Cynet

Solution Brief

How Cynet Solves Alert Overload

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

The Real Problem of Alert Overload

Security teams have become bogged down with threat alerts - especially considering that most companies experienced a doubling or tripling of alerts as the Covid-19 pandemic spawned a massive increase in cyberattacks. Although alerts are critical for signaling potential threats, they have become unwieldy.

Along with increasing attacks, security monitoring tools often mistake legitimate actions for malicious ones. This leads to false positives, illegitimate alerts that must be treated as legitimate ones, wasting valuable and limited analyst time chasing false flags. The more detection tools a company has, the more alerts and the more false positives. Many surveys indicate that analyst teams expend as much or more time chasing false positive alerts as legitimate security threats.

Alert overload creates a dangerous situation because security teams cannot appropriately address all the alerts they receive. Security professionals are therefore forced to ignore so-called lower risk alerts. Given the stealthy nature of advanced alerts, it's often the benign-looking alerts that are the ones to worry about. Ignoring alerts defeats the purpose of threat detection technologies and leads to breaches and disruption.

The stress associated with cybersecurity also makes it difficult to fill needed positions. Many studies indicate that there continue to be millions of unfilled cybersecurity positions worldwide. This means that security staffs are covering for the resource shortage and are stretched to their limits. Stress and lack of time lead to subpar performance and oversights.

The keys to solve alert overload involve improving alert accuracy and automating response actions. Alert accuracy leads to less time chasing false positive signals. Automation leads to less manual intervention so security professionals can spend more time on the truly important issues. Outsourcing is also an option but should only be considered after the above steps are taken or the cost will be excessive. Solving alert overload has never been easier, or more necessary.

How Cynet Solves Alert Overload

Previous attempts to tackle alert overload were very expensive and inconsistent. Companies that could afford multiple detection technologies relied on Security Information and Event Management (SIEM) tools to integrate alerts from all of the detection tools and aggregate similar alerts in the hopes of improving accuracy and reducing alert volume. This goal was seldom achieved despite the enormous cost of technology and human resources to implement and sustain the technology.

Companies also relied on Security Orchestration and Response (SOAR) tools to automate their response to alerts. While this technology has mostly proven to be helpful, yet typically out of the reach of companies with lean security teams that cannot afford the technology and manpower expense required.

Integrated Prevention and Detection Technologies

Let's be clear – multiple prevention and detection technologies are required to provide threat visibility across the environment. Smaller companies typically cannot afford the range of technologies required and therefore may not suffer with alert overload as much as companies with a broad range of detection technologies, each emitting a steady stream of alerts. However, this does mean that smaller companies don't have the threat visibility of their larger counterparts – which could actually be worse than receiving too many alerts.

While more technologies may seem better, the key is choosing the right set of technologies that prevent and detect threats over the most important parts of the IT environment. Cynet XDR natively provides multiple prevention and detection technologies out-of-the-box designed to extend and deepen visibility across the environment. The Cynet XDR platform includes:

- NGAV – Next Generation Anti-Virus is fundamental endpoint protection based on known bad signatures and behaviors.
- EDR – Endpoint Detection and Response detects and prevents more complex endpoint threats that bypass NGAV solutions.
- NTA – Network Traffic Analytics detects threats that have made their way into the network as well as lateral movement between assets.
- UBA – User Behavior Analytics detects unusual activity that could signal stolen credentials, a rogue insider, or bots.
- Deception – Deception uses decoy files, networks, devices and users to uncover intrusions that have bypassed other detection technologies.
- CLM – Centralized Log Management is used to mine and find threat indicators in the extensive log data generated by IT systems.
- SSPM – SaaS Security Posture Management is used to find and correct configuration mistakes in SaaS applications.

All Signals Integrated and Coordinated

Multiple detection and prevention tools, as listed above, are required to begin to see across the entire IT environment. It also leads to alert overload as each technology independently streams a steady flow of alerts that overwhelm security teams.

Cynet XDR solutions integrates real-time signals from multiple points of telemetry on a single platform that result in more accurate alerts. It also reduces alert volume so security teams can focus on what's important.

There are multiple benefits associated with this approach:

- Quickly and accurately determine the severity of each alert by connecting it to related alerts across the environment – this dramatically reduces the volume of false positive alerts you face today.
- Determine if a seemingly benign alert is actually just one stealthy part of a larger attack by combining related alerts from the other controls – this improves detection accuracy and ensures weaker, but important, signals are not ignored.
- Because these controls are natively combed, this all works out of the box and always will. You don't need to integrate multiple components, you don't have to normalize signals, you don't have to dealing with:
    - The issues of combining/ assessing/prioritizing alerts from different controls
    - Updating, reconfiguring and testing for any change to any single control
    - Coordinating multiple vendors
    - And, of course, there's far lower costs associate with all of this

Reduce Manual Load with Automated Response

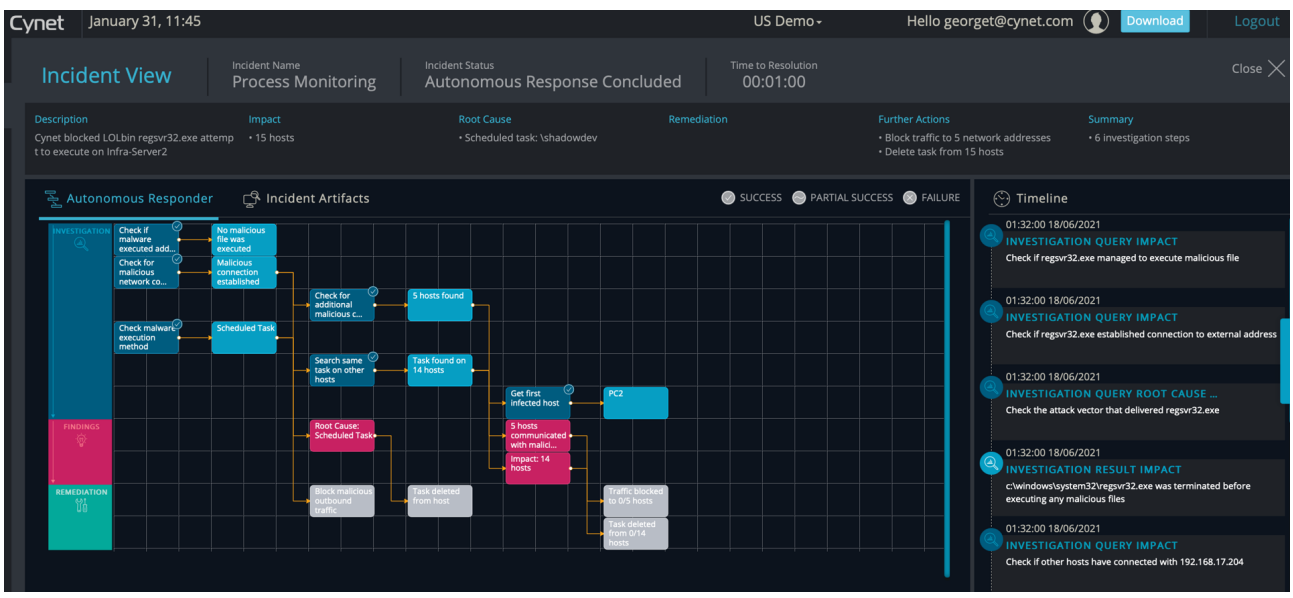
Response automation improves both speed and scale more than an army of security pros could–so long as it is integrated within the XDR. When both work together, all the signals and data collected by the constituent parts of the XDR feed into the automation engine to give it an enhanced understanding. That enables the automation to investigate the attack faster to determine its root cause and full impact. Then, based on what's known about the attack, automation can orchestrate a playbook recommended for that attack, taking specific steps to neutralize the threat and mitigate the damage.

Automated Investigation

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. Complete investigation to resolution typically takes seconds to just a few minutes - saving you the considerable time and effort required to manually investigate alets.

Cynet's Incident Engine launches an automatic investigation of risky threats to uncover the root cause and extent of the attack across the environment. The Incident Engine uncovers all associated alerts and threats across files, hosts, users and networks so the full attack can be automatically or manually remediated depending on the user's preference. Figure 2 is an example of the output of an Incident Investigation that graphically shows the investigation steps, findings and remediation actions across the environment.

Figure X, Cynet Incident Engine example showing an attack's root cause and scope



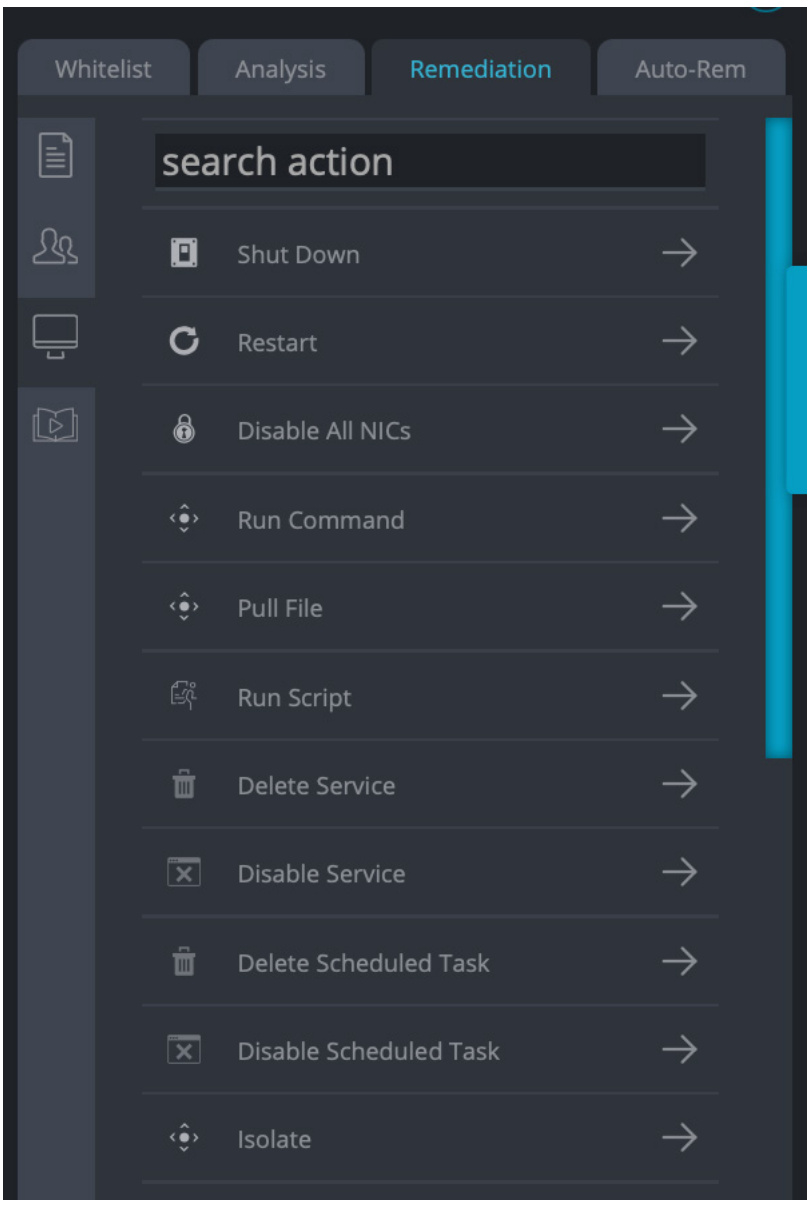
Automated Remediation

Cynet provides the widest available set of remediation tools for infected hosts, malicious files, compromised user accounts and attacker-controlled traffic. Figure 3 shows a subset of remediation actions that can be invoked manually or automatically when specific threats are detected.

Preset Remediation Actions

The widest available set of remediation tools for infected hosts, malicious files, compromised user accounts and attacker-controlled traffic. Remediation actions can be invoked manually across the multiple environmental components and can be set to automatically execute when defined threats or conditions are detected.

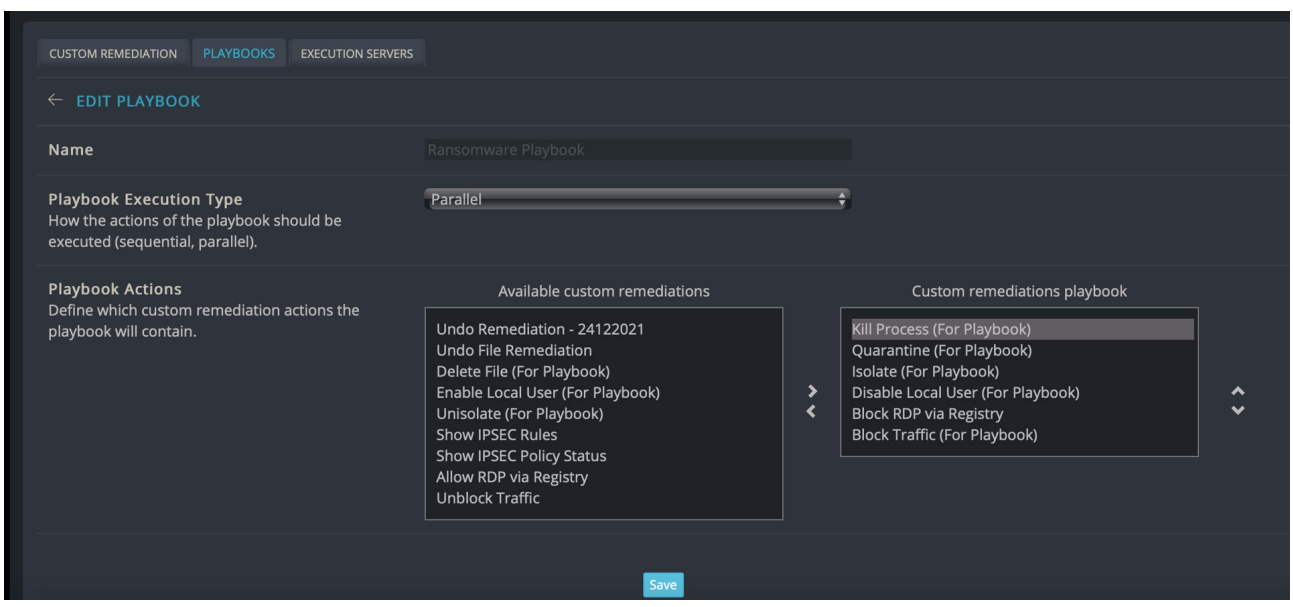
Figure x, a subset of potential Cynet host remediation actions available



Remediation 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. Figure 4 shows Cynet's simple drag-and-drop custom playbook builder within the Cynet 360 platform.

Figure x, Cynet's custom playbook editor



Cynet MDR Provides a Failsafe

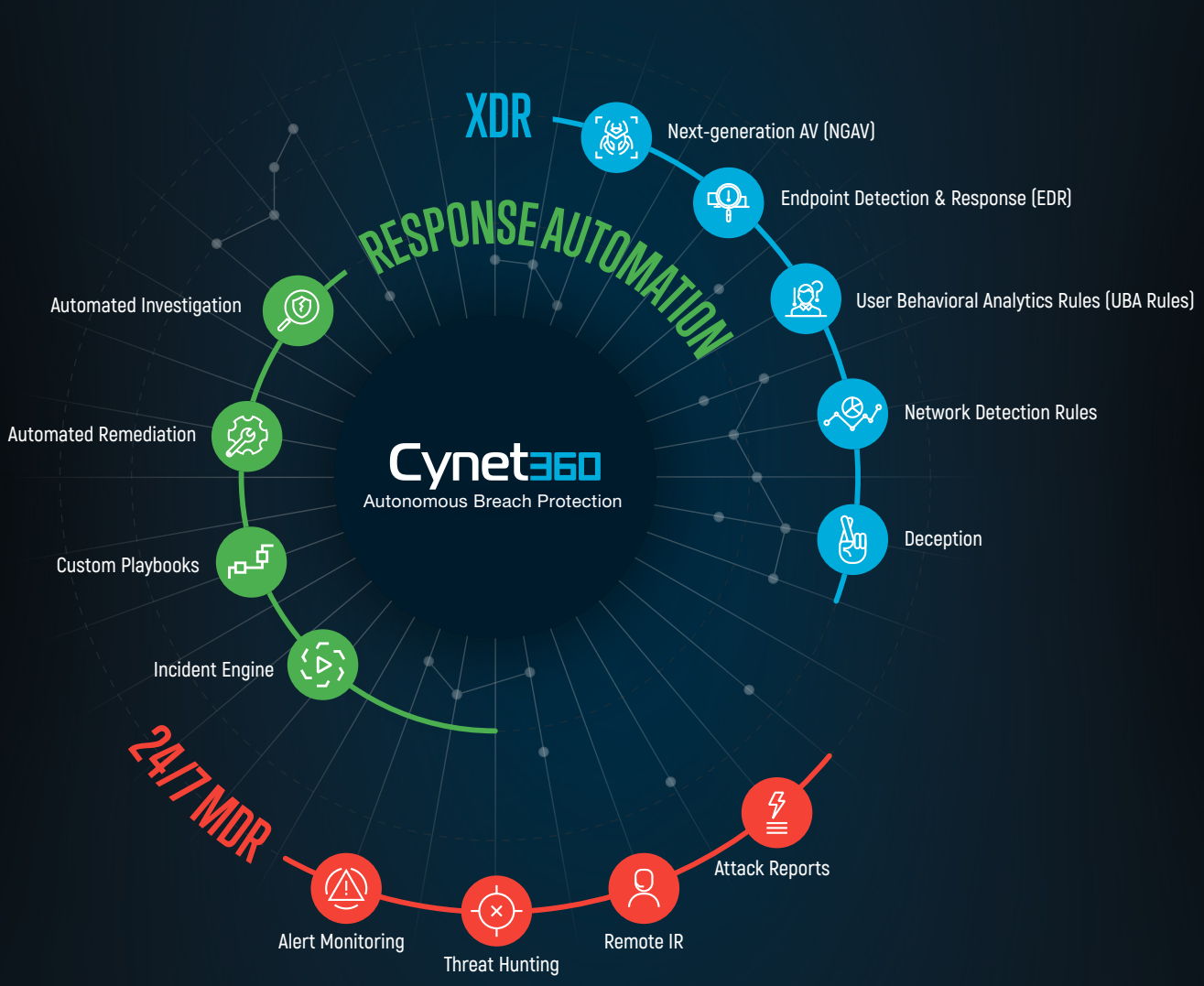
Cynet complements its breach protection technology with integrated security services at no additional cost. CyOps is a 24/7 Managed Detection and Response (MDR) team of threat analysts and security researchers that leverage their expertise to provide valuable services to Cynet's customers based on each customer's specific needs and security preferences.

CyOps continuously monitors client environments – 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. Lean security teams can rely on CyOps for guidance rather than wasting cycles trying to figure out the best course of action – and risk making dangerous mistakes.

The CyOps team proactively contacts clients when more dangerous 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. When requested, the CyOps helps Cynet clients speed time to response by ensuring that dangerous threats are quickly, properly and thoroughly addressed.

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