RAPID7

Rapid7 Incident Response Services

Are You Ready For The Inevitable?

Breaches used to be a thing to "stop."

Now, at a relentless pace, they're called unavoidable, fated. You and your team are expected to respond, investigate, contain, and recover – cooly, calmly, quickly. And now, with Rapid7's suite of proactive and responsive Incident Response services, you can.

You'll have access to world-class technical expertise and technologies. Our teams work closely with your in-house and outsourced teams through every stage of incident response, from pre-incident planning and preparation through analysis, containment, remediation, and cleanup.

HOW IT WORKS:

Top Incident Response tools and experts on your team

Rapid7's Incident Response Services help organizations of any maturity, size, and skillset better prepare for and manage a breach. Our team combines a proven Digital Forensic and Incident Response (DFIR) methodology with industry-leading experts and technology to help you develop, run, or improve every stage of your incident response program, from detection and analysis, right on through cleanup.

Led by humans, amplified by technology

It's humans and machines, each doing what they do best, and fully dedicated to giving bad guys the boot. Our 24x7 team of incredibly skilled, versatile security pros is always armed with award-winning technology and an unmatched understanding of threats, forensics and triage, malware analysis, and attacker behavior—and always ready to tackle any IR challenge. Whether you need help managing an ongoing breach, or taking steps to get ahead of a potential one, we can help you take back control of your environment and program.

Attackers are gone once, and gone forever

Our proven incident response methodology ensures the attackers are gone from your environment and reveals steps you can take to keep them from getting back in. It's a unique approach that also helps us better understand attackers at large—valuable insight that informs and advances all of our IR services and ensures greater success for our customers.any facet of incident response.

Breached?

Here's how we help:

- **Incident management:** Our team provides a single point of contact for the investigation, manages all analysis, threat detection, and communications, and documents all of our findings.
- **Investigation and analysis:** We perform investigation of incident scope, impact, and root cause using InsightIDR, our open-source DFIR tool Velociraptor, your existing log sources, and our years of experience.
- **Communications:** Regular and consistent communications ensuring the right people are kept informed of key events at the right time.
- **Remediation and cleanup:** Detailed recommendations to get you back to normal including how to remove all attacker remote access capabilities, restore prioritized business processes and systems, and secure compromised user accounts.

Rapid7 Incident Response Services:

IR Program Development

Attackers are constantly evolving. To ensure you're always prepared, you need a plan, and you need to review it regularly. Our experts will evaluate your environment—from technology and assets to people, processes, and policy—to rate your current capabilities and offer relevant, business-based recommendations to help you meet (and exceed) your IR program goals. Need to build your program from the ground-up? We can help with that, too. Our IR Program Development offering can be customized to help build or improve your aptitude in any facet of incident response.

Compromise Assessment

From verifying compromise to validating remediation efforts, a Compromise Assessment can confirm your house is clean (or not). By applying threat intelligence and behavioral analytics with innovative hunting techniques, our experts assess your environment to identify malware and evidence of attacker activity and report on misconfigurations, significant risks, and potential vulnerabilities.

Detection and Response Workshop

This program puts your detection-and-response capabilities to the test against a live, emulated attack within your environment. The goal of this workshop is to evaluate how well your unique detection and response capabilities and current IR plan work to ensure your team can recognize and properly respond to an attack. Our experts will help your team understand how current security measures and controls handle the breach while providing coaching to strengthen your approach to incident response.

Tabletop Exercises

Tabletop exercises simulate threats on-site to evaluate your detection and response capabilities in a controlled environment. We work with you to create and deliver a meaningful scenario, analyze the results, and provide a list of actionable improvements you can apply to your incident response program.

Breach Response

Need immediate help with a breach? Call us at 1-844-RAPID-IR (1-844-727-4347). Our incident response team is ready to collaborate closely with your in-house team to investigate incidents, document findings, and recommend the right remediation activities to help ensure attackers are out and can't find their way back in. Our incident response consultants can collaborate with your critical stakeholders, ensuring various parts of the business are making key considerations throughout the response process.

Rapid7 Retainer

An incident response retainer is an easy way to keep IR experts on standby. In the event of a compromise, retainer customers alert the Rapid7 team, who respond within one hour to gather details and discuss planned incident response activities. All technical investigations are done remotely, and are ready to begin as soon as

our InsightAgent can be deployed (or access given to detection and response systems). Retainers are available in 40 hour blocks, and in the (hopeful) event they're not needed for breach response, can be repurposed into a variety of other Rapid7 professional services. Give us a call, and we'll set you up with a project manager who can help you assess which services are right for your organization. We can then connect you with the best consultants to get you started on the path to stronger incident response.

The amount of organizations world-wide that have experienced a 0-day attack rose from 51% in 2021 to 62% in 2022 (VMware Global Threat Report 2022)

11%

INCREASE

in organizations that have experienced 0-day attack

According to the IBM 2021 Cost of a Data Breach Report, the average data breach in the US costs 4.24 million. But breaches cost a lot more than money, they cost business disruption and brand reputation.

$4.24

MILLION

Average data breach cost

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

HAVE YOU BEEN COMPROMISED?

Call us right away at 1-844-RAPID-IR.
Not yet? We'll help you prepare.

Learn more at **www.rapid7.com/services/incident-response**