The Respond Analyst, an XDR Engine | Investigation Power at Machine Speed

What is XDR?

eXtended Detection and Response (XDR) solutions integrate a set of products unifying control points, security data, analytics and operations into a single enterprise solution. XDR support includes multiple telemetries such as endpoint, network, web filters and cloud sensors. XDR promises to provide technology integration between data sources and security operations to accelerate detection and response, while reducing engineering headaches.

Four considerations for an Extended Detection and Response solution

The growth of security related data coupled with the shortage of skilled security personnel leaves companies at risk. Security teams of all sizes are resource constrained, filtering alerts to match analysis capacity. In doing so, clues to potential threats stay hidden and attackers are able to achieve longer dwell times, increasing the likelihood and impact of a security incident.

1. SIEM challenges for incident detection

Many organizations are using Security Information and Event Management (SIEM) systems that require rules to reduce the number of events security teams analyze. Output from SIEMs can be unreliable and inconsistent. SIEM rules are based on boolean, deterministic rule logic, too simplistic to isolate and analyze real attacks. Additionally, SIEM rules and the people who write them, can vary in terms of quality resulting in inaccurate or incomplete analysis.

Additionally, most organizations lack the time and budgetary resources to deploy and maintain their SIEM infrastructure.

2. SOAR challenges for incident detection

Some organizations are using Security Orchestration Automation and Remediation (SOAR) platforms programmed by security engineers to automate analyst tasks, i.e., data collection, correlation, enrichment and response to low-level security events. However, SOAR tools can choke on the volume of data that needs to be analyzed, significantly reducing their remediation capability.

3. XDR limitations

New XDR solutions are limited to a vendor's proprietary technology stack, reducing the volume of security data that can be correlated, scoped and triaged, while locking customers into expensive tools. Likewise, detection capabilities are limited or require customization through professional services or security engineers.

4. Open XDR

Open or agnostic XDR gives security teams the best of both worlds - analytics that work across a broad range of security technologies and the capability to find incidents in real-time.

Disparate data and evidence generated by security sensors in the environment need to be correlated and analyzed at scale. XDR solutions must work with a broad range of vendors, telemetries and threat intelligence to be effective in escalating only malicious and actionable incidents. Many solutions generate too many false positives or are not successful in finding the real incidents that require remediation. In this way, XDR tools become costly and ineffective.

Why use the Respond Analyst?

The Respond Analyst is the simple, open and intelligent XDR engine that finds and scopes incidents in real-time. It makes decisions at machine speed to force multiply tier one monitoring.

Open

Choose best-of-breed controls to modernize your sensor grid. Works with **over 65 vendor offerings** across important categories such as EDR, IPS, Web Filtering, EPP, Vulnerability Scanning, Authentication and more.

Intelligent

Connects the SOC's disparate evidence using probabilistic mathematics and **Integrated Reasoning** to determine the likelihood that events are malicious and important enough to escalate.

Simple

Deploys in hours and constantly learns without tuning, coding or content writing. Cloud-native, so you don't have to manage infrastructure.

> "The Respond Analyst provides a needed roadmap right out-of-the-box to apply context and advanced data science models – it is exactly what we need. XDR is no longer a question of when, but how soon."

CyberPeak Solutions

Travis Abrams
Founder and CEO of CyberPeak Solutions

respond

www.respond-software.com. For more information, email info@respond-software.com.