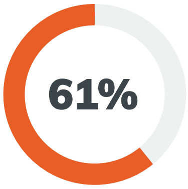
Detection & Response Services Curriculum

Drive your security program forward with assessment, response training, and testing.

Understanding where your security program stands is a crucial part of enhancing it. Rapid7 detection and response services help your team build proficiencies by:

- Evaluating existing systems, documentation, and tools
- Setting program goals based on specific needs
- Providing tailored recommendations for potential security investments
- Evaluating your ability to detect and respond by testing security controls against multiple simulated scenarios



According to Forrester Research, 61% of CISOs recognize there is an incident detection and response skills deficit in their organization.

This service package is designed as a complete 101 to 401 curriculum. From planning to full attack simulations, your team can level up its skills with tailored guidance and coaching, no matter its current skill set or program competency. Choose one course, a combination, or register for the entire curriculum.

Course 101	Course 201	Course 301	Course 401
Incident Response (IR) Program Development	Tabletop Exercise (TTX)	Detection & Response Workshop	Purple Team Exercise

Not sure which Detection & Response Service is right for you? Get insight from our sales team at **866.7.RAPID7** or **sales@rapid7.com**. Learn more at **www.rapid7.com/IR-services**.

Complete Detection & Response Service Curriculum:

Course 101:

Coaching and Planning

Incident Response Program Development

- Evaluate your existing technology, processes, people, policies, regulatory compliance, users, assets, and data to rate capabilities and define severity ratings.
- A dedicated team of experts provide relevant and business-based recommendations for an efficient and sustainable security program.
- Maturity goals are tailored to your needs, but can include:
    - Building confidence through preparation
    - Automating known threat prevention
    - Detecting unknown threats
    - Responding with a purpose
    - Remediating threats to minimize impact
    - Prioritizing cleanup

Course 201:

Practice and Drills

Tabletop Exercise (TTX)

- Take stock of your documented incident response plan by putting your incident response team through a hypothetical threat simulation in a safe and controlled setting.
- Receive feedback on critical documents from incident response plans to crisis communication procedures, IT policies, and network topologies.
- Experts develop and facilitate a breach scenario — realistic to your environment and current controls — to evaluate your organization's breach response process.
- Go beyond technical analysis and response to learn how stakeholders across your company react, communicate, and manage in the event of a breach - including technical teams, legal, marketing, and executives.

Course 301:

Scrimmage

Detection & Response Workshop

- Simulate an attack on your environment to assess how well you detect and respond with current capabilities and incident response tactics.
- Receive guidance from our experts who walk you through a response process tailored to the severity and nature of the breach.
- Get a detailed report of the outcome of your response, the impact on your environment and team, and how you can improve.

Course 401:

Live Game

Purple Team Exercise

- A cyber-range exercise to get a realistic look into your defense, detection, and response capabilities with simulated attacks tailored to specific risks you face with both Blue team and Red team support.
- Red team operators carry out real-world adversarial behavior, leveraging tactics, techniques, and procedures (TTPs) common to your environment.
- Blue team responders assess the maturity of your detection and monitoring controls, how your team adheres to the stated incident response plan, their coordination and communication throughout the breach, and technical analysis capabilities.
- This live-action exercise helps you pinpoint technical and organizational defense gaps so your team emerges empowered to take on attackers.

Always be prepared with an Incident Response Retainer

In the event of a compromise, you can engage our team of IR experts at a moment's notice. We'll spring into action within 1 hour to plan an approach. We'll begin remote technical investigations within 24 hours and can be on-site within 48 hours. Retainers are available in 80- and 120-hour blocks (120-hour retainers include a Breach Readiness Assessment). And in case you purchased a retainer but didn't have to use it, you can apply those hours toward any of our Incident Response Services — or any Rapid7 Consulting offering — so it never goes to waste.

It goes beyond an insurance policy: An Incident Response Retainer is an easy way to keep experts on standby.

About Rapid7 Incident Response

Rapid7's expert incident responders have conducted hundreds of investigations and have decades of experience responding to compromises of all sizes and severity. From small-scale opportunistic threats to enterprise-wide breaches by sophisticated attackers, our professionals quickly apply their expertise in threat analysis, forensics, and malware analysis. Their current knowledge of industry-leading technology platforms for rapid analysis and incident scoping — such as Velociraptor, Rapid7's open-source Digital Forensics and Incident Response (DFIR) tool — ensure they're using the latest knowledge to help you detect and defeat threats.

Looking to offload detection and response? We can help.

Rapid7 Managed Detection and Response (MDR) services allow you to offload the burdens of detection and response plans. No matter your current maturity level, our mission is to accelerate your security program with the tools, resources, and people necessary to protect your business.

- Receive tailored service based on a deep knowledge of your unique environment and security goals.
- Rely on operations analysts to provide ongoing support for configuration, tuning, and/or monitoring of your service.
- Mature and evolve your program with guidance from security advisors with strong technical expertise.
- Receive detailed reporting that prioritizes findings, next steps, and remediation guidance.