Cynet

Solution Brief

How CYNET Accelerates Time to Response

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

The Need for Speed

Today's attacks only need a few hours or less to achieve their malicious objectives. Ransomware starts encrypting files just seconds after being unleashed. How quickly a security team identifies an attack, investigates the forensics, and eradicates the threat couldn't be more important. There is precious little time to spare. Delays at any point can spell disaster.

Delays amplify damage because they give attacks the opportunity to extend their reach, infect more assets, hide their tracks, or lay traps for the remediation effort. Attacks that persist can also expose a company to operational disruption, revenue losses, compliance costs, legal liability, and reputational damage – on top of massive fees to third parties to help with emergency remediation efforts. To put these forces into perspective, IBM found that breaches lasting less than 30 days cost $5.7 million on average, compared to $8.8 million for breaches that last longer.

Organizations have a powerful incentive to speed up time to response. They also have some powerful obstacles in the way. For incident response to kick into high gear at the earliest sign of attack, the security team needs a 360-degree view of the attack surface. It must correlate all the available evidence to understand threats and how to stop them. And it needs adequate resources (time, staff, experience, expertise) to remediate whatever arrives on the doorstep. Anything less than perfect vision and execution can (and often does) result in delays – with consequences ranging from costly to catastrophic.

Automation: Fighting Fire with Fire

Incident response can only move as fast as the team behind it. And whether that team has three members or three hundred, it probably can't keep up with the threats it faces.

Any process that relies on human monitoring, input, and decision making suffers from our cognitive limitations. There are thresholds for how much information our minds can ingest and act upon. And in a high-pressure situation like the outbreak of a cyberattack, clear thinking only suffers. An incident response plan can tell people exactly what to do. It can't, however, ensure the right outcome.

Incident response driven by the security team will always be too slow. Humans will hold back every stage (with the exception of the final one) and make it impossible to improve time to response in a meaningful way. What's the solution? Put parts of incident response in the hands of automation.

Cynet Response Automation

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

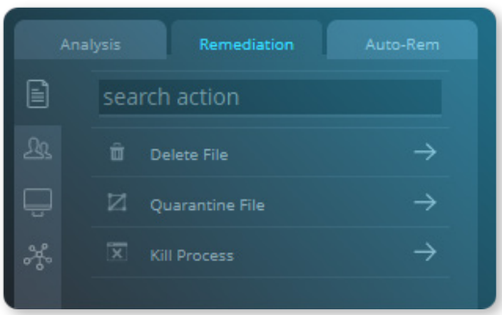
Alerts are logically grouped into incidents, reducing alert fatigue and providing context of the threat. This includes:

- **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.

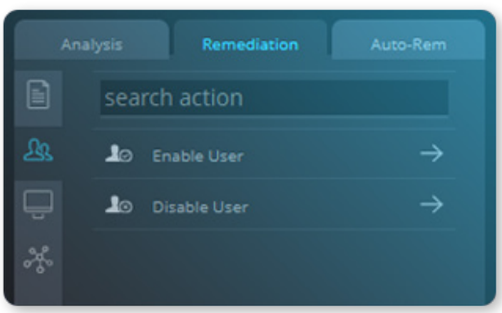
Preset Remediation Actions

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

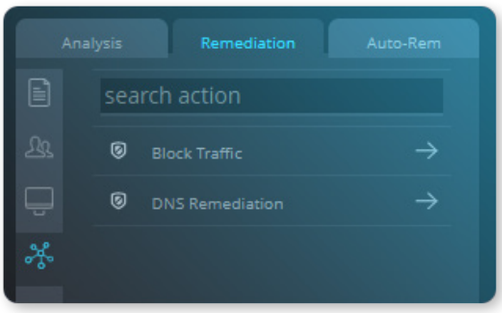
File



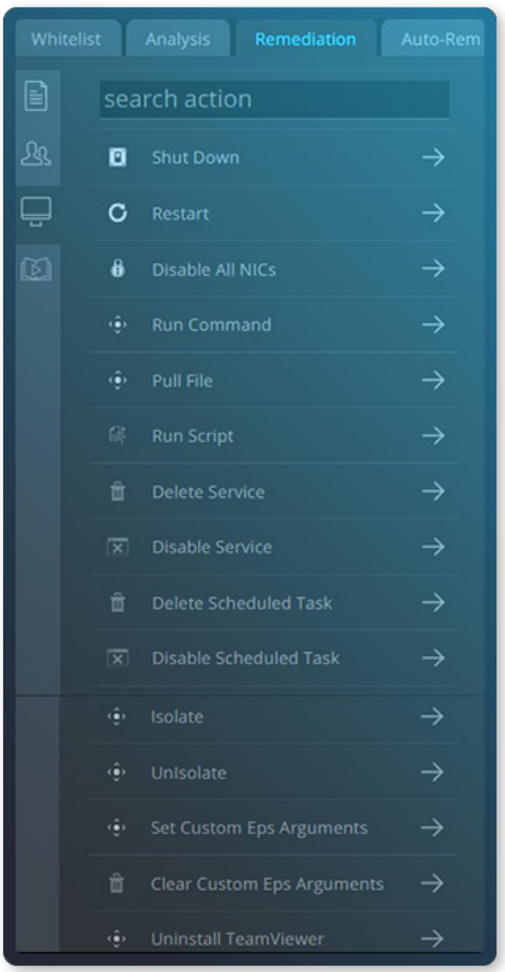
User



Network



Host

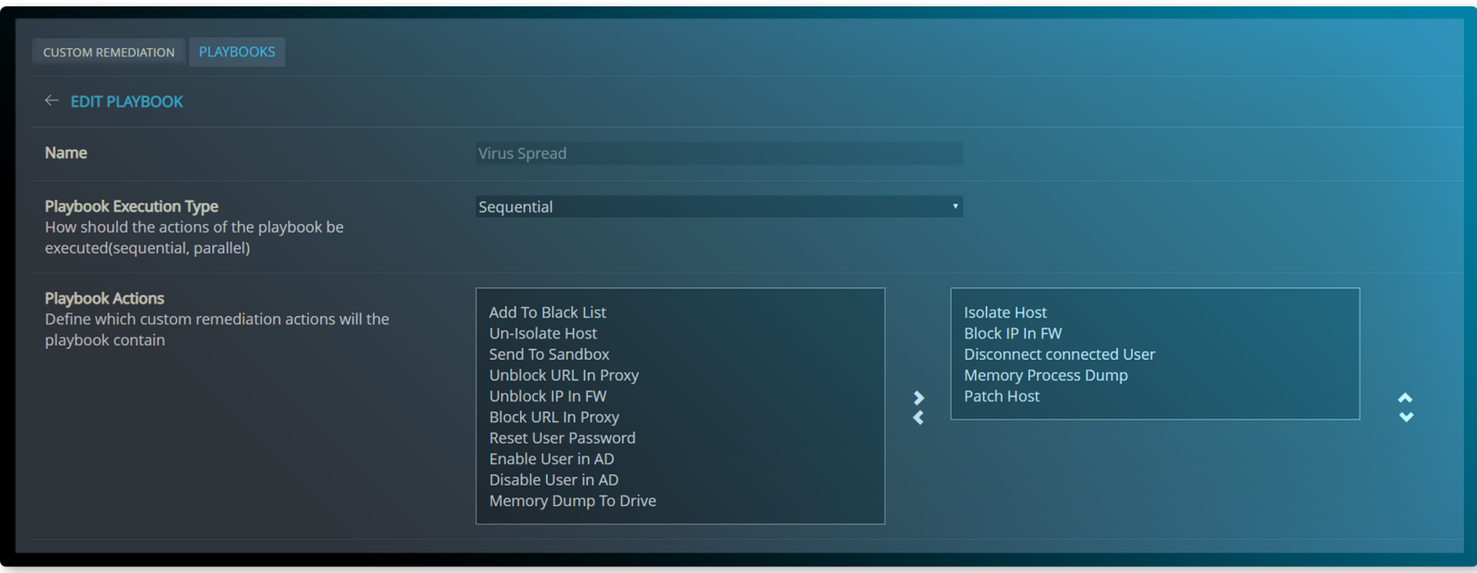


Remediation Playbooks

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.

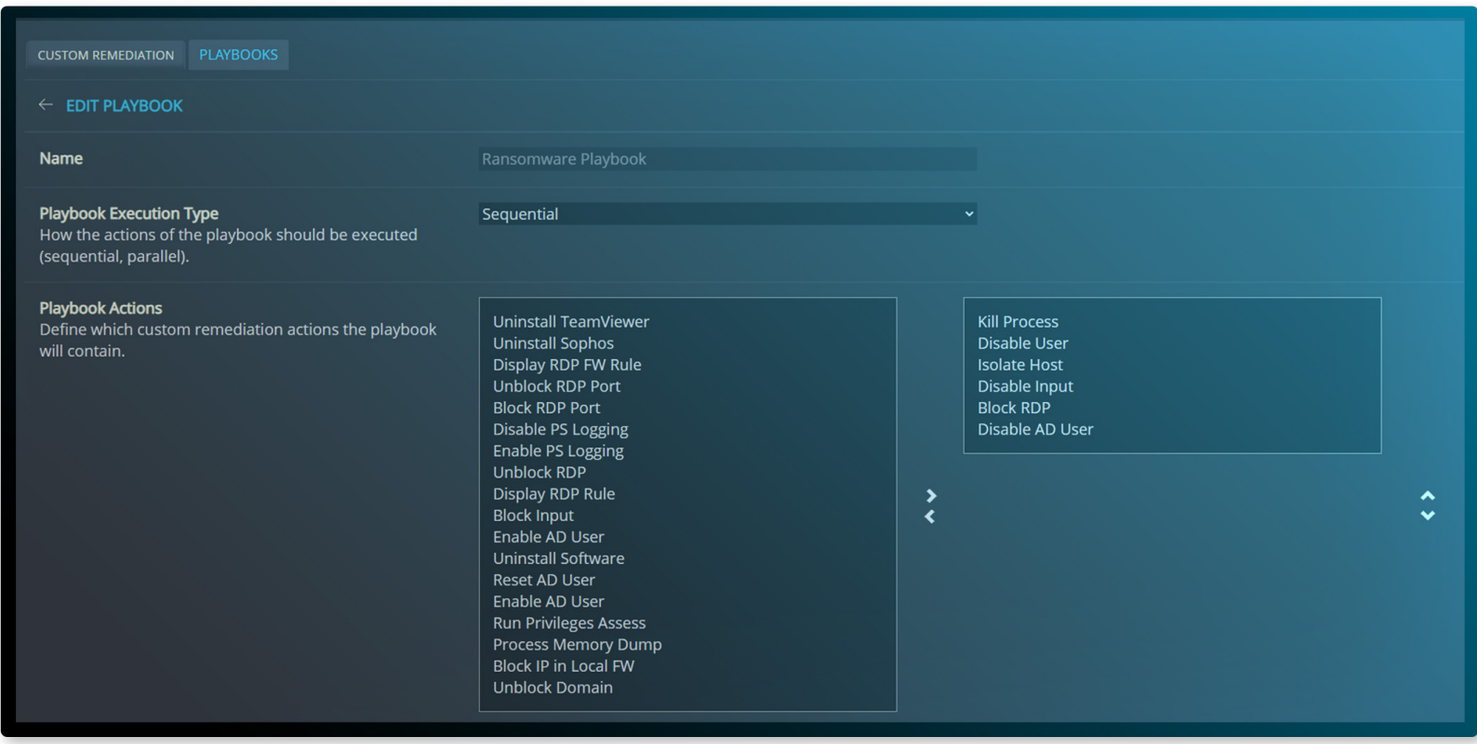
Playbook example 1: Virus Spread



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

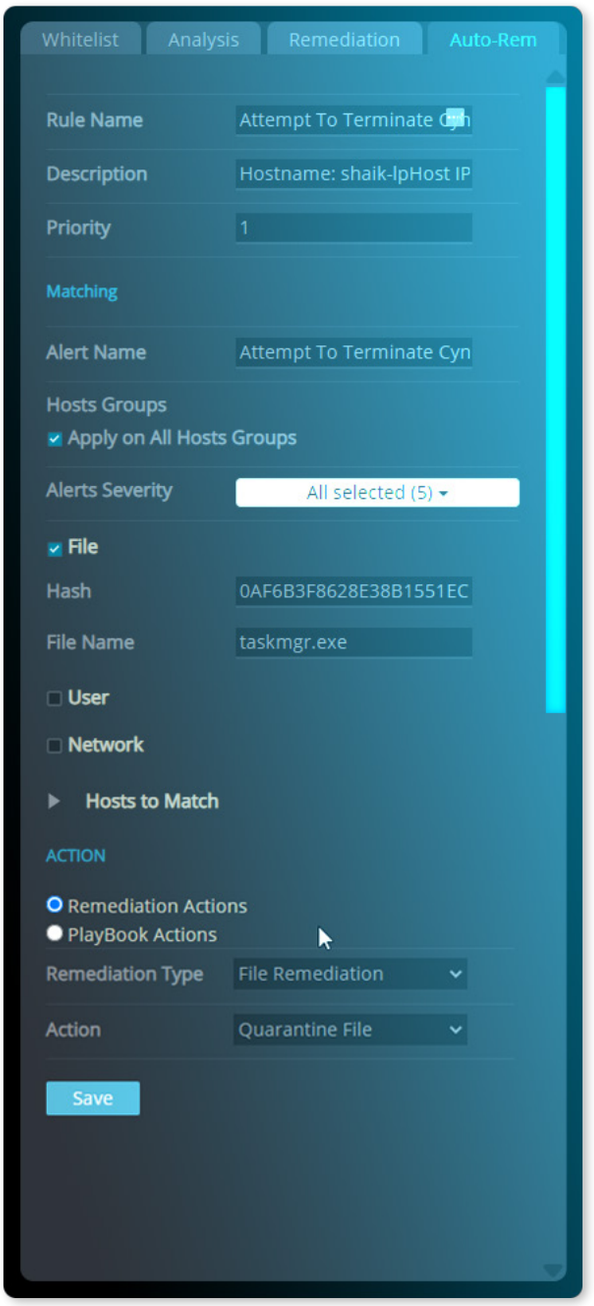
Playbook example 2: Editing a Playbook

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.

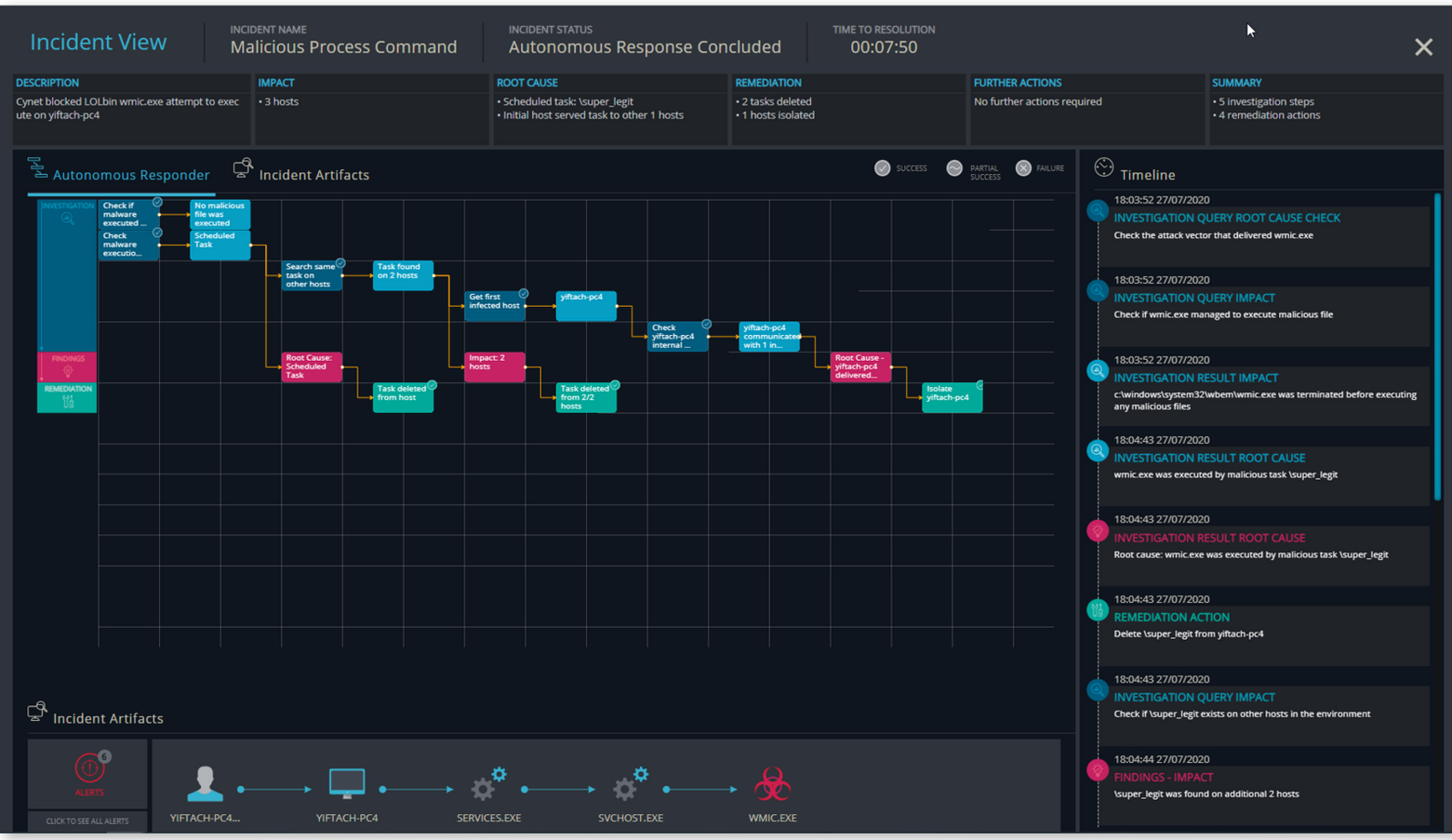
The Incident Engine saves you immense time and efforts. Complete investigation to resolution typically takes seconds to just a few minutes.

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.



Accelerating Response with CyOps: 24/7 MDR Team

Cynet complements its breach protection technology with integrated security services at no additional cost. CyOps is a 24/7 Managed Detection and Response (MDR) team of threat analysts and security researchers that leverage their expertise to provide valuable services to Cynet's customers based on each customer's specific needs and security preferences. CyOps helps Cynet clients speed time to response by ensuring that dangerous threats are quickly and properly addressed. Following are examples of how the CyOps team helps clients speed time to response.

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 high-risk alerts or events are detected along with specific actions that should be taken. This ensures threats are addressed at the earliest possible moment, before they spiral into bigger problems.

Attack Investigation

Deep-dive into validated attack bits and bytes to gain the full understanding of scope and impact, providing you with updated IoCs.

Indicators of compromize

Type	Indicator
Registry Key	• HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Ran • HKCU\software\ • HKCU\ software\classes\virtualstore\machine\software
Payload instance locations	• C:\User\AppData\Local\Temp****.exe • C:\User\AppData\Roaming********.exe
Ransom note name	• {Random}@cock.li • {random}@tuta.io
Emails related to the attacker	Ad8fdfkljsdf90435kjdfhgj90345kljsdflkj34904534kljsfklj435fdgdfklj43598dfjghjkfdhg90435kljdfgkdfg90435kljdlfgj90435jkldfgukheoishq982345yjhs efsjkjhxcv893425jhksdfjkasdf9804358 9yerhtjh3eroitxcmmn3456awqweoi93245kjxgfdg89034jkhsdfbxcvfd gmnfgi43509sdjkhz0ghgvhdsdf0435kljdlfgj90435jkldfgukheoishq982345yjhsefsjkjhxcv893425jhksdfjkasdf98043589yerhtjh3eroitxcmmn3456awqweoi93245kjxgfdg8903

Example of IOCs taken from Netwalker malware analysis

Remediation Instructions

Conclusion of investigated attacks entails concrete guidance on which endpoints, files, users and network traffic should be remediated.

Recommendations

In order to clean up an infected host, it is crucial to revert of the steps taken by the payload of the attack

- Clean the Registry of any of the manipulated values.
- Delete Malicious Childs instances from the memory
- Block Network Traffic to any domain contacted throughout the attack

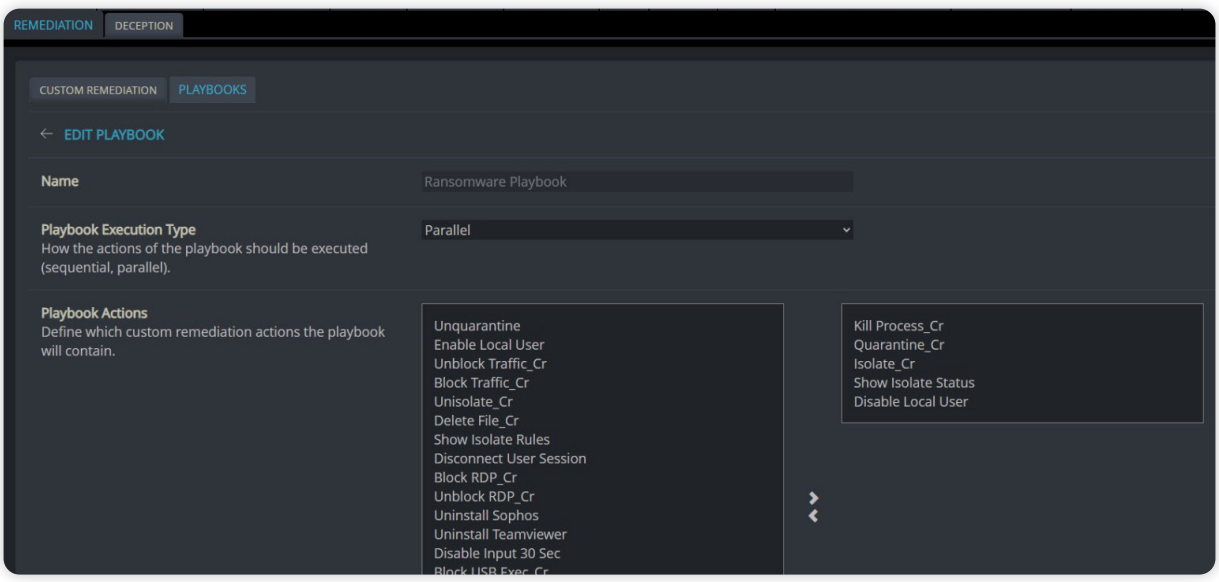
Indicators of Compromise

Type	Indicator
Registry Key	HKCU\SOFTWARE\Microsoft\windows\CurrentVersion\Run
Payload instance location	C:\User*use*\”119.exe”
Payload instance location	C:\User*use*\AppData\Local\”ThemesMaker”
PowerShell Domain	107.180.3.11
PowerShell Domain	166.62.10.28
Child Domain	186.90.29.228
Child Domain	181.135.153.203
Child Domain	74.208.68.48
Child Domain	104.131.58.132

Example of remediation instructions and IOCs from Emotet threat report

Custom Remediation Playbooks

CyOps can assist you to quickly and accurately build customized remediation playbooks that take into consideration the unique requirements and restrictions of your specific environment when remediating threats. For example, an ecommerce or health care provider may address server remediation differently than a manufacturing or office environment.



Example of Cynet platform Customized Playbook Editor GUI

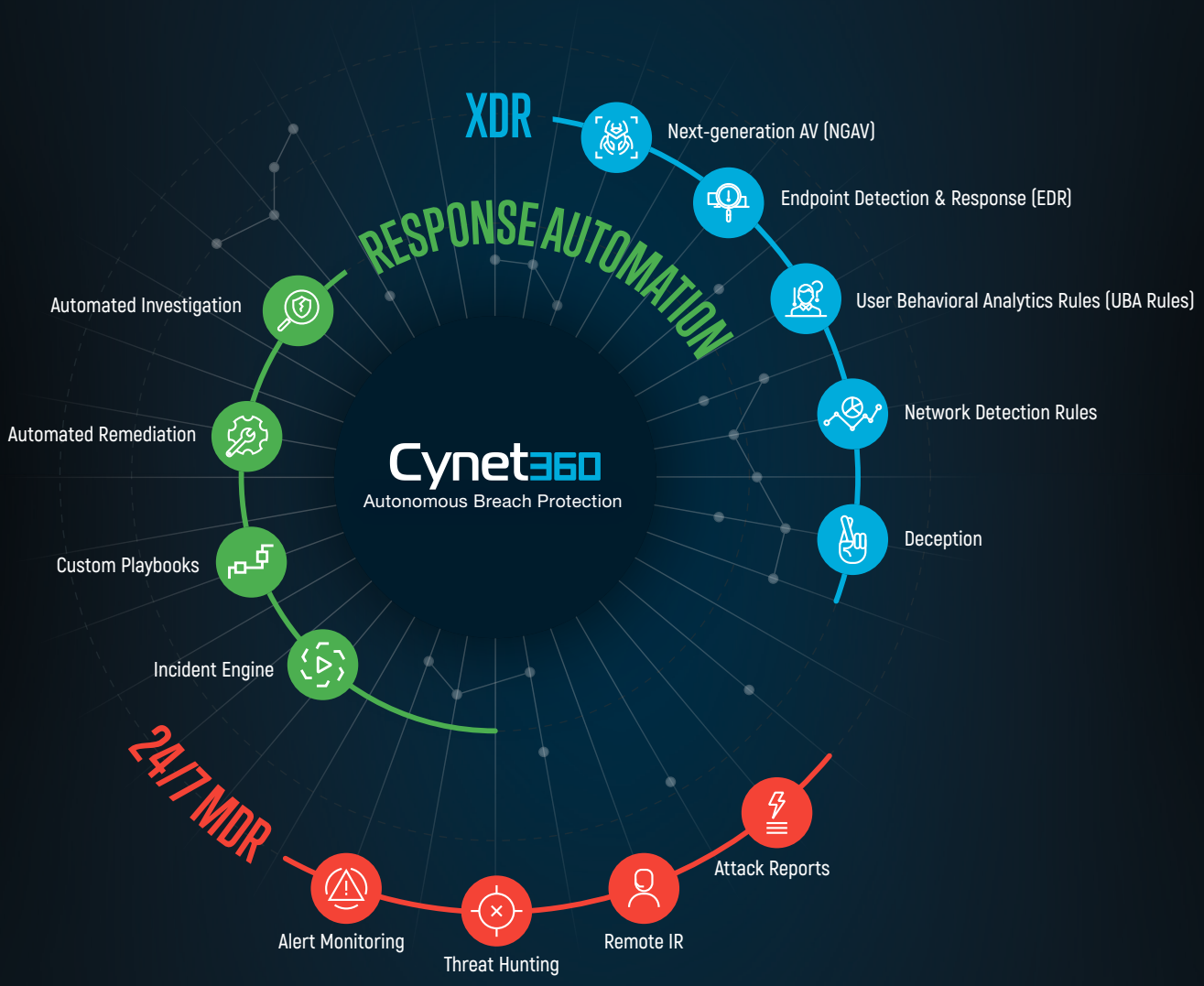
Expert Advice

CyOps is available around the clock to answer any questions you may have and provide expert guidance when responding to threat.

- Is an alert not 100% clear? Ask us anything!
- Were you informed of something suspicious? Share files and information and the CyOps team will investigate and get back to you with our findings!
- Do you want to investigate an activity or enforce your security policy by using Cynet? Let us know and we will gladly assist!
- Do you know of any abnormal, internal activity? Let us know and we'll help with a profile suggestion. Whitelist and exclusion features usability are our domain!
- Did you receive IOCs and want to make sure that Cynet has it? We can implement the IOCs in our VPC and we can assist you with implementing them in your Cynet server!

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



Learn more