RAPID7

SERVICE BRIEF

Incident Response Services

Accelerate your incident investigation and containment

When Ben Franklin famously quipped, "An ounce of prevention is worth a pound of cure," he clearly wasn't considering the sophistication and persistence of targeted attacks on complex corporate networks in the 21st Century. Of course, he didn't totally miss the mark—continuously reducing your attack surface is always smart security strategy. But in a time when attacks are as complicated as the networks they're targeting, prevention isn't enough. Attackers will get in. And when they do, you must be able to act fast to minimize the impact. With all due respect to Mr. Franklin, Rapid7's Incident Response (IR) Services can help when more than simply prevention is needed.

The IR dream for any IR team

From teams without the time, technology, or techniques to effectively investigate and contain incidents to those with a mature plan that's ready to optimize, Rapid7's Incident Response Services help organizations of any maturity, size, and skillset better prepare for and manage a breach. How? By combining our proven methodology with industry-leading experts and technology, we're well-positioned to help you develop, run, or improve every stage of your incident response program, from detection and analysis, right on through containment, remediation, and cleanup.

Not cyborgs, but close

Part human. Part technology. Fully dedicated to giving bad guys the boot. We wouldn't call our IR experts RoboCops, but we'd understand if you wanted to. After all, they're incredibly skilled and versatile security pros, 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.

Gone, but not forgotten

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. Here's how it works:

- 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.
- Detection and analysis: We trace attacker activity via thorough, technology-assisted endpoint, network, log, event, malware, and forensic analysis.
- Scoping: Leveraging threat detection technology, existing log sources, and the insight uncovered during detection and analysis, we effectively scope the compromise.

Has your network been compromised?

Call us right away at 1-844-RAPID-IR.

Not yet? Let us help you prepare. Learn more at www.rapid7.com/services/incident-response

- Communications: Daily and weekly status reports, as well as close coordination on internal and external communications, ensure the right people are kept informed of key events.
- Remediation and cleanup: Armed with a thorough scoping of the incident, we focus on removing all attacker remote access capabilities, restoring prioritized business processes and systems, and securing compromised user accounts to get you back to normal.

OUR INCIDENT RESPONSE SERVICES

Whatever your incident response needs, Rapid7 offers proactive and reactive services to give you the confidence to remain cool, calm, and collected while managing a potential crisis.

Breach Response

Need immediate help with a breach? Call us at 1-844-RAPID-IR (844-727-4347). Our incident response team is ready to collaborate closely with your in-house team to detect threats, document findings, and recommend the right remediation activities to help ensure attackers are out and can't find their way back in. We can even support your crisis communications to help present critical details to the public or to the Board, should it come to that.

Compromise Assessment

From verifying compromises to validating remediation efforts, a Compromise Assessment can confirm your house is clean (or not). Applying threat intelligence and behavioral analytics, and using cutting-edge technology, experts assess your environment to identify malware and evidence of attacker activity and report on misconfigurations, significant risks, and vulnerabilities.

Breach Readiness Assessment

A Breach Readiness Assessment provides a full evaluation of your threat detection and incident response capability to show you how yours stacks up against best practice, and to identify steps to take your program to the next level. (We'll even help you justify necessary investments to the powers that be.)

Tabletop Exercises

Tabletop exercises provide on-site threat simulation to evaluate your detection and response capability 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.

IR Program Development

Attacks and 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 to assets to people, process, and policy—to rate your capability and offer relevant, business-based recommendations to help you meet 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 capability in any area of the Security Program Lifecycle (Preparation, Prevention, Detection, Response, Remediation, Cleanup, Lessons Learned).

Blended and Custom Engagements

Need help and don't see an offering that meets your requirements? Call us. We tailor offerings to your specific needs and can even partner with experts from other Rapid7 teams—including Penetration Testing and Advisory Services—to run blended engagements such as Red/Blue Team exercises and full-scope assessments of security programs.

By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 20% in 2016.

–Gartner, Special Report: Cybersecurity at the Speed of Digital Business (August 2016)

Rapid7 Retainer: Way more than an insurance policy

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 plan an approach. We begin technical investigations within 24 hours remotely and we can be on-site within 48 hours. Retainers are available in 80 and 120-hour blocks (120 hour retainers include a Breach Readiness Assessment).

Of course, we love to hear from you outside of emergencies too. That's why retainer hours can be applied toward any of our Incident Response Services (or any Rapid7 Consulting offering, for that matter). 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.

Get started today.

1-866-7RAPID7
1-617-247-1717
www.rapid7.com/services/request