RAPID7 PRODUCT CONSULTING BRIEF

Quick Start Services
For Rapid7 InsightIDR

Rapid7 products are easy to install and use, and our team can provide expert guidance to take your usage of the product much further. The Quick Start Services for InsightIDR help you through deployment and ensure that you get the most value out of your investment.

MAXIMIZE THE VALUE OF YOUR PRODUCTS

Get up and running quickly—because you value your time.

Rapid7 InsightIDR is easy to set up and use, but as with any complex topic, expert guidance maximizes the value you get out of the solution. We help you set up collectors and event sources for your new deployment so you can turn into a power user in no time.

Learn how to optimize the quality of your data.

You might be experiencing information overload from existing monitoring solutions which send you many more alerts than you can investigate. InsightIDR only sends you a handful of alerts filled with context, so you can make informed containment and remediation decisions. We'll also help you optimize your environment to identify misconfigurations and prioritize risk.

Investigate efficiently to save time when it counts.

When you detect an incident, all eyes will be on you to provide context and valuable insights. We'll teach you how to build an incident timeline that clearly communicates what happened, so you can focus on containment.

83%

83% of compromises take weeks or longer to discover.

- 2016 Verizon Data Breach Investigations Report

50%

50% of ex-employees still have access to corporate applications after leaving a company.

- 2017 OneLogin IT Survey

> “Rapid7 InsightIDR is a detection and response tool that uses deception technology to answer a couple of important questions: “Is the enterprise compromised, and, if so, how do I respond?”
>
> — Peter Stephenson, Technology Editor
> SC Media

YOUR GUIDE TO DEPLOYMENT, OPTIMIZATION, AND OPERATIONS FOR THE INSIGHT PLATFORM

Rapid7 InsightIDR helps you find the attacks you’re missing by thoroughly collecting and analyzing user behavior across endpoints, networks, and clouds. You’ll be able to detect attackers even when they are hiding behind stolen user credentials—today’s most common attack tactic.

Set up collectors and event sources

Security analytics provides the best results when it can draw on a lot of data. First, we’ll focus on setting up collectors in your environment. Then, we’ll collect logs from your data sources, or augment an existing log aggregator or SIEM. The more data sources you have connected, such as the included Insight Agent for real-time endpoint data, the higher the quality of incoming alerts.

Deploy easy-to-use deception technology

You may not be collecting some of the most useful data. We’ll help you deploy honeypots and honey users in your environment to detect network scans and brute forcing attempts—both early signs of an attacker on your network. We’ll also work with you to collect the right endpoint data, giving you visibility into lateral movement using local credentials, a common attacker technique that is notoriously hard to detect.

Achieve optimum performance and the highest quality alerting

Every organization is different, so we’ll help you improve the quality of your incident alerts for your business. It’s easy if you know how, and it will greatly reduce the number of incidents you’ll need to investigate: This means saved time and resources you can use to focus on other aspects of your security strategy.

Investigate incidents efficiently

When you want to determine the scope and exact users behind an incident, we’ll show you how to quickly search through your log data and map your findings on an incident timeline. This graphical investigation can be shared with your peers and other stakeholders to accelerate containment and remediation.

FOR MORE INFORMATION OR TO GET STARTED, CONTACT YOUR ACCOUNT EXECUTIVE.