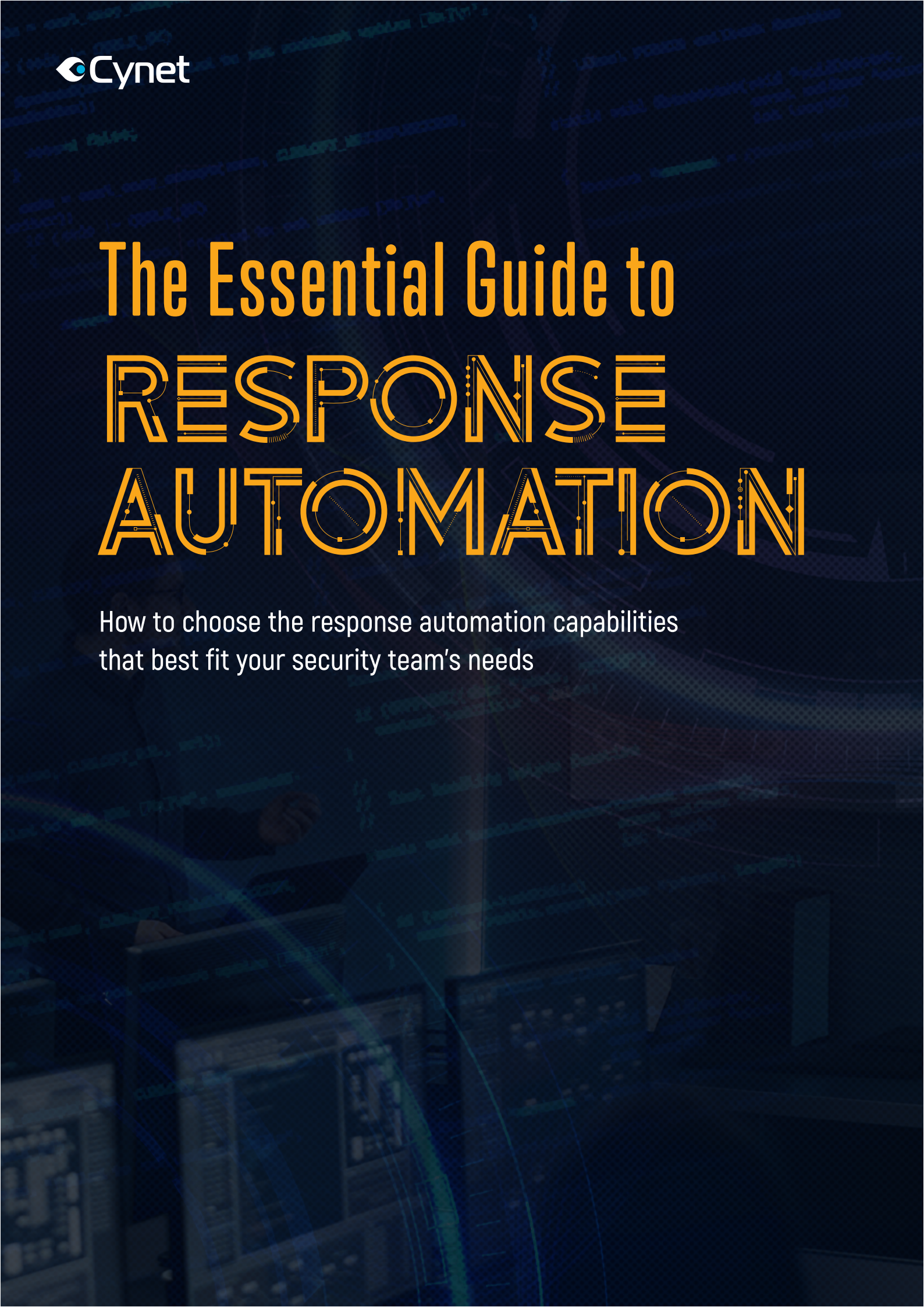
Cynet

The Essential Guide to RESPONSE AUTOMATION

How to choose the response automation capabilities that best fit your security team's needs



Overview

Improved threat detection capabilities have led to the unintended consequence of "alert overload." Whether due to detecting an abundance of real threats or generating an excess of false positive alerts, security analysts have become overloaded with alerts from their cybersecurity controls. Most cybersecurity teams today do not have enough bandwidth to properly address every alert. Additionally, smaller cybersecurity teams often lack the expertise necessary to properly address even high-risk alerts.

Most threat detection platforms, such as EDR and NDR solutions include some level of automated response capabilities to help understaffed security teams address detected threats. As the need for automated response becomes more urgent, it seems every threat detection and response (TDR) vendor is claiming some type of response automation capability. But, what does a vendor mean when they offer "response automation?" How can the average security person make sense of everything the vendors are saying?

This Guide Will Help You Make Sense of The Term "Response Automation"

What are the different types and levels of response automation?

What is the value of each?

What questions should you ask a vendor that tells you they have response automation?

What level of response automation would best fit your needs?

The Five Levels of Response Automation

The term response automation means different things to different people. Response automation can range from rudimentary, commonly available remediation capabilities to highly advanced, automated incident response workflows. To better understand and frame the range of capabilities, we defined five increasingly capable levels of response automation available today.

1 Basic Automated Remediation on A Single Endpoint

The ability to automatically take remediation actions in response to an alert is now table stakes for NGAV and EDR solutions. Most of these solutions can quarantine a suspicious file before it executes, kill a malicious process, isolate an infected device, and other rudimentary endpoint-centric remediation actions. The remediation actions are in response to a single threat detected on an endpoint device.

The ability to auto-remediate a threat provides several benefits, such as the ability to rapidly respond to a threat before it successfully further infiltrates the environment or exfiltrates sensitive data. It also provides the ability to quickly respond to dangerous threats when security analysts are otherwise unavailable.

This level of response automation is available in virtually all NGAV, EDR, XDR and SOAR solutions.

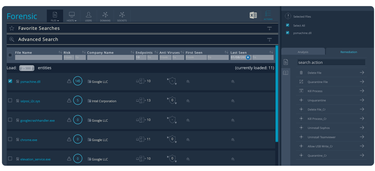
Example of a single malicious file automatically remediated on an endpoint

2 Basic Automated Remediation on Multiple Endpoints

The ability to expand remediation beyond a single device significantly reduces time required to take necessary remediation actions on multiple machines to fully remediate an identified threat. Multi-endpoint remediation includes the ability to search for a threat identified one endpoint on other endpoints across the environment and then take appropriate remediation actions.

This capability is especially critical for large and remote workforces so broader remediation actions can be accomplished without physical access to devices. It also provides a base level of threat hunting as newly discovered threats and IOCs can be found and remediated efficiently across endpoints.

This level of response automation is available in most EDR and virtually in all XDR and SOAR solutions.



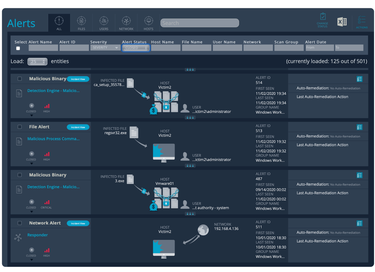
Example of file search across environment and remediation actions

3 Extended Automated Remediation Across Environment

Beyond identifying and remediating endpoint-specific threats, additional remediation actions are often necessary to fully eradicate all components of an attack. Many organizations are forced to move between multiple security applications to perform non-endpoint specific remediation actions, such as disable a user account or block certain network traffic.

The ability to perform multiple types of remediation (i.e., file, host, network and user remediation actions) from a single pane of glass not only provides significant time savings, but it also better positions the organization to address all components of a threat before damage can be done.

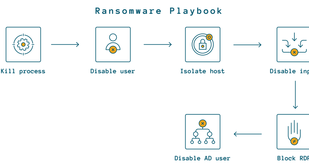
This level of response automation is available in most XDR and SOAR solutions.



Example of multiple alert types detected across the environment

4 Extended Remediation Playbooks Across Environment

Building upon the ability to perform multiple remediation actions across the environment, playbooks automate a predefined sequence of remediation actions in response specific threats. Remediation playbooks can be executed automatically in response to a detected threat for immediate response or can be triggered manually to provide more oversight and control.



Example of Cynet's Ransomware Remediation Playbook

An example of a remediation playbook could be one that responds to a detected ransomware threat. In response to detected ransomware, most responders would likely kill the malicious process on the endpoint and isolate the machine from the network. But, this is not enough to ensure the ransomware threat is fully addressed. Additional actions could involve disabling the user involved in case credentials have been compromised and perhaps blocking certain network traffic.

This level of response automation is available in many XDR and most SOAR solutions.

5 Automated Investigation with Extended Remediation Across Environment

While the ability to automate a gamut of remediation actions across the environment provides tremendous value, this next stage of response automation adds threat investigation. Automated threat investigation moves beyond responding to the single threat at hand to helping determine if the detected threat is only one part of a larger attack, and if so, uncovering and remediating related attack components.

Example of Cynet Incident Engine Automated Response Workflow

When a threat is detected, an automated investigation is launched to first uncover the root cause of the threat - how did the threat come to be in the environment. Was it downloaded from a specific site, embedded in a document, attached to an email? Was it spawned by an as-yet undetected malicious process or planted from an RDP connection? Automated root cause analysis peels back the layers to ensure all elements of the attack are exposed, and ultimately uncovering the so-called "patient 0", the origin of the attack.

Once additional components of a threat are uncovered automated investigation can search the environment to expose the full scope of the attack. This includes taking appropriate remediation actions across the environment to eradicate all attack components. Until the attack is fully rooted out, the organization cannot be assured of safety.

Manually performing these investigation steps takes time, takes skills, and takes effort. It means basically that behind every alert should come a lot of work. Unfortunately, many security teams do not have the bandwidth, and many smaller security teams do not have the skills to perform the necessary investigative steps required. Automating this workflow, at a minimum, provides security teams with a considerable head start on incident response. And, in many cases, it eliminates the need for manual intervention.

This type of response automation is available in limited XDR and SOAR solutions.

Response Automation Benefits

Increasing response automation capabilities from Level 1 through Level 5 compounds the benefits realized in two key areas.

Security

Response automation improves a company's security in two important ways. First, the faster threats are remediated the less likely they are to cause damage. Allowing a threat actor an extra moment of time might allow damage to unnecessarily occur. Second, performing automated investigations to quickly uncover an attack's root cause and scope may be otherwise overlooked in the day-to-day shuffle.

The best case outcome with automated investigation is the full extent of the attack is exposed and eradicated. At a minimum, the output from an automated investigation provides the security team with a significant head start on a full incident response effort. Response automation extends and augments the capabilities of your security team.

When every second counts, security teams benefit from "machine speed" and often more thorough handling of threats. Additionally, the alerts that are commonly not reviewed and investigated due to time and skill constraints can be automatically addressed, ensuring all threats are adequately and properly addressed.

Efficiencies

Typical threat investigation and remediation requires multiple manual steps across multiple security applications. Every time an analyst switches panes of glass, inefficiencies, potential errors and lost time results. With much of the organization's threat response actions on auto-drive using response automation tools, the security staff can focus on more urgent issues rather than ongoing alert-chasing. Response automation ultimately precludes the need to add more analysts to deal with the inefficiencies associated with siloed security systems and controls.

A security leader can quickly see the cost savings of response automation by tracking the time the security team spends investigating and responding to threats that could otherwise be handled automatically. Look at common/repetitive threat and remediation combinations as those can certainly be automated as well. Of course, robust response automation capabilities also help to avoid the significant time and expense required for major incident response activities due to inadequate threat handling.

Options for Obtaining Response Automation Capabilities

Most Antivirus, EDR and NDR solutions have, at least, rudimentary automated response capabilities, such as quarantining suspicious files or killing malicious processes. While these "point remediations" of the threat instance are critical – they often only represent what should be the first step to broader remediation actions. One must assume that the malicious artifact that was identified and remediated is the mere tip of an iceberg of a larger attack.

Combining multiple control technologies and extending automated response actions is a core benefit of XDR platforms. With controls natively built into the platform and a single source of data, an XDR platform works out of the box, without the integration time, expense and mis-steps associated with integrating and coordinating multiple security products from multiple vendors. As such, XDR platforms can extend response automation across the environment and automate investigation remediation functions. Many XDR solutions are priced comparably to EDR solutions, while greatly extending detection and response capabilities.

Some large organizations utilize Security Orchestration and Automation Response (SOAR) platforms to orchestrate and automate responses to detected threats. As SOAR platforms do not directly detect threats, purchasers must have multiple security control technologies in place (ex., EDR, NDR, UEBA, etc.) and then integrate these controls into the SOAR platform. Additionally, SOAR solutions generally require a SIEM solution to enable full response capabilities. The time, expertise and expense involved to implement and maintain this set of solutions relegates this approach to only the largest, very well-funded enterprises.

It's Just a Matter of Time

In today's hyper-complex world of cybersecurity, with limited budgets and an even more limited pool of cybersecurity talent available, organizations need to dramatically reduce the massive time sink required for excessive mundane tasks. And, with limited talent available, organizations need to augment the skills of existing staff to ensure the threats at hand are properly addressed. Automation is the future of cybersecurity and now is the time to jump in.

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.

LEARN MORE