Service Brief

Rapid7 Analytic Response

Your Army of Cyber Guardians

You've got valuable data. Naturally, other people want it. Organized criminals. Nation states. You know, the kinds of too-smart-for-their-own-good bad guys who can and will do whatever it takes to cripple an organization or make a quick buck. To make matters worse, there's a good chance you're under-staffed and under-tech'd. And finding talent and tools good enough to compensate? We wouldn't say it's like finding a needle in a haystack, but only because we don't like clichés.

But with Rapid7 Analytic Response services, none of that is your worry—it's ours. You read that right: our security experts act as an extension of your security team, providing 24/7 detection and response in your environment. People who understand the difference between user behavior and attacker behavior, and have the time to focus on hunting and processing threat intelligence. Technology that understands your environment and can be automated to detect and respond. A plan and a team with the experience required to solve your toughest problems. Your organization can finally have everything it needs to stay safe, without actually taking on anything more: consider us your army of cyber guardians.

It's More Than Just a Managed SOC

Many Security Operations Centers (SOCs) only focus on known threats, which means as threats evolve, incidents can go undetected and unmitigated for months – and even years – allowing attackers to get comfy within an environment and wreak havoc. To detect and respond to both known and unknown threats quickly and thoroughly, Analytic Response members combine their personal expertise with the industry-leading technology of Rapid7's incident detection and response solution, InsightIDR. InsightIDR itself combines user behavior analytics, SIEM, and endpoint detection capabilities all in one place—unsurprisingly, it's the backbone of our Analytic Response offering.

Out of the Great Unknown

Great incident detection and response is more than what you know—it's knowing what you don't know too. Unlike other SOCs and managed services, Analytic Response incorporates four distinct threat detection methodologies to detect the unknown:

1. Threat intelligence is gathered from Rapid7's 5000+ customers and 3rd-party intelligence groups, anonymized, and analyzed to further automate threat detection and response.

> **"[Managed detection and response (MDR) services] aim to remove the burden from clients of having to figure out "what method or device to use" for a security monitoring and response capability. MDR services focus on specific outcomes — threat detection, with 24/7 monitoring and alerting, and remote incident investigation and response included in the end-to-end service."**
>
> ***-Gartner defining the MDR services space***
> *Market Guide for Managed Detection and Response Services, May 2016*

Rapid7's Analytic Response team has detected and responded to over 1,000 breaches, most involving a targeted threat actor such as organized crime, nation state, or other organized, skilled attackers.

2. User behavior analysis utilizes knowledge of how regular users behave to spot anomalies that enable more efficient insider threat and stolen credential detection.

3. Attacker behavior analysis allows rules to be put in place to automatically make decisions based on a familiarity with hacker behavior.

4. Hunting methodology employs complex data analytics to identify unknown threats.

When employed by Rapid7 experts and with Rapid7 technology, these methodologies make it possible to validate threats before they're reported with a nearly zero percent false positive rate.

A Security Plan as Unique as Your Organization

Your Analytic Response team provides incident detection and response on applications, endpoints, and assets within your organization, including those in the cloud. What's that look like for you? To kick things off right, a Rapid7 Threat Assessment Manager works with your team for the first 30 days to understand your environment and make informed recommendations around identifying and assigning priorities. You will continue to meet with your Threat Assessment Manager monthly to ensure your plan is evolving with your needs. This initial 30 days combined with regular monitoring and hunting enables the team to detect and respond to threats quicker. And if we do find something, your team has a one-hour SLA for notifying you. Reports produced are robust and have input from expert analysts.

We're Ready to Pivot, So You're Ready to Respond

With Analytic Response, you're always prepared to deal with cyber threats. If there is an incident, such as a breach, the team is ready to pivot from detection to respond and act, and will work closely with you to create a remediation plan tailored to your organization. You will also be provided with a report with an executive summary and in-depth analysis of the issue to make sure your organization understands the incident. Additionally, this information is analyzed to help fuel threat intelligence to increase speed in detection and response in the future.

Get to Know Your (Non-)Resident Experts

Everybody ought to know their cyber guardians. Yours, as expected, eat, sleep, and breathe threat detection and response—when they're not guarding your network, there's a good chance they're at a local meetup, learning about the latest hacking tools and techniques. Like every good hunter, they're 50% methodical, 50% innovative, and 100% intense. How else could they cut incident detection to hours and days from weeks and months?

- Over 10 years of experience, on average
- Threat Intelligence Lead ran intelligence for public and private sector
- Even the most junior analyst has detected and responded to 300+ threats

Enlist your cyber guardians (or just learn more):
https://www.rapid7.com/services/analytic-response.jsp