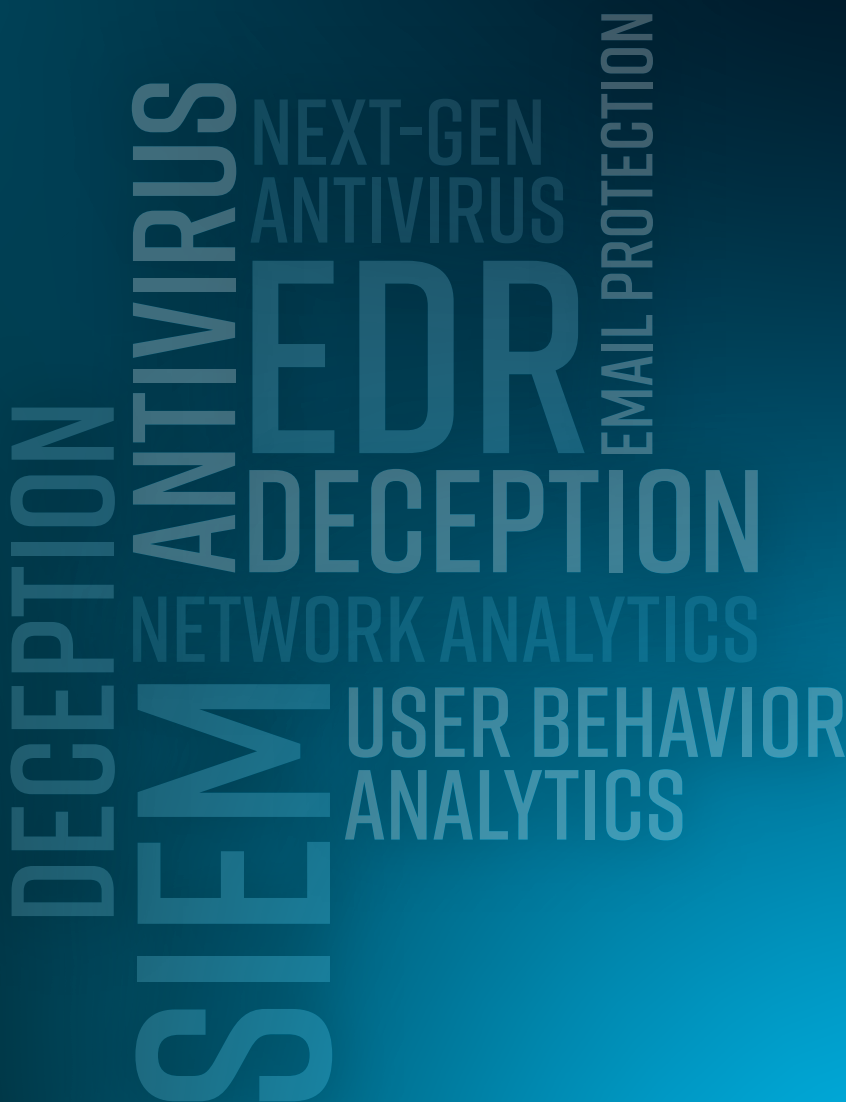
MANUAL INTEGRATION

Forming a holistic threat visibility requires significant skill and time resources.



PARTIAL THREAT COVERAGE

Critical attack vectors are left unattended.

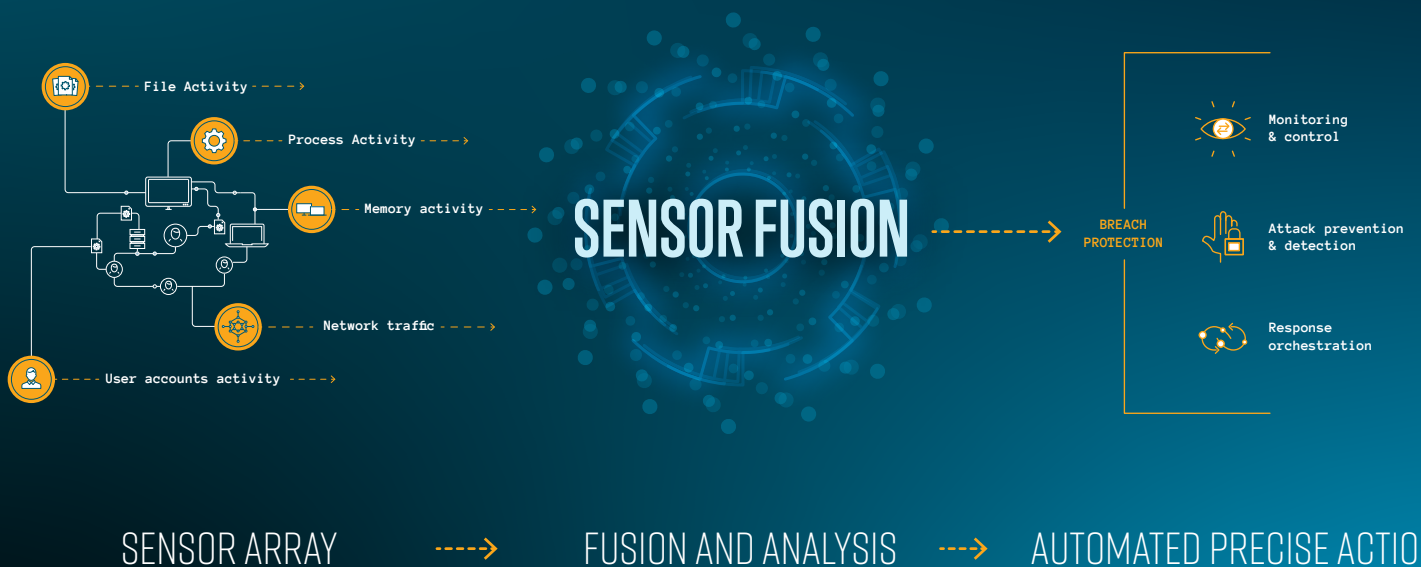


CYNET 360: AUTONOMOUS BREACH PROTECTION

Cynet 360 uses **Sensor Fusion** technology to deliver the world's first **autonomous breach protection platform**, overcoming the **limits** of today's siloed and manually-operated solutions. This includes complete automation of **monitoring & control**, **attack prevention & detection**, and **response orchestration** across the entire environment.

Cynet Sensor Fusion™ is a technology that continuously **collects and analyzes data across the entire environment**, including memory-based execution, network traffic behavior, user account activity and file access. This data provides visibility into the entire environment, enabling proactive discovery, monitoring and control of any exposed attack surface. **Cynet Sensor Fusion** combines all these input sources to understand the complete context of each individual event, yielding unparalleled threat prevention and detection accuracy. This enables the safe automation of response workflows for all for all detected threats with zero manual intervention.

Cynet 360 utilizes a proprietary, self-deployment technology installing across thousands of hosts within minutes and providing all the fundamental capabilities of NGAV, EDR, UBA, Network Analytics and Deception solutions. This is done via an integrated and unified platform, backed by CyOps, its team of threat analysts and security researchers that operates a 24/7 SOC service.



MONITORING & CONTROL

Continuous monitoring of all entities and activities in the environment enables users to discover exposed attack surfaces and address them (vulnerable systems and apps, unchanged user passwords, etc.), and by and by that, eliminate the risk of up to 60% of common attack vectors.

Cynet 360 uses Sensor Fusion technology to automate the collection and correlation of executed file/processes, user account activities, file access and network traffic, introducing unmatched speed and ease to all monitoring and control workflows.

Cynet 360 enables its users to automate the following tasks:

VULNERABILITY ASSESSMENT

Routine discovery and patching of missing security updates, significantly reduces risk exposure to all commoditized exploits.

Name	Date In	Status
2019-07 security monthly quality rollup for windows server 2012 ...	2019-07-09 17:11	Not Installed
2019-07 servicing stack update for windows server 2012 r2 for x6...	2019-07-09 17:01	Not Installed
2019-07 security and quality rollup for .net framework 3.5, 4.5.2, ...	2019-07-09 17:01	Not Installed

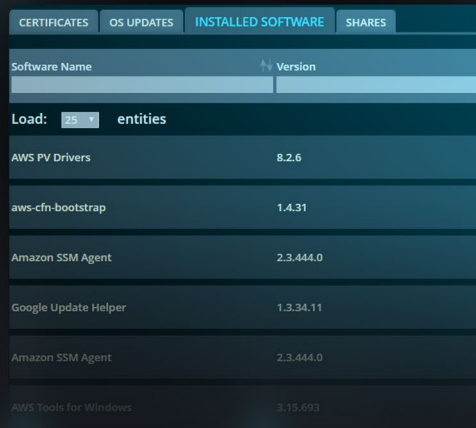
FILE INTEGRITY MONITORING

Ideal for a closed and deterministic environment. Any change in the 'known good' file status is brought immediately to the operator's attention by triggering an alert.

Action	File Name	Host
Execute	...tiworker.exe	DC1
Execute	...dllhost.exe	DC1
Execute	...trustedinstaller.exe	DC1
Execute	...wmiprvse.exe	DC1
Access	...conhost.exe	DC1
Access	...conhost.exe	DC1

INVENTORY MANAGEMENT

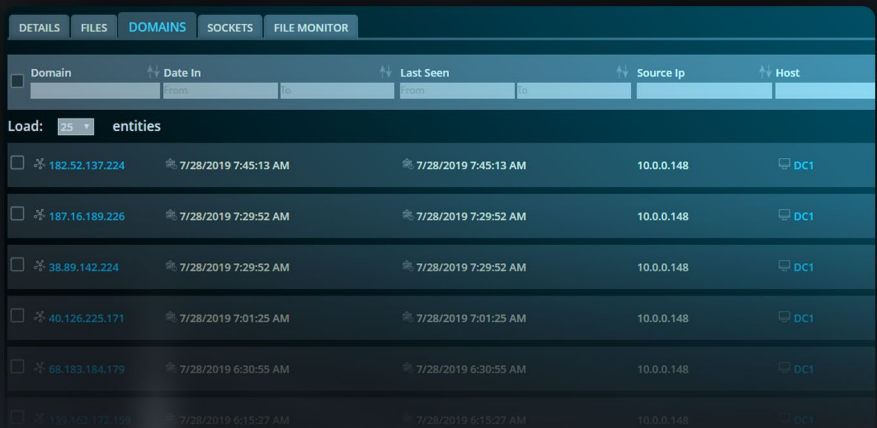
Granular visibility into and reporting of all existing entities – hosts, installed software etc. – is paramount for various security and IT management needs.



Software Name	Version
AWS PV Drivers	8.2.6
aws-cfn-bootstrap	1.4.31
Amazon SSM Agent	2.3.444.0
Google Update Helper	1.3.34.11
Amazon SSM Agent	2.3.444.0
AWS Tools for Windows	3.15.693

LOG COLLECTION & RETENTION

Retaining logs for an unlimited period of time enables organizations to comply with various regulative requirements.



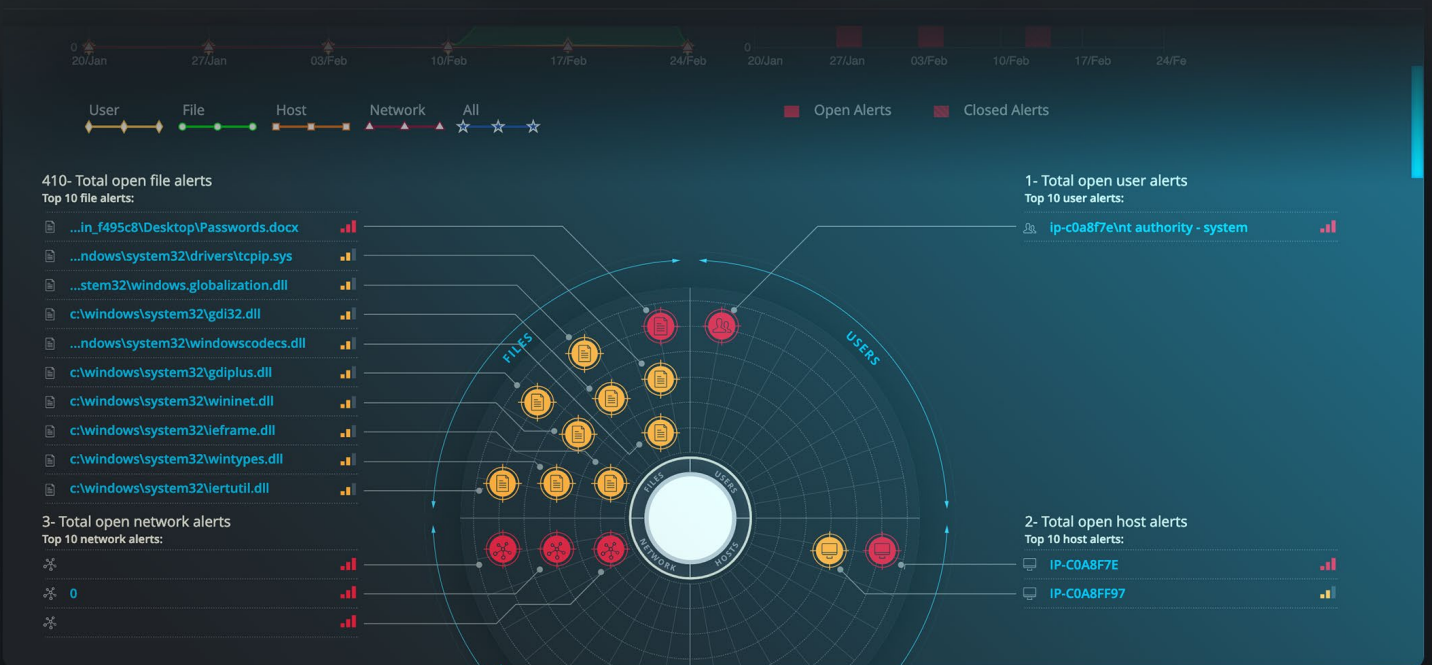
Domain	Date In	Last Seen	Source Ip	Host
182.52.137.224	7/28/2019 7:45:13 AM	7/28/2019 7:45:13 AM	10.0.0.148	DC1
187.16.189.226	7/28/2019 7:29:52 AM	7/28/2019 7:29:52 AM	10.0.0.148	DC1
38.89.142.224	7/28/2019 7:29:52 AM	7/28/2019 7:29:52 AM	10.0.0.148	DC1
40.126.225.171	7/28/2019 7:01:25 AM	7/28/2019 7:01:25 AM	10.0.0.148	DC1
66.183.184.179	7/28/2019 6:30:55 AM	7/28/2019 6:30:55 AM	10.0.0.148	DC1
194.182.110.196	7/28/2019 6:15:27 AM	7/28/2019 6:15:27 AM	10.0.0.148	DC1

PREVENTION & DETECTION

Cynet 360 utilizes Cynet Sensor Fusion to continuously collect, fuse and analyze endpoint, network and user activities, resulting in prevention and detection capabilities that match those of multiple security technologies combined

360° ALERT VIEW

Immediate view into the threat activity status across the entire environment: files, network, users and hosts.



Cynet 360 uses Cynet Sensor Fusion to deliver the following prevention and detection capabilities:



NGAV

- Intelligence-based malware protection
- AI static analysis malware protection
- Similarity-based malware protection
- Behavioral-based exploit protection
- Behavioral-based fileless, Macro and script protection

Host Alert	INFECTED FILE winword.exe	HOST IP-C0A8F7E	ALERT ID 262	Auto-Remediation: Auto-Remediation Applied
Exploitation Attempt via Word Document		USER cynetlab\zion	FIRST SEEN 31/01/2019 09:14	Last Auto-Remediation Action File Remediation -> Kill Process
OPEN CRITICAL			LAST SEEN 03/02/2019 20:45	

ALERT EXAMPLE 1: EXPLOIT PROTECTION

This alert shows an initial compromise attempt by luring the user to open a crafted Word document containing an exploit attack vector that Cynet proactively prevents.



EDR

Process behavioral analysis (malicious Powershell and other scripting tools).

User Alert	INFECTED FILE powershell.exe	HOST IP-C0A8F7E	ALERT ID 302	Auto-Remediation: Auto-Remediation Applied
Privilege Escalation via Powershell		USER ...t authority - system	FIRST SEEN 02/02/2019 18:19	Last Auto-Remediation Action Host Remediation -> Isolate
OPEN CRITICAL			LAST SEEN 03/02/2019 20:47	

ALERT EXAMPLE 2: PRIVILEGE ESCALATION

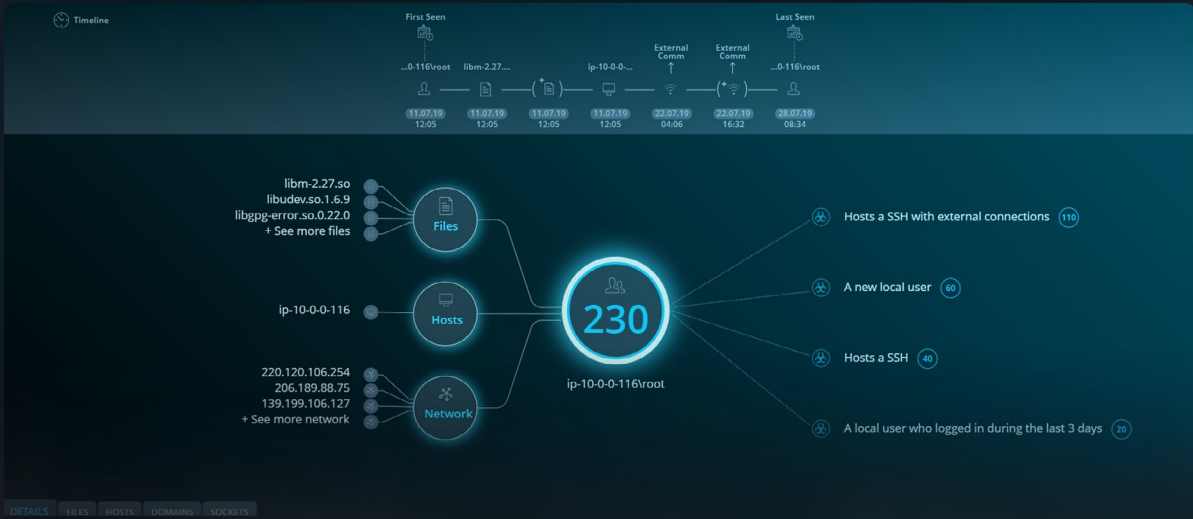
This alert detects a post-compromise privilege escalation from a local to a system user, a common action to establish the attacker's initial foothold.



USER BEHAVIOR ANALYTICS

USER ANOMALY DETECTION

Real-time monitoring of all the interactions users initiate: hosts that they log into, number of host, location, frequency, internal and external network communication, data files opened, executed processes and many more.



USER ACTIVITY RULES & VERIFICATION

Leverage internal knowledge of users' roles, group, geolocation and working hours to define access patterns to SaaS and on-prem resources that are likely to indicate user account compromise.

Name	Description	Interval Time	Is Disabled	Actions	Severity
SAP	user opens SAP for the first time	60 minutes	True	• SMS	High
Swift	user opens Swift for the first time	60 minutes	True	• SMS	High
Visual Studio	user opens Visual Studio for the first time	60 minutes	True	• SMS	High
Eclipse	user opens Eclipse for the first time	60 minutes	True	• SMS	High
Dropbox	user opens Dropbox	60 minutes	True	• SMS	High
Torrent	user opens Torrent	60 minutes	True	• SMS	High
Log to machine first time	user logs to a machine for the first time	30 minutes	True	• SMS	High



NETWORK ANALYTICS

- Network-based credential theft (ARP spoofing, DNS responder)
- Network based lateral movement
- Malicious outbound communication (C2C, phishing)
- Network-based reconnaissance (scanning attacks)
- Network-based data exfiltration (tunneling via various protocols)

ALERT EXAMPLE 3: DATA EXFILTRATION

This alert detects an advanced stage in the attack's lifecycle in which the attacker has gained access to its target data and attempts to exfiltrate it by disguising the compromised data as legitimate DNS traffic.



DECEPTION

Planting various types of decoys to lure attackers into revealing their presence.

- **Decoy types:** data files, credentials, configuration, network connection.
- **Beaconing:** once the attacker opens exfiltrated decoy data files, they send Cynet full information on both exfiltration details as well as their current location at the attacker's IP.

ALERT EXAMPLE 4: DECEPTION

This alert detects an attacker that was lured out to reveal its presence by planted decoy files. Deception is a highly efficient way to disclose the presence of advanced attackers that are skilled enough to evade other detection mechanisms.

RESPONSE ORCHESTRATION

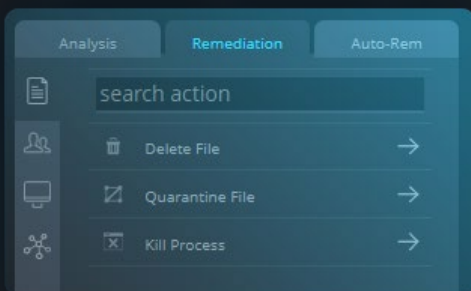
Advanced cyberattacks leave their mark across all parts of the targeted environment: endpoints, files, processes, user accounts and network traffic.

PRESET REMEDIATION ACTIONS

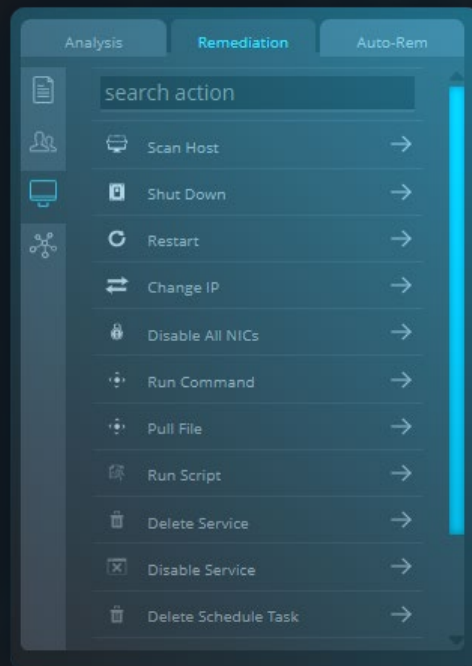
Cynet provides the widest available set of remediation tools for infected hosts, malicious files, compromised user accounts and attacker-controlled traffic.



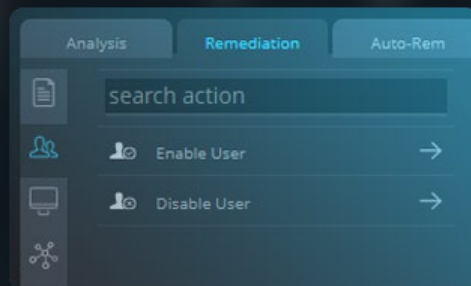
FILE



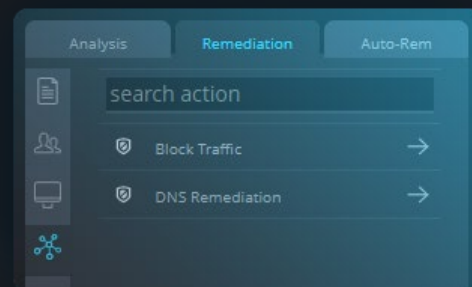
HOST



USER



NETWORK





CUSTOM REMEDIATION

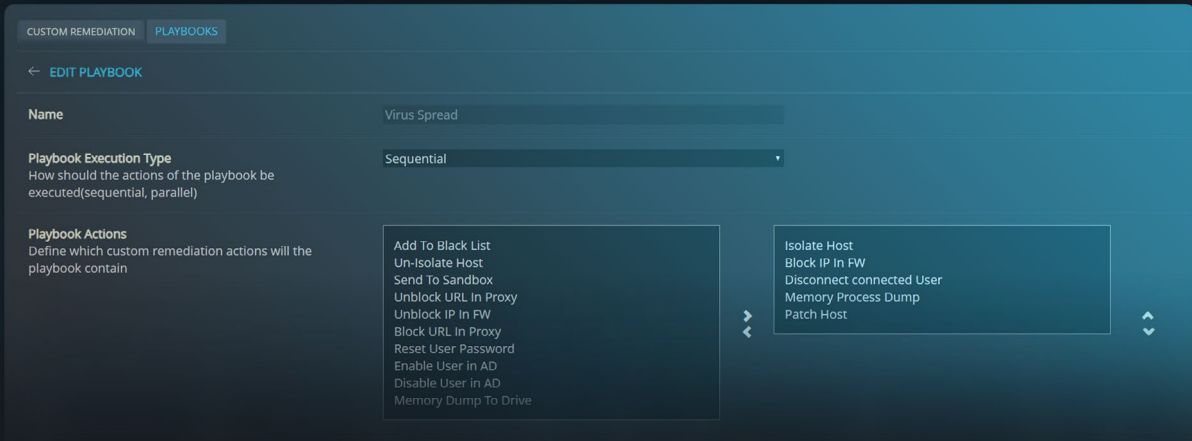
Cynet 360 enables its users to create custom remediations by either chaining together preset remediation actions, or a user-created script to communicate with core environment components such as Firewalls, Active Directory, etc.

CUSTOM REMEDIATION		PLAYBOOKS
CUSTOM REMEDIATION ACTIONS		
Name	Created	Last Modified
Patch Host	6/13/2019	6/13/2019
Add To Black List	6/13/2019	6/13/2019
Un-Isolate Host	6/13/2019	6/13/2019
Isolate Host	6/13/2019	6/13/2019
Send To Sandbox	6/13/2019	6/13/2019
Unblock URL In Proxy	6/13/2019	6/13/2019



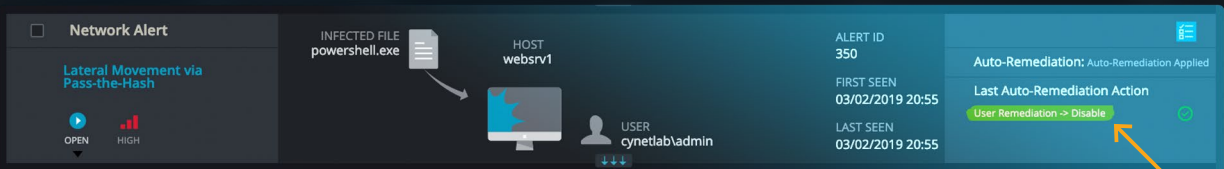
PLAYBOOKS

Cynet 360 supports the use of preset and custom-created remediation playbooks that automate response for detected threats by chaining together several discreet remediation actions (for example, isolate the endpoint + disable user account in Active Directory, as an automated response user account compromise detection). These playbooks both scale the security team alert-handling capacity by automating repetitive tasks and radically increase the share of attacks that are autonomously addressed and resolved by Cynet 360 without need for human intervention.



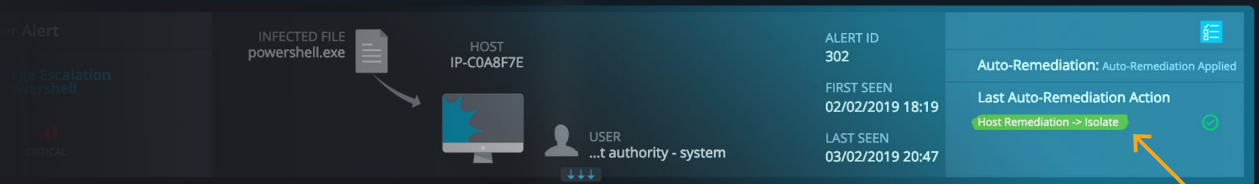
PLAYBOOK EXAMPLE 1: LATERAL MOVEMENT

Lateral movement involves an attacker expanding its foothold from by logging into a new host with a stolen user identity. The auto-remediation for this scenario is disabling the stolen identity to block the attacker's malicious logon.



PLAYBOOK EXAMPLE 2: PRIVILEGE ESCALATION

Privilege escalation involves an attacker that gains higher permissions on a compromised host. The auto-remediation in this case is to isolate the host, disabling both its external communication with the attacker and its ability to spread internally.



CYOPS: 24/7 SECURITY TEAM

Cynet complements its automated threat protection technology with integrated security services at no additional cost. CyOps is a 24/7 team of threat analysts and security researchers that leverage their expertise and Cynet's vast threat intelligence feeds to provide various services to Cynet's customers, in respect to each customer's specific needs and security preferences:



Proactive threat hunting across customer environments



Investigation of suspicious files per customer escalation



Assisting customers with incident response



Creation of tailored customer threat reports



DEPLOYMENT

The Cynet server can be deployed in in any of the following modes:

- On-prem
- SaaS
- Hybrid: suiting globally dispersed environments, with on-prem server at each location sending to a cloud-based centralized server
- Agent: a light-weight file with minimal memory footprint



OS SUPPORT



WINDOWS (32/64 BIT)

- [Windows XP SP3](#)
- [Windows Vista](#)
- [Windows 7](#)
- [Windows 8 and 8.1](#)
- [Windows 10](#)
- [Windows Server 2003 SP2](#)
- [Windows Server 2008 / 2008 R2](#)
- [Windows Server 2012 / 2012 R2](#)
- [Windows Server 2016](#)
- [Windows Server 2019](#)



LINUX (32/64 BIT)

- [Red Hat 6.4+](#)
- [Fedora 21+](#)
- [Ubuntu 14.04+](#)
- [CentOS 6.7+](#)
- [SUSE 12.0+](#)
- [Debian 6.0+](#)



MAC (64 BIT)

- [OS X Mavericks](#)
- [OS X Yosemite](#)
- [OS X El Capitan](#)
- [MacOS Sierra](#)
- [MacOS High Sierra](#)
- [MacOS Mojave](#)

ABOUT CYNET

Cynet was founded by an elite group of seasoned security entrepreneurs, researchers and SOC practitioners, to build the world's first autonomous breach protection platform, Cynet 360. The Cynet platform uses Cynet Sensor Fusion to provide Monitoring and Control, Prevention and Detection, and Response Orchestration.

Cynet is the partner of choice for multiple organizations worldwide. Small to large enterprises alike trust Cynet to guide them in their journey towards full automation of all breach protection workflows.

To learn more visit www.cynet.com.