

# RSA<sup>®</sup> RETAINER FOR INCIDENT RESPONSE

Resources and expertise to reduce Breach Exposure Time

## EXECUTIVE SUMMARY

**There is a short window of opportunity between the detection of an initial anomaly and the ability to prevent an attacker from fulfilling his objectives. This period is sometimes referred to as “Breach Exposure Time.” Early detection and rapid response is the key to defense against targeted attacks. How can organizations address these requirements? One approach is to implement a surge resourcing model, providing rapid access to the types of expertise required to handle incidents that involve advanced threat actors.**

## AT-A-GLANCE

**The RSA<sup>®</sup> Advanced Cyber Defense (ACD) Practice enables agile mitigation of targeted attack activities. Using an intelligence driven security model, the ACD team focuses on the protection of critical business assets by applying proven operational expertise to enable front-line cyber readiness, response and resilience.**

With the day-to-day demands of protecting the business, IT Security personnel are already stretched. This problem is compounded during sophisticated attacks. Incident Response typically impacts stakeholders across multiple segments of the organization, many of whom may struggle with participating in response activities while continuing to fulfill their day-to-day responsibilities.

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

- Development of a proactive process for engaging RSA’s Incident Response team.
- Conduct of the initial incident triage and the preliminary analysis to review the current state and scope the nature and extent of the response and remediation steps which are required.

The RSA<sup>®</sup> Retainer for Incident Response provides access to expert resources to address incident related intelligence gathering, research and analysis. It also facilitates addressing any further requirements for host and network-based forensics and malware analysis, leveraging RSA’s industry leading portfolio of technologies and services for incident response and remediation.

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, more ominously a security 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 Retainer for Incident Response helps organizations maintain focus on their business

objectives while also facilitating a flexible model to leverage outside expertise as required.

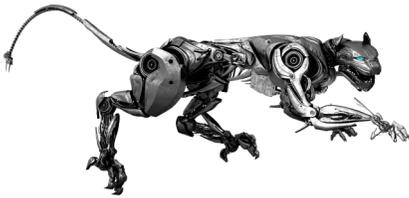
## CHOOSING A PARTNER TO "BE THE HUNTER"

RSA's portfolio of ACD 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 Retainer for Incident Response, organizations can enhance the overall security posture for defense against targeted attacks.

## LEARN MORE

For more information on the RSA's ACD capabilities which are available on a global basis, please visit the web site: <http://www.emc.com/services/rsa-services/advanced-cyber-defense/index.htm>.



### ABOUT RSA

Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, help prevent IP theft, fraud and cybercrime. For more information on RSA, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

*RSA and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other company and product names may be trademarks of their respective owners. ©2015 EMC Corporation. All rights reserved. Published in the USA.*

DS Retainer 2015 h11844

EMC<sup>2</sup>, EMC, RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

©2015 EMC Corporation. All rights reserved. Published in the USA.

