NETENRICH

HOW TO IMPROVE DETECTION AND RESPONSE WITH ADAPTIVE MDR

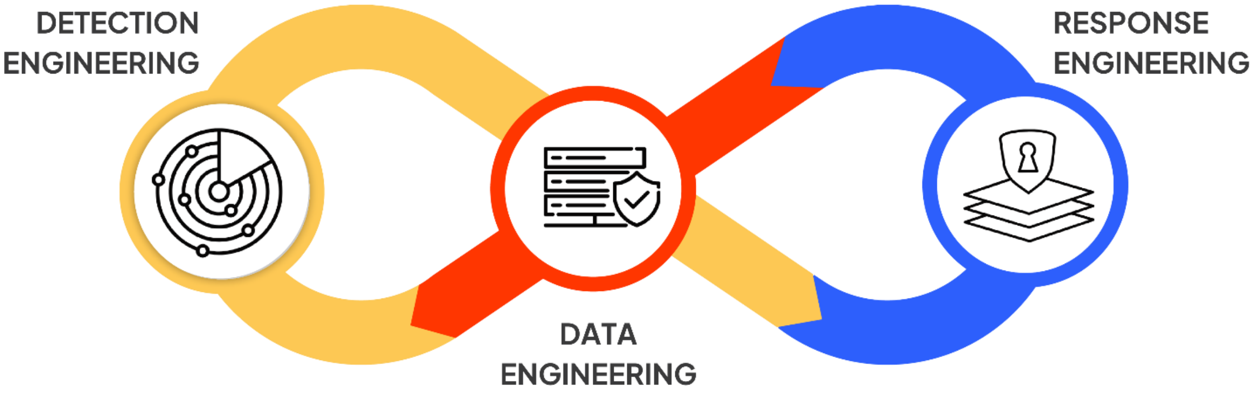
TABLE OF CONTENTS

When it comes to cybersecurity, what is detection and response?

The key components of effective detection and response systems typically include a combination of technology, processes, and human expertise. More specifically, components include continuous monitoring, detection and response tools, log management and analysis, threat intelligence integration, behavioral analytics, automation and response orchestration, and effective collaboration, communication, and reporting.

How can continuous detection and response help protect businesses?

Continuous detection and response (CDR) is part of a proactive cybersecurity strategy that recognizes the dynamic nature of cyber threats — in short, threat actors are innovative and relentless — and aims to minimize the impact of security incidents through rapid identification and response. CDR solutions monitor network traffic, system logs, and other relevant data sources to identify potential security incidents in real-time. They then seamlessly integrate potential incidents with other security tools and technologies, including threat intelligence feeds, which help organizations stay current on the latest threats, trends, and vulnerabilities.



For Google Chronicle Secops

CDR solutions are all about helping organizations detect threats early (before they can escalate into significant incidents), minimize bad actor dwell time, and adapt more quickly to new and emerging threats. They are designed to uncover weaknesses and provide the information needed to update and improve detection rules, response protocols, and preventative security measures as well as to become more proactive with defense.

Automation is a crucial component of CDR, especially when it comes to routine tasks and initiating predefined responses when suspicious or malicious activity is detected. CDR systems often use behavioral analysis to establish a baseline of normal behavior within an organization. Any deviations from this baseline may point to potential security incidents. It's also important that CDR solutions offer robust incident analysis and reporting and can scale to accommodate the growing needs and complexities of an organization's infrastructure and business.

By adopting a proactive CDR approach, organizations can enhance their overall security posture and strengthen their resilience against a wide range of cyber threats.

What is the difference between EDR, XDR, MDR, and adaptive MDR?

Endpoint detection and response (EDR), extended detection and response (XDR), managed detection and response (MDR), and adaptive MDR are different approaches for detecting and responding to security incidents.

EDR solutions combine antivirus with post-detection analysis capabilities to monitor endpoint activities and identify malware infections or endpoint-specific attacks. An EDR solution is designed to provide visibility into endpoint activities, detect suspicious behavior or indicators of compromise (IoCs), and facilitate incident response at the endpoint level.

While EDR focuses on endpoint security, XDR goes a step further by integrating and correlating data from multiple security sources, including endpoints, networks, and cloud environments. It provides a more comprehensive and holistic approach to threat detection and response by offering a unified view of security incidents across an entire organization and often, leveraging automation, artificial intelligence, and advanced analytics for more efficient detection and response to complex threats.

Next, there's MDR, which is not just a technology, but a service provided by cybersecurity vendors. Like XDR, MDR extends beyond endpoints to cover networks, cloud environments, and other parts of an organization's infrastructure with the goal of providing a holistic view of an organization's security landscape.

Finally, adaptive MDR is a solution designed to adapt to the dynamic threat landscape and meet the unique and evolving security requirements of each organization. Unlike standardized, one-size-fits-all MDR approaches, it emphasizes agility and refinement based on ongoing insights and experiences.

For example, Netenrich Adaptive MDR™, powered by Resolution Intelligence Cloud™ technology and integrated with Google's SecOps technologies (SIEM, SOAR, Mandiant, and more), exemplifies this approach. It offers 24/7 monitoring and response by experts and operates on an continuous loop of data engineering, detection engineering, and response engineering to provide customized, adaptable protection aimed at facilitating autonomic security operations (ASO).

While EDR, XDR, and traditional MDR solutions offer valuable insights into security incidents, today's cyber threats demand a more adaptive approach. As we delve into the role of threat intelligence in Netenrich Adaptive MDR, you'll see how this solution leverages real-time insights and pivots as necessary to stay ahead of emerging threats and ensure proactive defense measures.

The role of threat intelligence in Netenrich Adaptive MDR

Effective detection and response requires relevant and timely threat intelligence. This intelligence provides requisite context about potential threats and helps organizations understand the evolving tactics, techniques, and procedures (TTPs) used by adversaries. Threat intelligence can include indicators of compromise (for example, IP addresses, domain names, file hashes, and signatures associated with known malicious behavior), malware signatures, and information about software vulnerabilities, exploits, and industry-specific threats.

Knowledge Now (**KNOW**) is Netenrich's proprietary threat intelligence that is deployed in Netenrich Adaptive MDR. It combines machine and human insight to identify and assess risk exposure by criticality, likelihood, and impact of an exploit and help organizations make real-time informed decisions when responding to potential threats.

Task automation and response orchestration with Netenrich Adaptive MDR

Again, automation of routine tasks is crucial for streamlining processes, including the coordination of actions taken in response to security incidents or IT operations events (aka response orchestration).

Netenrich Adaptive MDR reduces manual effort by creating and automating response workflows based on specific triggers, such as security alerts. The combination of technology and expertise allows us to quickly assess the severity and business impact of an incident, prioritize response, and help IT and security teams determine the appropriate course of action. Often, we can automate remediation actions, including isolating affected endpoints, blocking malicious IP addresses, and taking other predefined steps to neutralize threats.

In some cases, response orchestration involves collaboration among security teams and other stakeholders. Netenrich facilitates coordination during incident response by enabling complete visibility and ensuring all parties are working from the same information. As mentioned above, we also incorporate threat intelligence to enhance the context and accuracy of response actions.

Intelligent routing and collaboration with Netenrich Adaptive MDR

Intelligent routing (also known as impact-based routing) is the use of advanced algorithms and technologies to efficiently direct and manage alerts and notifications. The goal is to get the right information in the hands of the right people so they can take appropriate and timely action to maintain business continuity and mitigate potential damage. Intelligent routing requires complex data analysis along with a deep understanding of what's important to different industry sectors and what assets are *most* critical to the business — because ultimately, the impact of a threat highly depends on the targeted asset.

For example, if a targeted server holds a company's secret sauce, a compromise could be very impactful. If, however, the server stores an organization's cafeteria menu, maybe less so. At Netenrich, our security engineers build that kind of business-impact information into an organization's system so that when teams get an alert, they know whether it's mission-critical and something they need to act on immediately versus something less urgent.

This intelligence also feeds into the adaptability of the system in general as an organization continually assesses and reassesses what's most important to its business.

Additionally, our team analyzes vast volumes of data from across data centers, third-party systems, the cloud and then routes pertinent situational intelligence (based on a likelihood, impact, and confidence score) to the correct group or individual. This way, when an alert is routed, the recipient has a clear picture of what's affected, what the impact is, what the risks are, and what the associated threat intelligence is. Because this actionable intelligence is also tied into a collaborative workbench, organizations can easily bring in other relevant people as needed — for example, representatives across SecOps, Digital Ops, and DevOps — to decide on a prompt course of action.

Self-sufficient and self-healing systems – a vision for Netenrich Adaptive MDR

Self-healing systems allow an IT environment or security infrastructure to automatically detect, respond to, and recover from security incidents without the need for manual intervention. These systems leverage automation and orchestration to enhance an organization's resilience against cyber threats.

At Netenrich, we don't design systems to assign operational tasks. We design systems to enable them to be self-sufficient and self-healing to reduce human involvement while speeding detection and response to minimize potential damage. We also understand that everything in security is based on a point in time and that the way a business secures itself one day may need to change the next. Thus, from every lesson learned, we tune our systems and make changes to improve processes — and the same goes for every organization we work with.

Discover how **Netenrich Adaptive MDR** can elevate your security systems with data visibility, security analytics, intelligent routing, and response orchestration. Our cloud-native Resolution Intelligence Cloud technology seamlessly ingests, correlates, and analyzes data, delivering data-driven, actionable insights that empower us to prioritize critical issues and rapidly adapt to your evolving security challenges.