Cynet

primenet

Solution Brief

CYNET 360 AUTONOMOUS BREACH PROTECTION

XDR AND RESPONSE AUTOMATION IN ONE PLATFORM BACKED BY 24/7 MDR SERVICES

Intro

Security stacks are costly and complex for small security teams to operate and manage In an attempt to deal with the ever increasing amount of common and advanced threats, security teams use numerous technologies to prevent the next breach.

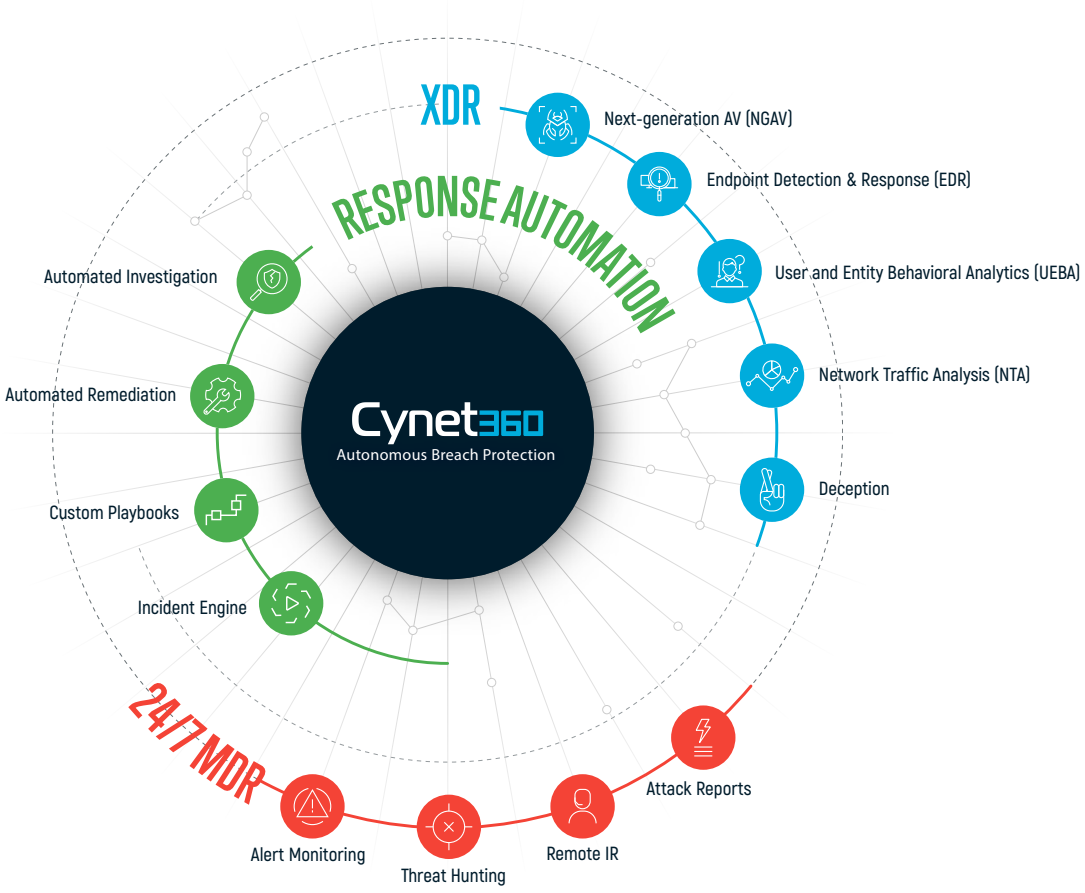
As a result, security teams face the following challenges:

- **Complex deployment:** piecing together disparate products that were not designed to work together.
- **Inefficient and ineffective security stack:** disparate technologies 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.
- **Dedicated skillsets:** the required skills to efficiently operate and maintain these technologies are in high shortage, practically placing security out of reach for most organizations.

The irony of the security stack despairs most security teams. While the point of adding technologies is to protect the organization, the more technologies stacked on means that the security teams cannot operate them efficiently to properly protect the organization.

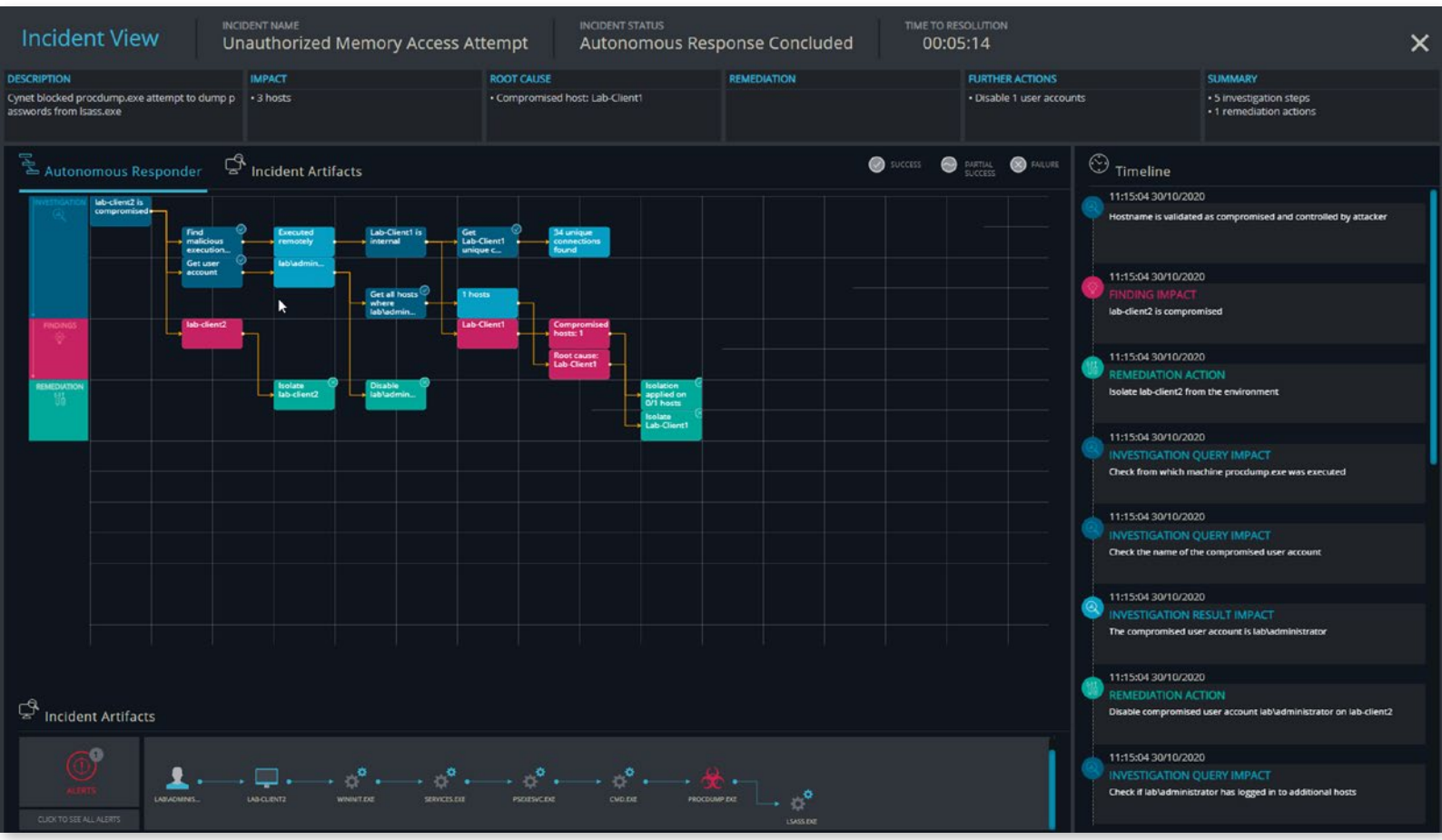
About Cynet 360 Autonomous Breach Protection Platform

Cynet natively combines three capabilities in a single unified offering: eXtended Detection and Response (XDR), Response Automation and 24/7 Managed Detection and Response (MDR) services. With Cynet 360, also the smallest security teams receive a wholesome security solution against threats within their internal environment.



The Cynet XDR component provides a single, unified platform to prevent, detect, investigate and fully remediate the broad range of attack vectors. Visibility across endpoint, network and user activities, plus the power of deception provides the broadest and deepest protection against all threats.

Cynet 360 triggers an automated investigation allowing each endpoint, user, or network alert, fully disclosing its root cause and scope and applying all the required remediation activities to fully eliminate the threat.



Cynet also provides a broad set of automated and highly customizable remediation actions to address threats according to your preferences.

Moreover, Cynet provides an expert team of cybersecurity experts to augment and guide your team 24 hours a day, 7 days a week – included with the Cynet 360 platform.

LEARN MORE

XDR - Extended Prevention and Detection

Cynet's XDR component natively combines several prevention and detection capabilities out of the box, providing teams with seamless multi-layer protection. This saves teams the time and effort of purchasing, integrating and managing multiple third party solutions.

360 Alert View

Receive an immediate view into the threat activity status across the entire environment.

NGAV

Scans files at rest and non-executable files to protect against known malware.

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

Alert Example 1: Malicious Binary Alert

Cynet's intelligence-based malware protection blocks a file with a malicious binary from executing.

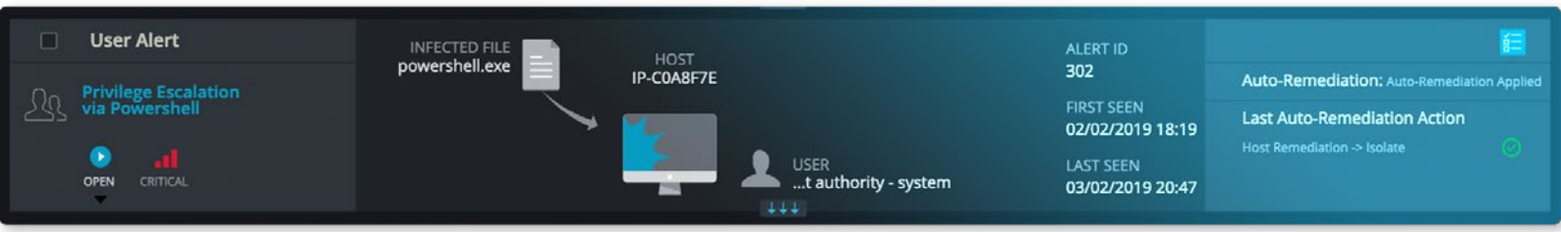
EDR

Analyzes process behavior to detect rogue processes and applications through various mechanisms, including:

- SSDEEP Scan – uses a compression algorithm that searches for similarities to known malware (aka Fuzzy fingerprints) commonly used for reusing existing tools without their detection via traditional signature-based solutions.
- Memory Patterns – analyzes a host's loaded memory for processes and searches for the following: patterns of activity, structure and behavior of data, data with suspicious strings and similarities to known malware, malware activities, processes that load suspicious or malicious DLLs to memory to gain access to sensitive operating system areas or be injected into other processes.
- Advanced Detection Technology (ADT)– heuristic tools to inspect operating systems for malicious behavior performed by file-based and fileless based malware and threats. This detects malicious activities in legitimate processes like PowerShell or cmd. ADT analyzes a command's structure, results and the connection between the command to the parent process that searches for malicious patterns like a WinWord file running a PowerShell command.
- Driver Mode (kernel) – gain visibility to kernel-level threats. This mechanism also prevents the Cynet Endpoint Protection Scanner (EPS) from being terminated. Protective mechanisms include: anti-tampering – protecting Cynet processes from being terminated or manipulated, write protection to sensitive OS areas in the hard disk, proxy to critical system resources such as Lsass.

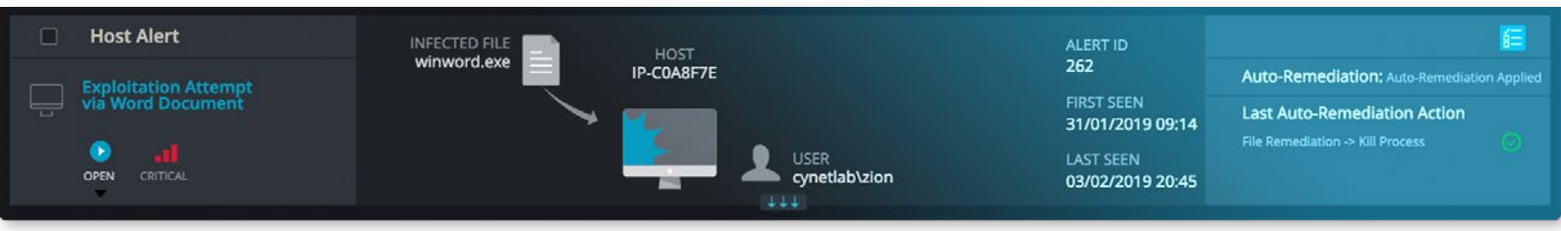
Alert Example 2: Privilege Escalation

Cynet detects and blocks PowerShell, a legitimate admin process, from attempting to perform a user privilege escalation.



Alert Example 3: Exploitation Protection

Cynet detects and blocks a crafted Word document containing an exploit.



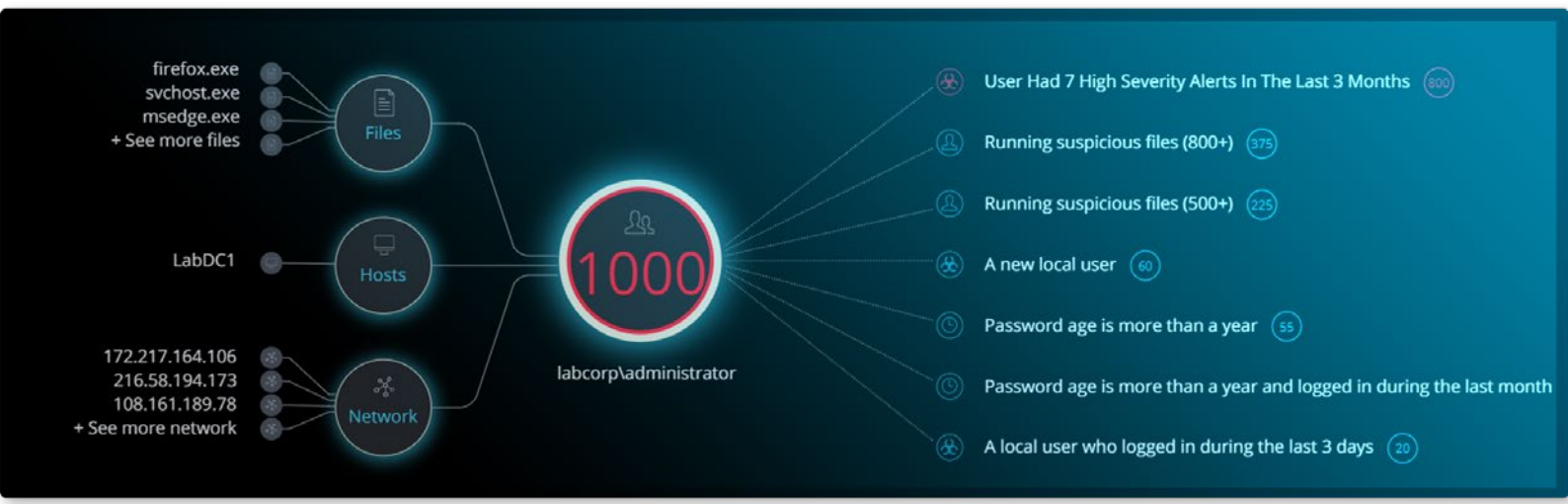
User and Entity Behavior Analytics (UEBA)

Learns the behavior of user and entities and alerting upon abnormal activity, including:

- Real-time monitoring of all the interactions users initiate
- Hosts users log into, number of hosts, location and frequency
- Internal and external network communication
- Data files users opened
- Executed processes

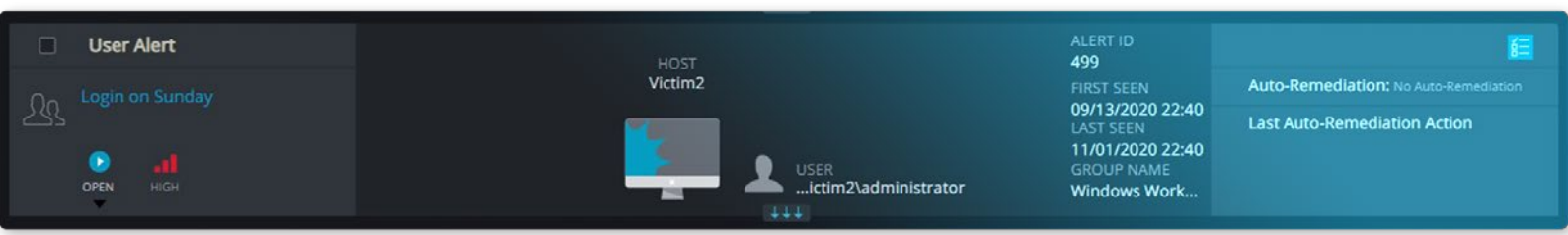
Forensics Example 4: User Behavior

Cynet's forensics displays highly suspicious user behavior by correlating various abnormal activities



Alert Example 5: Login on Sunday

Cynet's UEBA component detects abnormal weekend login activity



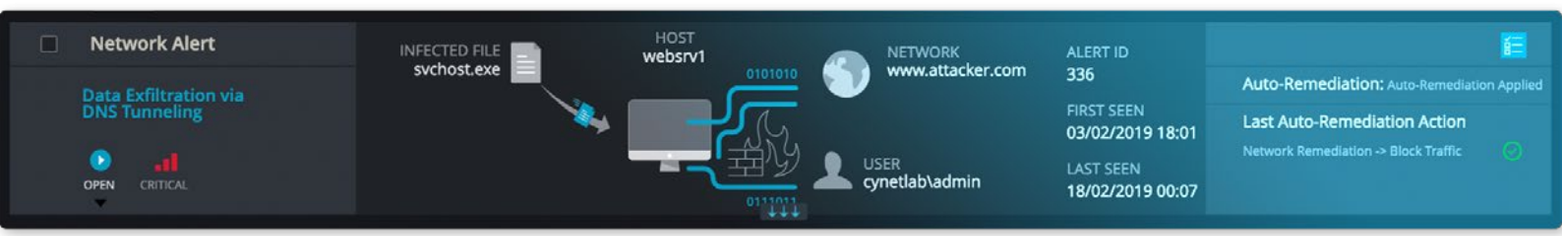
Network Traffic Analysis

Analyzes activities to detect attacks on the network, such as:

- 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)

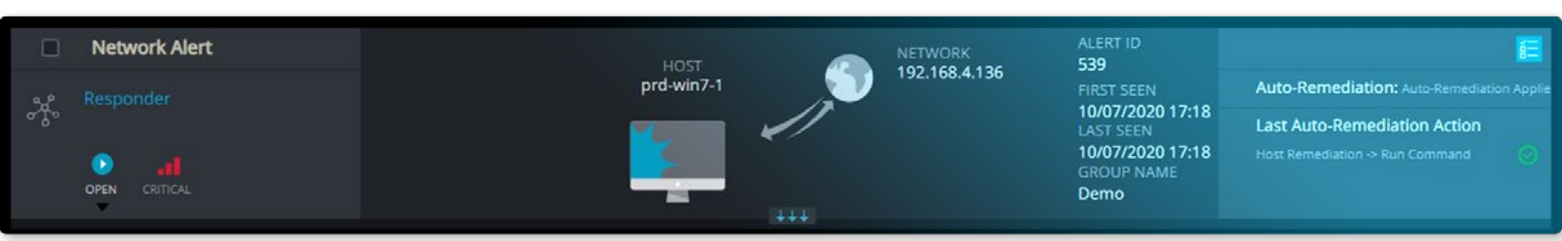
Alert Example 6: Data Exfiltration

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



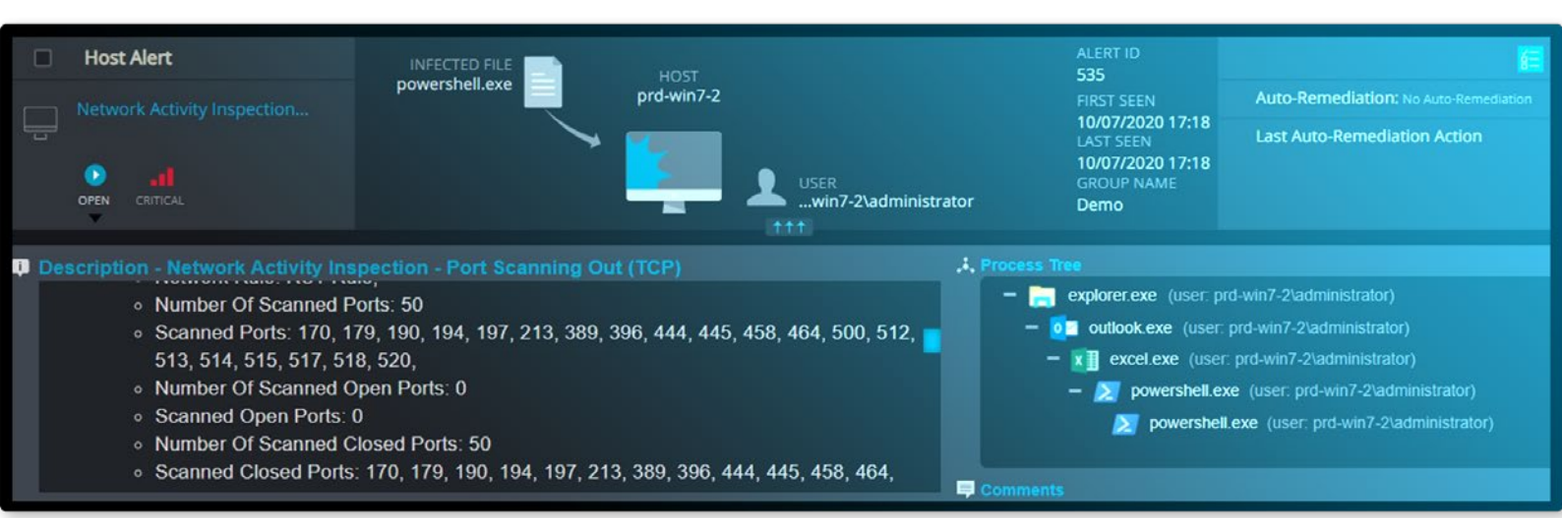
Alert Example 7: Responder

Cynet detects and blocks the Responder malware which exploits network protocols



Alert Example 8: Port Scanning

Cynet detected that a host started to perform a port scan on the network



Alert Example 9: Communicating Out of High Ports

A Linux-based machine performed suspicious root activities by communicating to high ports.

Deception

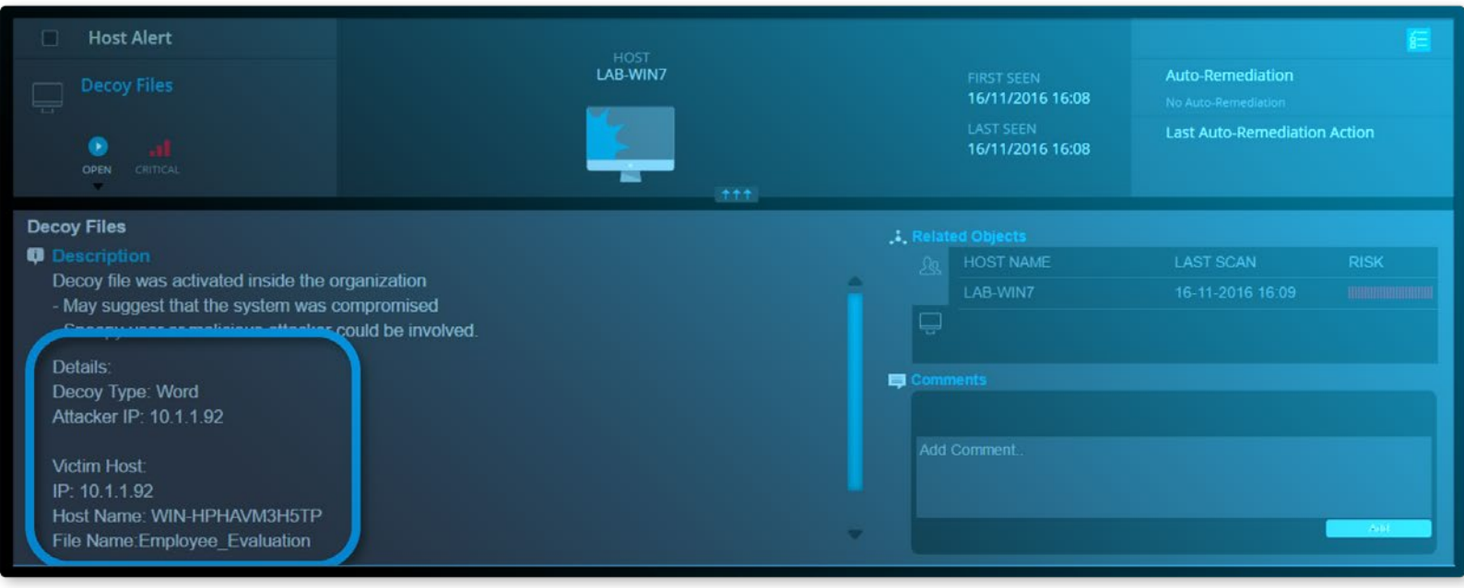
Using honeypot tactics, Cynet places decoys in the environment and monitors them to lure, detect and alert on attempted attack incidents.

Alerts are generated on detection of:

- Ransomware decoys
- Suspicious files
- User decoys
- Network decoys

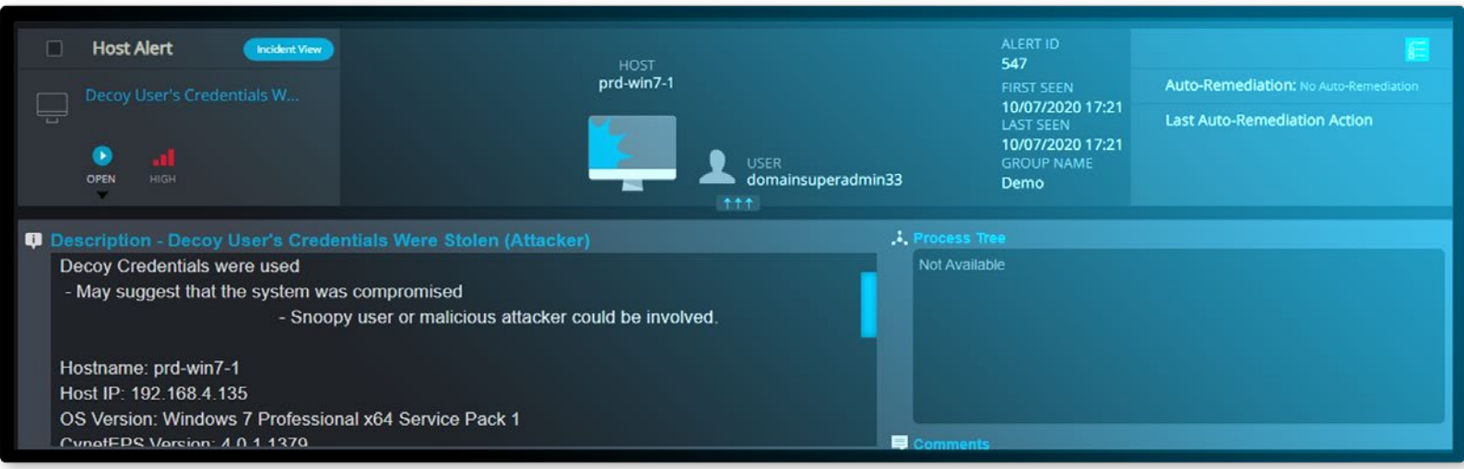
Alert Example 10: Deception (Files)

The attacker was lured into revealing its presence through a planted decoy Word file.



Alert Example 11: Deception (Users)

The attacker was lured into revealing its presence by attempting to authenticate as a decoy user.

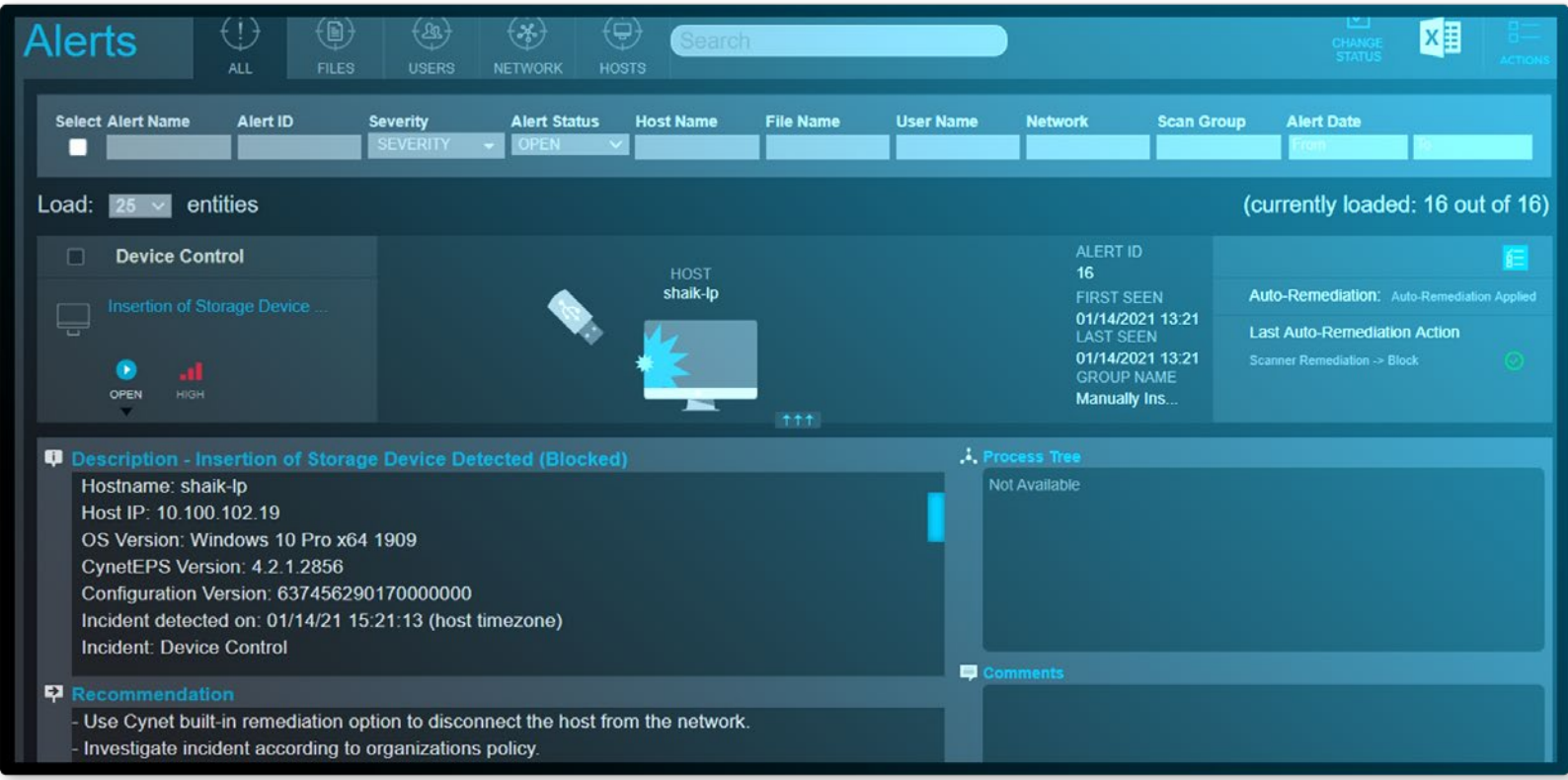


Device Control

Detection and blocking of external devices that are inserted into the endpoint (for example, a USB device or SD card)

Alert Example 12: Alert on an inserted storage device

Detection and blocking of an inserted storage device against security policy



Response Automation

Cynet fully automates the entire response workflow, removing manual efforts and ensuring important response details and actions are performed.

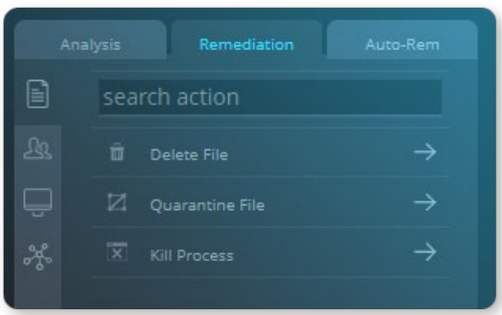
Alerts are logically grouped into incidents, reducing alert fatigue and providing context of the threat. This includes:

- **Investigation.** Automated root cause and impact analysis
- **Findings.** Actionable conclusions on the attack's origin and its affected entities
- **Remediation.** Elimination of malicious presence, activity, and infrastructure across user, network, and endpoint attacks.

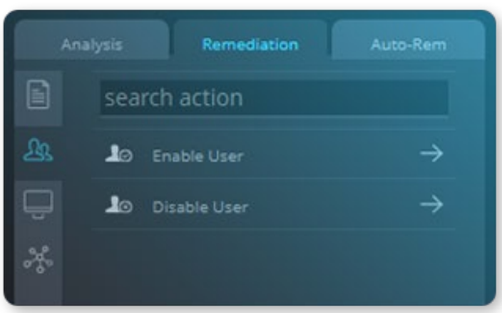
Preset Remediation Actions

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

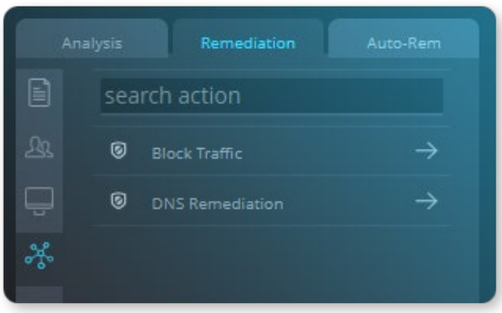
File



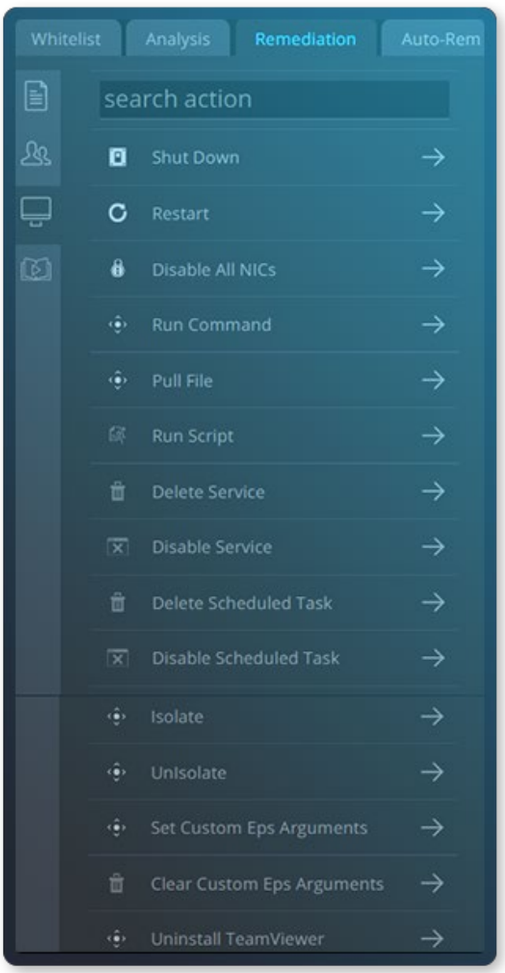
User



Network



Host

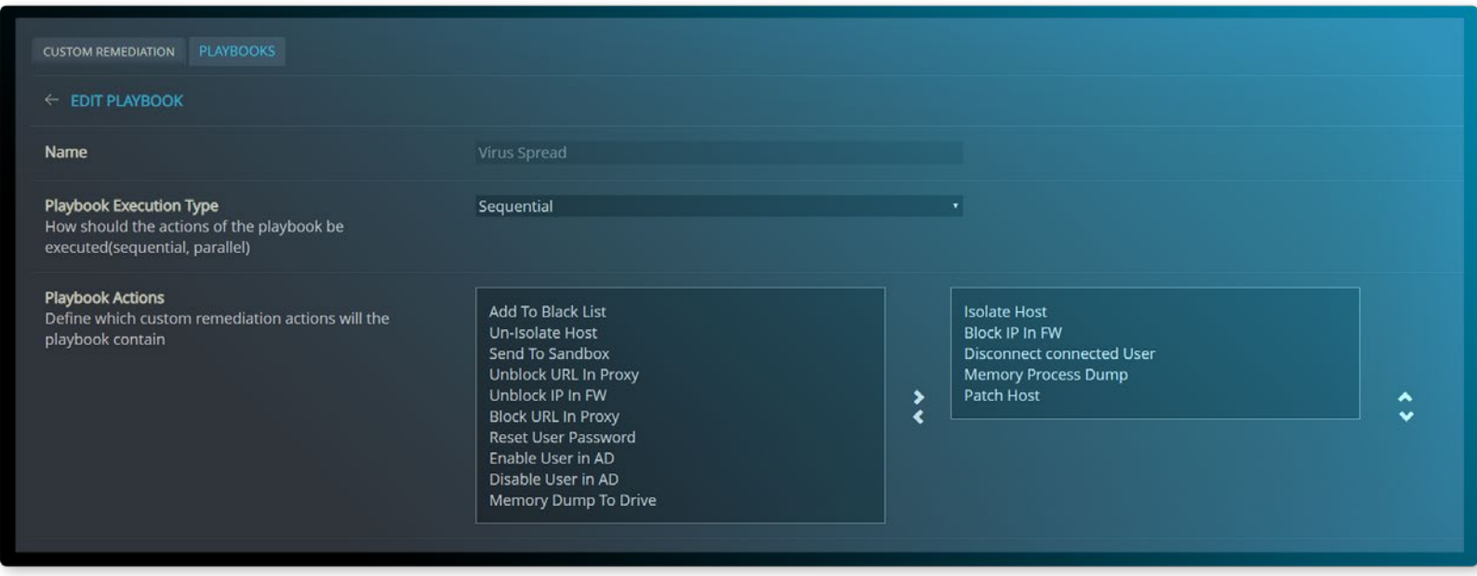


Remediation Playbooks

Playbooks chain together multiple associated remediation actions. This allows your security team to scale their alert-handling capacity by removing repetitive tasks and radically increases the share of attacks that are autonomously addressed and resolved by Cynet 360 without need for human intervention.

Cynet 360 provides out-of-the-box a wide number of remediation actions and supports the ability to create or edit your own playbook.

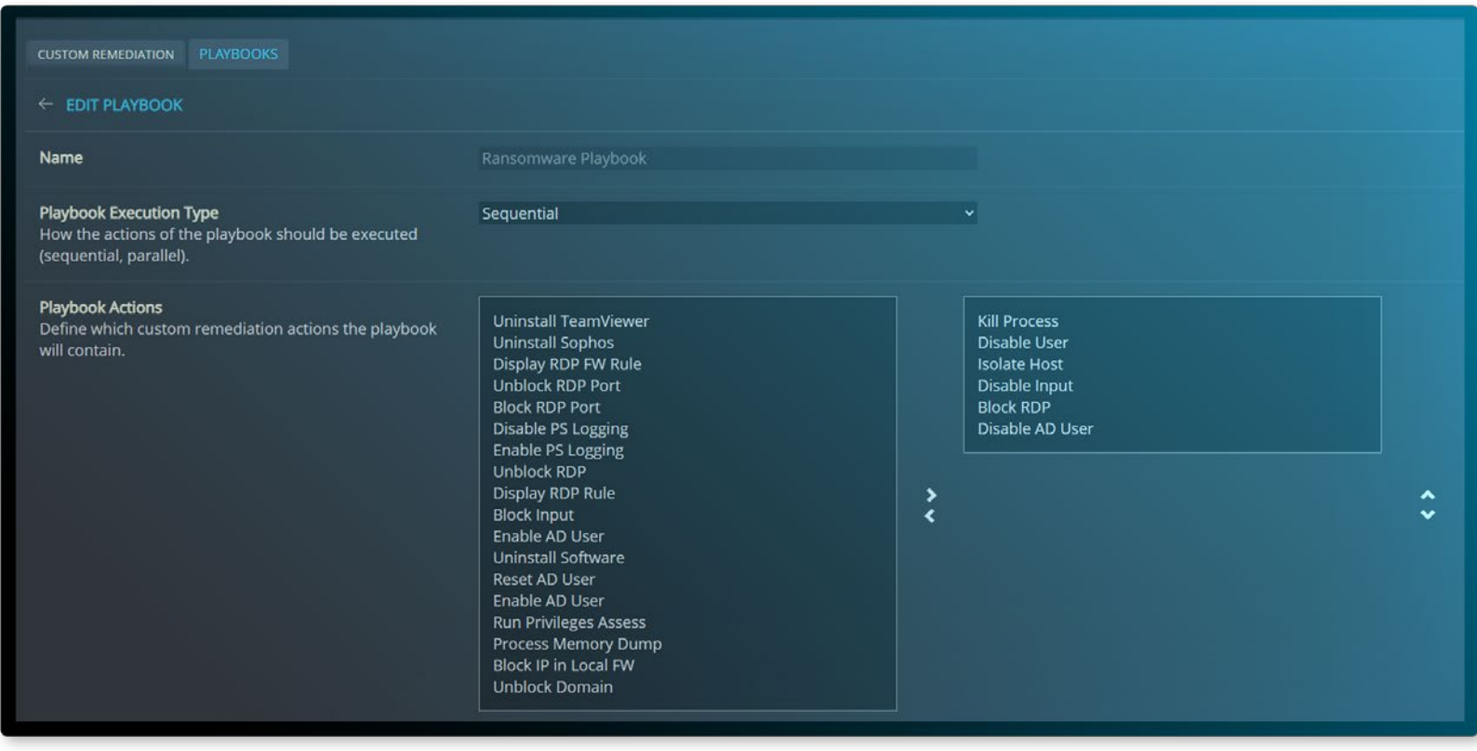
Playbook example 1: Virus Spread



In this customized playbook, the displayed remediation actions are automatically run in parallel in order to disable the malware from jumping between machines.

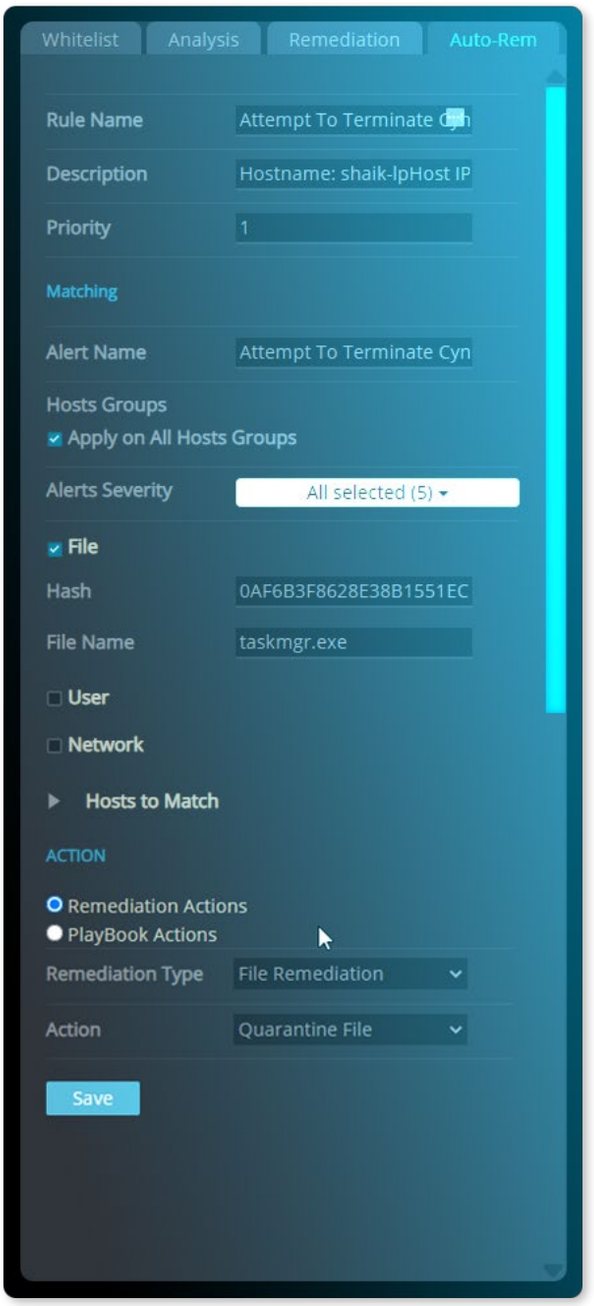
Playbook example 2: Editing a Playbook

Editing your own playbook is easy – you can add or change the flow through a simple drag and drop menu.



Automated Remediation

Cynet 360 allows you to automatically run a built-in or customized playbook on a specific alert.



Incident Engine

Unique to Cynet, the Incident Engine provides automated incident response actions laid out on a visual timeline for immediate understanding of the attack – from root cause and scope of attack to resolution.

The Incident Engine starts by asking a series of questions to determine the root cause and scope of attack. When it has findings, it can take automated actions to remediate the threat. The visual timeline shows you all the necessary remediation actions that were taken to resolve the threat.

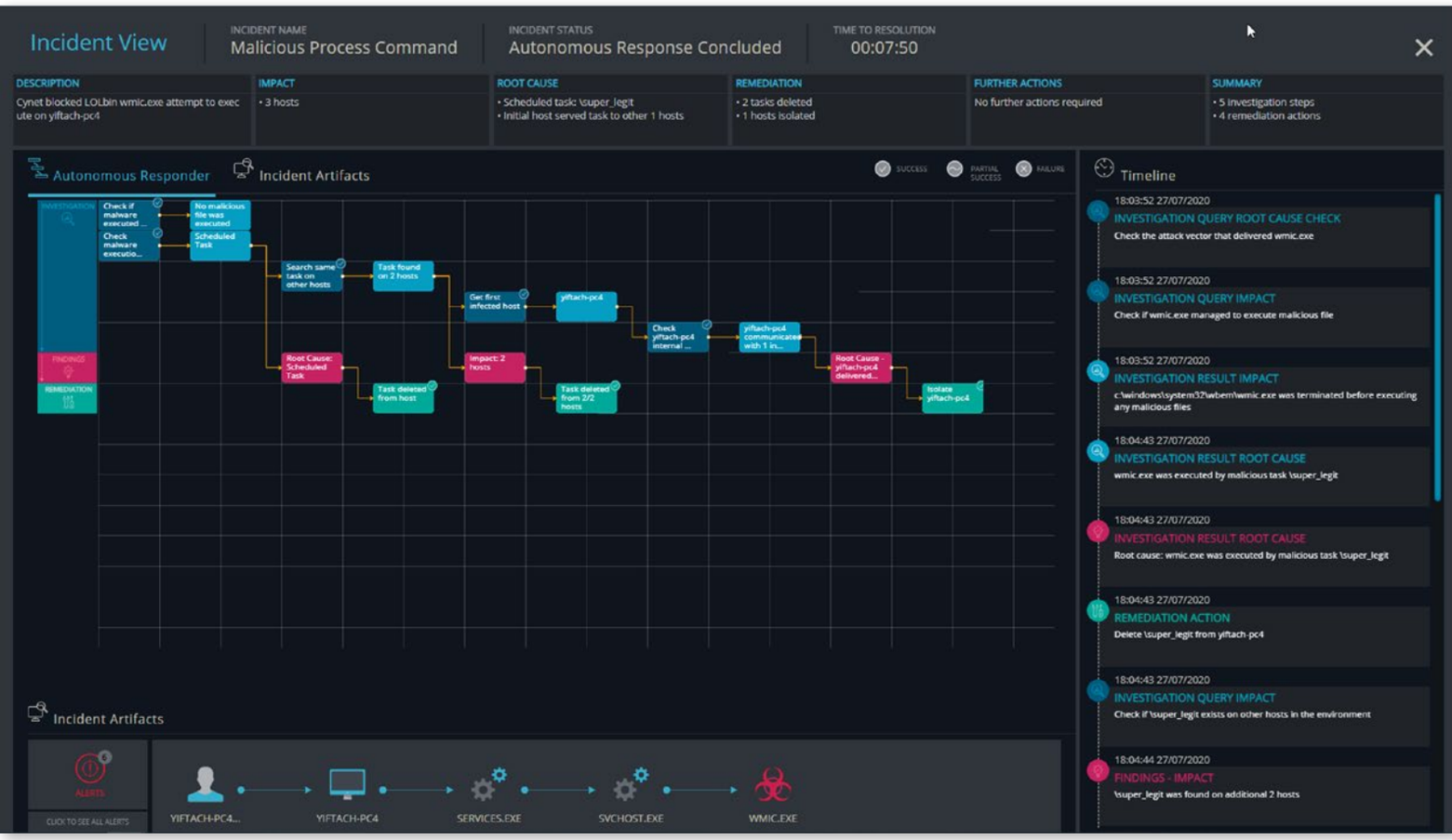
The Incident Engine saves you immense time and efforts. Complete investigation to resolution typically takes seconds to just a few minutes.

Incident Engine Example 1: Malicious Process Command

As part of its automated investigation, the Incident Engine reveals that the process was terminated early enough, preventing the execution of any malicious files. It then identifies that this malicious command was first executed by a Scheduled Task, a common utility leveraged by attackers to bypass security controls. Many attackers plant a Scheduled Task that may lay dormant for a while and then begin executing a malicious file. In this case, it's the wmic.exe file, which leads to the first finding - the root cause is the Scheduled Task.

The Incident Engine immediately takes action and removes the Scheduled Task from the host. It's important to note that if we were to rely only on the prevention level, that Scheduled Task may have continued to execute malicious files, maybe several files, hoping that one would not be detected. The Incident Engine, however, eliminated the root cause before it had the chance to happen.

As part of the investigation, the Incident Engine checks whether the malicious task made its way to other hosts and indeed finds this scheduled task on two other machines. The Incident Engine automatically deletes the scheduled task from them. Finally, the Incident Engine finds the first host to be infected - Yiftach-pc4. This machine communicated with the other two infected hosts so it is automatically isolated before any more damage can be done.



CyOps: 24/7 Managed Detection and Response (MDR) Team

Cynet complements its autonomous breach 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.

Alert Monitoring

The CyOps team continuously monitors your environment – every hour of every day throughout the year. The team manages events, alerts, customer inquiries and incidents. The team also provides alert analysis and correlation to other Cynet 360 alerted events.

The CyOps team will proactively contact you when certain alerts or events are detected along with specific actions that should be taken.

Threat Hunting

CyOps continually searches for new emerging threats in order to implement Indicators of Compromise (IoCs) and patterns into Cynet 360 mechanisms. These proactive actions enable Cynet 360 to collect, analyze and alert for events while giving the forensics feature its ability to assess an entity's risk level.

Remote Incident Response (IR)

The CyOps IR experts work in close partnership with the affected company to resolve incidents as fast as possible. Their process includes creating customized policies within Cynet 360 to scope and analyze the threat as well as providing recommendations and mitigations on the endpoint as across the IT and security environment.

Attack Reports

The CyOps teams often generates comprehensive reports in response to client questions.

Attack Reports Example 1: 13 Seconds Attack

The Cynet Threat Research Report contains an executive level summary, analysis description including involved processes and associated indicators of compromise, on the "13 Seconds Attack" where malware compromises a single host within 13 seconds.

EXECUTIVE SUMMARY

In this article, the Cynet Research team reveals a highly complex attack that runs for only 13 seconds by using several malwares and different tactics. From our analysis, the threat that we discovered within our investigation is name the **"ClipBanker" trojan**.

The attack flow contains several stages of LOLBins (Living Off the Land) abuse, masquerading, persistency, enumeration techniques, credential thieving, fileless attacks, and finally banking trojan activities.

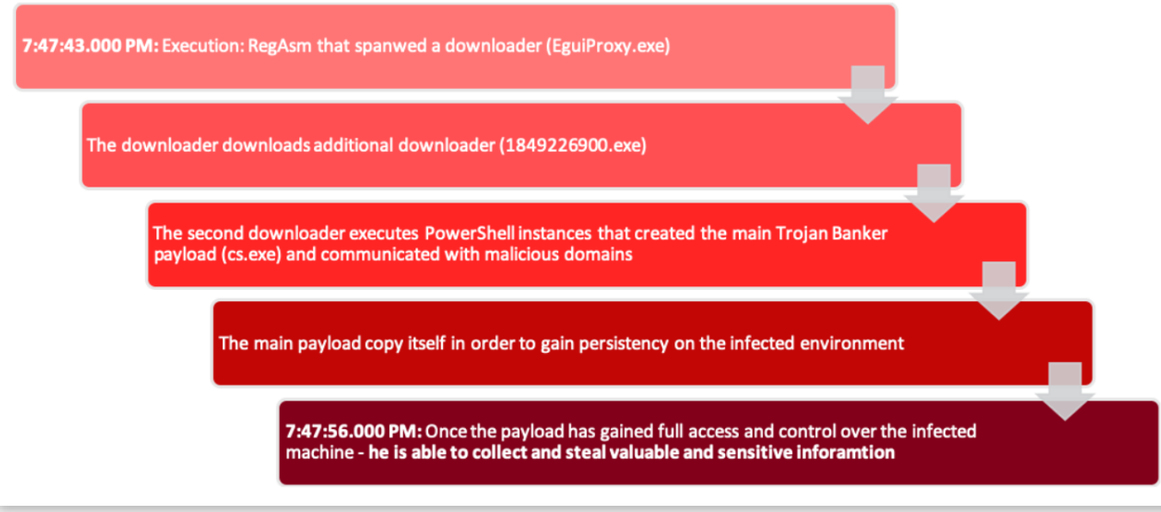
This attack is also using Fileless techniques in order to evade from security detections. Fileless attack has been a growing threat since 2017 and require highly sophisticated detection and prevention tools to detect and block. The most common Windows tools used in "Fileless" attacks are PowerShell, JS, VBA and WMI. PowerShell is a highly popular tool used for Fileless attack, because PowerShell commands can be executed natively on Windows without writing data to disk.

The ClipBanker Trojan is known as an information stealer and spy trojan, it aims to steal and record any type of sensitive information from the infected environment such as browser history, cookies, Outlook data, Skype, Telegram, or cryptocurrency wallet account addresses. The main goal of this threat is to steal confidential information.

The ClipBanker uses PowerShell commands for executing malicious activities. The thing that made the ClipBanker unique is its ability to record various banking actions of the user and manipulate them for its own benefit.

The distribution method of the ClipBanker is through phishing emails or through social media posts that lure users to download malicious content.

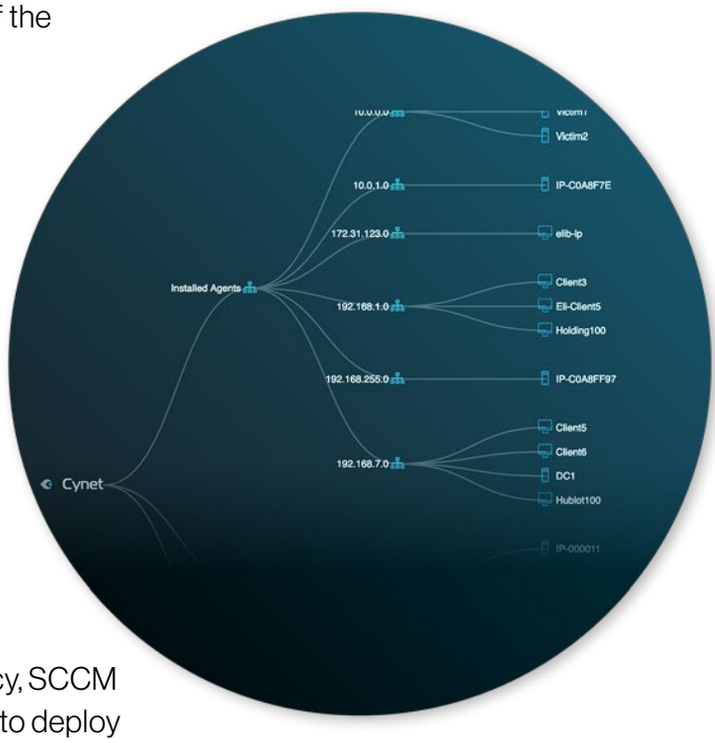
Cynet 360 is protecting your assets against this type of exploit.



Deployment

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

- **On-premises**
- **SaaS**
- **Hybrid:** suiting globally dispersed environments, with on-premises server at each location sending to a cloud-based centralized server



The Cynet agent is a lightweight file with minimal memory footprint.

Cynet supports various methods of agent deployment such as RMM, MSI, Group Policy, SCCM and Cynet's own dispatcher with the ability to deploy to up to 5000 hosts in less than an hour.

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
- MacOS Catalina

About Cynet

Cynet 360 is the world's first Autonomous Breach Protection platform that natively integrates XDR endpoint, user and network attack prevention and detection capabilities with an incident engine that fully automates investigation and remediation actions, backed by a 24/7 world - class MDR service. End to end, fully automated breach protection is now within reach of any organization, regardless of security team size and skill level. For additional information, please visit: https://www.cynet.com