SERVICE BRIEF

Rapid7 Compromise Assessment

Get definitive answers, so you can stop guessing

From teams without the time, technology, or techniques to effectively investigate and contain incidents to those with a mature plan ready for optimization, Rapid7's Incident Response Services can help organizations of any maturity, size, and skill set 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 through containment and remediation.

Gain confidence in turbulent times with Rapid7's expertise

From verifying compromises to validating remediation efforts, a Rapid7 Compromise Assessment can confirm whether or not you've got a clean house. Our experts pair threat intelligence and behavioral analytics with cutting-edge, ever-evolving technology to assess your environment and identify malware and evidence of attacker activity. Our versatile security pros possess a thorough understanding of threats, forensics and triage, malware analysis, and attacker behavior, giving you unparalleled clarity during uncertain times.

THE RAPID7 DIFFERENCE

Methodical approach using Indicators of Compromise (IOC)

Our proven compromise assessment methodology validates whether or not attackers have infiltrated your environment, and provides actionable steps you can take to keep them out with considerations that include (but are not limited to) the following:

- **Operating system-specific malware persistence mechanisms and process injection methods:** We review currently running processes, scheduled tasks and common hiding places to detect anomalies in behavior and communications.
- **Attacker lateral movement:** We apply threat intelligence and user behavior analytics to uncover the attacker pathway in real time. Our threat intelligence is garnered from industry and proprietary sources, as well as our threat intelligence team.
- **Common attacker tools:** We find evidence of attacker activity, including modified registry keys or executable files left behind, to validate suspected compromise.
- **Indicators derived from investigations:** We evaluate an exhaustive list of compromise indicators, such as privileged user account anomalies, geographical irregularities, or suspicious registry changes.
- **Environment-specific considerations:** We take the time to understand your environment and the relationships between users, hosts, and processes to identify any artifacts in the kill chain.

Efficient and protected data use

Your data is the key to the castle; we adopt a surgical approach to deploying agents and pulling back artifacts for analysis. This offers two main advantages:

1. **It requires less time and is less intrusive:** By pulling back only the relevant data in our assessment, we're able to hit the hands-on work faster and reduce the amount of traffic across your network and potential performance degradation.

2. **Your data is protected:** By analyzing only what is absolutely necessary and forensically valuable, we pull fewer files than other compromise assessments; this keeps control of your data squarely in your hands.

Delivery through technology

We trace attacker activity via technology-assisted endpoint, network, log, event, malware, and forensic analyses. The combination of Rapid7 solutions and other powerful software ensures that the environment is thoroughly assessed and provides a comprehensive hunt for current and previous compromises.

Environmental awareness

Leave those other cookie cutter service offerings behind. At Rapid7, an integral part of our preparation for compromise assessments is learning and familiarizing ourselves with your security environment. Speaking of novel ideas, we know attackers are the persistent type, so we go beyond the baseline IOCs typically offered by other security services; our experts identify weaknesses in your current program via User, Host, Process (UHP) relationships and binary analysis and Application System Profiling (ASP). They also pinpoint risks in systems deployed in production through forensic analyses, network heuristics, and configuration analyses.

Impactful reporting, regardless of assessment results

If a compromise is detected, our reporting distills complex information into a clear chain of actionable insights. We highlight areas of compromise and provide guidance on remediation activities to optimize every hour of your team's response time.

Security is more than a binary state—there is always something to learn from a compromise assessment. Even if our assessment points to a clean house, we take the opportunity to identify steps your organization can take to improve resiliency and breach readiness. Our recommendations are actionable and bolster your security posture, and—if enacted—reduce risk of future compromise.

Quick pivot to IR Services

The compromise assessment is just one offering from our IR Services team; the results from the compromise assessment may guide you to other offerings to build out your IR program, such as breach readiness, tabletop exercise, and program development. The Rapid7 team provides recommendations to remediate any issues that were identified, and creates a plan to keep attackers out in the future. That's not all: The team supports crisis communications and helps your organization present critical details to the public or your executives, should the need arise.

IR Services can be purchased as specific services or through retainer hours; if you purchase a 120-hour retainer, a breach readiness assessment is included.

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 can alert the Rapid7 team, who will 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.

READY TO GET STARTED?

Contact our sales team at 866.7.RAPID7 or sales@rapid7.com, or learn more at www.rapid7.com/IR-services.