

RSA® Incident Response Retainer Services

Resources & Expertise to Reduce Breach Exposure Time

Executive summary

There is a short window of opportunity between the detection of an initial compromise and the ability to prevent an attacker from fulfilling his objectives. This period is sometimes referred to as “breach exposure time” or “dwell time.” Early detection and rapid response are the key requirements to defend against a breach of security. How can organizations address these requirements? One approach is to implement a surge resourcing model using Incident Response (“IR”) retainers as a best practice. This approach provides rapid access to toptier security analysts from RSA who will help reduce dwell time and mitigate the impact. IR Retainers can also help an organization to align with the requirements and incentives offered by cybersecurity insurance providers.

With the day-to-day demands of protecting the business, IT Security personnel are already stretched. This problem is compounded when security incidents are confirmed and a breach may be imminent. Incident and breach Response typically impacts stakeholders across multiple segments of the organization, many of whom may struggle with participating in IR activities while continuing day-to-day responsibilities.

In these situations organizations can benefit by complementing in-house resources with outside expertise. The RSA IR Retainer services help organizations anticipate the process required to access technical analytic expertise, including:

- A proactive, “around the clock” process for engaging RSA’s Global IR team
- Conduct of pre-breach activities to streamline communications protocols
- Accelerated timelines for rapid access to RSA’s top-tier security talent to assist with IR triage (identification and selection of a trusted advisor and negotiation of terms and conditions is something that should be done in advance)
- Conduct of the initial triage and response effort, along with a preliminary analysis to scope the nature of any incident
- Rapid access to RSA technologies as a core element of our IR capabilities (including the RSA NetWitness® Suite for full packet capture and endpoint anomaly detection, RSA NetWitness Live threat intelligence and the RSA SecurID® Access Suite for hardening of the security infrastructure, etc.)
- Determination of recommended next steps for incident response and remediation

At-A-Glance

RSA is the industry’s original pureplay cybersecurity company with over 35 years of solution delivery. RSA’s Global Incident Response Practice provides expert technical analysis, guidance and direction for advanced threat mitigation. Using an intelligence-driven and analytic approach, the IR Practice leverages customer-owned and RSA technologies to protect critical assets by applying battle-tested methodologies to hunt for signs of compromise before harm is done to the organization. Having an IR Retainer in place before a breach gives your organization peace of mind in knowing that you’ll be able to respond accordingly, should an incident be confirmed.

The RSA IR Retainer services provide access to NSA-accredited, battle-tested resources to address incident-related intelligence gathering, research and analysis. It also facilitates any further requirements for host and networkbased forensics and malware analysis, leveraging the RSA NetWitness Suite of technologies for proactive threat detection, incident response and remediation. If requested, the RSA IR Practice can also provide support for activities that involve incident-related litigation. To contact RSA IR services now, click here: <https://www.rsa.com/en-us/services/rsa-incident-response-practice/immediate-help>.

While some aspects of incident response are highly technical in nature, the biggest challenge to the organization often results from the broader operational impact of an incident or breach and the need to coordinate the activities of a variety of participants, many of whom are outside of the IT and security functions. The RSA IR Retainer services help organizations to maintain the focus on their business objectives by providing them with a flexible procurement model for leveraging outside expertise as required.

Choosing the right Service Level

RSA offers a portfolio of IR services, which can be tailored to accommodate discrete customer needs. In addition, RSA also offers a variety of packaged IR Retainer services, which provide customers with a range of Service Level Agreement (“SLA”) options, as indicated in the table below.

RSA Packaged IR Retainer Services, SLA Op ons & Effort (in hours)				
	Bronze	Silver	Gold	Platinum
SLA for Initial Response	8	6	3	3
SLA for Initial Analysis	24	24	12	12
SLA for On-site Analysis	72	48	24	24
Estimated Hours Incl.	24	68	120	242

IR Retainer Services can also be used for technical IR consulting activities before expiration of the retainer term. Other additional optional activities include proactive hunting for advanced threats and executive-level RSA participation if a breach is confirmed, both of which are included in the Platinum-level IR Retainer service.

Choosing a partner for Incident Response

The RSA portfolio of Advanced Cyber Defense and Incident Response solutions enables organizations to evolve from “being the hunted” to “be the hunter” and develop the maps, strategies and solutions required to navigate the new terrain of targeted attacks.

Surge access to technical expertise is a key component of an incident management program. With RSA's IR Retainer services, organizations can enhance their overall security posture for targeted attack defense.

Learn more

For more information on the RSA incident response capabilities which are available on a global basis, please visit the web site: <https://www.rsa.com/en-us/services/rsa-incident-response-practice>.

About RSA

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime.

RSA Advanced Cyber Defense and Incident Response Practices are part of the RSA Risk & Cybersecurity Practice. The RSA Global Services organization also provides Professional Services in support of RSA product platforms, education services from RSA University and 24x7x365 product maintenance services from RSA Customer Support. For more information, go to [rsa.com](https://www.rsa.com).